

PSP0201

Week 5

Writeup

GROUP NAME: Cyborgs

MEMBERS

ID NUMBER	NAME	ROLE
1211102066	Hemma Ravindran	Leader
1211100614	Tivaasheny Ananthan	Member
1211102168	Nicholas Cheok Jia Jie	Member
1211100986	Sarvesh Munusamy	Member

Day 16 - Help! Where is Santa?

Tool used: google and try hackme

Solution/walkthrough:

Question 1:

We are supposed to find the port number using the nmap.

The terminal output shows the following nmap command and results:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-12 02:14 BST
Initiating ARP Ping Scan at 02:14
Scanning 10.10.110.46 [1 port]
Completed ARP Ping Scan at 02:14, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:14
Completed Parallel DNS resolution of 1 host. at 02:14, 0.00s elapsed
Initiating SYN Stealth Scan at 02:14
Scanning ip-10-10-110-46.eu-west-1.compute.internal (10.10.110.46) [1000 ports]
Discovered open port 80/tcp on 10.10.110.46
Discovered open port 22/tcp on 10.10.110.46
Completed SYN Stealth Scan at 02:14, 1.65s elapsed (1000 total ports)
Nmap scan report for ip-10-10-110-46.eu-west-1.compute.internal (10.10.110.46)
Host is up (0.060s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 02:85:9A:D1:0B:B7 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.08 seconds
Raw packets sent: 1159 (50.980KB) | Rcvd: 1159 (46.356KB)
```

Question 2:

We got the answer from the hint given.

Category	Category	Category
Lorem ipsum dolor sit amet Vestibulum errato isse Lorem ipsum dolor sit amet Asia caisia Murphy's law Flimsy Lavenrock Maven Mousie Lavender	Labore et dolore magna aliqua Kanban airis sum eschelor Modular modern free The king of clubs The Discovery Dissipation Course Correction Better Angels	Objects in space Playing cards with coyote Goodbye Yellow Brick Road The Garden of Forking Paths Future Shock

Question 3

We guessed it from the links given.

Answer the questions below

What is the port number for the web server?

80 Correct Answer

Without using enumerations tools such as Dirbuster, what is the directory for the API?
(without the API key)

Answer format: /***/ Submit Hint

Where is Santa right now?

Answer format: ***** ***** *, **** *, ***** Submit

Find out the correct API key. Remember, this is an odd number between 0-100. After too many attempts, Santa's Sled will block you.

To unlock yourself, simply terminate and re-deploy the target instance (10.10.110.46)

Answer format: ** Submit

Task 19 [Day 17] Reverse Engineering ReverseELFneering Submit

Task 20 [Day 18] Reverse Engineering The Bits of Christmas Submit

Task 21 [Day 19] Web Exploitation The Naughty or Nice List Submit

Task 22 [Day 20] Blue Teamng PowersELF to the rescue Submit

Applications Places System Tue 12 Jul, 02:23 AttackBox IP:10.10.12.3 http://10.10.110.46 - Mozilla Firefox Santa's Tracker x http://10.10.110.46 view-source:http://10.10.110.46 TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo/... >

```
<ul>
  <li><a href="#">Vestibulum errato isse</a></li>
  <li><a href="#">Alius ipsum sit amet</a></li>
  <li><a href="#">Alius ipsum</a></li>
  <li><a href="#">Murphy's Law</a></li>
  <li><a href="#">Flimsy Lavenrock</a></li>
  <li><a href="#">Maven Mousie Lavender</a></li>
</ul>
</div>
<div class="column is-3">
  <b><strong>Category</strong></b>
  <ul>
    <li><a href="#">Labore et dolore magna aliqua</a></li>
    <li><a href="#">Kanban airis sum eschelor</a></li>
    <li><a href="#">Modular modern free</a></li>
    <li><a href="#">The king of clubs</a></li>
    <li><a href="#">The discovery Dissipation</a></li>
    <li><a href="#">Course Correction</a></li>
    <li><a href="#">Better Angels</a></li>
  </ul>
</div>
<div class="column is-4">
  <b><strong>Category</strong></b>
  <ul>
    <li><a href="#">Objects in space</a></li>
    <li><a href="#">Playing cards with coyote</a></li>
    <li><a href="#">Goodbye Yellow Brick Road</a></li>
    <li><a href="#">The garden of Forking Paths</a></li>
    <li><a href="#">Future Shock</a></li>
  </ul>
</div>
</div>
<div class="content has-text-centered">
  <p>
    <a class="icon" href="https://github.com/BulmaTemplates/bulma-templates">
      <i class="fa fa-github"></i>
    </a>
  </p>
</div>
```

THM AttackBox 52m 06s

Question 4

We click the 'View Page Source' and then scroll to the bottom. Find the link, click it, then show up the answer.

Answer the questions below

What is the port number for the web server?

Correct Answer

Without using enumerations tools such as Dirbuster, what is the directory for the API?
(without the API key)

Correct Answer Hint

Where is Santa right now?

Correct Answer

Find out the correct API key. Remember, this is an odd number between 0-100. After too many attempts, Santa's Sled will block you.

To unlock yourself, simply terminate and re-deploy the target instance (10.10.110.46)

Correct Answer

Task 19 [Day 17] Reverse Engineering ReverseEngineering

Task 20 [Day 18] Reverse Engineering The Bits of Christmas

Task 21 [Day 19] Web Exploitation The Naughty or Nice List

Applications Places System Tue 12 Jul, 03:15 AttackBox IP:10.10.12.3 http://10.10.110.46/js/bulma.js - Mozilla Firefox Problem loading page http://10.10.110.46/js/bulma.js + TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo/... {"detail": "Not Found"}

THM AttackBox

Question 5 , 6

We can type out a simple code and put the range to make it more easier.

