Lab 1: Performing Reconnaissance from the WAN

Objective:

1. Performing reconnaissance
2. Banner Grabbing.
3. Advance Scanning with Nmap.
4. Analysis and Exploitation

Takeaways:

1. **Netcat (nc)** and **TELNET** can be used to perform a banner grab.

   - Netcat (or nc) is a command-line utility that reads and writes data across network connections, using the TCP or UDP protocols.

   - **TELNET** is a network protocol that allows you to remotely log on to and control another device or system.

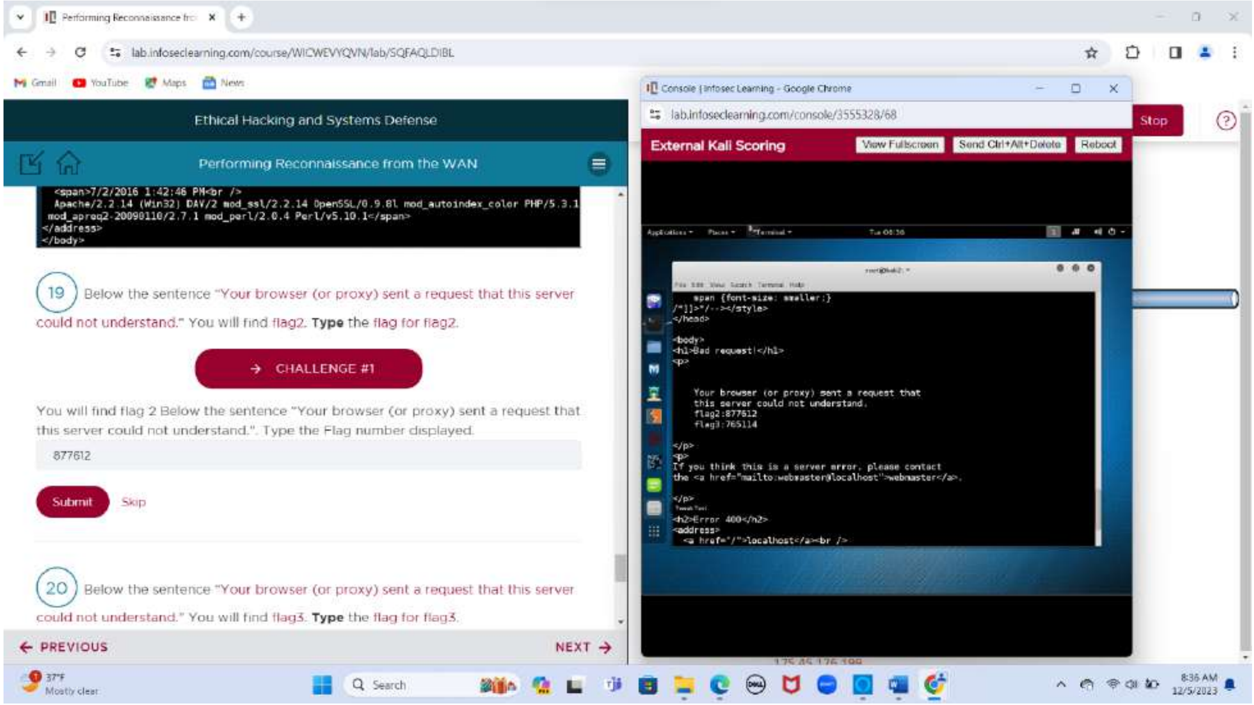
2. **Metasploit** is a widely used open-source penetration testing framework designed to help security professionals and ethical hackers perform penetration testing, security assessments, and exploit development. It provides a comprehensive suite of tools that assist in the identification of vulnerabilities, as well as the development and execution of exploit code against remote systems.

3. **Nmap** (Network Mapper) is a powerful open-source network scanning tool used for discovering hosts and services on a computer network, thus creating a "map" of the network. Within Nmap, there are various scan options available, including service and script scan options (‘-sV’, ‘-sC’), which allow for more detailed information gathering and analysis.

4. Leafpad is a lightweight and simple text editor primarily designed for Linux-based operating systems. It is known for its minimalistic interface and ease of use, catering to users who prefer a straightforward and uncluttered text editing experience.

5. John the Ripper (often abbreviated as "John") supports multiple password hash types and can be used to crack passwords stored in different formats, including hashes from operating systems like Windows, Unix, macOS, and various applications.

Challenges:


Performing Reconnaissance fro
lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
CHALLENGE #1
Submit
Skip
PREVIOUS
NEXT
37°F
Mostly clear
Search
8:36 AM
12/5/2023

```
  <span>7/2/2016 1:42:46 PM<br />
  Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1
 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1</span>
</address>
</body>
```

