D4RK PR0GR4MS

Technology, Hacks.

Written By Rahul Dixit

December 11, 2022

TRYHACKME- ADVENTOFCYBER4 WRITEUP

Dear readers,

Today's write-up is on AdventOfCyber4, TryHackMe. It was launched on 01 December 2022. AdventOfCyber4 is a 24-day beginner-friendly security challenge every day leading up to Christmas. This Write-up covers Day1, Day2, Day3 and will be updated as days go on. So, let's start hacking.

D4RK PR0GR4MS

Fig. 1 Day1, Day2, Day3 of The Challenge.

[Day 1] Frameworks

Files Provided

No files were provided.

Tools Needed

No Tools Are Required

To solve the Day 1 problems, you must go through the paragraphs written about the Security Framework, NIST Security Framework, ISO 27000 Series, MITRE ATT&CK Framework these give you an idea that how securities are implemented in organizations, and Cyber Kill Chain, Unified Kill Chain these frameworks describe the structure of an attack.

D4RK PR0GR4MS

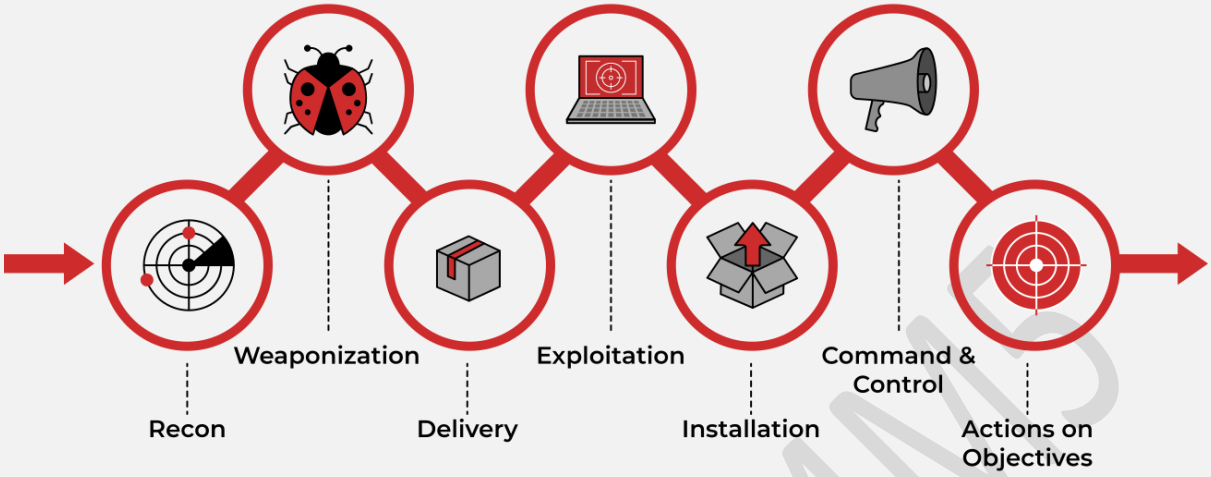


Fig. 2 Cyber Kill Chain

Now to solve the challenge you must visit the website that is on the top right.

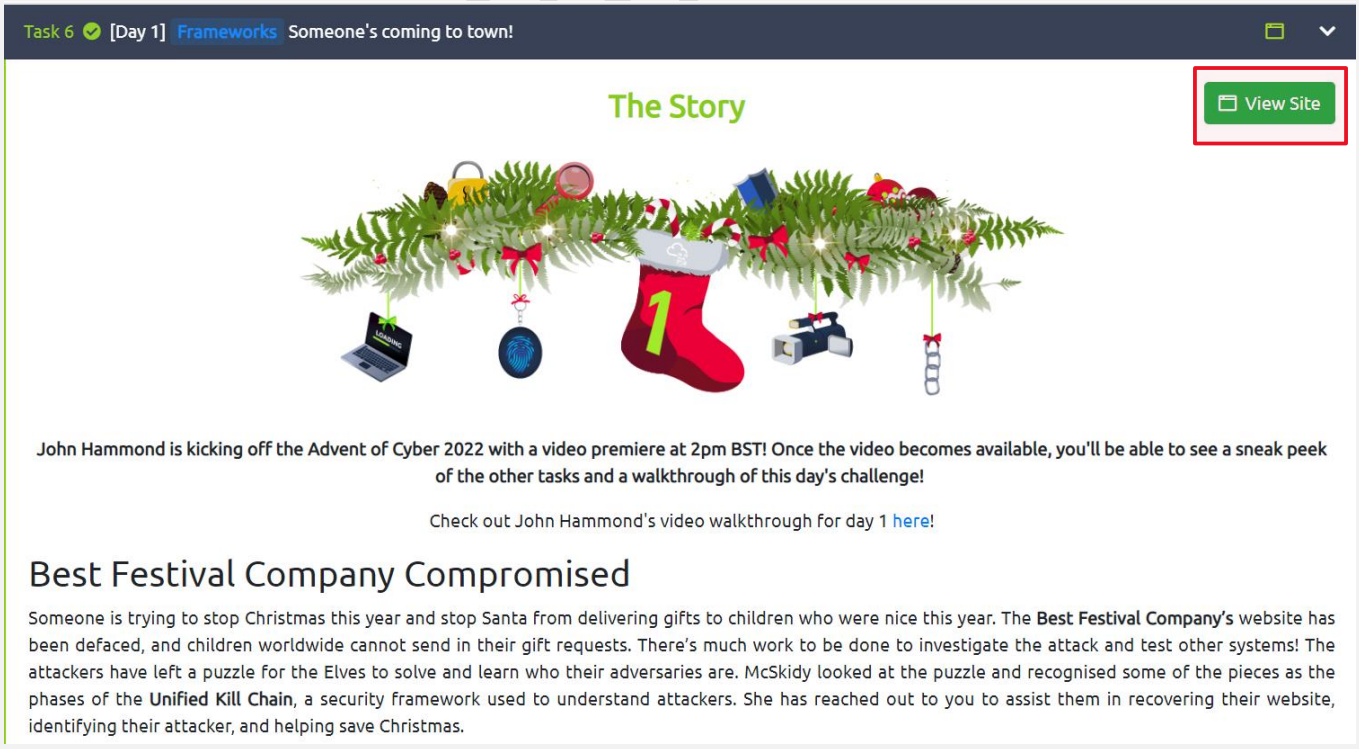
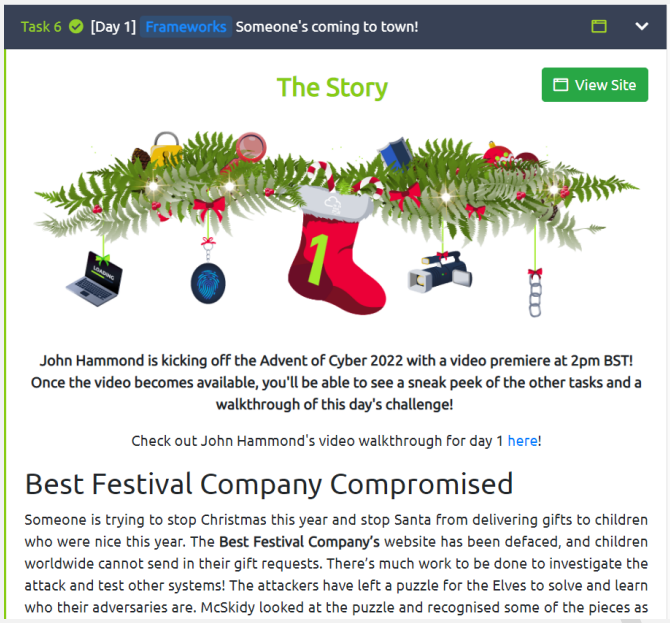
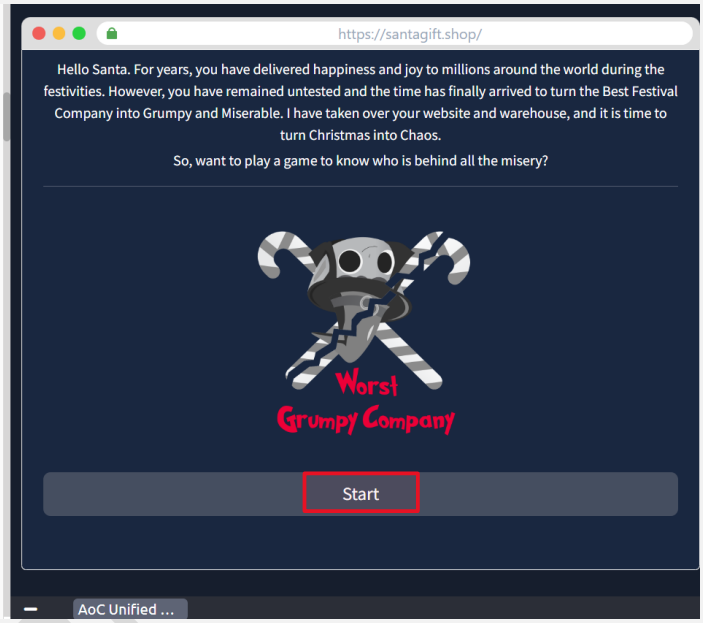