```
api_key 47
{"item_id":47,"q":"Error. Key not valid!"}
api_key 49
{"item_id":49,"q":"Error. Key not valid!"}
api_key 51
{"item_id":51,"q":"Error. Key not valid!"}
api_key 53
{"item_id":53,"q":"Error. Key not valid!"}
api_key 55
{"item_id":55,"q":"Error. Key not valid!"}
api_key 57
{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."}
api_key 59
{"item_id":59,"q":"Error. Key not valid!"}
api_key 61
{"item_id":61,"q":"Error. Key not valid!"}
api_key 63
```

Thought Process/Methodology:

Firstly, find the port number using the nmap and then put the Ip address and the port number in mozilla firefox. We'll get a page. we must right click and go to the view page source. From there we can get the answer for the second and third question. For question number 4 we should go to the bottom of the view page source and then press the link. The answer will be displayed. Question 5,6 should be done using coding. We must type out a basic code and run it . We will get the answers .

Day 17 - ReverseELFneering

Tool used: google and try hack me attack box

Solution/walkthrough:

Question 1:

We refer to this table that given in try hack me to get the answers.

The screenshot shows a browser window with several tabs open. The active tab is titled "3. Register me this, register me that...". The content discusses assembly language register usage and includes a table mapping initial data types to suffixes and sizes.

Initial Data Type	Suffix	Size (bytes)
Byte	b	1
Word	w	2
Double Word	l	4
Quad	q	8
Single Precision	s	4
Double Precision	l	8

Below the table, it says: "When dealing with memory manipulation using registers, there are other cases to be considered:" followed by a list of memory location formulas.

- $(Rb, Ri) = \text{MemoryLocation}[Rb + Ri]$
- $D(Rb, Ri) = \text{MemoryLocation}[Rb + Ri + D]$
- $(Rb, Ri, S) = \text{MemoryLocation}[Rb + S * Ri]$
- $D(Rb, Ri, S) = \text{MemoryLocation}[Rb + S * Ri + D]$

Question 2:

We can get the answer from the try hack me and also we can do at the terminal to see it's function.

The screenshot shows a browser window with several tabs open. The active tab is titled "Let's proceed to run through how Radare2 works exactly. Although you shouldn't do this if the program is unknown, it is safe for us to execute to see what should be happening like so:". It shows a terminal window with the command `./file1` and its output: "the value of a is 4, the value of b is 5 and the value of c is 9".

Below the terminal, it says: "The above program shows that there are 3 variables(a, b, c) where c is the sum of a and b."

It then instructs: "Time to see what's happening under the hood! Run the command `r2 -d ./file1`".

It continues: "This will open the binary in debugging mode. Once the binary is open, one of the first things to do is ask r2 to analyze the program, and this can be done by typing in: `aa`".

Note: "When using the `aa` command in radare2, this may take between 5-10 minutes depending on your system."

It explains: "Which is the most common analysis command. It analyses all symbols and entry points in the executable. The analysis, in this case, involves extracting function names, flow control information, and much more! r2 instructions are usually based on a single character, so it is easy to get more information about the commands."

I.e. For general help, we can run: `?` or if we wish to understand more about a specific feature, we could provide `a?`

3. Computer says...Done?!

Once the analysis is complete, you would want to know where to start analysing from - most programs have an entry point defined as main. To find a list of the functions run: `afl`

```
[0x00400a30]> afl | grep main
```



1. Story.

McSkidy has never really touched low-level languages - this is something they must learn in their quest to defeat the Christmas monster.

Follow along with Darkstar7474 and solve Day 17!

2. Introduction to x86-64 Assembly

Computers execute machine code, which is encoded as bytes, to carry out tasks on a computer. Since different computers have different processors, the machine code executed on these computers is specific to the processor. In this case, we'll be looking at the Intel x86-64 instruction set architecture which is most commonly found today. Machine code is usually represented by a more readable form of the code called assembly code. This machine code is usually produced by a compiler, which takes the source code of a file, and after going through some intermediate stages, produces machine code that can be executed by a computer.

Without going into too much detail, Intel first started out by building a 16-bit instruction set, followed by 32 bit, after which they finally created 64 bit. All these instruction sets have been

```
elfmceager@tbfc-day-17:~$ ./file1
the value of a is 4, the value of b is 5 and the value of c is 9
elfmceager@tbfc-day-17:~$ r2 -d ./file1
Process with PID 1634 started...
= attach 1634 1634
bin.baddr 0x00400000
Using 0x400000
Warning: Cannot initialize dynamic strings
asm.blts 64
[0x00400a30]> aa
[+] WARNING : block size exceeding max block size at 0x006ba220
[+] Try changing it with e anal.bb.maxsize
WARNING : block size exceeding max block size at 0x006bc860
[+] Try changing it with e anal.bb.maxsize
[+] Analyze all flags starting with sym. and entry0 (aa)
[0x00400a30]>
```

THM AttackBox 45m 26s 9:35 AM 12/7/2022

Question 3:

We can get the answer from the try hack me and also we can do at the terminal to see it's function.

WS TLS Cyborgs - Google Docs | TryHackMe | 25 Days of Cyber Security | Week 5 Tutorial Progress | PSP0201 T2130 - Tutorial Week 5 | +

tryhackme.com/room/learncyberin25days

```
0x00400b5b    8945fc    movl %eax, local_4h
0x00400b6e    8b4dfc    movl local_4h, %ecx
0x00400b71    8b55f8    movl local_8h, %edx
0x00400b74    8b45f4    movl local_ch, %eax
0x00400b77    89c6    movl %eax, %esi
0x00400b79    488d3d881409. leaq str.the_value_of_a_i
0x00400b80    b800000000    movl $0, %eax
```

The line starting with `sym.main` indicates we're looking at the `main` function. The next 3 lines are used to represent the variables stored in the function. The second column indicates that they are integers(`int`), the 3rd column specifies the name that `r2` uses to reference them and the 4th column shows the actual memory location.

The first 3 instructions are used to allocate space on that stack (ensures that there's enough room for variables to be allocated and more). We'll start looking at the program from the 4th instruction (`movl $4`). We want to analyse the program while it runs and the best way to do this is by using `breakpoints`.

A `breakpoint` specifies where the program should stop executing. This is useful as it allows us to look at the state of the program at that particular point. So let's set a breakpoint using the command `db`, in this case, it would be `db 0x00400b55`. To ensure the breakpoint is set, we run the `pdf @main` command again and see a little `b` next to the instruction we want to stop at.

```
0x00400a30]> pdf @main
;; main:
(fcn) sym.main 68
sym.main (int argc, char **argv, char **envp);
; var int local_ch @ rbp-0xc
; var int local_8h @ rbp-0x8
; var int local_4h @ rbp-0x4
; DATA XREF from entry0 (0x400a4d)
0x00400b4d    55        pushq %rbp
0x00400b4e    4889e5    movq %rsp, %rbp
0x00400b51    4883ec10  subq $0x10, %rsp
0x00400b55    b         c745f4040000. movl $4, local_ch
```

1:28 PM 13/7/2022

As seen here, there actually is a function at main. Let's examine the assembly code at main by running the command `pdf @main`. Where pdf means print disassembly function. Doing so will give us the following view:

```

elfmceager@tbfc-day-17:~$ pdf @main
[0x004000a30]> pdf @main
[0x004000a30]>
;; main:
(fcn) sym.main 68
sym.main ()
; var int local_ch @ rbp-0xc
; var int local_bh @ rbp-0x8
; var int local_4h @ rbp-0x4
; DATA XREF From 0x004000d (entry0)
0x00400b4d    55          push rbp
0x00400b4e    489e5       mov rbp, rsp
0x00400b51    4883ec10   sub rsp, 0x10
0x00400b55    b745f4040000  mov dword [local_ch], 4
0x00400b5c    c745f8050000  mov dword [local_bh], 5
0x00400b63    8b55f4      mov edx, dword [local_ch]
0x00400b66    8b45f8      mov eax, dword [local_bh]
0x00400b69    01d0        add eax, edx
0x00400b6b    8945fc      mov dword [local_4h], eax
0x00400b6e    8b4dfc      mov ecx, dword [local_4h]
0x00400b71    8b55f8      mov edx, dword [local_bh]
0x00400b74    8b45f4      mov eax, dword [local_ch]
0x00400b77    89c6        mov est, eax

```

3. Register me this, register me that...

The core of assembly language involves using registers to do the following:

- Transfer data between memory and register, and vice versa
- Perform arithmetic operations on registers and data
- Transfer control to other parts of the program Since the architecture is x86-64, the registers are 64 bit and Intel has a list of 16 registers:

Initial Data Type	Suffix	Size (bytes)
Byte	b	1
Word	w	2
Double Word	l	4

Question 4:

We can get the answer from the try hack me and also we can do at the terminal to see it's function.