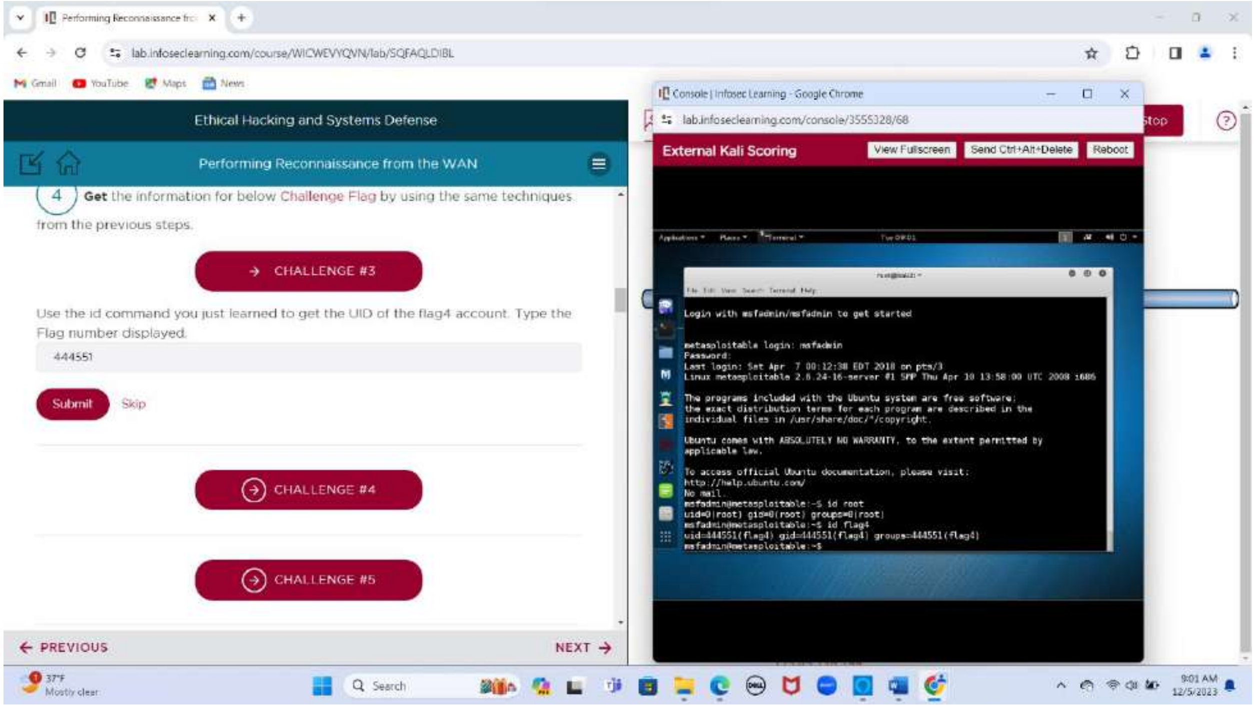
19 Below the sentence "Your browser (or proxy) sent a request that this server could not understand." You will find flag2. **Type** the flag for flag2.

You will find flag 2 Below the sentence "Your browser (or proxy) sent a request that this server could not understand.". Type the Flag number displayed.

877612

20 Below the sentence "Your browser (or proxy) sent a request that this server could not understand." You will find flag3. **Type** the flag for flag3.

```
    span {font-size: smaller;}
/*]]>*/--></style>
</head>

<body>
<h1>Bad request!</h1>
<p>


    Your browser (or proxy) sent a request that
    this server could not understand.
    flag2:877612
    flag3:765114

</p>
<p>
If you think this is a server error, please contact
the <a href="mailto:webmaster@localhost">webmaster</a>.

</p>

<h2>Error 400</h2>
<address>
  <a href="/">localhost</a><br />
```


Performing Reconnaissance fro
lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
PREVIOUS
NEXT
37°F
Mostly clear
9:01 AM
12/5/2023

4 **Get** the information for below Challenge Flag by using the same techniques from the previous steps.

→ CHALLENGE #3

Use the id command you just learned to get the UID of the flag4 account. Type the Flag number displayed.

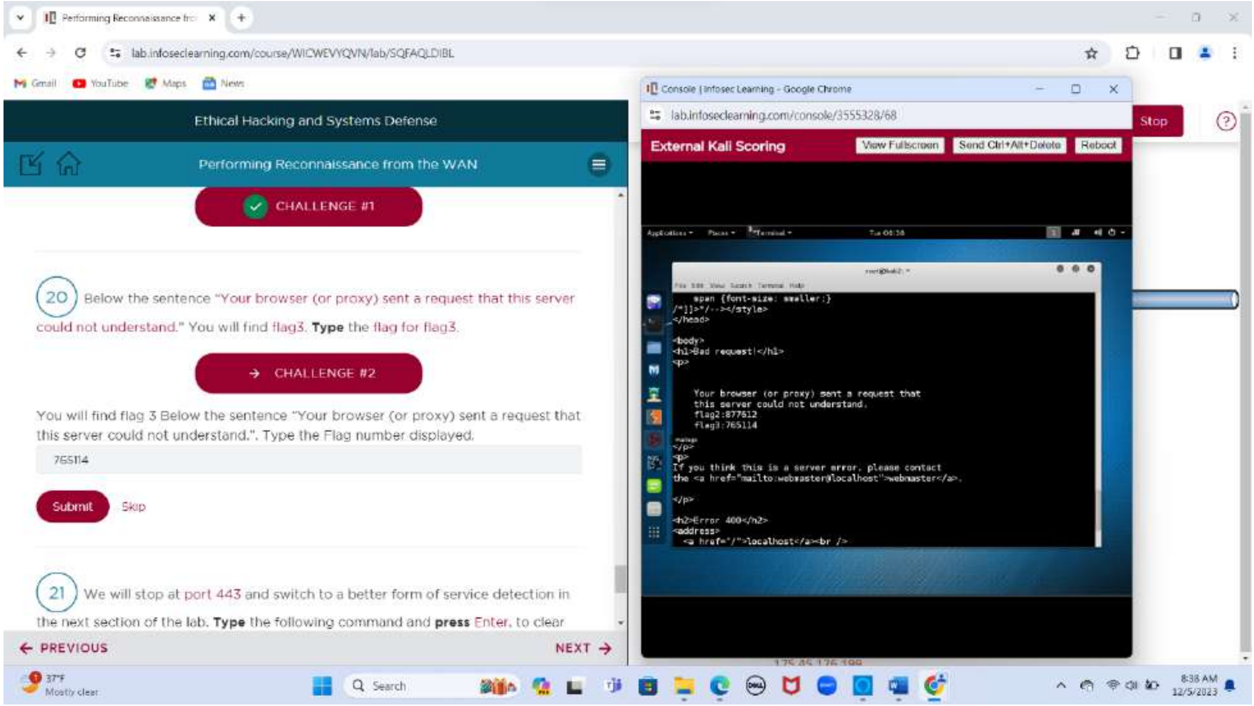
444551

Submit Skip

CHALLENGE #4

CHALLENGE #5

```
Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Sat Apr  7 00:12:38 EDT 2018 on pts/3
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ id root
uid=0(root) gid=0(root) groups=0(root)
msfadmin@metasploitable:~$ id flag4
uid=444551(flag4) gid=444551(flag4) groups=444551(flag4)
msfadmin@metasploitable:~$
```


Performing Reconnaissance fro
lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
Stop
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
PREVIOUS
NEXT
37°F
Mostly clear
8:38 AM
12/5/2023

CHALLENGE #1

20 Below the sentence "Your browser (or proxy) sent a request that this server could not understand." You will find flag3. **Type** the flag for flag3.

