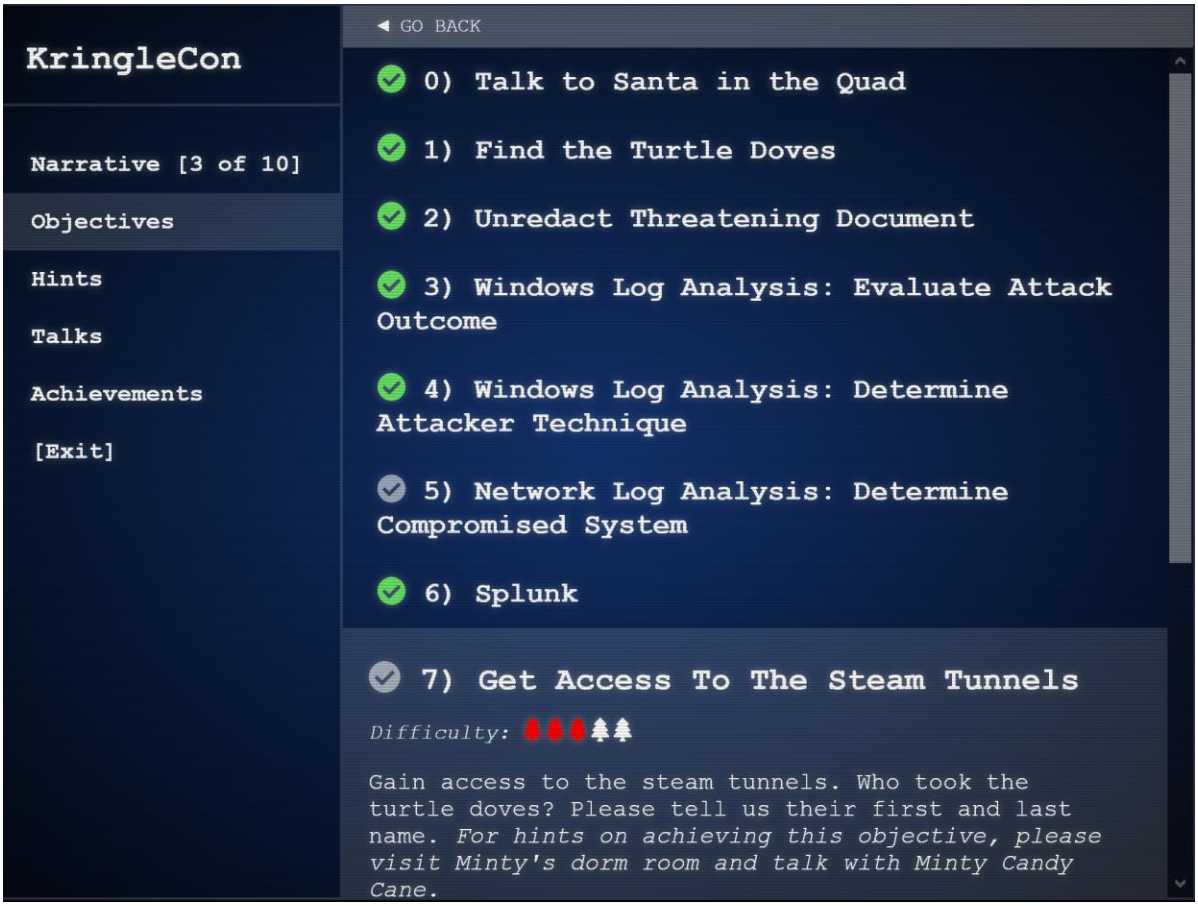
KringleCon 2: 2019 Walkthrough

Completed By: Akvile Kiskis

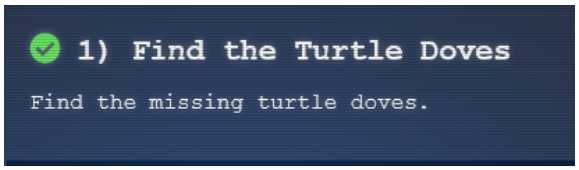
Round 2 for KringleCon! SANS brought back their free online security conference with the Holiday Hack Challenge. This year it was at Elf University instead of Santa's Castle and the challenges were more blue team oriented. After this I have even more respect for blue teaming as I genuinely believe it's more difficult than red teaming...maybe because I think like a hacker and not like a defender. Either way, I enjoyed the challenge and even though I didn't complete as many challenges as I did last year, I learned a lot from this experience. The table of contents is below for easy browsing; this time around I listed the coinciding elf challenge under the objective as some of these were more involved than last year.



Proof that Krampus didn't make me lie about my accomplishments (or lack thereof)

Table of Contents

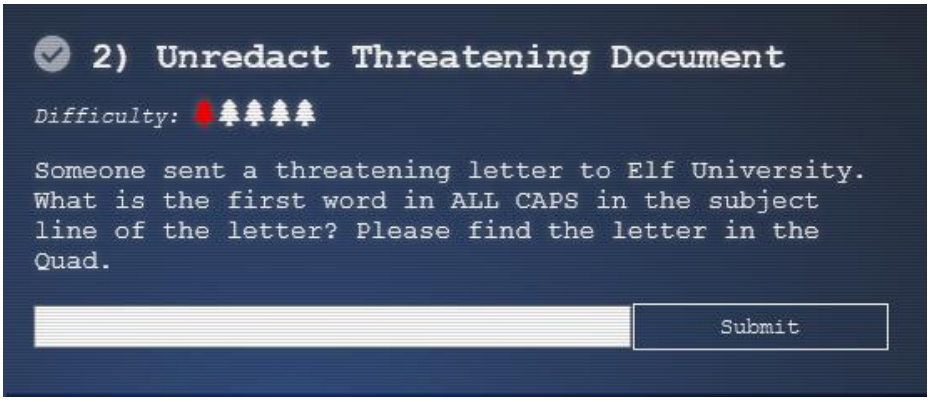
Find the Turtle Doves



Not much explanation needed for this one, just walk around and you'll find them!

Location: Student Union by the fireplace

Unredact Threatening Document



The letter is located in the top left of the quad.

When you click on it, the letter opens in a new tab:

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

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

Sincerely,

--A Concerned and Aggrieved Character

I remember a similar challenge in another CTF I've done – the easiest way is to save the file and open it in MS word. Then, you can remove the blocks that are blocking the text.

Date: February 28, 2019

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

From: A Concerned and Aggrieved Character
Subject: DEMAND: Spread Holiday Cheer to Other Holidays and Mythical Characters… OR
Confidential
ELSE!

Attention All Elf University Personnel,

~~It remains a constant source of frustration that Elf University, and the entire enterprise 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~~

Confidential characters.

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

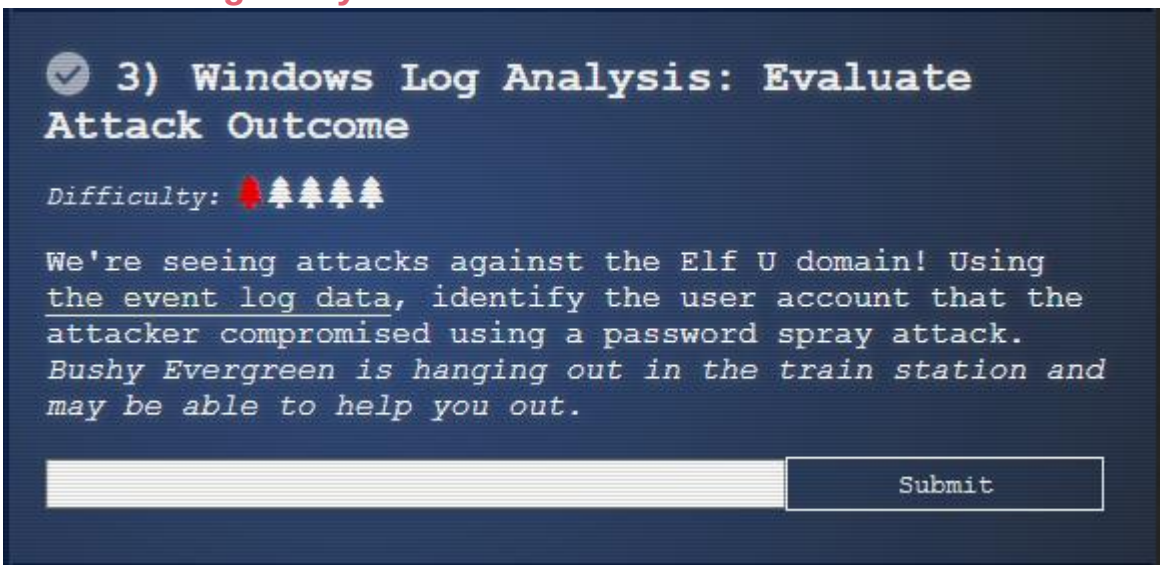
If you do not accede to our demands, we will be forced to take matters into our own hands. We do not make this threat lightly. You have less than six months to act demonstrably.