Fig3. Visiting The Site

D4RK PR0GR4MS

After you click on the view website your screen will split into two halves and you will see a screen as shown below in the figure:





Now click on start to start the challenge. As you click on start a screen appears which asks you to solve 1/3 puzzles to proceed further.

D4RK PR0GR4MS

Puzzle 1: -

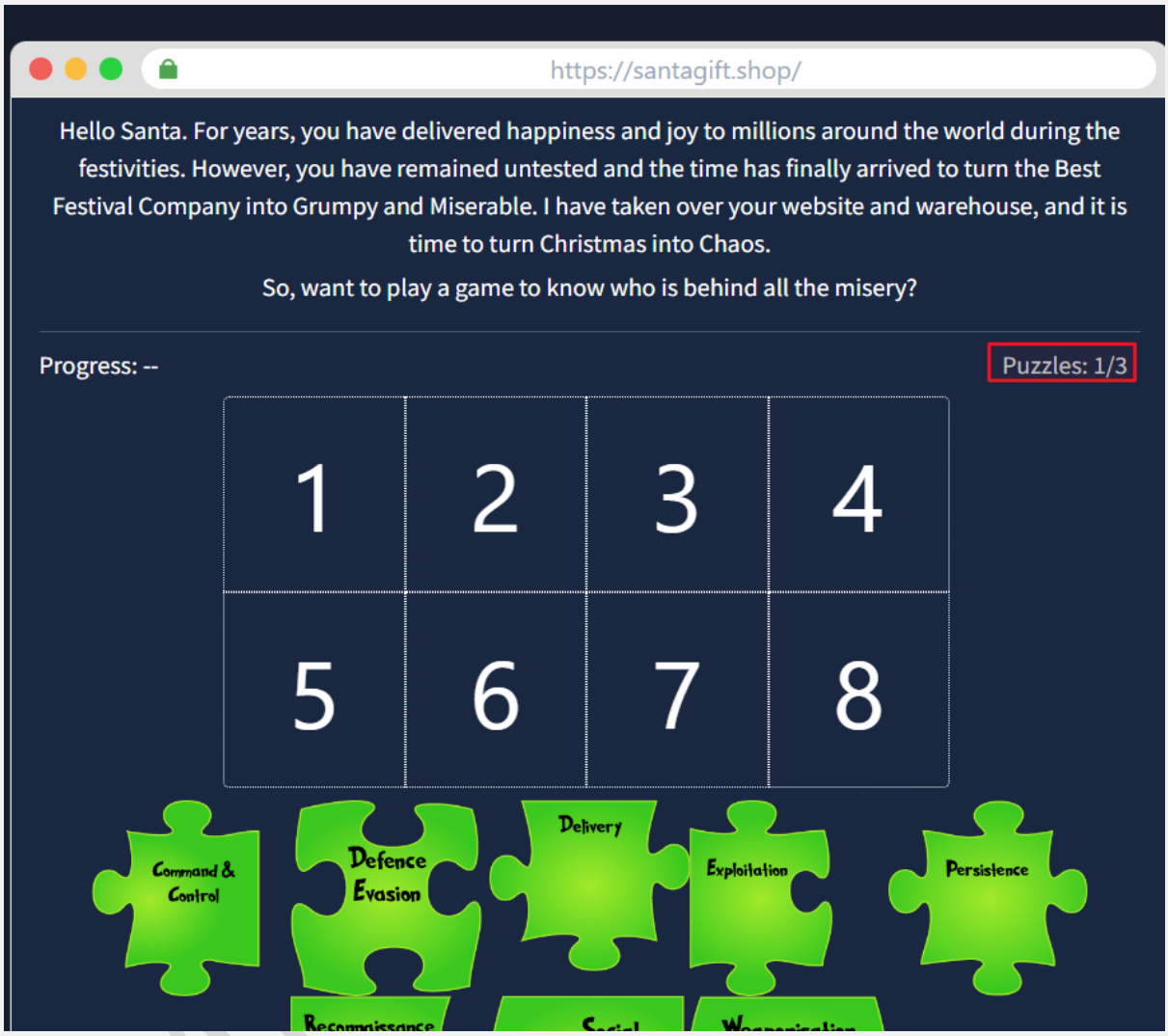


Fig3. Puzzle 1 out of 3

D4RK PR0GR4MS

Solution: -

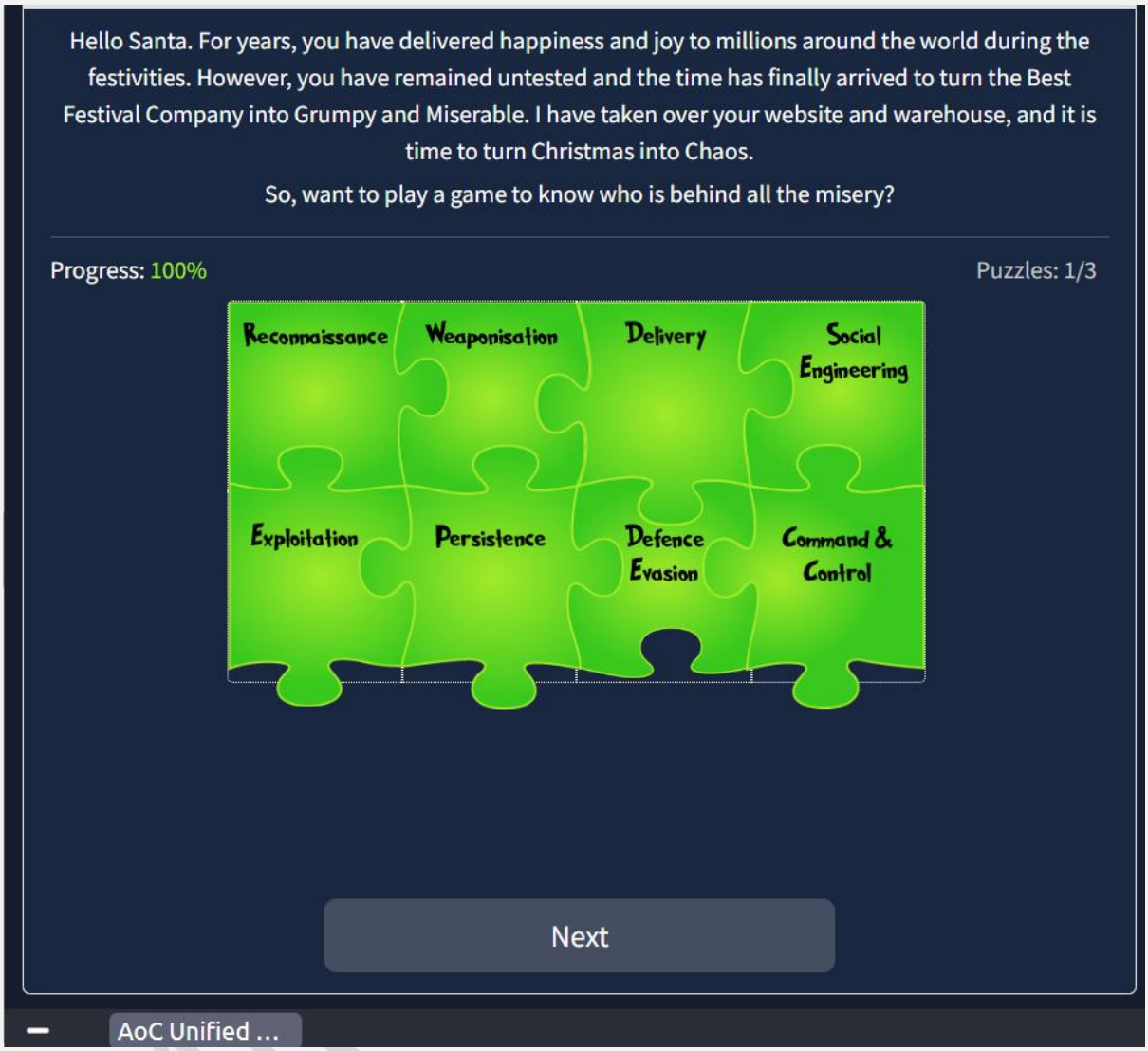


Fig4. Solved Puzzle 1 out of 3

This puzzle highlights the critical steps of gaining access to a system or network.

Unified Kill Chain

Cycle 1: In

- Reconnaissance
- Weaponisation
- Delivery
- Social Engineering
- Exploitation
- Persistence
- Defence Evasion
- Command & Control