```

W5 TLSI Cyborgs - Google Docs | TryHackMe | 25 Days of Cyber Security | Week 5 Tutorial Progress | PSP0201 T2130 - Tutorial Week 5 | TryHackMe Advent...
[0x004000a30]> sym.main 68
sym.main (int argc, char **argv, char **envp);
; var int local_ch @ rbp-0xc
; var int local_bh @ rbp-0x8
; var int local_4h @ rbp-0x4
; DATA XREF from entry0 (0x4000d4)
0x00400b4d    55          pushq %rbp
0x00400b4e    489e5       movq %rsp, %rbp
0x00400b51    4883ec10   subq $0x10, %rsp

```

Running `dc` will execute the program until we hit the breakpoint. Once we hit the breakpoint and print out the rip which is the current instruction shows where execution has stopped. From the notes above, we know that the `mov` instruction is used to transfer values. This statement is transferring the value 4 into the `local_ch` variable. To view the contents of the `local_ch` variable, we use the following instruction `px @memory-address`. In this case, the corresponding memory address for `local_ch` will be `rbp-0xc` (from the first few lines of `@pdf main`) This instruction prints the values of memory in hex:

```

[0x00400b55]> px @ rbp-0xc
- offset - 0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0x7ffc914f7bc4 0000 0000 1890 6b00 0000 0000 7018 4000 .....k.....p.@
0x7ffc914f7bd4 0000 0000 1911 4000 0000 0000 0000 0000 .....@.0.
0x7ffc914f7be4 0000 0000 0000 0000 0100 0000 f87c 4f91 .....|0.
0x7ffc914f7bf4 fc7f 0000 4d0b 4000 0000 0000 0000 0000 ....M.@
0x7ffc914f7c04 0000 0000 0000 0000 8e00 0000 8000 0000 ....@.0.
0x7ffc914f7c14 0a00 0000 0000 0000 0000 0000 0000 0000 ....R..A93_..@.
0x7ffc914f7c24 0000 0000 0000 0000 0000 0000 0000 0000 ....R...R...
0x7ffc914f7c34 0000 0000 0000 0000 fe41 3933 915f 1019 4000 .....R..A93_..@.
0x7ffc914f7c44 0000 0000 0000 0000 52db de41 3933 915f 1019 4000 .....R..A93_..@.
0x7ffc914f7c54 0000 0000 0000 0000 0000 0000 0000 0000 1890 6b00 .....R...R...
0x7ffc914f7c64 0000 0000 0000 0000 0000 0000 0000 0000 52db de86 .....R...R...

```

As seen here, there actually is a function at main. Let's examine the assembly code at main by running the command `pdf @main` Where pdf means print disassembly function. Doing so will give us the following view:

```

0x00400b4d  1 68      sym.main
0x00400e10  114 1657   sym._libc_start_main
0x00403870  346 6038 -> 5941  sym._nl_find_domain
0x00415fe0  1 43      sym._IO_switch_to_main_get_area
0x0044cf00  1 8       sym._dl_get_dl_main_map
0x0047b520  1 49      sym._IO_switch_to_main_wget_area
0x0048fae0  7 73     -> 69  sym._nl_fnddomain_subfreeres
0x0048fb30  16 247    -> 237 sym._nl_unload_domain

Note that memory addresses may be different on your computer.

```

The core of assembly language involves using registers to do the following:

- Transfer data between memory and register, and vice versa
- Perform arithmetic operations on registers and data

Question 5, 6 and 7:

We need to do the challenge in terminal to get the answers.

Luckily for us, everything we need has been provided to you via an instance that you can deploy and log into:

- Press the "Deploy" button on the top-right of this task
- Wait for the IP address of the target instance to display
- Log into your Instance using the following information:

IP Address: 10.10.181.79
 Username: elfmceager
 Password: adventofcyber

Let's proceed to run through how Radare2 works exactly. Although you shouldn't do this if the program is unknown, it is safe for us to execute to see what *should* be happening like so:

```

ashu@ashu-Inspiron-5379 ~$ /bin/c/christmas-re > ./file1
the value of a is 4, the value of b is 5 and the value of c is 9

```

The above program shows that there are 3 variables(a, b, c) where c is the sum of a and b.

Time to see what's happening under the hood! Run the command `r2 -d ./file1`

This will open the binary in debugging mode. Once the binary is open, one of the first things to do is ask r2 to analyze the program, and this can be done by typing in: `aa`

Note, when using the `aa` command in radare2, this may take between 5-10 minutes

Thought Process/Methodology:

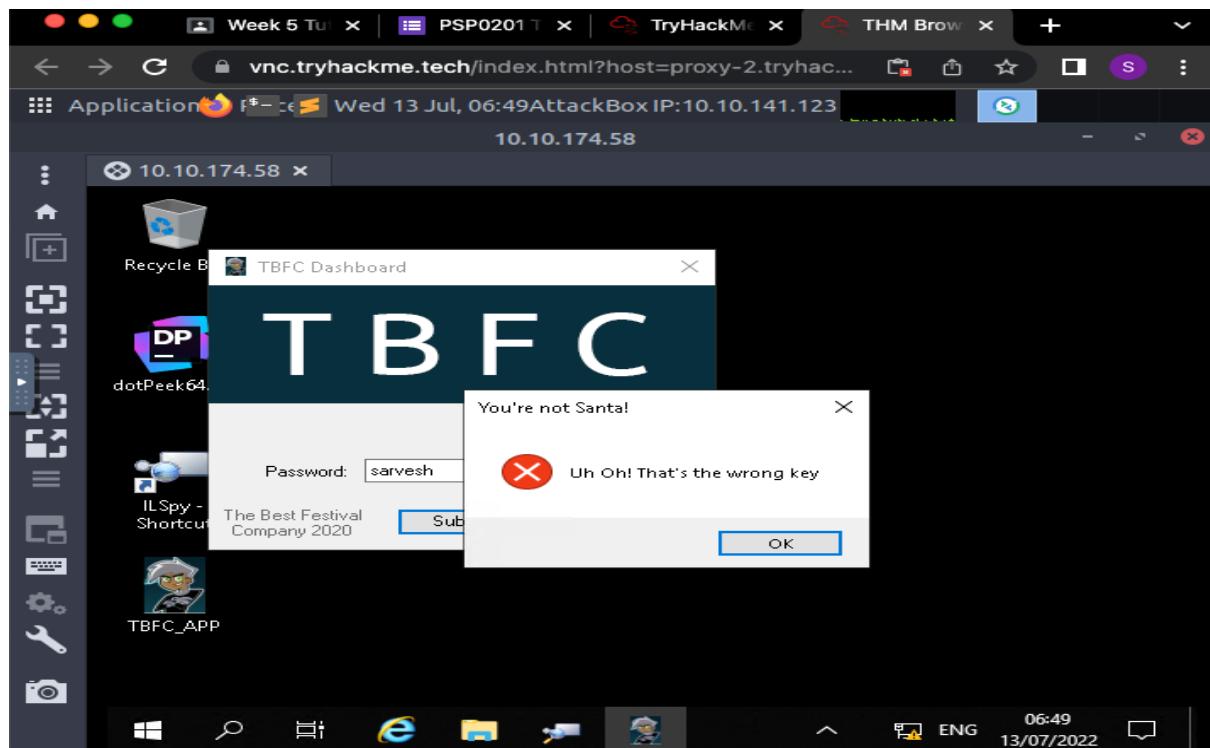
We need to open the attack box in kali. Then if we follow the youtube video we manage to file1. We did it to learn the function dc db dr aa and more. But the main thing is we need to do the challenge to get the answers. Firstly, we need to type echo “our IP address” > target.txt enter cat target.txt enter ssh elfmceager@IP address enter. Then we need to type yes and the password. Later we need type ls enter ls -lsa enter then r2 -d ./challange1. Then we have to type aa and wait for awhile. Finally we need to type pdf @main in order to get the answers.

Day 18 - The bits of christmas

Tools used : attackbox, TBFC APP, ILspy

Question 1:

If we enter the wrong password in the TBFC APP, the message that pops up is “You’re not Santa”.



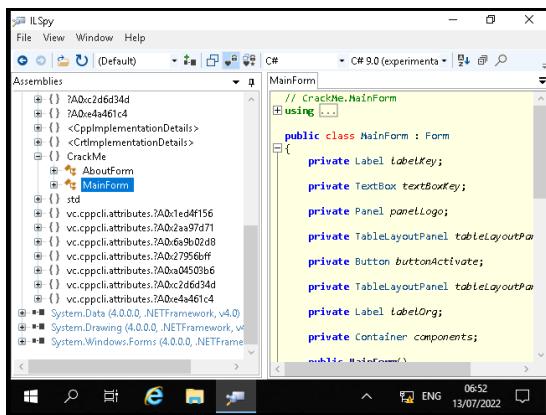
Question 2:

TBFC stands for The Best Festival Company.



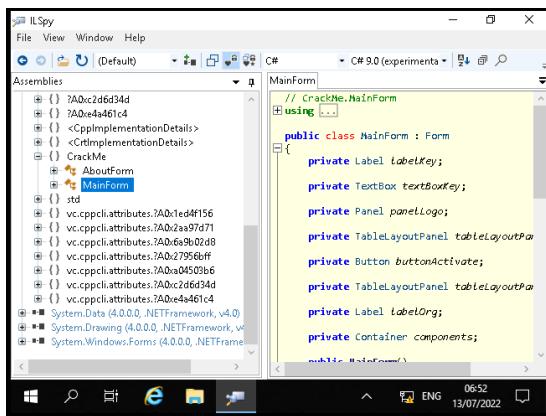
Question 3:

After decompiling the TBFC APP with ILspy. The module that catches my attention is CrackMe.



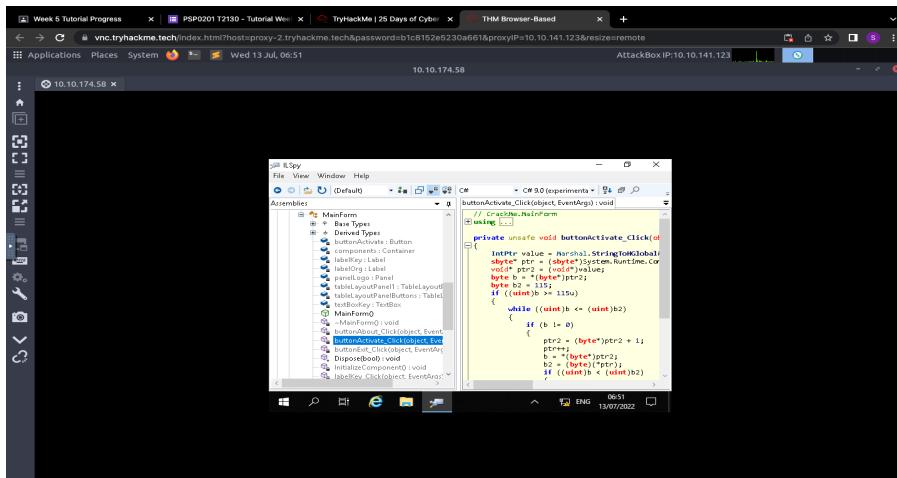
Question 4:

Within the module Crack me, “Main Form” is the form that contains the information we need.



Question 5:

`"buttonActivate_Click"` is the method that we can use to contain the information that we need.



Question 6:

After getting the password that we want from “buttonActivate_Click” , we should copy and paste it in cyberchef, and then get santa’s password.

The screenshot shows the CyberChef interface. In the 'Input' section, there is a long string of hex values: 73 61 6E 74 61 70 61 73 73 77 6F 72 64 33 32 31. In the 'Output' section, the converted base64 string is shown: santapassword321. The 'From Hex' recipe is selected in the center panel.

Question 7:

Since we retrieved the password, we can re-login again in TBFC and get the flag.

The screenshot shows a VNC session connected to an AttackBox IP at 10.10.141.123. The desktop environment is Windows 7. A window titled 'TBFC Dashboard' is open, displaying the message 'That's the right key!'. Below it, a message box says 'Welcome, Santa, here's your flag thm[D46af]'. The taskbar at the bottom shows various icons, including a browser and file explorer.

Thought Process/Methodology:

After starting the machine, we should open the remmina and run the ip address given. Then we should open the TBFC application. Since we don't know the password of santa, we should open IL spy and open the Tbfc application file. After decompiling the application, we should open the module called, "Crack me". Within the module, we should open main form and gain the information we need. After getting the password that we want from "buttonActivate_Click", we should copy and paste it in cyberchef, and then get santa's password. Since we retrieved the password, we can re-login again in TBFC and get the flag.

Day 19 - The Naughty or Nice List

Tool used: google and try hackme

Solution/walkthrough:

Question 1:

Enter your IP address to run the browser then scroll to the bottom and enter any names in the Name Box and search about it. You will get a display on whether the name is a nice or naughty list.

Note that while the example of SSRF used in this task is effectively a Remote File Inclusion (RFI) vulnerability as well, not every SSRF is. Some SSRF vulnerabilities only trigger a DNS lookup, while others may not return any kind of response to the web app, but can still be used to "port scan" internal systems by measuring the time each request takes to complete. In other cases, SSRF may be used as a form of Denial of Service (DoS) since the attacker can continually request that the server download large files simultaneously (taking up memory, disk space, and network bandwidth).

Walkthrough

1. Once the VM is deployed, connect to the web app: <http://10.10.14.72>

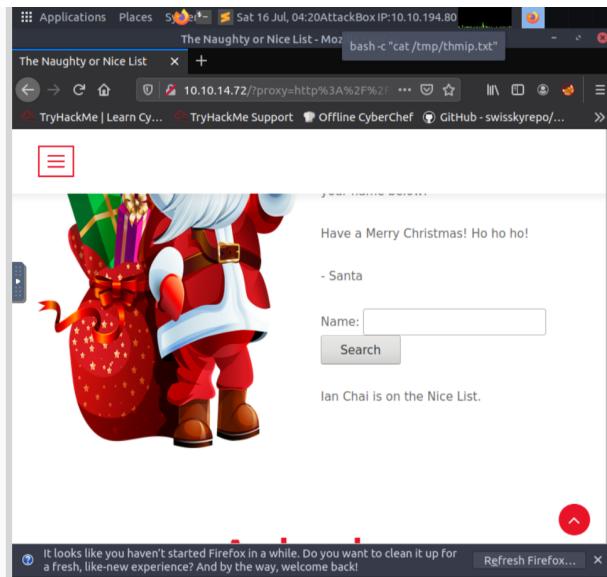
2. Enter a name in the form and click the "Search" button. When the page loads, it should tell you whether that name is on the Naughty List or the Nice List. Notice that the URL for the page looks something like this: <http://10.10.14.72/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3DTib3rius>

If we use a URL decoder on the value of the "proxy" parameter, we get: <http://list.hohoho:8080/search.php?name=Tib3rius>

Since "list.hohoho" is not a valid hostname on the Internet (.hohoho is not a top-level domain), this hostname likely refers to some back-end machine. It seems that the web app works by taking this URL, making a request at the back-end, and then returning the result to the front-end web app. If the developer has not been careful, we may be able to exploit this functionality using Server-Side Request Forgery (SSRF).

3. The most obvious thing we can try to do first is to fetch the root of the same site. Browse to: <http://10.10.14.72/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F>

This seems to have potential, as in place of the original "Tib3rius is on the Nice List."



Question 2:

Browse in the website "http://MACHINE_IP/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F" to get a display at the bottom saying "Not Found. The requested URL was not found on this server."

If we use a URL decoder on the value of the "proxy" parameter, we get: <http://list.hohoho:8080/search.php?name=Tib3rius>

Since "list.hohoho" is not a valid hostname on the Internet (.hohoho is not a top-level domain), this hostname likely refers to some back-end machine. It seems that the web app works by taking this URL, making a request at the back-end, and then returning the result to the front-end web app. If the developer has not been careful, we may be able to exploit this functionality using Server-Side Request Forgery (SSRF).