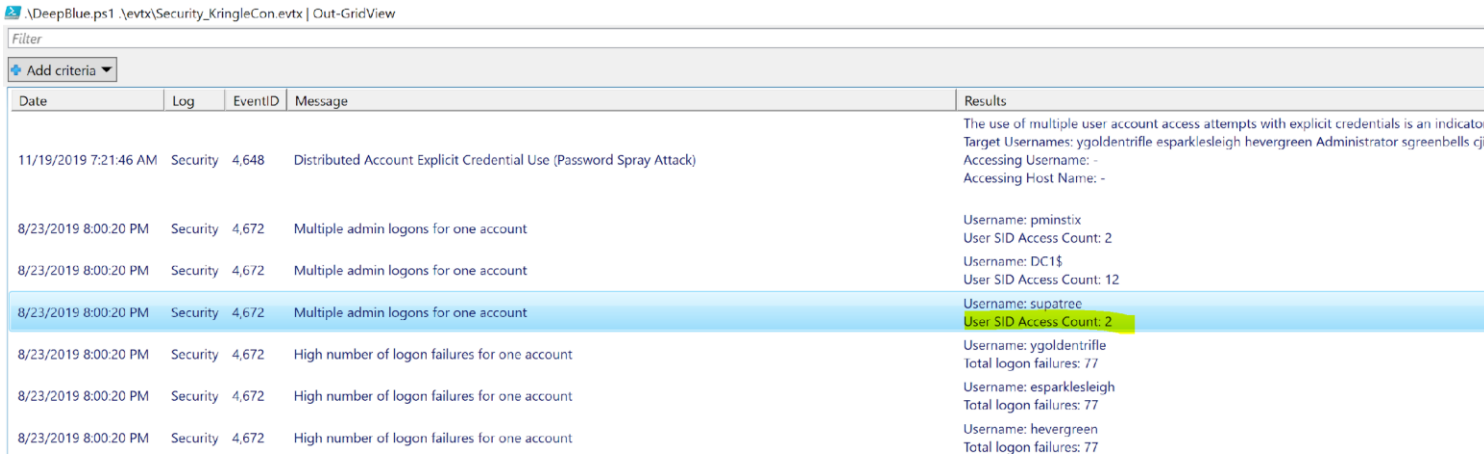
Sincerely,

--A Concerned and Aggrieved Character

Flag: DEMAND

Windows Log Analysis: Evaluate Attack Outcome





.\DeepBlue.ps1 .\evtx\Security_KringleCon.evtx | Out-GridView

Filter

Add criteria

Date	Log	EventID	Message	Results
11/19/2019 7:21:46 AM	Security	4,648	Distributed Account Explicit Credential Use (Password Spray Attack)	The use of multiple user account access attempts with explicit credentials is an indicato Target Usernames: ygoldentrifle esparklesleigh hevergreen Administrator sgreenbells cj Accessing Username: - Accessing Host Name: -
8/23/2019 8:00:20 PM	Security	4,672	Multiple admin logons for one account	Username: pminstix User SID Access Count: 2
8/23/2019 8:00:20 PM	Security	4,672	Multiple admin logons for one account	Username: DC1$ User SID Access Count: 12
8/23/2019 8:00:20 PM	Security	4,672	Multiple admin logons for one account	Username: supatree User SID Access Count: 2
8/23/2019 8:00:20 PM	Security	4,672	High number of logon failures for one account	Username: ygoldentrifle Total logon failures: 77
8/23/2019 8:00:20 PM	Security	4,672	High number of logon failures for one account	Username: esparklesleigh Total logon failures: 77
8/23/2019 8:00:20 PM	Security	4,672	High number of logon failures for one account	Username: hevergreen Total logon failures: 77

After completing Bushy Evergreen's challenge (see here), he hints that Deep Blue CLI would be a useful tool for this challenge. After downloading it, I used the **| Out-GridView** output method to make it easier to parse through the log. There weren't many log entries to begin with, so I didn't filter them. I just scrolled to the bottom and saw that for the "Multiple admin logons for one account" log entries, only one of them actually had an account. *pminstix* wasn't a user and *DC1$* was just gobbledygook so by power of elimination, the compromised account was *supatree*.

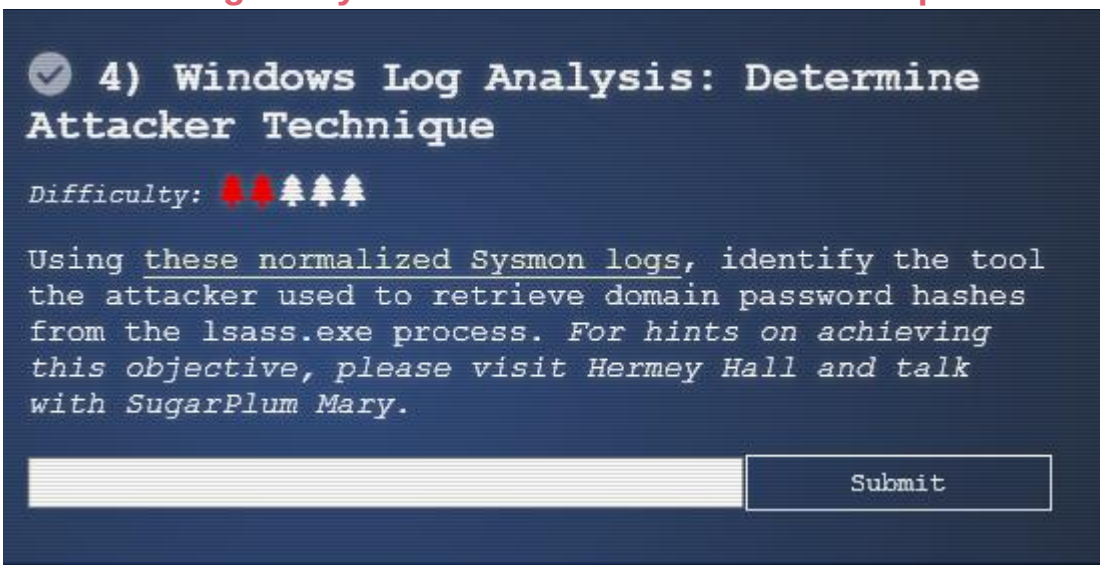
Flag: supatree

Bushy Evergreen - Exit Ed

Similar to last years Vim challenge, we had an elf struggle with exiting the terminal again. I couldn't remember who it was last year, but I have a feeling it was Bushy again. This time it was with Ed. The solution is listed in the screenshot below (you just type in q).

```
                  ........................................
               .;oooooooooooooo;,,,,,,,,:loooooooooooooll:
             .:oooooooooooooc;,,,,,,,,:oooooooooooooolloo:
          .';;;;;;;;;;;;;;;,''''''''';;;;;;;;;;;;;;;;oooo:
        .''''''''''''''''''''''''''''''''''''''''''''''';oooo:
      ;oooooooooooooo;''''''',:loooooooooooolc;',,;oooo:
    .:oooooooooooooc;',,,,,,,:oooooooooooolccoc,,,;oooo:
  .coooooooooooooo:,''''''',:oooooooooooolcloooc,,,;oooo,
  coooooooooooooo,,,,,,,,,;oooooooooooooloooooc,,,;ooo,
  coooooooooooooo,,,,,,,,,;oooooooooooooloooooc,,,;l'
  coooooooooooooo,,,,,,,,,;oooooooooooooloooooc,,,..
  coooooooooooooo,,,,,,,,,;oooooooooooooloooooc.
  coooooooooooooo,,,,,,,,,;oooooooooooooloooo:.
  coooooooooooooo,,,,,,,,,;oooooooooooooloo;
  :lllllllllllllll,''''''''';lllllllllllllllc,



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

-Bushy Evergreen

Exit ed.

1100
q
Loading, please wait......



You did it! Congratulations!

elf@45c3211732b8:~$
```

Windows Log Analysis: Determine Attacker Technique



I started by using EQL for this based off of the references in this link, but after seeing that there was only one lsass.exe process in the log I resorted to using the trusty Notepad. The next event used the ntdsutil.exe process and after some research, I saw that this process was the culprit.