D4RK PR0GR4MS

For Puzzle 2/3 click next

Puzzle 2: -

Fig5. Puzzle 2 out of 3

D4RK PR0GR4MS

Solution: -

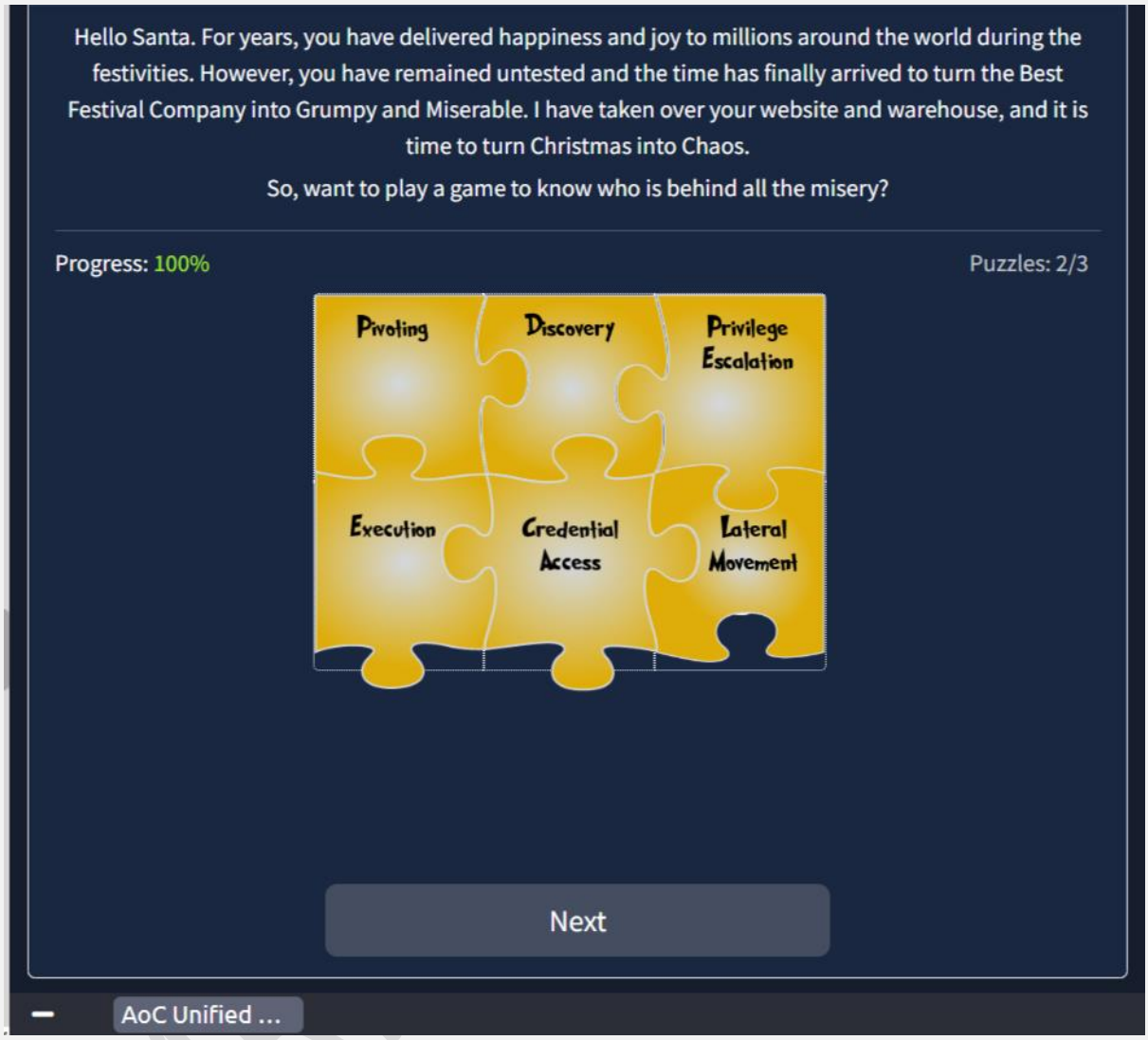


Fig. 6 Solved Puzzle 2 out of 3

This puzzle highlights how an attacker accesses your system/network and tries to bypass restrictions imposed to access data by a particular user.

Unified Kill Chain

Cycle 2: Through

- Pivoting
- Discovery
- Privilege Escalation
- Execution
- Credential Access
- Lateral Movement