→ CHALLENGE #2

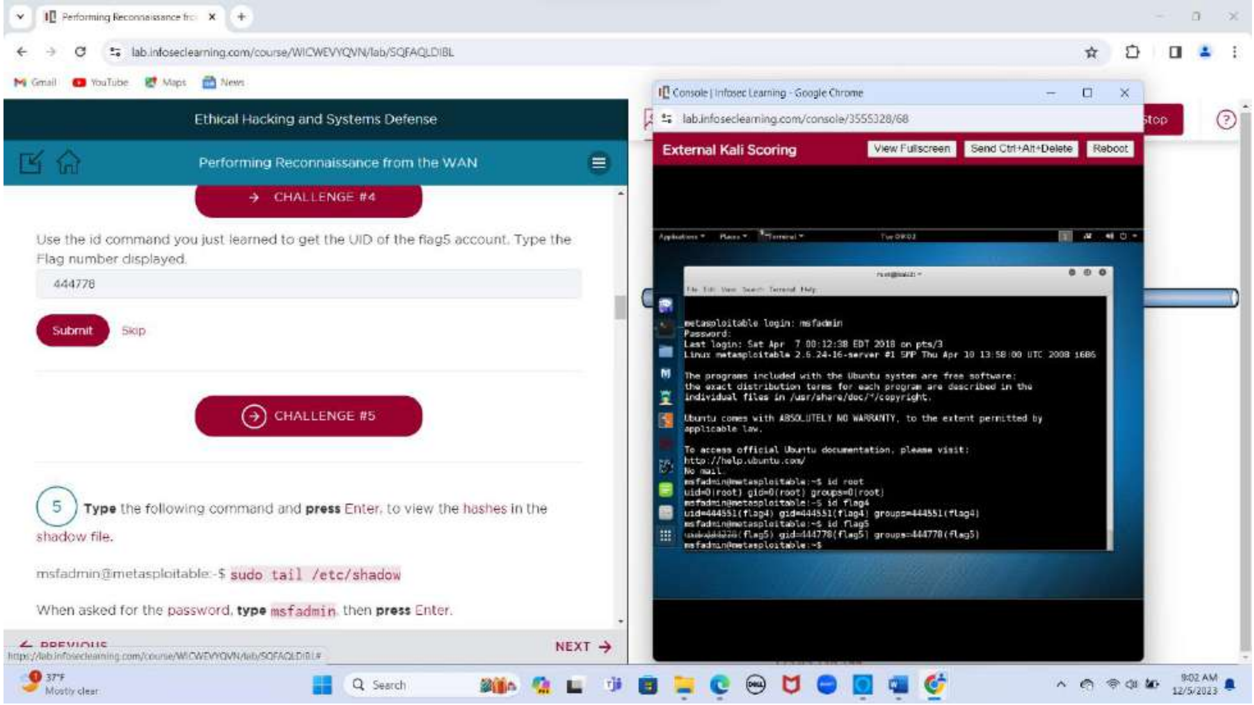
You will find flag 3 Below the sentence "Your browser (or proxy) sent a request that this server could not understand.". Type the Flag number displayed.

765114

Submit Skip

21 We will stop at port 443 and switch to a better form of service detection in the next section of the lab. **Type** the following command and **press** Enter, to clear

```
    span {font-size: smaller;}
/*]]>*/--></style>
</head>

<body>
<h1>Bad request!</h1>
<p>


    Your browser (or proxy) sent a request that
    this server could not understand.
    flag2:877612
    flag3:765114

</p>
<p>
If you think this is a server error, please contact
the <a href="mailto:webmaster@localhost">webmaster</a>.

</p>

<h2>Error 400</h2>
<address>
  <a href="/">localhost</a><br />
```


Performing Reconnaissance fro
lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
CHALLENGE #4
Submit
Skip
CHALLENGE #5
PREVIOUS
NEXT
Search
37°F
Mostly clear
9:02 AM
12/5/2023

Use the id command you just learned to get the UID of the flag5 account. Type the Flag number displayed.

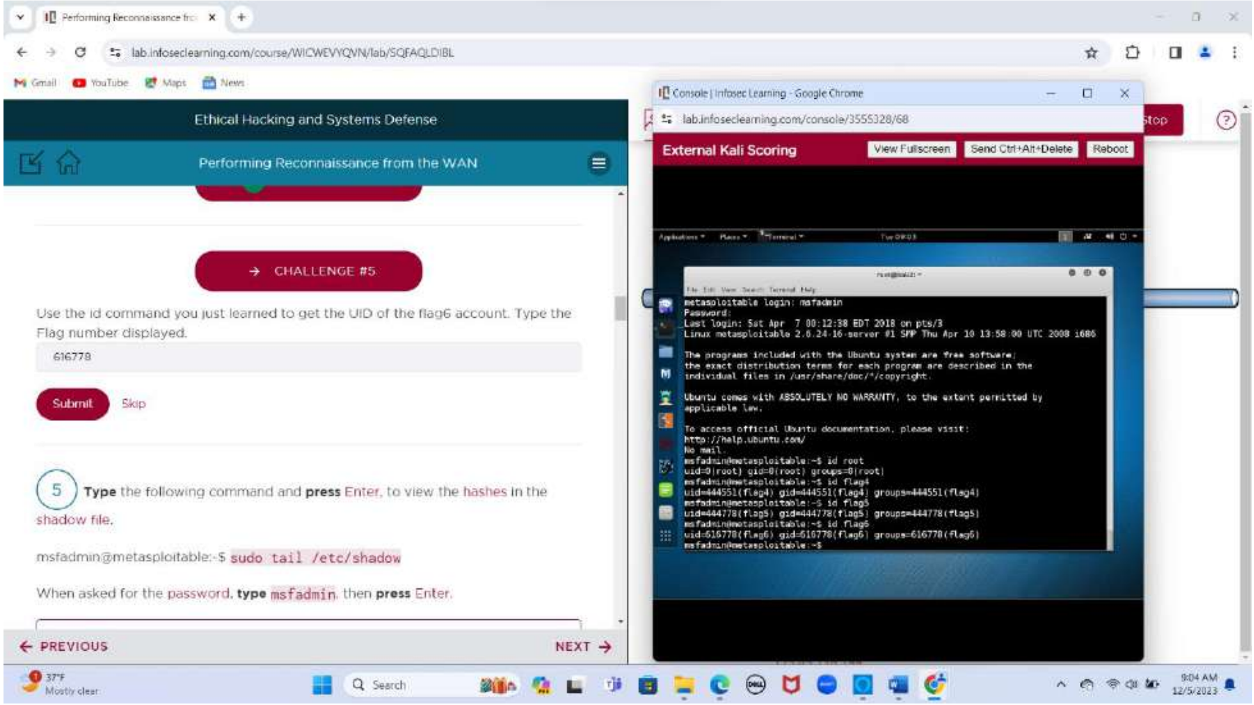
444778

5 **Type** the following command and **press** Enter, to view the hashes in the shadow file.