3. The most obvious thing we can try to do first is to fetch the root of the same site. Browse to: <http://10.10.14.72/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F>

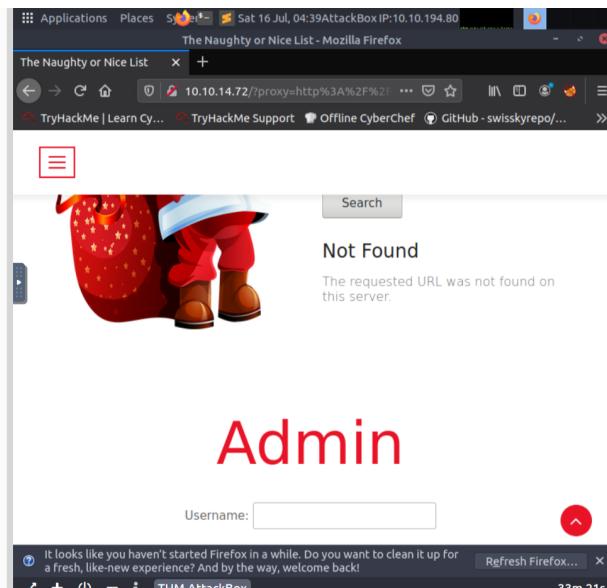
This seems to have potential, as in place of the original "Tib3rius is on the Nice List." message, we instead see "Not Found. The requested URL was not found on this server." This seems like a generic 404 message, indicating that we were able to make the server request the modified URL and return the response.

There are many things we could do now, such as trying to find valid URLs for the "list.hohoho" site. We could also try changing the port number from 8080 to something else, to see if we can connect to any other services running on the host, even if these services are not web servers.

4. Try changing the port number from 8080 to just 80 (the default HTTP port): <http://10.10.14.72/?proxy=http%3A%2F%2Flist.hohoho%3A80>

The message now changes to "Failed to connect to list.hohoho port 80: Connection refused" which suggests that port 80 is not open on list.hohoho.

5. Try changing the port number to 22 (the default SSH port): <http://10.10.14.72/?proxy=http%3A%2F%2Flist.hohoho%3A22>



Question 3:

Change the port number from 8080 to just 80 in the default http port and you will get a display at the bottom saying "Failed to connect to list.hohoho port 80: Connection refused".

3. The most obvious thing we can try to do first is to fetch the root of the same site. Browse to: <http://10.10.14.72/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F>

This seems to have potential, as in place of the original "Tib3rius is on the Nice List." message, we instead see "Not Found. The requested URL was not found on this server." This seems like a generic 404 message, indicating that we were able to make the server request the modified URL and return the response.

There are many things we could do now, such as trying to find valid URLs for the "list.hohoho" site. We could also try changing the port number from 8080 to something else, to see if we can connect to any other services running on the host, even if these services are not web servers.

4. Try changing the port number from 8080 to just 80 (the default HTTP port): <http://10.10.14.72/?proxy=http%3A%2F%2Flist.hohoho%3A80>

The message now changes to "Failed to connect to list.hohoho port 80: Connection refused" which suggests that port 80 is not open on list.hohoho.

5. Try changing the port number to 22 (the default SSH port): <http://10.10.14.72/?proxy=http%3A%2F%2Flist.hohoho%3A22>

The message now changes to "Recv failure: Connection reset by peer" which suggests that port 22 is open but did not understand what was sent (this makes sense, as sending an HTTP request to an SSH server will not get you anywhere!)

Enumerating open ports via SSRF can be performed in this manner, by iterating over common ports and measuring the differences between responses. Even in cases where error messages aren't returned, it is often possible to detect which ports are open vs closed by measuring the time each request takes to complete.

Question 4:

Change the port number again from 80 to 22 in the default http port and you will get a display at the bottom saying "Recv failure: Connection reset by peer".

The message now changes to "Failed to connect to list.hohoho port 80: Connection refused" which suggests that port 80 is not open on list.hohoho.

5. Try changing the port number to 22 (the default SSH port): <http://10.10.14.72/?proxy=http%3A%2F%2Flist.hohoho%3A22>

The message now changes to "Recv failure: Connection reset by peer" which suggests that port 22 is open but did not understand what was sent (this makes sense, as sending an HTTP request to an SSH server will not get you anywhere!).

Enumerating open ports via SSRF can be performed in this manner, by iterating over common ports and measuring the differences between responses. Even in cases where error messages aren't returned, it is often possible to detect which ports are open vs closed by measuring the time each request takes to complete.

6. Another thing we can try to do with SSRF is access services running locally on the server. We can do this by replacing the list.hohoho hostname with "localhost" or "127.0.0.1" (among others). Try this now: <http://10.10.14.72/?proxy=http%3A%2F%2Flocalhost>

Oops! It looks like the developer has a check in place for this, as the message returned says "Your search has been blocked by our security team."

Indeed, if you try other hostnames (e.g. 127.0.0.1, example.com, etc.) they will all be blocked. The developer has implemented a check to ensure that the hostname provided starts with "list.hohoho", and will block any hostnames that don't.

7. As it turns out, this check can easily be bypassed. Since the hostname simply needs to start with "list.hohoho", we can take advantage of DNS subdomains and create our own domain "list.hohoho.evilsite.com" which resolves to 127.0.0.1. In fact, we don't even need to buy a domain or configure the DNS, because multiple domains already exist that let us do this. The one we will be using is localhost, which receives our subdomain to

Question 5:

Replace the "list.hohoho hostname" with "localhost" or "127.0.0.1" and you will get a display at the bottom saying "Your search has been blocked by our security team."

error messages aren't returned, it is often possible to detect which ports are open vs closed by measuring the time each request takes to complete.

6. Another thing we can try to do with SSRF is access services running locally on the server. We can do this by replacing the list.hohoho hostname with "localhost" or "127.0.0.1" (among others). Try this now: <http://10.10.14.72/proxy=http%3A%2F%2Flocalhost>

Oops! It looks like the developer has a check in place for this, as the message returned says "Your search has been blocked by our security team."

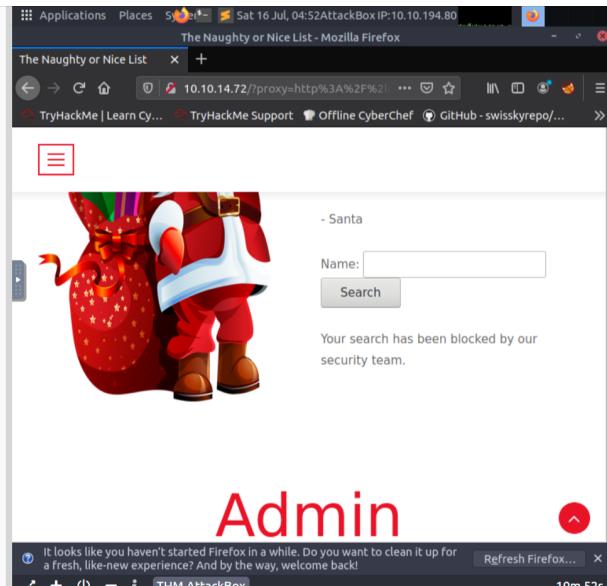
Indeed, if you try other hostnames (e.g. 127.0.0.1, example.com, etc.) they will all be blocked. The developer has implemented a check to ensure that the hostname provided starts with "list.hohoho", and will block any hostnames that don't.