D4RK PR0GR4MS

For Puzzle 3/3 click next

Puzzle 3: -

Fig. 7 Puzzle 3 out of 3

D4RK PR0GR4MS

Solution: -

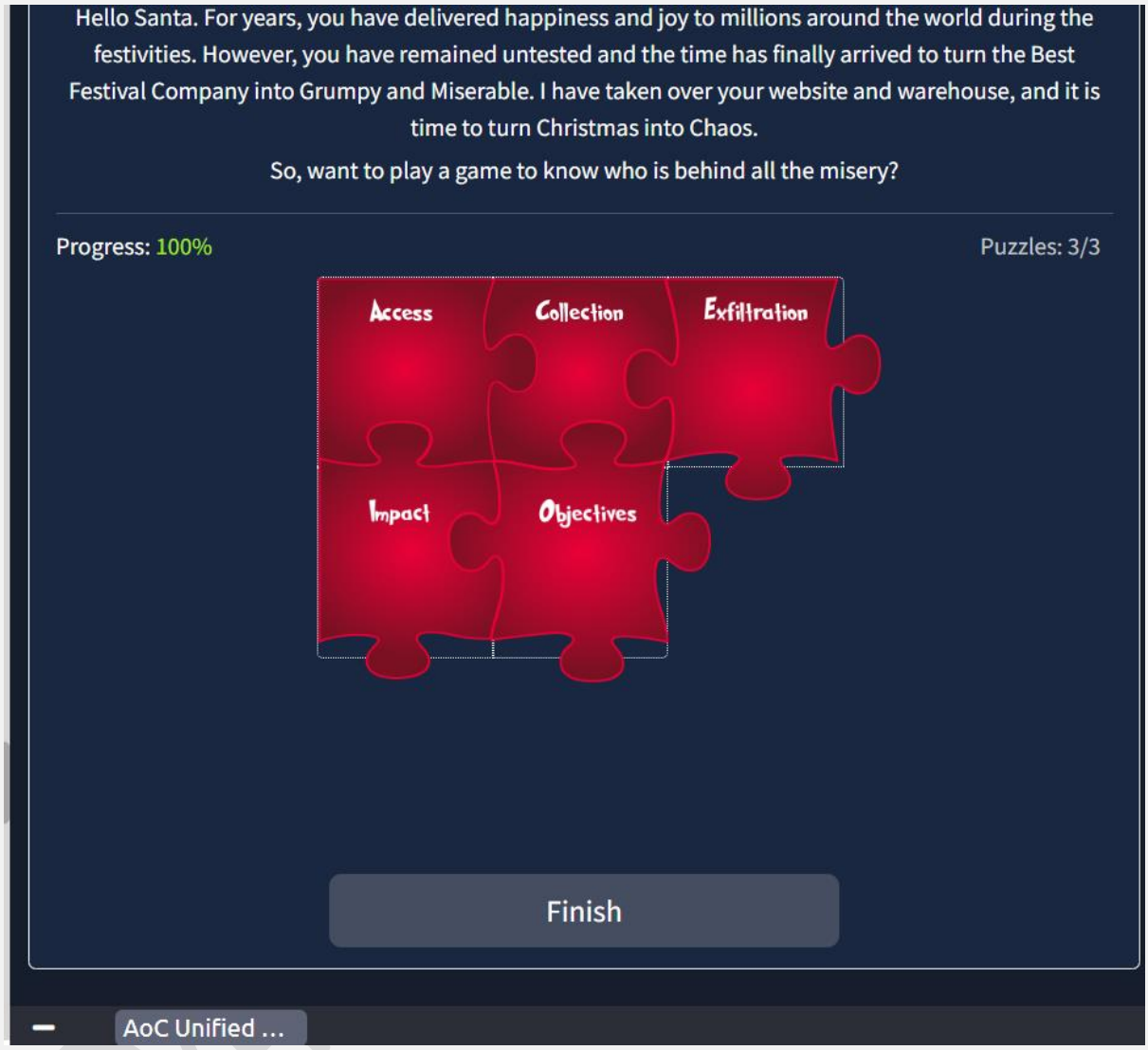


Fig. 8 Solved Puzzle 3 out of 3

This puzzle conveys how attackers executes its attack and gathers the information for which he executed the attack and cause as much as damage possible and leaves without being tracked.

Unified Kill Chain

Cycle 3: Out

- Collection
- Exfiltration
- Impact
- Objectives

D4RK PR0GR4MS

After finishing the puzzles, you will come across a screen which gives you the flag as well as the answer to the questions asked in the tasks

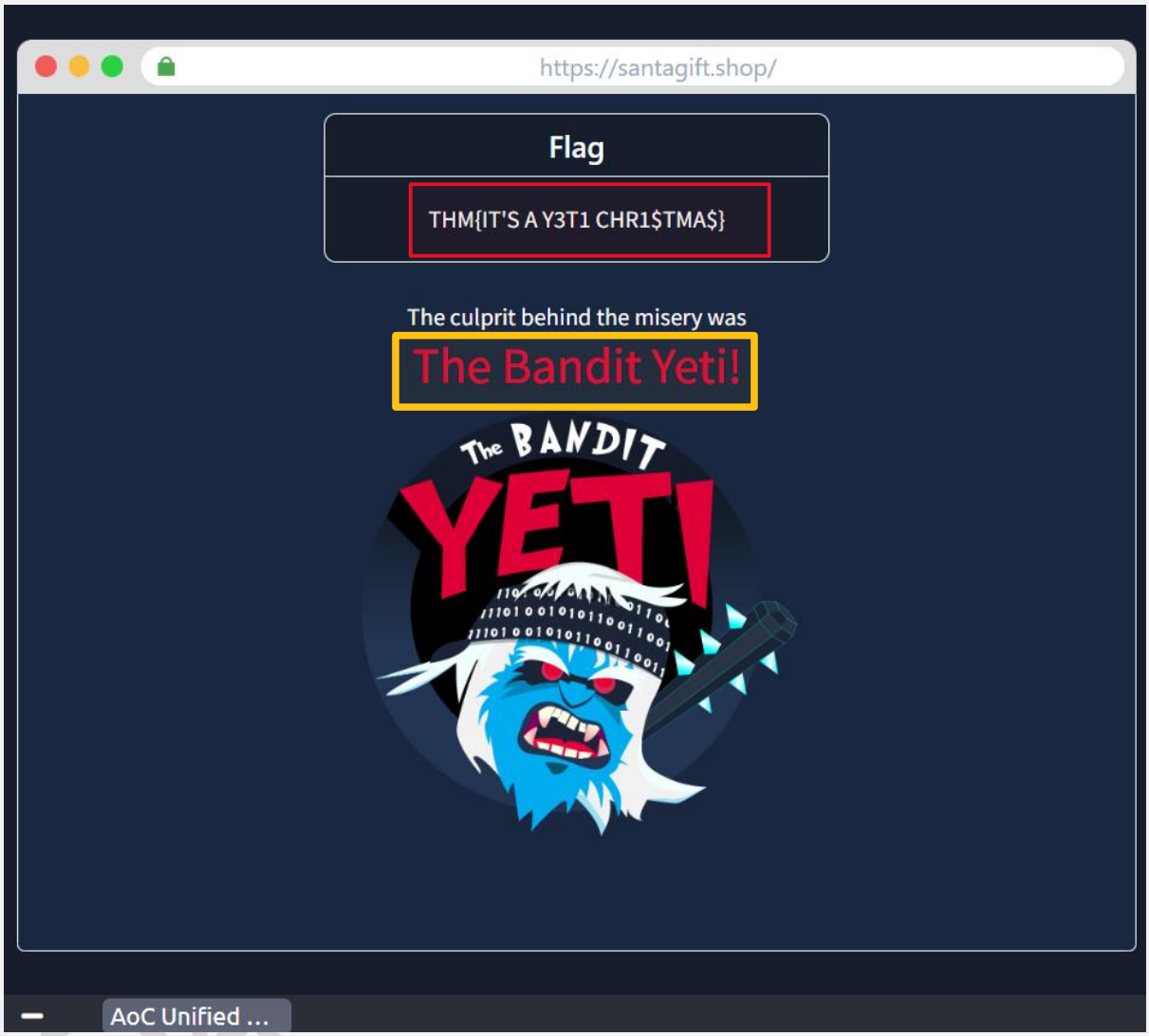


Fig. 9 The Flag

D4RK PR0GR4MS

Now let's solve the questions that are asked: -

Question 1: -

Who is the adversary that attacked Santa's network this year?

Answer: - The Bandit Yeti

[Hint: - The webpage that appears after solving the puzzle states the name of culprit]

Question 2: -

What is the root flag that they left behind?

Answer: - THM{IT'S A Y3T1 CHR1TMA}

[Hint: - The webpage that appears after solving the puzzle contains the Flag]

D4RK PR0GR4MS

[Day 2] Log Analysis

Files Provided

No files were provided.

Tools Needed

grep

grep is a command-line utility for searching plain-text data sets for lines that match a regular expression.

To solve Day 2, you must have knowledge about the log files.

Log Files: - Log files are files that contain historical records of events and other data from an application.

Some common examples of events that you may find in a log file:

- *Login attempts or failures*
- *Traffic on a network*
- *Things (website URLs, files, etc.) that have been accessed*
- *Password changes*
- *Application errors (used in debugging)*

D4RK PR0GR4MS

Now let's solve the challenge,

Fig. 1 Start the challenge

As soon as you start the machine your screen will split in two halves, and you will have a Linux terminal in half of your screen via which you are going to solve this challenge.