msfadmin@metasploitable:~$ `sudo tail /etc/shadow`

When asked for the password, **type** `msfadmin`, then **press** Enter.

```
metasploitable login: msfadmin
Password:
Last login: Sat Apr  7 00:12:38 EDT 2018 on pts/3
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ id root
uid=0(root) gid=0(root) groups=0(root)
msfadmin@metasploitable:~$ id flag4
uid=444551(flag4) gid=444551(flag4) groups=444551(flag4)
msfadmin@metasploitable:~$ id flag5
uid=444778(flag5) gid=444778(flag5) groups=444778(flag5)
msfadmin@metasploitable:~$
```


Performing Reconnaissance fro
lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
CHALLENGE #5
Submit
Skip
PREVIOUS
NEXT
Search
37°F
Mostly clear
9:04 AM
12/5/2023

Use the id command you just learned to get the UID of the flag6 account. Type the Flag number displayed.

616778

5 **Type** the following command and **press** Enter, to view the hashes in the shadow file.

msfadmin@metasploitable:~$ `sudo tail /etc/shadow`

When asked for the password, **type** `msfadmin`, then **press** Enter.

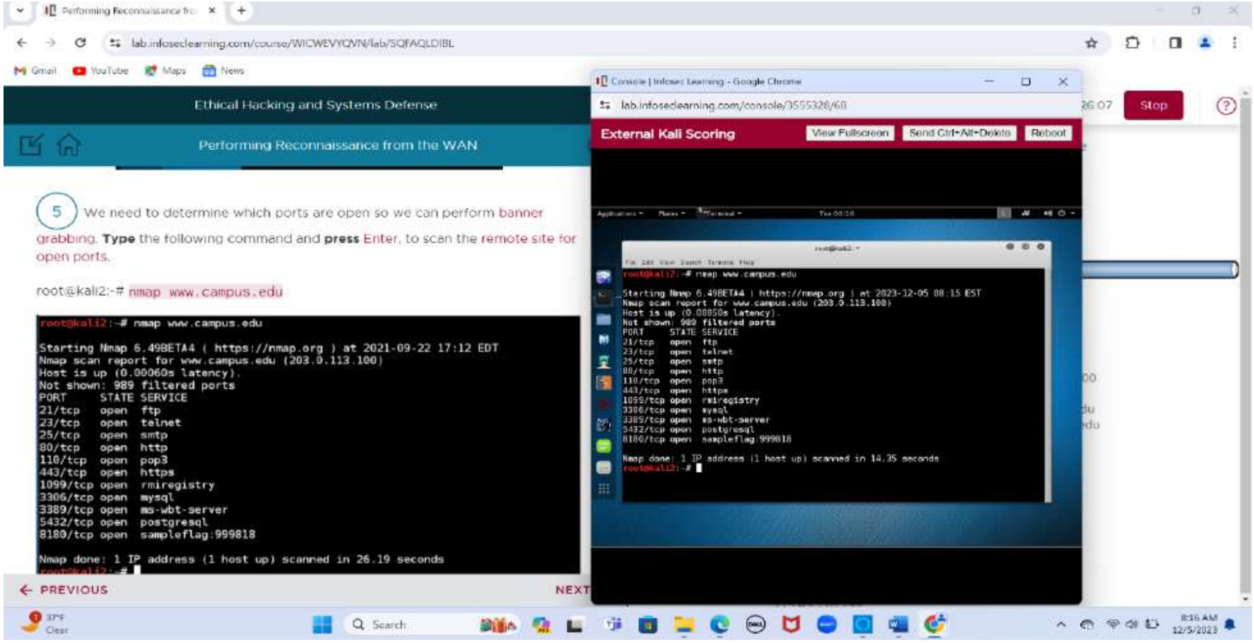
```
metasploitable login: msfadmin
Password:
Last login: Sat Apr  7 00:12:38 EDT 2018 on pts/3
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ id root
uid=0(root) gid=0(root) groups=0(root)
msfadmin@metasploitable:~$ id flag4
uid=444551(flag4) gid=444551(flag4) groups=444551(flag4)
msfadmin@metasploitable:~$ id flag5
uid=444778(flag5) gid=444778(flag5) groups=444778(flag5)
msfadmin@metasploitable:~$ id flag6
uid=616778(flag6) gid=616778(flag6) groups=616778(flag6)
msfadmin@metasploitable:~$
```

The flags are:

- Flag 1: 999818
- Flag 2: 877612
- Flag 3: 444551
- Flag 4: 765114
- Flag 5: 444778
- Flag 6: 616778

Screenshots:

Nmap:


Performing Reconnaissance fr
lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
PREVIOUS
NEXT
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
Applications
Places
Terminal
Search
37°F
Clear
8:16 AM
12/5/2023