7. As it turns out, this check can easily be bypassed. Since the hostname simply needs to start with "list.hohoho", we can take advantage of DNS subdomains and create our own domain "list.hohoho.evilsite.com" which resolves to 127.0.0.1. In fact, we don't even need to buy a domain or configure the DNS, because multiple domains already exist that let us do this. The one we will be using is localtest.me, which resolves every subdomain to 127.0.0.1.

We can therefore set the hostname in the URL to "list.hohoho.localtest.me", bypass the check, and access local services: <http://10.10.14.72/proxy=http%3A%2F%2Flist.hohoho.localtest.me>

Success! It appears that there is a web server running locally, and it has a message from Elf McSkidy that contains some sensitive information we can use!

8. Click the "Admin" link at the top or scroll down to the login. Guess the username and use the password you found to login as Santa.



Question 6:

Replace the “localhost” with "list.hohoho.localtest.me" to get the password of Santa “Be good for goodness sake!”

says "Your search has been blocked by our security team."

Indeed, if you try other hostnames (e.g. 127.0.0.1, example.com, etc.) they will all be blocked. The developer has implemented a check to ensure that the hostname provided starts with "list.hohoho", and will block any hostnames that don't.

7. As it turns out, this check can easily be bypassed. Since the hostname simply needs to start with "list.hohoho", we can take advantage of DNS subdomains and create our own domain "list.hohoho.evilsite.com" which resolves to 127.0.0.1. In fact, we don't even need to buy a domain or configure the DNS, because multiple domains already exist that let us do this. The one we will be using is localtest.me, which resolves every subdomain to 127.0.0.1.

We can therefore set the hostname in the URL to "list.hohoho.localtest.me", bypass the check, and access local services: <http://10.10.14.72/proxy=http%3A%2F%2Flist.hohoho.localtest.me>

Success! It appears that there is a web server running locally, and it has a message from Elf McSkidy that contains some sensitive information we can use!

8. Click the "Admin" link at the top or scroll down to the login. Guess the username and use the password you found to login as Santa.

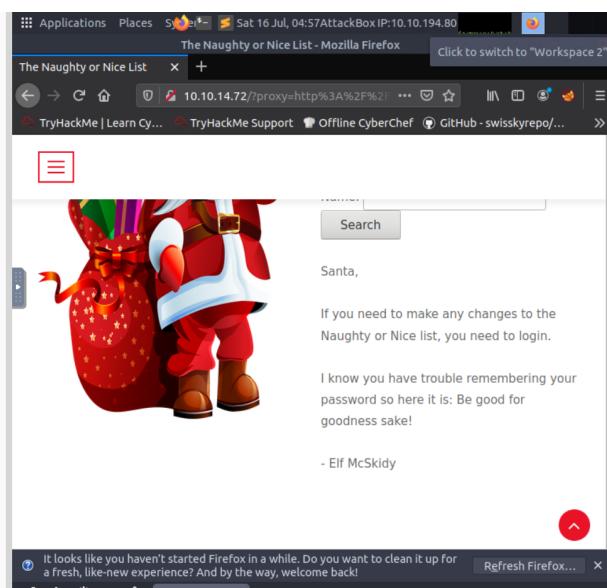
9. Delete the naughty list to find the challenge flag!

Answer the questions below

What is Santa's password?

Be good for goodness sake

Correct Answer



Question 7:

Login as Santa and enter the password in the administration and click on “DELETE NAUGHTY LIST” to get the flag “THM{EVERYONE_GETS_PRESENTS}.

starts with `list.nonono`, and will block any nosnames that don't.

7. As it turns out, this check can easily be bypassed. Since the hostname simply needs to start with "list.hohoho", we can take advantage of DNS subdomains and create our own domain "list.hohoho.evilsite.com" which resolves to 127.0.0.1. In fact, we don't even need to buy a domain or configure the DNS, because multiple domains already exist that let us do this. The one we will be using is localtest.me, which resolves every subdomain to 127.0.0.1.

We can therefore set the hostname in the URL to "list.hohoho.localtest.me", bypass the check, and access local services: <http://10.10.14.72/?proxy=http%3A%2F%2Flist.hohoho.localtest.me>

Success! It appears that there is a web server running locally, and it has a message from Elf McSkidy that contains some sensitive information we can use!

8. Click the "Admin" link at the top or scroll down to the login. Guess the username and use the password you found to login as Santa.

9. Delete the naughty list to find the challenge flag!

Answer the questions below

What is Santa's password?

Correct Answer

What is the challenge flag?

Correct Answer

Common `list.hohoho.evilsite.com`, which resolves to 127.0.0.1. In fact, we don't even need to buy a domain or configure the DNS, because multiple domains already exist that let us do this. The one we will be using is localtest.me, which resolves every subdomain to 127.0.0.1.

We can therefore set the hostname in the URL to "list.hohoho.localtest.me", bypass the check, and access local services: <http://10.10.14.72/?proxy=http%3A%2F%2Flist.hohoho.localtest.me>

Success! It appears that there is a web server running locally, and it has a message from Elf McSkidy that contains some sensitive information we can use!

8. Click the "Admin" link at the top or scroll down to the login. Guess the username and use the password you found to login as Santa.

9. Delete the naughty list to find the challenge flag!

Answer the questions below

What is Santa's password?

Correct Answer

What is the challenge flag?

Correct Answer

Task 22 [Day 20] Blue Teaming Powershell to the rescue

Task 23 [Day 21] Blue Teaming Time for some ELForensics

Thought Process/Methodology:

Firstly, we start our machine and attack box to start our process. Then, we should Enter your IP address to run the browser then scroll to the bottom and enter any names in the Name Box and search for it. You will get a display on whether the name is a nice or naughty list. Browse in the website "http://MACHINE_IP/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F" to get a display at the bottom saying "Not Found. The requested URL was not found on this server. Later on, Change the port number from 8080 to just 80 in the default http port and you will get a display at the bottom saying "Failed to connect to list.hohoho port 80: Connection refused". Then, we should Change the port number again from 80 to 22 in the default http port and you will get a display at the bottom saying "Recv failure: Connection reset by peer" and Replace the "list.hohoho hostname" with "localhost" or "127.0.0.1". Lastly, we should Replace the "localhost" with "list.hohoho.localtest.me" to get the password of Santa and then DELETE NAUGHTY LIST" to get the flag "THM{EVERYONE_GETS_PRESENTS}.

Day 20 - Powershell to the rescue

Tool used: google and try hackme

Solution/walkthrough:

Question 1:

Parameter -l helps to connect with the local host using “ssh -l mceager MACHINE_IP” and its password “r0ckStar!”.