sysmon-data.json - Notepad

File Edit Format View Help


```
        "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"
    }
```

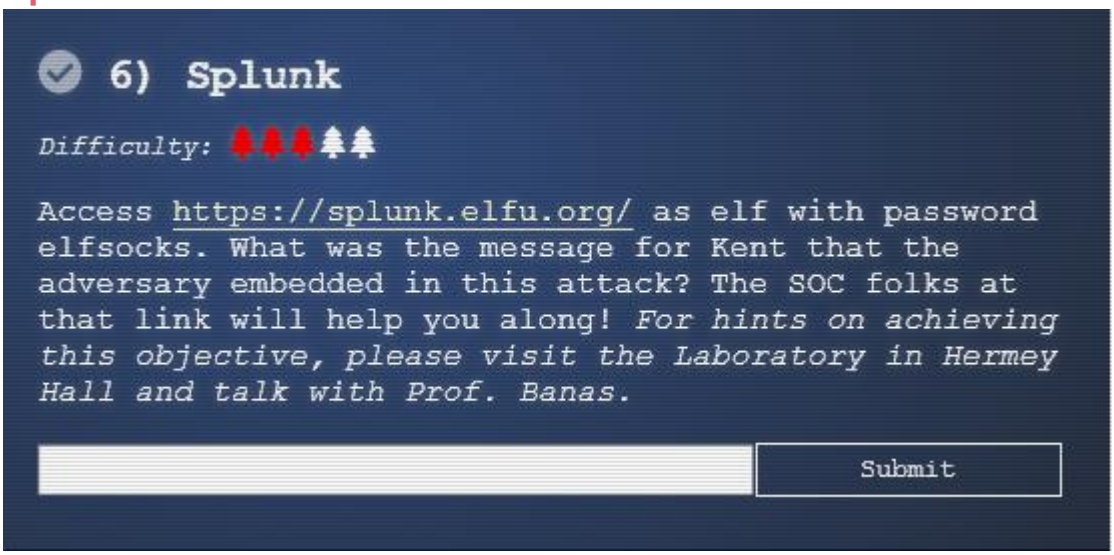

Flag: ntdsutil

Hermey Hall – SugarPlum Mary

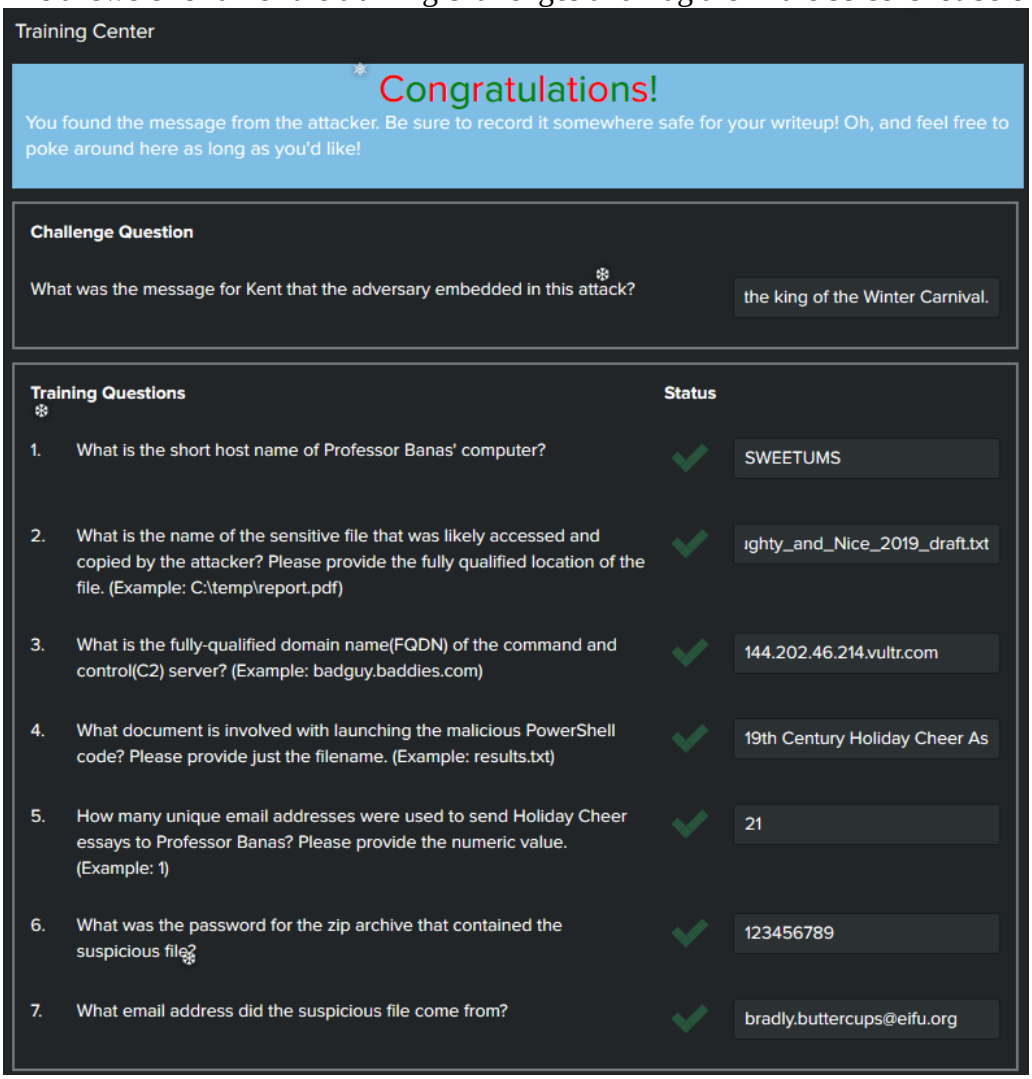
SugarPlum Mary's ls command isn't working properly. Thankfully, there's a command that lets you run ls from its full path and you're able to fix it for her. To breakdown the screenshot below, the "which" command gives you the full path of a command. Then, based on the output of that command you can use the path to run the command from its full path. In this case I did "/bin/ls" and the txt file.

```
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@f77b6dd3f83f:~$ ls
This isn't the ls you're looking for
elf@f77b6dd3f83f:~$ which ls
/usr/local/bin/ls
elf@f77b6dd3f83f:~$ /bin/ls
' '   rejected-elfu-logos.txt
Loading, please wait......



You did it! Congratulations!

elf@f77b6dd3f83f:~$
```

Splunk



The answers for all of the training challenges and flag are in the screenshot below.



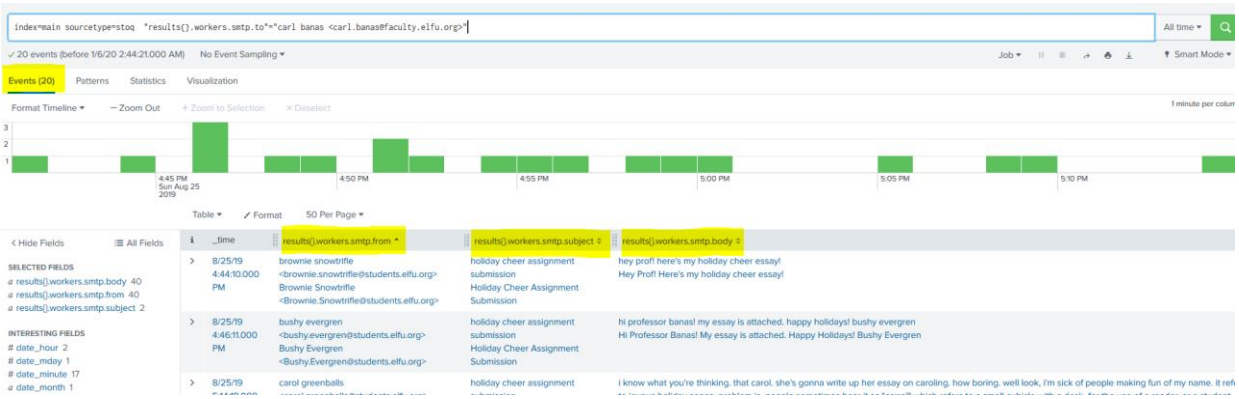
I'll break them down by each question for your convenience. I didn't include number one because I believe the chatbot gave that one to you right away as a freebie.