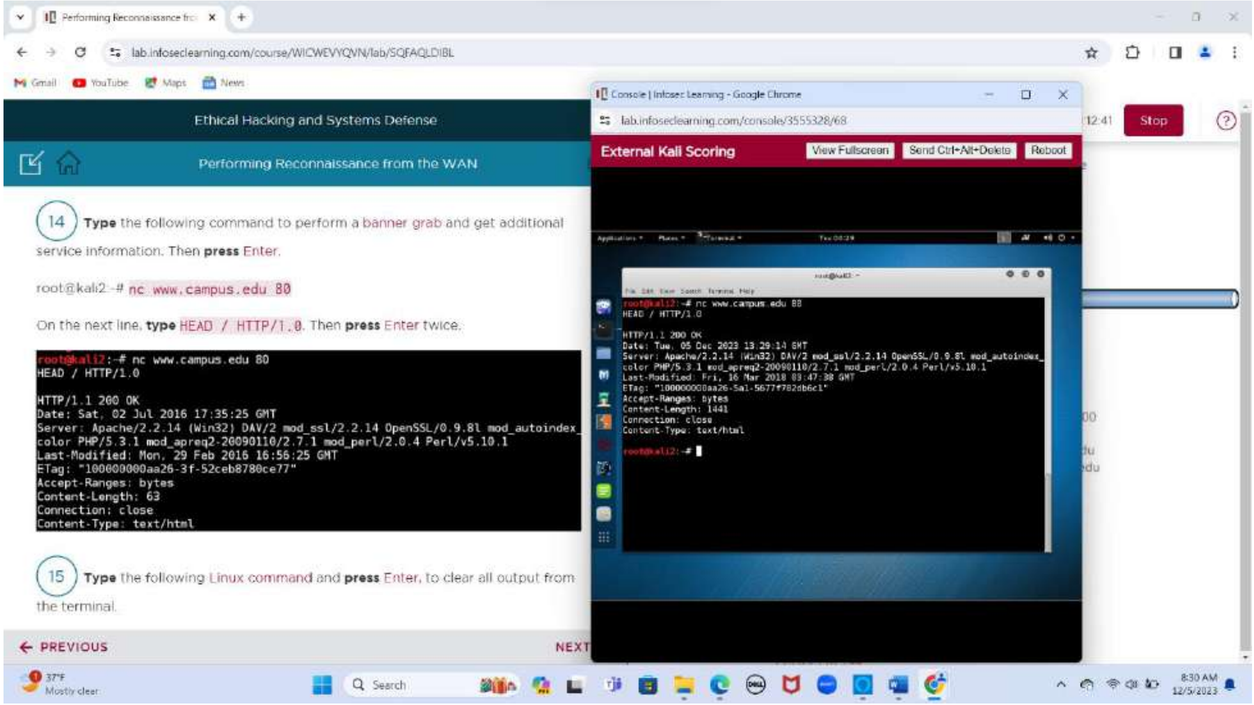
5 We need to determine which ports are open so we can perform banner grabbing. **Type** the following command and **press** Enter, to scan the remote site for open ports.

root@kali2:~# nmap www.campus.edu

```
root@kali2:~# nmap www.campus.edu

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2021-09-22 17:12 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00060s latency).
Not shown: 989 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
443/tcp  open  https
1099/tcp open  rmiregistry
3306/tcp open  mysql
3389/tcp open  ms-wbt-server
5432/tcp open  postgresql
8180/tcp open  sampleflag:999818

Nmap done: 1 IP address (1 host up) scanned in 26.19 seconds
root@kali2:~#
```

```
root@kali2:~# nmap www.campus.edu

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-12-05 08:15 EST
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00050s latency).
Not shown: 989 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
443/tcp  open  https
1099/tcp open  rmiregistry
3306/tcp open  mysql
3389/tcp open  ms-wbt-server
5432/tcp open  postgresql
8180/tcp open  sampleflag:999818

Nmap done: 1 IP address (1 host up) scanned in 14.35 seconds
root@kali2:~#
```

Performing banner grab:


Performing Reconnaissance fro
lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
PREVIOUS
NEXT
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
37°F
Mostly clear
Search
8:30 AM
12/5/2023

14 **Type** the following command to perform a banner grab and get additional service information. Then **press** Enter.

root@kali2:~# `nc www.campus.edu 80`

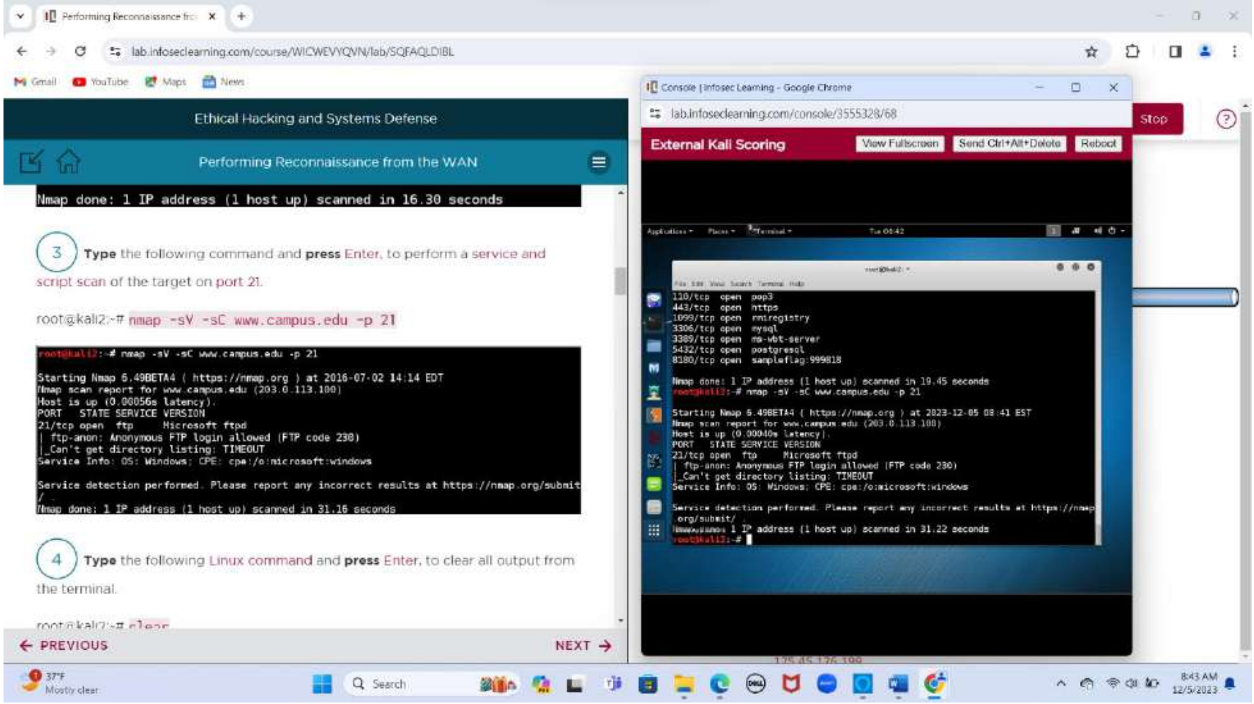
On the next line, **type** `HEAD / HTTP/1.0`. Then **press** Enter twice.

```
root@kali2:~# nc www.campus.edu 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Sat, 02 Jul 2016 17:35:25 GMT
Server: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_
color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
Last-Modified: Mon, 29 Feb 2016 16:56:25 GMT
ETag: "100000000aa26-3f-52ceb8780ce77"
Accept-Ranges: bytes
Content-Length: 63
Connection: close
Content-Type: text/html
```