Let's Hack…

D4RK PR0GR4MS

```
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-1029-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun Dec 11 05:39:04 UTC 2022

  System load:  0.0               Processes:             112
  Usage of /:   5.8% of 29.02GB   Users logged in:       1
  Memory usage: 22%               IPv4 address for ens5: 10.10.115.194
  Swap usage:   0%


1 update can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Sun Dec 11 05:26:21 2022 from 10.100.1.242
elfmcblue@day-2-log-analysis:~$ ls
SSHD.log  webserver.log
elfmcblue@day-2-log-analysis:~$
```

Fig. 2 Analysing the log files

In your terminal go and type ls [command for listing the files in the current working directory] as you type ls in the command line you will see two files that appear on your screen

1. SSHD.log

2. webserver.log

Now let's analyse these log files for the answers and flag:

For reading these log files we can type the following command: -

elfmcblue@day-2-log-analysis: ~$ cat webserver.log

elfmcblue@day-2-log-analysis: ~$ cat SSHD.log

D4RK PR0GR4MS

These commands will show you the data inside the log files, but we will use grep to search pattern inside these log files as they contain a huge amount of data.

```
remote-eu-10.tryhackme.tech/#/client/MTQ1MTg4MQBjAG15c3Fs?token=F69FCA7224ED71C002FCC6AE1F838C7B4A398CC80CF14C6B7A7AA8A2599EAE32
10.10.249.191 - - [18/Nov/2022:12:35:27 +0000] "GET /secexgateeval HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:27 +0000] "GET /s_main HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:27 +0000] "GET /enscreen HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:27 +0000] "GET /how_secexmail_gate_works HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:05 +0000] "GET / HTTP/1.1" 200 2980 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:05 +0000] "GET /2030ccdd-81d0-432c-ba2d-2bbbeca1caa9 HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET / HTTP/1.1" 200 2980 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /aefea665-d63b-4bf8-9b7f-aad84dca9ee7 HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /cgi-script HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /.htpasswd HTTP/1.1" 403 440 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /dummy HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /.htaccess HTTP/1.1" 403 440 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /cgi HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /access_log HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /.meta HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /error_log HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /.web HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /cgi-bin HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /htdocs HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /httpd HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /error HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /cgi-pub HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /httpd.pid HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /icons HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /manual HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /phf HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /index.html HTTP/1.1" 200 2980 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /test-cgi HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /tmp HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /logs HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /printenv HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /~bin HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /server-info HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /~ftp HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /server-status HTTP/1.1" 403 440 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /~root HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /status HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /~nobody HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:38:10 +0000] "GET /php.ini HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
elfmcblue@day-2-log-analysis:~$
```

Fig. 3 Data inside webserver.log

After analysing the webserver.log you will come to know that the attack was initiated on 18/Nov/2022 Friday and attackers IP Address is 10.10.249.19 as the request codes are 404 means that the attacker was unable to access the file from the webserver.

D4RK PR0GR4MS

```
Dec 10 11:04:30 LabSZ sshd[25521]: pam_unix(sshd:auth): check pass; user unknown
Dec 10 11:04:30 LabSZ sshd[25521]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=103.99.0.122
Dec 10 11:04:32 LabSZ sshd[25523]: Failed password for root from 183.62.140.253 port 34100 ssh2
Dec 10 11:04:32 LabSZ sshd[25523]: Received disconnect from 183.62.140.253: 11: Bye Bye [preauth]
Dec 10 11:04:32 LabSZ sshd[25521]: Failed password for invalid user cisco from 103.99.0.122 port 50890 ssh2
Dec 10 11:04:32 LabSZ sshd[25525]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=183.62.140.253  user=root
Dec 10 11:04:33 LabSZ sshd[25521]: error: Received disconnect from 103.99.0.122: 14: No more user authentication methods available. [preauth]
Dec 10 11:04:34 LabSZ sshd[25527]: Invalid user test from 103.99.0.122
Dec 10 11:04:34 LabSZ sshd[25527]: input_userauth_request: invalid user test [preauth]
Dec 10 11:04:34 LabSZ sshd[25527]: pam_unix(sshd:auth): check pass; user unknown
Dec 10 11:04:34 LabSZ sshd[25527]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=103.99.0.122
Dec 10 11:04:35 LabSZ sshd[25525]: Failed password for root from 183.62.140.253 port 34642 ssh2
Dec 10 11:04:35 LabSZ sshd[25525]: Received disconnect from 183.62.140.253: 11: Bye Bye [preauth]
Dec 10 11:04:35 LabSZ sshd[25530]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=183.62.140.253  user=root
Dec 10 11:04:36 LabSZ sshd[25527]: Failed password for invalid user test from 103.99.0.122 port 51592 ssh2
Dec 10 11:04:37 LabSZ sshd[25527]: error: Received disconnect from 103.99.0.122: 14: No more user authentication methods available. [preauth]
Dec 10 11:04:37 LabSZ sshd[25530]: Failed password for root from 183.62.140.253 port 35101 ssh2
Dec 10 11:04:37 LabSZ sshd[25530]: Received disconnect from 183.62.140.253: 11: Bye Bye [preauth]
Dec 10 11:04:37 LabSZ sshd[25532]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=183.62.140.253  user=root
Dec 10 11:04:38 LabSZ sshd[25534]: Invalid user guest from 103.99.0.122
Dec 10 11:04:38 LabSZ sshd[25534]: input_userauth_request: invalid user guest [preauth]
Dec 10 11:04:38 LabSZ sshd[25534]: pam_unix(sshd:auth): check pass; user unknown
Dec 10 11:04:38 LabSZ sshd[25534]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=103.99.0.122
Dec 10 11:04:40 LabSZ sshd[25532]: Failed password for root from 183.62.140.253 port 35545 ssh2
Dec 10 11:04:40 LabSZ sshd[25532]: Received disconnect from 183.62.140.253: 11: Bye Bye [preauth]
Dec 10 11:04:40 LabSZ sshd[25534]: Failed password for invalid user guest from 103.99.0.122 port 52172 ssh2
Dec 10 11:04:40 LabSZ sshd[25537]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=183.62.140.253  user=root
Dec 10 11:04:41 LabSZ sshd[25534]: error: Received disconnect from 103.99.0.122: 14: No more user authentication methods available. [preauth]
Dec 10 11:04:41 LabSZ sshd[25537]: Failed password for root from 183.62.140.253 port 36027 ssh2
Dec 10 11:04:41 LabSZ sshd[25537]: Received disconnect from 183.62.140.253: 11: Bye Bye [preauth]
Dec 10 11:04:41 LabSZ sshd[25541]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=183.62.140.253  user=root
Dec 10 11:04:42 LabSZ sshd[25539]: Invalid user user from 103.99.0.122
Dec 10 11:04:42 LabSZ sshd[25539]: input_userauth_request: invalid user user [preauth]
Dec 10 11:04:42 LabSZ sshd[25539]: pam_unix(sshd:auth): check pass; user unknown
Dec 10 11:04:42 LabSZ sshd[25539]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=103.99.0.122
Dec 10 11:04:43 LabSZ sshd[25541]: Failed password for root from 183.62.140.253 port 36300 ssh2
Dec 10 11:04:43 LabSZ sshd[25541]: Received disconnect from 183.62.140.253: 11: Bye Bye [preauth]
Dec 10 11:04:43 LabSZ sshd[25544]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=183.62.140.253  user=root
Dec 10 11:04:45 LabSZ sshd[25539]: Failed password for invalid user user from 103.99.0.122 port 52683 ssh2
elfmcblue@day-2-log-analysis:~$
```