2) What is the name of the sensitive file that was likely accessed and copied by the attacker?
Command: Index = main santa -> since we know that Santa is the target, we can narrow the search for logs related to him. Once you search this, the .txt file is pretty easy to find.
Answer: C:\Users\cbanas\Documents\Naughty_and_Nice_2019_draft.txt

3) *What is the FQDN of the C2 server?*
Command: index=main sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational powershell EventCode=3 -> The chatbot told us to search for this as well, I highlighted "Interesting Fields" and "DestinationHostname" to find the answer for this one.
Answer: 144.202.46.214.vultr.com

4) What document is involved with launching the malicious PowerShell code?
Command: sourcetype=stoq | 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 → I found the command [from this KringleCon talk.](#) Interestingly enough, I found most of the following answers from this command. I highlighted them in the screenshot below, I have no idea why I didn't include the portion where it showed the assignment name. I blame sleep deprivation.
Answer: 19th Century Holiday Cheer Assignment.docm

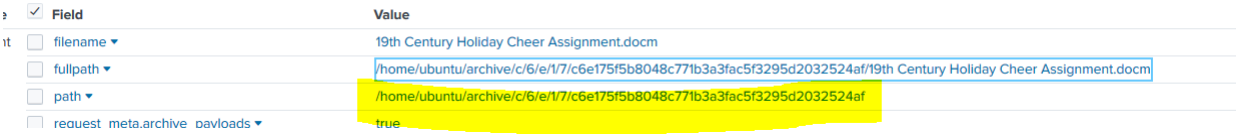
5) How many unique email addresses were used to send Holiday Cheer essays to Professor Banas?
Command: index=main sourcetype=stoq "results{}.workers.smtp.to"="carl banas <carl.banas@faculty.elfu.org>" -> This helped trim down the results to only the ones sent to Professor Banas since some log entries had his reply emails and we didn't want those. This brought the event number down to 20 (see screenshot below). I also had to add in the one from Bradly Buttercups from question #4 since that was not included in the results.
Answer: 20 events + the one in answer #4 = 21



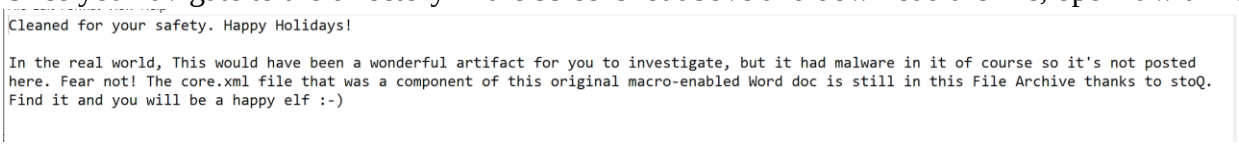
6) What is the password for the zip archive that contained the suspicious file?
Answer: 123456789 -> see screenshot for #4, I found the answer from that same command.

7) What email address did the suspicious file come from?
Answer: bradly.buttercups@eifu.org → I expanded the event from answer #4 to find his email address.

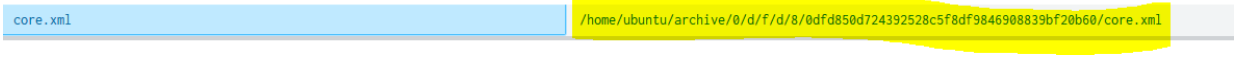
Challenge: What was the message for Kent that the adversary embedded in the attack?
The easiest way to go about this is to go to the file path in file archive and download it. I found the path from question #4, my goldmine.



Once you navigate to the directory in the screenshot above and download the file, open it with notepad:



I did the same stoq search as earlier to find the path for this file:



Download and open the XML:

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

Tangle Coalbox– Dormitory Keypad

Tangle asks you to open the dormitory by using the keypad. He gives you the hints that one digit is repeated and that the pin is a prime number. You can tell from the screenshot below that the pin number uses 1, 3, and 7.

There are not many prime numbers that it could be, so I used this website to guess and check to find it (Ctrl + F to save a life).

Flag: 7331

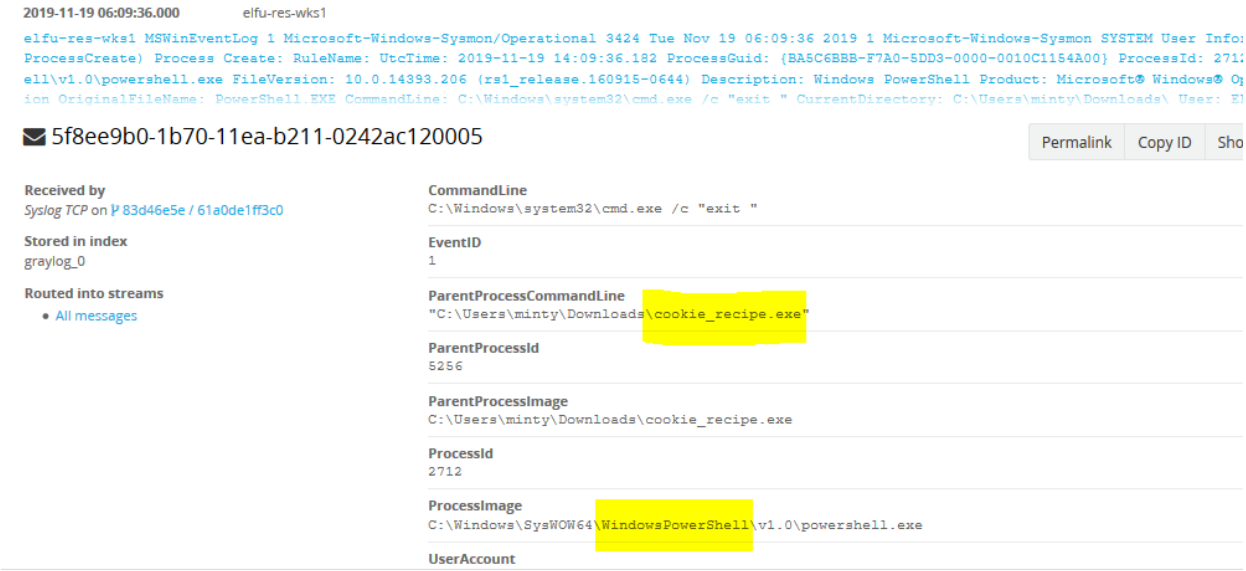
Pepper Minstix – Graylog

Pepper needs you to fill out the incident response report for her by using the information on Graylog.

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

There were explanations for all of these, but most of the time I did something different. I'll explain how I did for each one. For this one, I just looked up "minty", then "useraccount: minty" and then found this:



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

For this one I actually looked up the ParentProcessID of 5256, went to the first whoami command and clicked "show surrounding messages" for a minute out and organized by timestamp to find the classic nc loopback. nc is shorthand for netcat, a commonly used utility by pen testers to listen in on network connections.

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

Answer: whoami

As I mentioned in the previous answer, I used that original ParentProcessID of 5256 search to find the whoami command. It was a two for one!

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

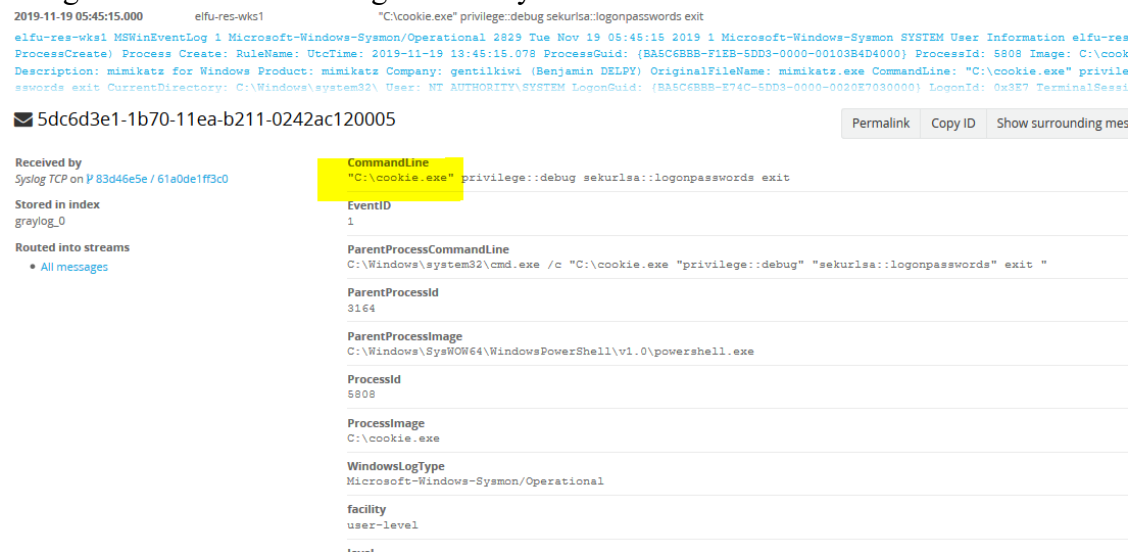
Answer: webexservice

This one built off of the other two answers. If you keep searching the logs, you'll see other commands the attacker used which lead to finding the service.