```
You will use SSH to connect to the remote machine.

The command to run to connect to the remote machine: ssh -l mceager 10.10.190.155

root@lp-10-10-7-58:~# ssh -l mceager 3.248.248.133

Note that your IP address will be different. When prompted, enter the password: r0ckStar!

If you logged in successfully, you will see the following prompt.

Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

mceager@ELFSTATION1 C:\Users\mceager>

Before we begin, launch PowerShell and navigate to the Documents folder.

mceager@ELFSTATION1 C:\Users\mceager>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\mceager>
PS C:\Users\mceager> Set-Location ..\Documents\

PS C:\Users\mceager>
Note: The virtual machine may take up to 3 minutes to load.

The official explanation of PowerShell is: "PowerShell is a cross-platform task automation and configuration management framework, consisting of a command-line shell and scripting language. Unlike most shells, which accept and return text, PowerShell is built on top of the .NET Common Language Runtime (CLR), and accepts and returns .NET objects. This fundamental change brings entirely new tools and methods for automation." 

PowerShell has grown in popularity in the last few years among defenders and especially
```

```
Applications Places Sobre... Wed 13 Jul, 15:12 AttackBoxIP:10.10.194.9

c:\windows\system32\cmd.exe

File Edit View Search Terminal Help

root@lp-10-10-194-9:~# ssh -l mceager 10.10.190.155
ssh: connect to host 10.10.190.155 port 22: Connection refused
root@lp-10-10-194-9:~# ssh -l mceager 10.10.190.155
The authenticity of host '10.10.190.155 (10.10.190.155)' can't be established.
ECDSA key fingerprint is SHA256:El2k8bgMMy7A+lsJWuKj0ZAdILuMSVC7KY9lnS8moIu.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.190.155' (ECDSA) to the list of known hosts.

Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

mceager@ELFSTATION1 C:\Users\mceager>
```

Question 2:

Cat out “elfone.txt” to get what Elf 1 wants as it wants its 2 front teeth.

```
mceager@ELFSTATION1 C:\Users\mceager>

Before we begin, launch PowerShell and navigate to the Documents folder.

mceager@ELFSTATION1 C:\Users\mceager>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\mceager>
PS C:\Users\mceager> Set-Location ..\Documents\

PS C:\Users\mceager>
Note: The virtual machine may take up to 3 minutes to load.

The official explanation of PowerShell is: "PowerShell is a cross-platform task automation and configuration management framework, consisting of a command-line shell and scripting language. Unlike most shells, which accept and return text, PowerShell is built on top of the .NET Common Language Runtime (CLR), and accepts and returns .NET objects. This fundamental change brings entirely new tools and methods for automation." 

PowerShell has grown in popularity in the last few years among defenders and especially attackers. Knowing PowerShell is a necessary skill. If you have only heard of PowerShell but never dabbled with it, fret not, today you will.

Recall from the definition above that PowerShell is a command-line shell. We must enter commands into the command prompt to instruct PowerShell on what we want it to do for us. PowerShell commands are known as cmdlets.

To list the contents of the current directory we are in, we can use the Get-ChildItem cmdlet.
```

There are various other options we can use with this cmdlet to enhance its capabilities further.

- Path Specifies a path to one or more locations. Wildcards are accepted.
- File / -Directory To get a list of files, use the File parameter. To get a list of directories, use the Directory parameter. You can use the Recurse parameter with File

```
Applications Places Sobre... Wed 13 Jul, 15:24 AttackBoxIP:10.10.194.9

c:\windows\system32\cmd.exe - powershell

File Edit View Search Terminal Help

Mode LastWriteTime Length Name
---- ----- ----- -----
-a-hs- 12/7/2020 10:29 AM 402 desktop.ini
-arh-- 11/18/2020 5:05 PM 35 elfone.txt

PS C:\Users\mceager\Documents> ls

Directory: C:\Users\mceager\Documents

Mode LastWriteTime Length Name
---- ----- ----- -----
-a--- 11/23/2020 12:06 PM 22 elfone.txt

PS C:\Users\mceager\Documents> Get-Content elfone.txt
Nothing to see here...
PS C:\Users\mceager\Documents> cat elfone.txt
All I want is my '2 front teeth'!!!
PS C:\Users\mceager\Documents>
```

Question 3

Set-Location Desktop to the folder and find the hidden folder that contains the file for Elf 2. Cd the directory and “Get-ChildItem” and cat out “e70smsW10Y4k.txt” to get the movie Elf 2 wanted.

You can run numerous operations with the `Get-Content` cmdlet to give you more information about the particular file you are inspecting. Such as how many words are in the file and the exact positions for a particular string within a file.

To get the number of words contained within a file, you can use the `Get-Content` cmdlet and pipe the results to the `Measure-Object` cmdlet.

You run this command as follows: `Get-Content -Path file.txt | Measure-Object -Word`

To get the exact position of a string within the file, you can use the following command:

`(Get-Content -Path file.txt)[index]`

The index is the numerical value that is the location of the string within the file. Since indexes start at zero, you typically need to subtract one from the original value to extract the string at the correct position. This is not necessary for this exercise.

To change directories, you can use the `Set-Location` cmdlet.

For example, `Set-Location -Path c:\users\administrator\Desktop` will change your location to the Administrator's desktop.

The last cmdlet that is needed to solve this room is `Select-String`. This cmdlet will search a particular file for a pattern you define within the command to run.

An example execution of this command is:

`Select-String -Path 'c:\users\administrator\Desktop' -Pattern '*.pdf'`

Note: You can always use the `Get-Help` cmdlet to obtain more information about a specific cmdlet. For example, `Get-Help Select-String`

Answer the questions below

```
bash-c "cat /tmp/thmip.txt"
c:\windows\system32\cmd.exe - powershell
File Edit View Search Terminal Help
Mode LastWriteTime Length Name
d--h-- 12/7/2020 11:26 AM elf2wo
PS C:\Users\nceager\Desktop> cd elf2wo
PS C:\Users\nceager\Desktop\elf2wo> Get-ChildItem
Directory: C:\Users\nceager\Desktop\elf2wo