Fig. 4 Data inside SSHD.log

After analysing SSHD.log you notice one thing this log file deals with the login information or authentication.

Now as we analysed both the log files, we are going to answer the questions asked and find the root flag for the completion of the challenge.

D4RK PR0GR4MS

Let's Begin…

Question 1: -

Use the ls command to list the files present in the current directory. How many log files are present?

Answer: - 2

Question 2: -

Elf McSkidy managed to capture the logs generated by the web server. What is the name of this log file?

Answer: - webserver.log

[Hint: - This log files contains all the history of the events that happened on the webserver.]

Question 3: -

On what day was Santa's naughty and nice list stolen?

Answer: - Friday

[Hint: - The webserver.log contains the date on which the attack was initiated on the webserver.]

D4RK PR0GR4MS

Question 4: -

What is the IP address of the attacker?

Answer: - 10.10.249.191

[Hint: - webserver.log shows the IP Address of the attacker who tried to access the files on the webserver.]

Question 5: -

What is the name of the important list that the attacker stole from Santa?

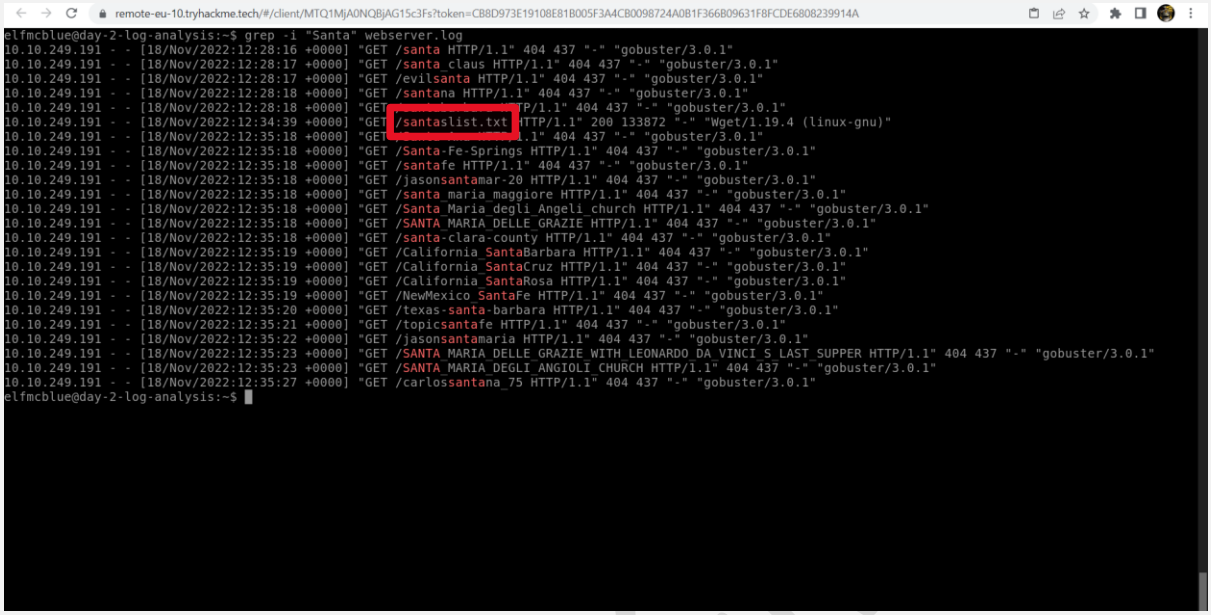
Answer: - For this we must investigate the webserver.log file that which file has got 200 request OK in response to the attacker's request. For this we will use grep.

Command: -

elfmcblue@day-2-log-analysis: ~$ grep -i "Santa" webserver.log

This command will look after all the words containing pattern Santa and return the output on the console. As mentioned in the question that it was a list so it must be in the format of txt and we got a file named "santalist.txt"

D4RK PR0GR4MS



```
remote-eu-10.tryhackme.tech/#/client/MTQ1MjA0NQBjAG15c3Fs?token=CB8D973E19108E81B005F3A4CB0098724A0B1F366B09631F8FCDE6808239914A
elfmcblue@day-2-log-analysis:~$ grep -i "Santa" webserver.log
10.10.249.191 - - [18/Nov/2022:12:28:16 +0000] "GET /santa HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:28:17 +0000] "GET /santa_claus HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:28:17 +0000] "GET /evilsanta HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:28:18 +0000] "GET /santana HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:28:18 +0000] "GET [redacted]TP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:34:39 +0000] "GET /santaslist.txt HTTP/1.1" 200 133872 "-" "Wget/1.19.4 (linux-gnu)"
10.10.249.191 - - [18/Nov/2022:12:35:18 +0000] "GET [redacted].1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:18 +0000] "GET /Santa-Fe-Springs HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:18 +0000] "GET /santafe HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:18 +0000] "GET /jasonsantamar-20 HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:18 +0000] "GET /santa_maria_maggiore HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:18 +0000] "GET /Santa_Maria_degli_Angeli_church HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:18 +0000] "GET /SANTA_MARIA_DELLE_GRAZIE HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:18 +0000] "GET /santa-clara-county HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:19 +0000] "GET /California_SantaBarbara HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:19 +0000] "GET /California_SantaCruz HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:19 +0000] "GET /California_SantaRosa HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:19 +0000] "GET /NewMexico_SantaFe HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:20 +0000] "GET /texas-santa-barbara HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:21 +0000] "GET /topicsantafe HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:22 +0000] "GET /jasonsantamaria HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:23 +0000] "GET /SANTA_MARIA_DELLE_GRAZIE_WITH_LEONARDO_DA_VINCI_S_LAST_SUPPER HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:23 +0000] "GET /SANTA_MARIA_DEGLI_ANGIOLI_CHURCH HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:27 +0000] "GET /carlossantana_75 HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
elfmcblue@day-2-log-analysis:~$
```