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

Answer: C:\cookie.exe

For this one I searched around cookie_recipe2.exe and found the other cookie binary. The "privilege:: debug" in the command line gave it away.



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

I used the Windows Event Id **4624** to search for potential RDP connections. With that, I was able to find Alabaster.

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

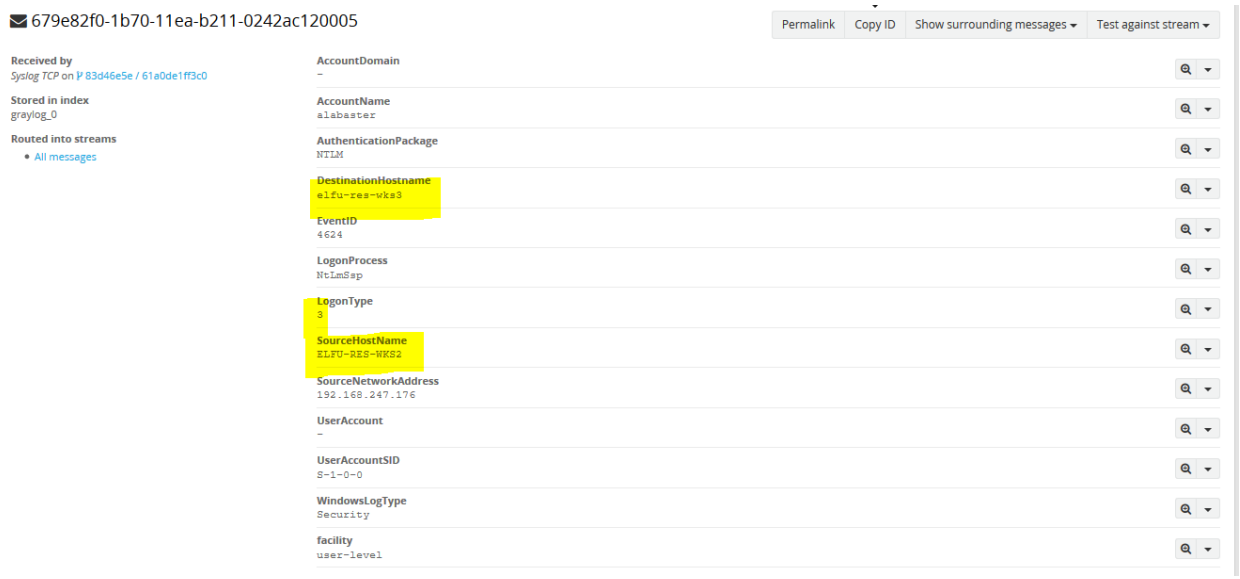
Answer: 06:04:28

To build off of the last answer, I used EventID: 4624 (Account Successfully Logged In) and LogonType: 10 since that's a successful RDP login.

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

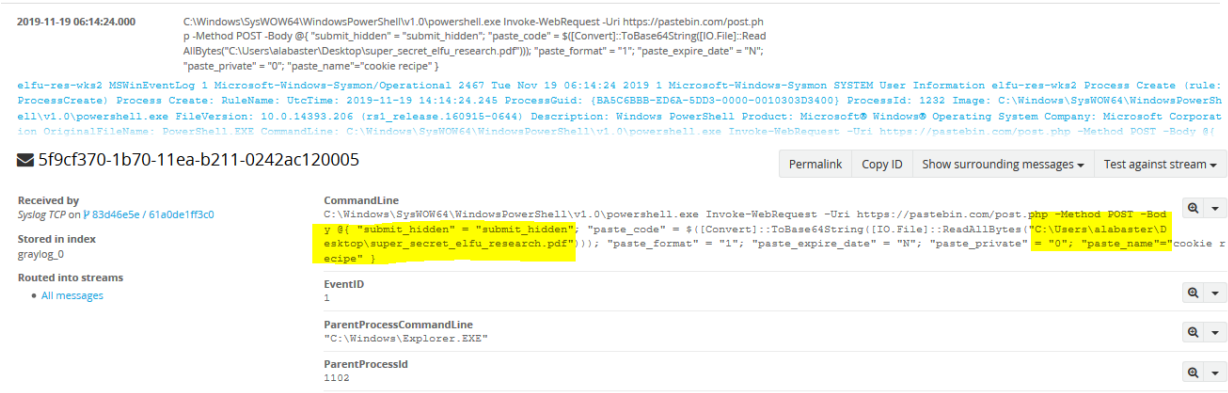
I used [this website]() as a reference and searched for _exists_:LogonType. Then I looked for first instance for wks3 after the connection at 6:04 (from the previous answer).



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

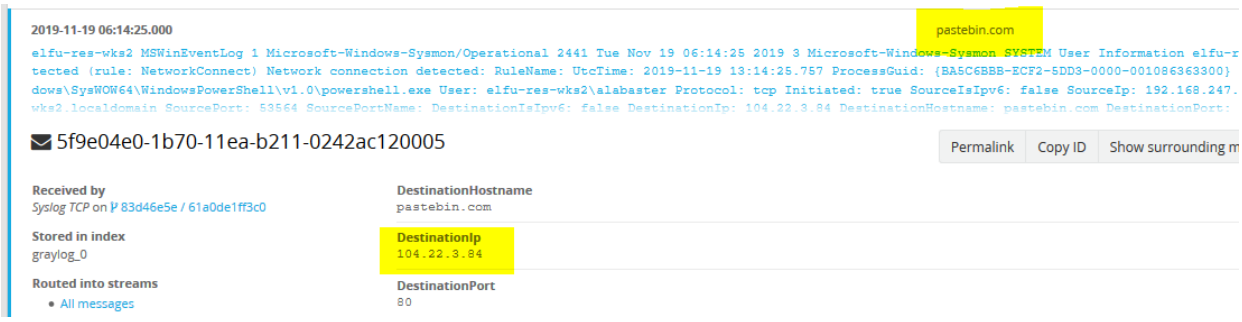
I was actually looking for the answer to question 8 when I stumbled on this one. I used _exists_:WindowsLogType and found the log entry below.



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

Answer: 104.22.3.84

The log entry above the one I found for question 9 had the IP address; I knew it was the one because it showed the destination as "pastebin.com".



Incident Response Report #7830984301576234 Submitted.

Incident Fully Detected!

Proof that I actually finished this

Holly Evergreen – MongoDB

```
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@d391e6dccaca:~$ mongo
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27017
2020-01-05T22:34:12.124+0000 W NETWORK  [thread1] Failed to connect to 127.0.0.1:27017, in(che
cking socket for error after poll), reason: Connection refused
2020-01-05T22:34:12.124+0000 E QUERY    [thread1] Error: couldn't connect to server 127.0.0.1:
27017, connection attempt failed :
connect@src/mongo/shell/mongo.js:251:13
@(connect):1:6
exception: connect failed


Hmm... what if Mongo isn't running on the default port?


elf@d391e6dccaca:~$ netstat -ltp
(No info could be read for "-p": geteuid()=1001 but you should be root.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program na
me
tcp        0      0 localhost:12121         0.0.0.0:*               LISTEN      -

elf@d391e6dccaca:~$ mongo --port 12121
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:
2020-01-05T22:34:05.347+0000 I CONTROL  [initandlisten]
2020-01-05T22:34:05.347+0000 I CONTROL  [initandlisten] ** WARNING: Access control is not enab
led for the database.
2020-01-05T22:34:05.347+0000 I CONTROL  [initandlisten] **          Read and write access to d
```