15 **Type** the following Linux command and **press** Enter, to clear all output from the terminal.

```
root@kali2:~# nc www.campus.edu 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Tue, 05 Dec 2023 13:29:14 GMT
Server: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_
color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
Last-Modified: Fri, 16 Mar 2018 03:47:38 GMT
ETag: "10000000aa26-5a1-5677f782db6c1"
Accept-Ranges: bytes
Content-Length: 1441
Connection: close
Content-Type: text/html

root@kali2:~# 
```

Performing service and script scan of the target:


Performing Reconnaissance fro
lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
PREVIOUS
NEXT
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
37°F
Mostly clear
Search
8:43 AM
12/5/2023

```
Nmap done: 1 IP address (1 host up) scanned in 16.30 seconds
```

3 **Type** the following command and **press** Enter, to perform a service and script scan of the target on port 21.

root@kali2:~# `nmap -sV -sC www.campus.edu -p 21`

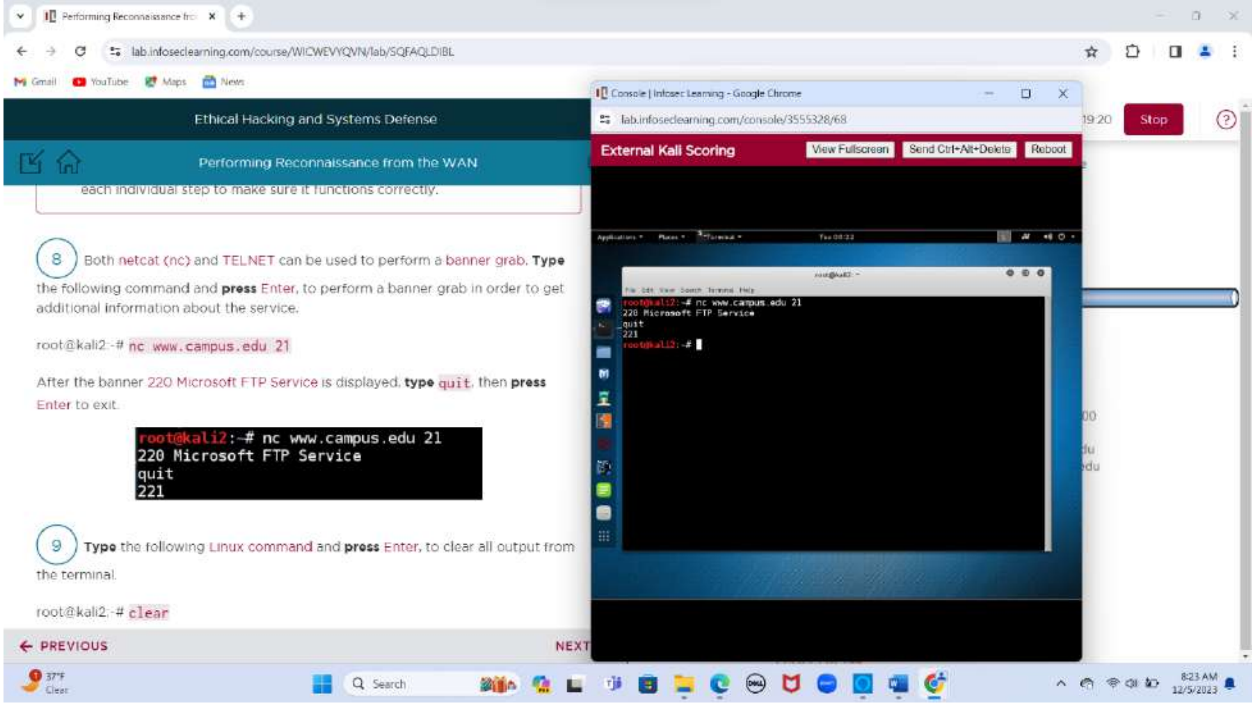
```
root@kali2:~# nmap -sV -sC www.campus.edu -p 21

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-07-02 14:14 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00056s latency).
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 31.16 seconds
```

4 **Type** the following Linux command and **press** Enter, to clear all output from the terminal.

root@kali2:~# `clear`

```
110/tcp  open  pop3
443/tcp  open  https
1099/tcp open  rmiregistry
3306/tcp open  mysql
3389/tcp open  ms-wbt-server
5432/tcp open  postgresql
8180/tcp open  sampleflag:999818

Nmap done: 1 IP address (1 host up) scanned in 19.45 seconds
root@kali2:~# nmap -sV -sC www.campus.edu -p 21

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-12-05 08:41 EST
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00040s latency).
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.22 seconds
root@kali2:~# 
```

Netcat:



Ethical Hacking and Systems Defense

Performing Reconnaissance from the WAN

each individual step to make sure it functions correctly.

8 Both netcat (nc) and TELNET can be used to perform a banner grab. **Type** the following command and **press** Enter, to perform a banner grab in order to get additional information about the service.

root@kali2:~# `nc www.campus.edu 21`

After the banner 220 Microsoft FTP Service is displayed, **type** `quit`, then **press** Enter to exit.

```
root@kali2:~# nc www.campus.edu 21
220 Microsoft FTP Service
quit
221
```

9 **Type** the following Linux command and **press** Enter, to clear all output from the terminal.