Fig. 5 Data after filtration of webserver.log

D4RK PR0GR4MS

Question 6: -

Look through the log files for the flag. The format of the flag is: THM{}

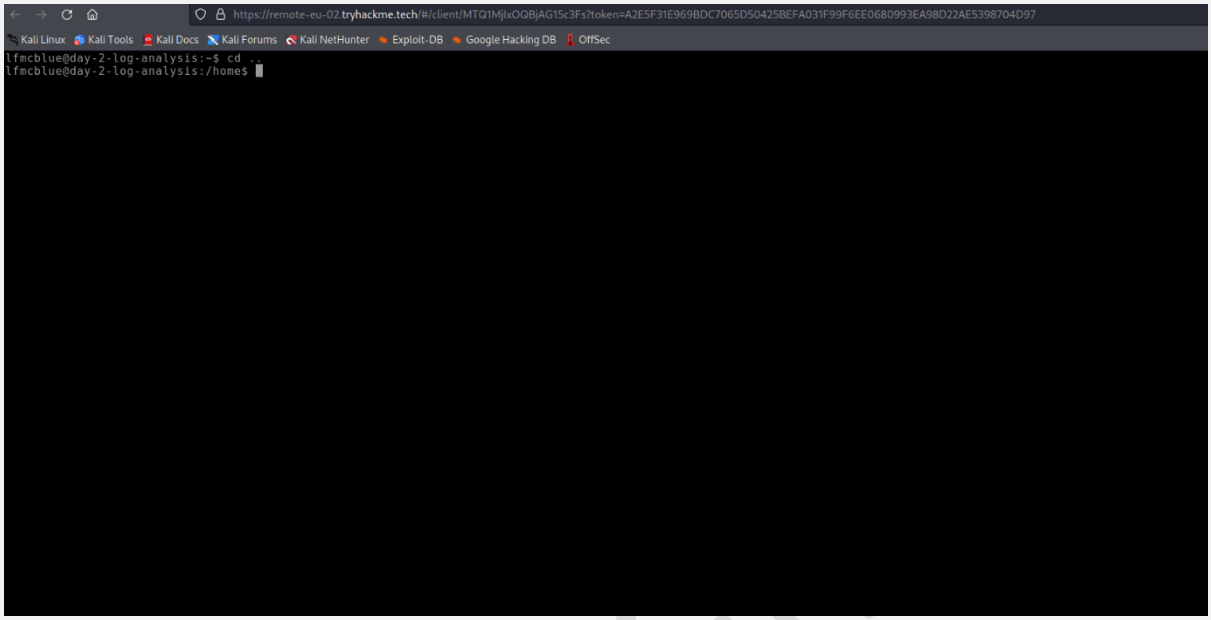
Answer: - As the question states the format of the log file for finding the flag, we will use recursive searching method of grep. But for that you must come back one directory because the current directory in which we are working is /home/elfmcblue and the recursive search works on a file of a directory hence we have to type the following commands to achieve our goal

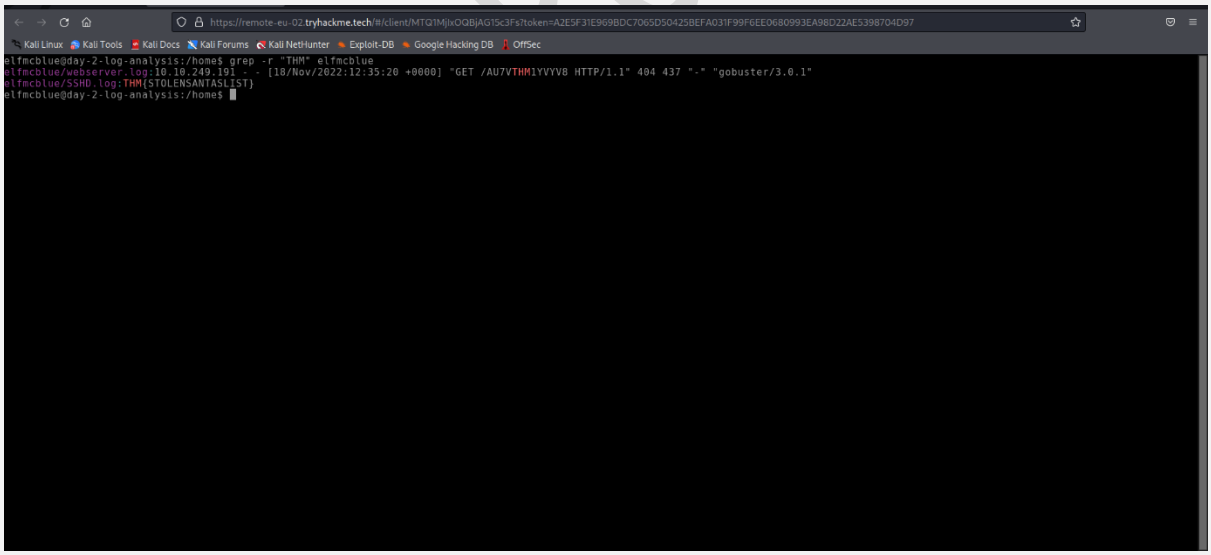
Commands: -

elfmcblue@day-2-log-analysis: ~$ cd ..

elfmcblue@day-2-log-analysis: ~$ grep -r "THM" elfmcblue

D4RK PR0GR4MS





Root Flag: - THM{STOLENSANTALIST}