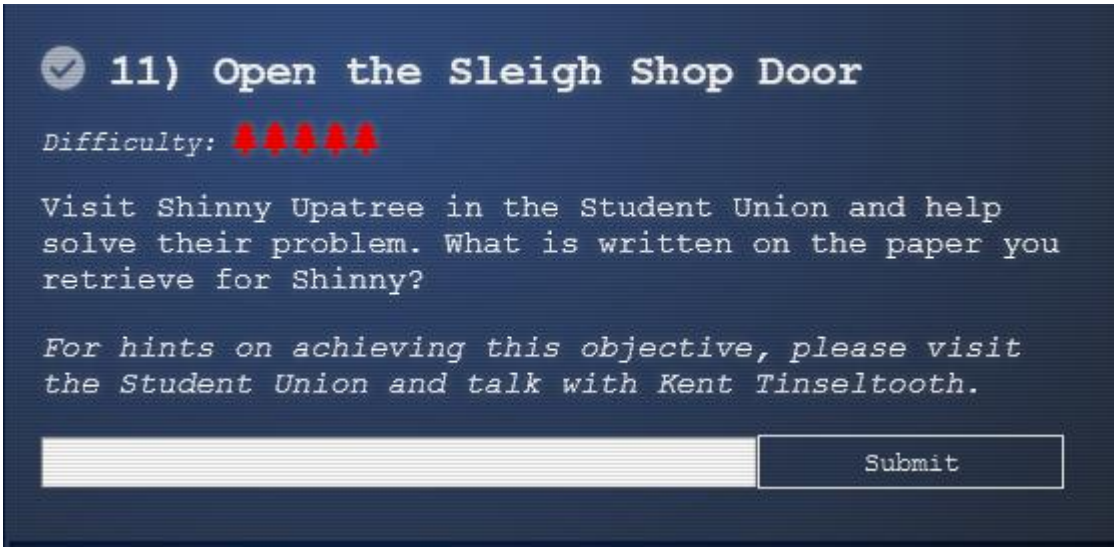
The screenshot explains my thought process; I used netstat to check what port was used for Mongo since it wasn't the default.

```
_hugepage/enabled is 'always'.
2020-01-05T22:34:05.347+0000 I CONTROL  [initandlisten] **        We suggest setting it to 'ne
ver'
2020-01-05T22:34:05.347+0000 I CONTROL  [initandlisten]
> db
test
> show collections
redherring
> show dbs
admin  0.000GB
elfu   0.000GB
local  0.000GB
test   0.000GB
> use elfu
switched to db elfu
> show collections
bait
chum
line
metadata
solution
system.js
tackle
tincan
> db.solution.find()
{ "_id" : "You did good! Just run the command between the stars: ** db.loadServerScripts();dis
playSolution(); **" }
>
```

Once I connected to the server, I switched to the elfu database and saw the solution in collections. I followed the instructions and got Holly up and running again!

```
          .
       __/ __
             /
       /.'o'.
        .o.'.
       .'.'o'.
      o'.o.'.*.
     .'.o.'.'.*.
    .o.'.o.'.o.'.
       [_____]
        ___/


  Congratulations!!


>
```

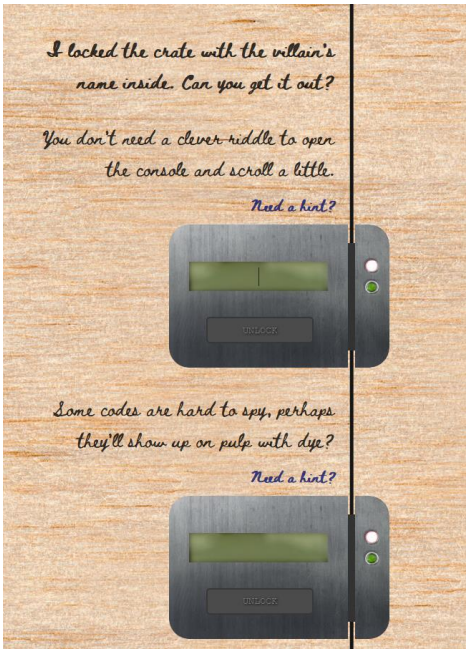
Open the Sleigh Shop Door



Kent hints that you need to use the browser developer tools to solve this one. In my case, I used Firefox. I used the inspector tool on the sleigh shop door to find the URL.

```
<div class="hearth-c"></div>
▸ <a href="http://sleighworkshopdoor.elfu.org">…</a>
▸ <div class="booth google">…</div>
```

When you reach the page, you find this:

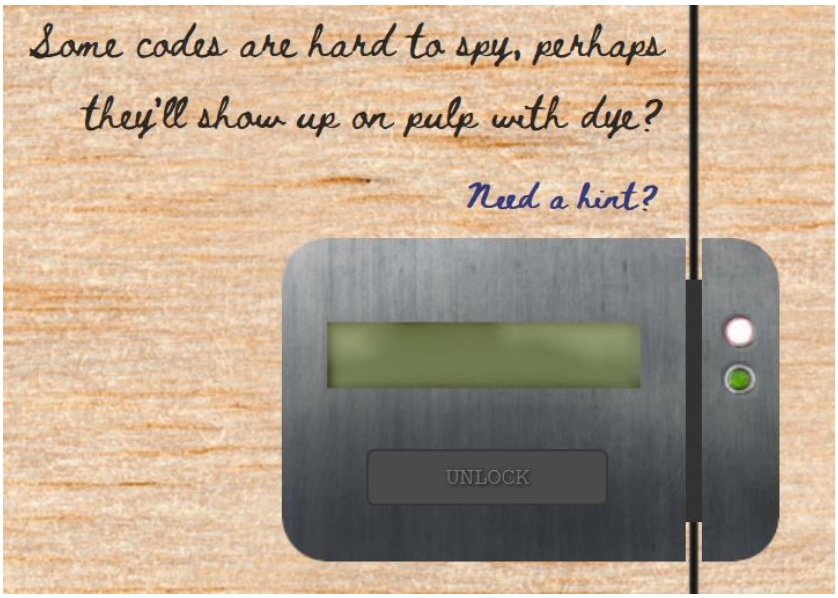


There's 10 locks total; I'll run through them all below.

Lock 1:

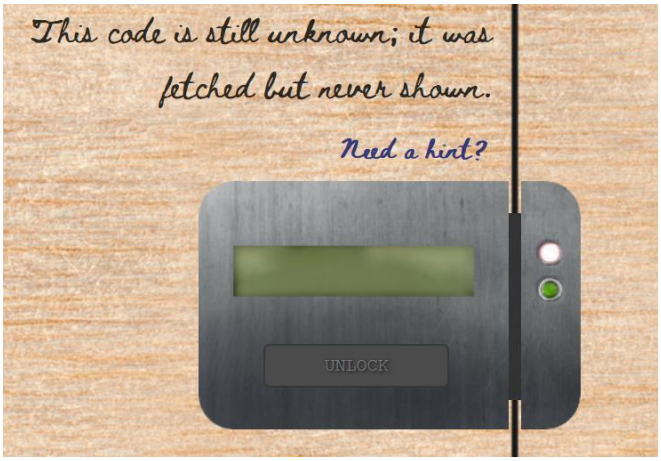
This is done by opening the "console" tab in Firefox developer tools.

Lock 2:

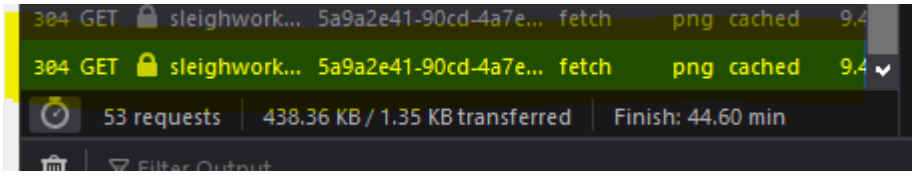


They hint at “pulp” which to me meant print - if you print preview the page, you find the code.

Lock 3:



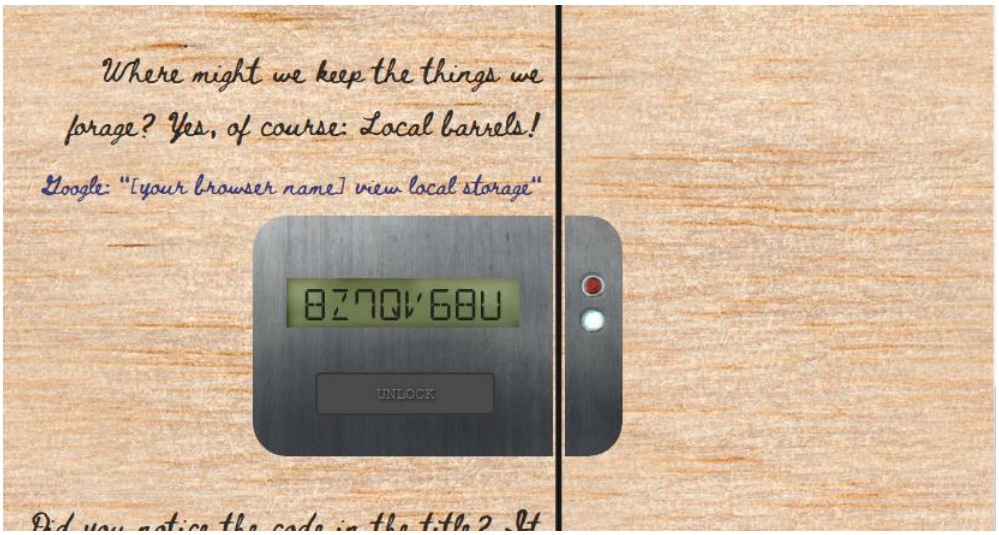
Fetch = GET in the web world. Find the GET request for Lock #3.