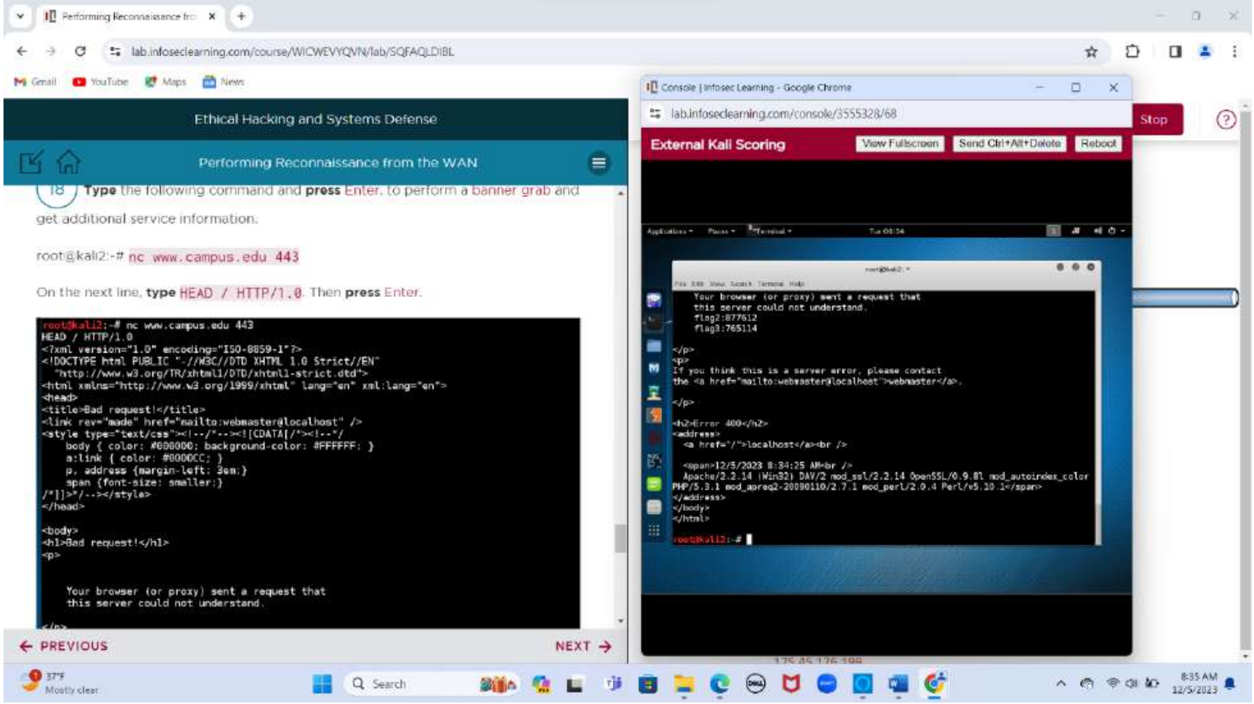
root@kali2:~# `clear`

External Kali Scoring

```
root@kali2:~# nc www.campus.edu 21
220 Microsoft FTP Service
quit
221
root@kali2:~#
```

Performing Reconnaissance fro
lab.infosecl earning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
19:20
Stop
← PREVIOUS
NEXT
37°F
Clear
Search
8:23 AM
12/5/2023

nc 443:



Ethical Hacking and Systems Defense

Performing Reconnaissance from the WAN

18 **Type** the following command and **press** Enter, to perform a banner grab and get additional service information.

root@kali2:~# `nc www.campus.edu 443`

On the next line, **type** `HEAD / HTTP/1.0`. Then **press** Enter.

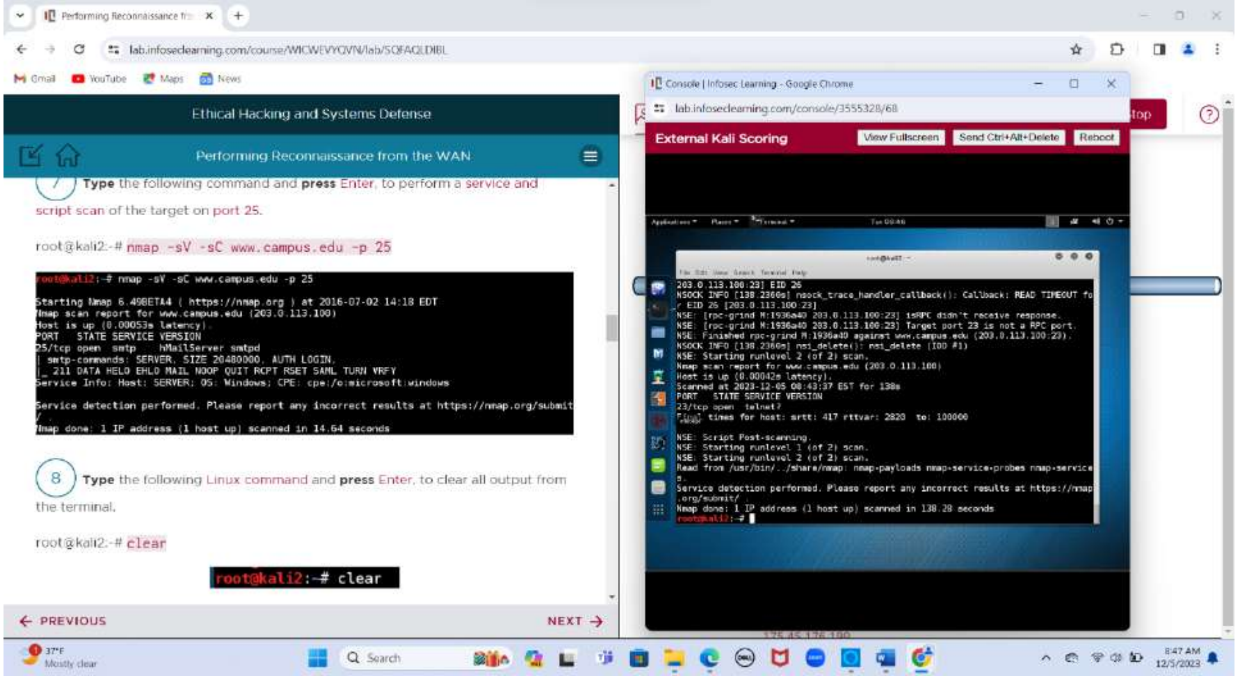
```
root@kali2:~# nc www.campus.edu 443
HEAD / HTTP/1.0
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en">
<head>
<title>Bad request!</title>
<link rev="made" href="mailto:webmaster@localhost" />
<style type="text/css"><!--/*--><![CDATA[/*><!--*/
    body { color: #000000; background-color: #FFFFFF; }
    a:link { color: #0000CC; }
    p, address {margin-left: 3em;}
    span {font-size: smaller;}
/*]]>*/--></style>
</head>

<body>
<h1>Bad request!</h1>
<p>


    Your browser (or proxy) sent a request that
    this server could not understand.

</p>
```