Mode LastWriteTime Length Name
-a--- 11/17/2020 10:26 AM 64 e70smsW10Y4k.txt
PS C:\Users\nceager\Desktop\elf2wo>
PS C:\Users\nceager\Desktop\elf2wo> cat e70smsW10Y4k.txt
I want the movie Scrooged <3!
PS C:\Users\nceager\Desktop\elf2wo>
```

Question 4:

Set up the windows with `cd C:/Windows` and `cd System32` to “Get-ChildItem” to find the hidden folder in the directory by filter “*3*” to get the length name “3lfthr3e” .

particular file or pattern you define within the command to run.

An example execution of this command is:

`Select-String -Path 'c:\users\administrator\Desktop' -Pattern '*.pdf'`

Note: You can always use the `Get-Help` cmdlet to obtain more information about a specific cmdlet. For example, `Get-Help Select-String`

Answer the questions below

Search for the first hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want?

2 front teeth

Correct Answer

Search on the desktop for a hidden folder that contains the file for Elf 2. Read the contents of this file. What is the name of that movie that Elf 2 wants?

Scrooged

Correct Answer

Search the Windows directory for a hidden folder that contains files for Elf 3. What is the name of the hidden folder? (This command will take a while)

3lfthr3e

Correct Answer

💡 Hint

How many words does the first file contain?

9999

Correct Answer

What 2 words are at index 551 and 6991 in the first file?

Red Ryder

Correct Answer

```
Click to switch to "Workspace 4"
c:\windows\system32\cmd.exe - powershell
File Edit View Search Terminal Help
PS C:\Windows\System32> Get-ChildItem -Hidden -Directory -Filter "*3*"
Directory: C:\Windows\System32

Mode LastWriteTime Length Name
d--h-- 11/23/2020 3:26 PM 3lfthr3e
PS C:\Windows\System32> cd 3lfthr3e
PS C:\Windows\System32\3lfthr3e> ls
PS C:\Windows\System32\3lfthr3e> dir
PS C:\Windows\System32\3lfthr3e>
```

Question 5:

Get content for 1.txt by “Measure object” to get the number of words contained in the first file which is 9999 words count.

Scrooged

Correct Answer

Search the Windows directory for a hidden folder that contains files for Elf 3. What is the name of the hidden folder? (This command will take a while)

3lfthr3e

Correct Answer Hint

How many words does the first file contain?

9999

Correct Answer

What 2 words are at index 551 and 6991 in the first file?

Red Ryder

Correct Answer

This is only half the answer. Search in the 2nd file for the phrase from the previous question to get the full answer. What does Elf 3 want? (use spaces when submitting the answer)

Red Ryder BB Gun

Correct Answer Hint

```
c:\windows\system32\cmd.exe -powershell
File Edit View Search Terminal Help
PS C:\Windows\System32\3lfthr3e> Get-Content 1.txt | Measure-Object
Count : 9999
Average :
Sum :
Maximum :
Minimum :
Property :

PS C:\Windows\System32\3lfthr3e> Get-Content 1.txt | Measure-Object -Word
Lines Words Characters Property
----- -----
9999

PS C:\Windows\System32\3lfthr3e>
```

THM AttackBox 01m 35s

Task 23 [Day 21] Blue Teaming Time for some ELForensics

Task 24 [Day 22] Blue Teaming Elf McEager becomes CyberElf

Task 25 [Day 23] Blue Teaming The Grinch strikes again!

Task 26 [Day 24] Final Challenge The Trial Before Christmas

Question 6:

Wrap the command “Get-Content 1.txt” with brackets/parentheses and wrap the number 551,6991 with square brackets to get the 2 words which is red ryder.

Scrooged

Correct Answer

Search the Windows directory for a hidden folder that contains files for Elf 3. What is the name of the hidden folder? (This command will take a while)

3lfthr3e

Correct Answer Hint

How many words does the first file contain?

9999

Correct Answer

What 2 words are at index 551 and 6991 in the first file?

Red Ryder

Correct Answer

This is only half the answer. Search in the 2nd file for the phrase from the previous question to get the full answer. What does Elf 3 want? (use spaces when submitting the answer)

Red Ryder BB Gun

Correct Answer Hint

```
c:\windows\system32\cmd.exe -powershell
File Edit View Search Terminal Help
PS C:\Windows\System32\3lfthr3e> (Get-Content 1.txt)(551)
Red
PS C:\Windows\System32\3lfthr3e> (Get-Content 1.txt)(551 6991)
Red
Ryder
PS C:\Windows\System32\3lfthr3e>
```

THM AttackBox 00m 25s

Task 23 [Day 21] Blue Teaming Time for some ELForensics

Task 24 [Day 22] Blue Teaming Elf McEager becomes CyberElf

Task 25 [Day 23] Blue Teaming The Grinch strikes again!

Task 26 [Day 24] Final Challenge The Trial Before Christmas

Question 7:

Use the command “Get-Content 2.txt” with “Select-String” command on “redryder” with a specific pattern to get the full answer “redryderbbgun”.

```
mceager@ELFSTATION1 ~ % [User:mceager]
Before we begin, launch PowerShell and navigate to the Documents folder.

mceager@ELFSTATION1 ~ % powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\mceager> Set-Location .\Documents
PS C:\Users\mceager\Documents>
Note: The virtual machine may take up to 3 minutes to load.
```

The official explanation of PowerShell is: "PowerShell is a cross-platform task automation and configuration management framework, consisting of a command-line shell and scripting language. Unlike most shells, which accept and return text, PowerShell is built on top of the .NET Common Language Runtime (CLR), and accepts and returns .NET objects. This fundamental change brings entirely new tools and methods for automation."

PowerShell has grown in popularity in the last few years among defenders and especially attackers. Knowing PowerShell is a necessary skill. If you have only heard of PowerShell but never dabbled with it, fret not, today you will.

Recall from the definition above that PowerShell is a command-line shell. We must enter commands into the command prompt to instruct PowerShell on what we want it to do for us. PowerShell commands are known as cmdlets.

To list the contents of the current directory we are in, we can use the `Get-ChildItem` cmdlet. There are various other options we can use with this cmdlet to enhance its capabilities further.

- `-Path` Specifies a path to one or more locations. Wildcards are accepted.
- `/ -Directory` To get a list of files, use the File parameter. To get a list of

```
c:\windows\system32\cmd.exe - powershell
File Edit View Search Terminal Help
PS C:\Windows\System32\3lfthr3e> (get-Content 1.txt)[551 6991]
Red
Ryder
PS C:\Windows\System32\3lfthr3e> Get-Content 2.txt | Select-String -Pattern "red
ryder"
redryderbbgun

PS C:\Windows\System32\3lfthr3e>
```

Thought Process/Methodology:

Firstly, we start our machine and attack box to start our process. We then opened our terminal and key in “ssh -l mceager MACHINE_IP” and password “r0ckStar!” to connect to the host. We then set up Powershell and set-location for our documents. After that, we Get-ChildItem for the hidden file and got the file in the documents. We then ls the Hidden file to get another user name and we cat out “elfone.txt” to get what Elf 1 wants which was its 2 front teeth. Secondly, we set the location for the desktop and ls the hidden folder and cat out “e70smsW10Y4k.txt” to get Scrooged as the name of the movie that Elf 2 wants. We set cd for Windows and System32 and get the hidden folder through directory by filter with “*3*” to get the length name “3lfthr3e”. We then used the command “Get content for 1.txt” by “Measure object” to get the number of words contained in the first file which is 9999 words count. We wrapped the command “Get-Content 1.txt” with brackets/parentheses and wrap the number [551,6991] with square brackets to get the 2 words which is red ryder. Last but not least, we finally used the command “Get-Content 2.txt” with “Select-String” command on “redryder” with a specific pattern to get the full answer “redryderbbgun”.