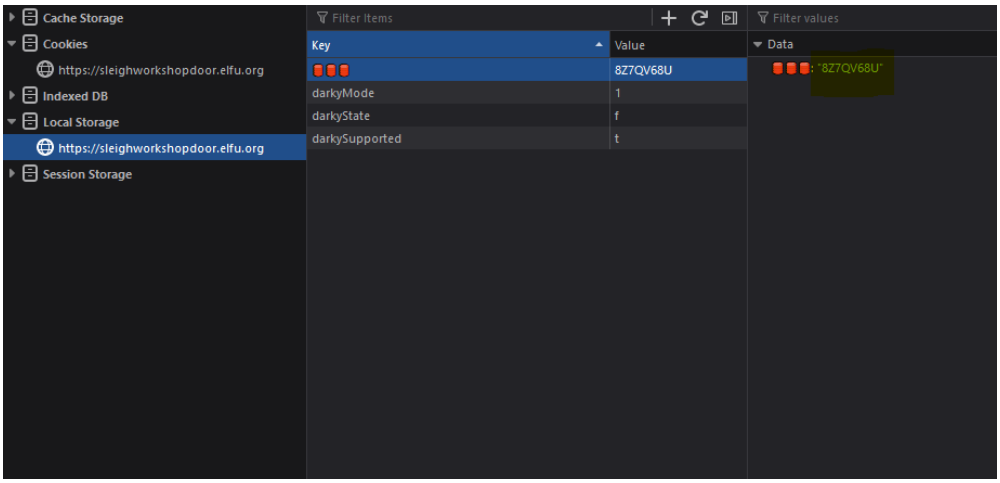


Right click and open in a new tab:

QIGG5NZW

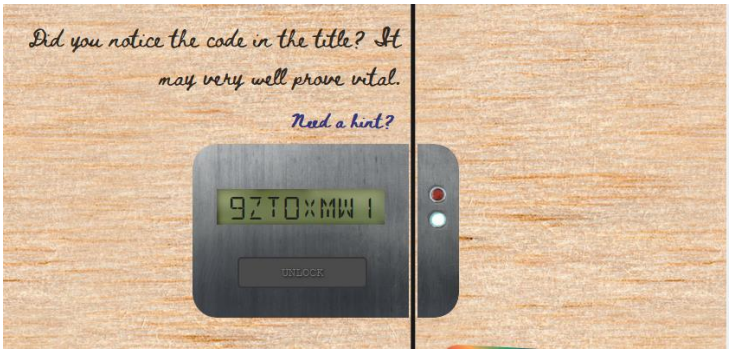
Lock 4:





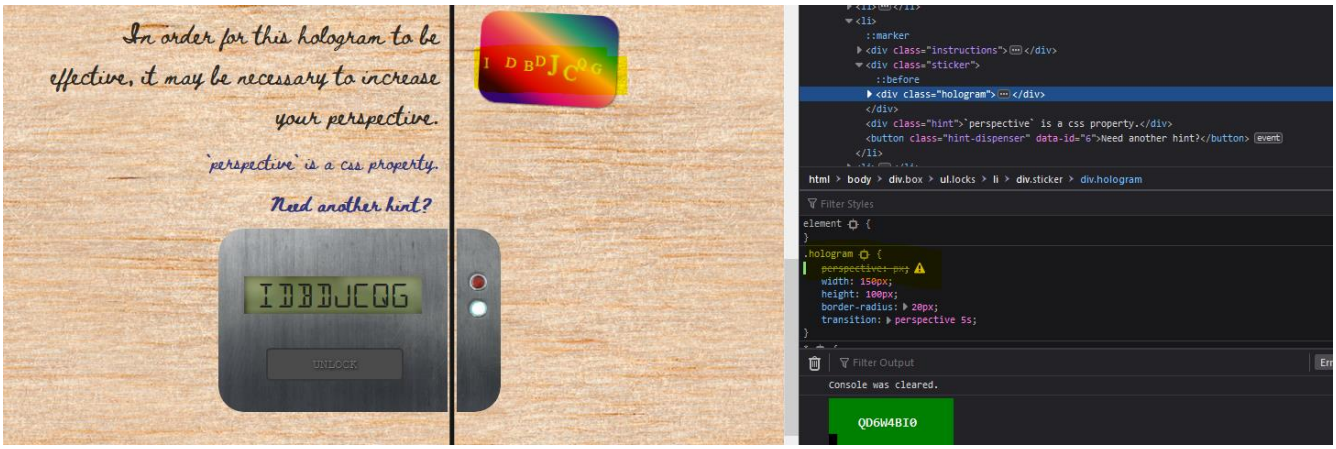
This is under the storage tab in the developer tools. I remember seeing those emotes in the obfuscated javascript and I thought they were gumdrops…

Lock 5:



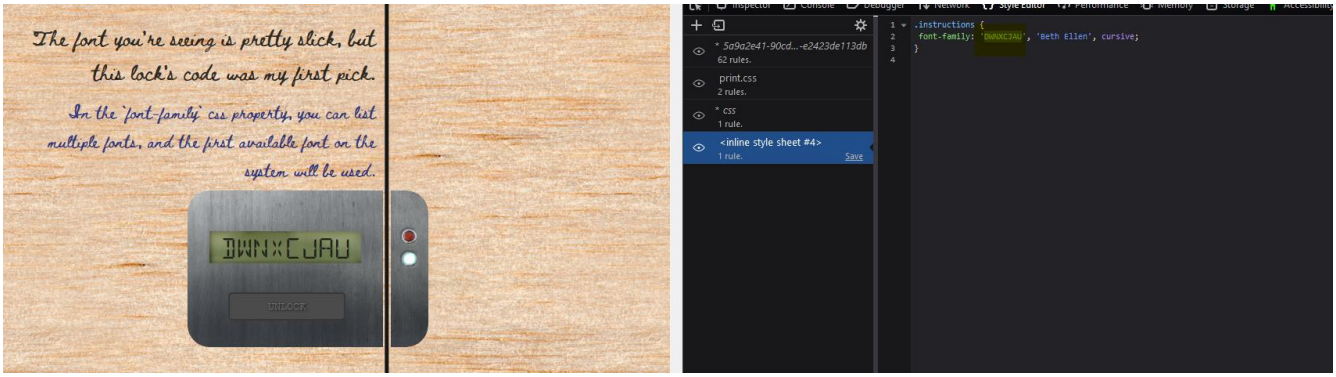
Open the <title> tag in the inspector tab to find this one.

Lock 6:



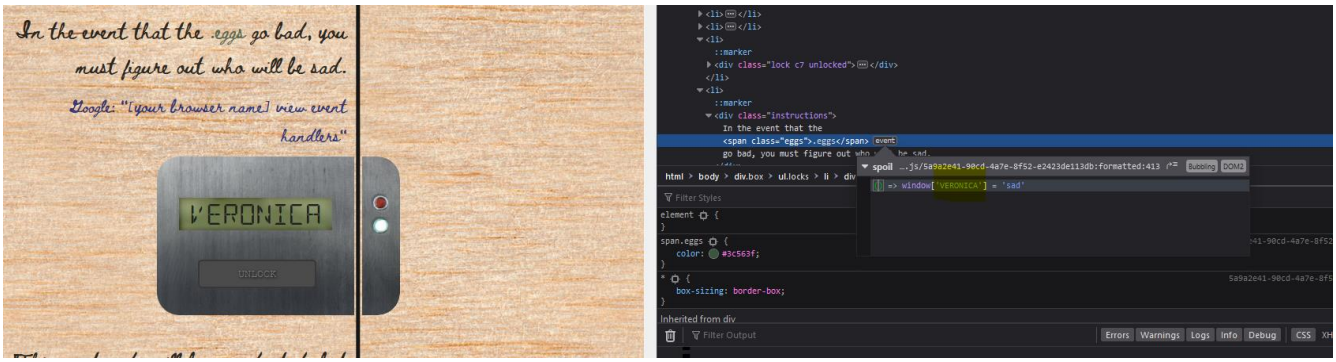
I picked the hologram element and actually erased the perspective numbers to show the code.

Lock 7:



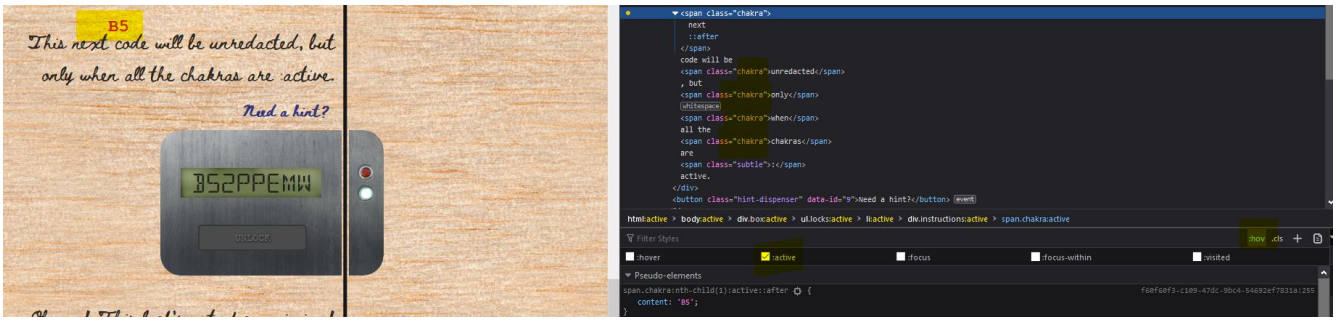
Go to the style editor tab and you can find the code in the last sheet.

Lock 8:



Click on the ".eggs" text with the inspector to find the event and expand it to find the code.

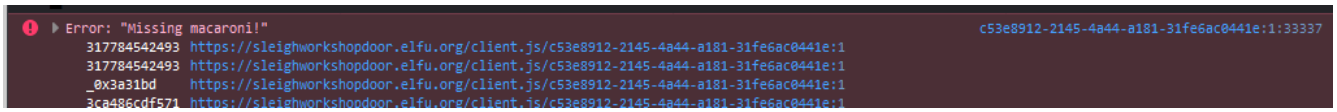
Lock 9:



Find each instance of “chakra” in the HTML and use the “:hov” (toggle pseudoclass) button to toggle the “:active” element for each one. They will pop up on the screen next to the class they coincide with to give you the code.

Lock 10:

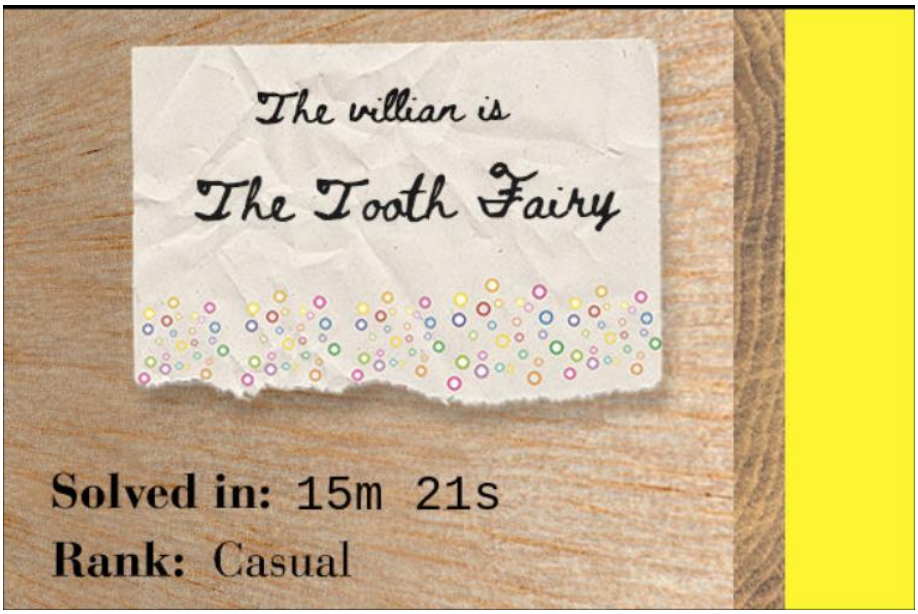
Find the cover element and remove the background. Code is on the bottom right. When you submit the code you get this error.



Find the “macaroni” element in the HTML, right click it, and copy the node. Then move it down underneath the cover in lock 10 and try unlocking again.

```
::before
▶ <div class="cover">…</div>
<input type="text" maxlength="8" data-id="10" disabled=""> event
<button class="switch" data-id="10"></button> event
<span class="led-indicator locked"></span>
<div class="component macaroni" data-code="K02"></div>
<div class="component swab" data-code="9XJ"></div>
<div class="component gnome" data-code="37"></div>
<span class="led-indicator unlocked"></span>
::after
</div>
</li>
</ul>
```

You have to do this two more times and then the crate unlocks afterwards.



Fun fact, in the answer code I thought the “D” was actually a “0”. So I did everything correctly and was losing my mind because I kept getting a “FAIL” error when trying to open the crate. The ranking is accurate, I am a casual for misreading the answer code.

Kent Tinseltooth – Smart Braces

```
Inner Voice: Kent. Kent. Wake up, Kent.
Inner Voice: I'm talking to you, Kent.
Kent TinselTooth: Who said that? I must be going insane.
Kent TinselTooth: Am I?
Inner Voice: That remains to be seen, Kent. But we are having a conversation.
Inner Voice: This is Santa, Kent, and you've been a very naughty boy.
Kent TinselTooth: Alright! Who is this?! Holly? Minty? Alabaster?
Inner Voice: I am known by many names. I am the boss of the North Pole. Turn to me and be
hired after graduation.
Kent TinselTooth: Oh, sure.
Inner Voice: Cut the candy, Kent, you've built an automated, machine-learning, sleigh devi
ce.
Kent TinselTooth: How did you know that?
Inner Voice: I'm Santa - I know everything.
Kent TinselTooth: Oh, Kringle. *sigh*
Inner Voice: That's right, Kent. Where is the sleigh device now?
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@adb540b1d75a:~$
```

The readme file below instructs on what iptable commands need to be used to successfully configure Kent's smart braces.

```
elfuuser@99ef2231c1ac:~$ cat /home/elfuuser/IOTteethBraces.md
# ElfU Research Labs - Smart Braces
### A Lightweight Linux Device for Teeth Braces
### Imagined and Created by ElfU Student Kent TinselTooth

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

## Proper Firewall configuration:

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

```
sudo iptables -P FORWARD DROP
```

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

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

A proper configuration for the Smart Braces should be exactly:

1. Set the default policies to DROP for the INPUT, FORWARD, and OUTPUT chains.
2. Create a rule to ACCEPT all connections that are ESTABLISHED,RELATED on the INPUT and t
he OUTPUT chains.
3. Create a rule to ACCEPT only remote source IP address 172.19.0.225 to access the local
SSH server (on port 22).
4. Create a rule to ACCEPT any source IP to the local TCP services on ports 21 and 80.
5. Create a rule to ACCEPT all OUTPUT traffic with a destination TCP port of 80.
6. Create a rule applied to the INPUT chain to ACCEPT all traffic from the lo interface.
elfuuser@99ef2231c1ac:~$ sudo iptables -P FORWARD DROP
elfuuser@99ef2231c1ac:~$ sudo iptables -P INPUT, OUTPUT DROP
Bad argument `DROP'
Try `iptables -h' or 'iptables --help' for more information.
```

```
elfuuser@6d2789848b46:~$ sudo iptables -P INPUT DROP
elfuuser@6d2789848b46:~$ sudo iptables -P FORWARD DROP
elfuuser@6d2789848b46:~$ sudo iptables -P OUTPUT DROP
elfuuser@6d2789848b46:~$ sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j AC
CEPT
elfuuser@6d2789848b46:~$ sudo iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j A
CCEPT
elfuuser@6d2789848b46:~$ sudo iptables -A INPUT -p tcp --dport 22 -s 172.19.0.225 -j ACCEP
T
elfuuser@6d2789848b46:~$ sudo iptables -A INPUT -p tcp --dport 21 -j ACCEPT
elfuuser@6d2789848b46:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
elfuuser@6d2789848b46:~$ sudo iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
elfuuser@6d2789848b46:~$ sudo iptables -A INPUT -i lo -j ACCEPT
elfuuser@6d2789848b46:~$ servoce o[tab;esKent TinselTooth: Great, you hardened my IOT Smar
t Braces firewall!
```

The commands above are what I used; there's even evidence of how tired I was, I was trying to type "service iptables start" and it interrupted me midway. I had my hands positioned on the keyboard wrong, which is why the command looks like a dumpster fire.