External Kali Scoring

```
    Your browser (or proxy) sent a request that
    this server could not understand.
    flag2:877612
    flag3:765114

</p>
<p>
If you think this is a server error, please contact
the <a href="mailto:webmaster@localhost">webmaster</a>.

</p>

<h2>Error 400</h2>
<address>
  <a href="/">localhost</a><br />

  <span>12/5/2023 8:34:25 AM<br />
  Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color
PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1</span>
</address>
</body>
</html>

root@kali2:~#
```

Performing Reconnaissance fro
lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
← PREVIOUS
NEXT →
37°F
Mostly clear
Search
8:35 AM
12/5/2023

Nmap port 23:


Performing Reconnaissance fr
lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
PREVIOUS
NEXT
37°F
Mostly clear
Search
8:47 AM
12/5/2023

7 Type the following command and press Enter, to perform a service and script scan of the target on port 25.

root@kali2:~# `nmap -sV -sC www.campus.edu -p 25`

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 25

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-07-02 14:18 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00053s latency).
PORT   STATE SERVICE VERSION
25/tcp open  smtp    hMailServer smtpd
| smtp-commands: SERVER, SIZE 20480000, AUTH LOGIN,
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
Service Info: Host: SERVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 14.64 seconds
```

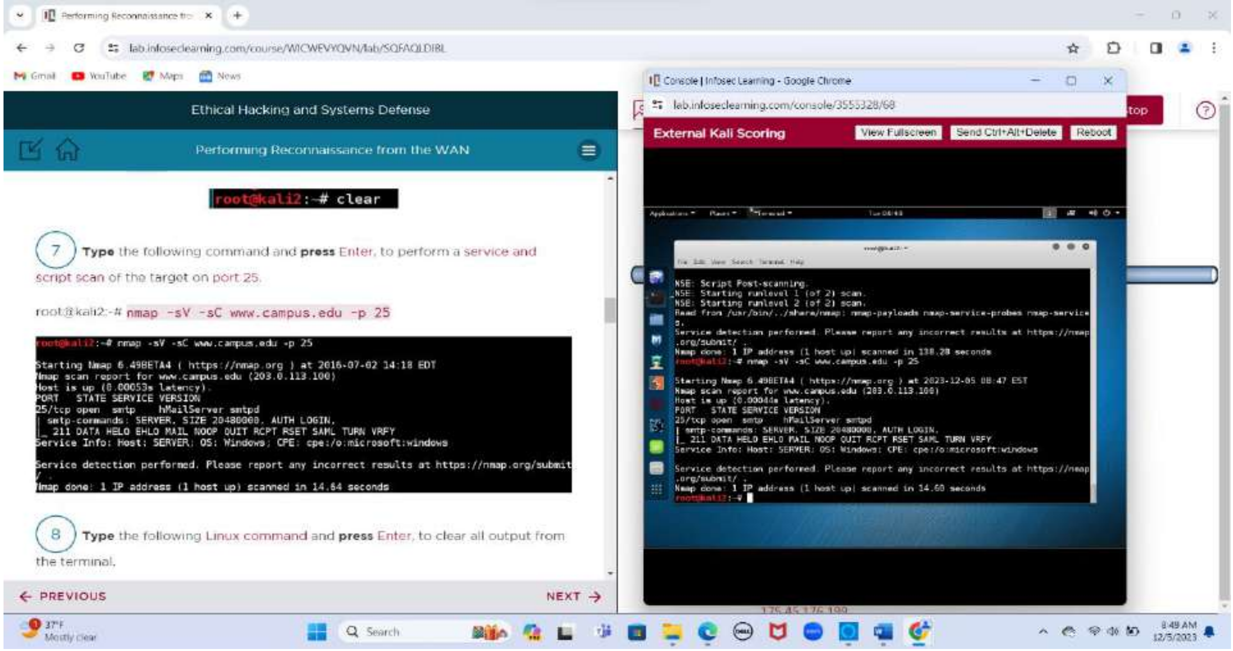
8 Type the following Linux command and press Enter, to clear all output from the terminal.

root@kali2:~# `clear`

```
root@kali2:~# clear
```

```
203.0.113.100:23] EID 26
NSOCK INFO [138.2360s] nsock_trace_handler_callback(): Callback: READ TIMEOUT fo
r EID 26 [203.0.113.100:23]
NSE: [rpc-grind M:1936a40 203.0.113.100:23] isRPC didn't receive response.
NSE: [rpc-grind M:1936a40 203.0.113.100:23] Target port 23 is not a RPC port.
NSE: Finished rpc-grind M:1936a40 against www.campus.edu (203.0.113.100:23).
NSOCK INFO [138.2360s] nsi_delete(): nsi_delete (IOD #1)
NSE: Starting runlevel 2 (of 2) scan.
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00042s latency).
Scanned at 2023-12-05 08:43:37 EST for 138s
PORT   STATE SERVICE VERSION
23/tcp open  telnet?
Final times for host: srtt: 417 rttvar: 2820  to: 100000

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
NSE: Starting runlevel 2 (of 2) scan.
Read from /usr/bin/../share/nmap: nmap-payloads nmap-service-probes nmap-service
s.
Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 138.28 seconds
root@kali2:~#
```

Nmap port 25:


Performing Reconnaissance fr
lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
PREVIOUS
NEXT
37°F
Mostly clear
Search
8:49 AM
12/5/2023

```
root@kali2:~# clear
```

7 Type the following command and press Enter, to perform a service and script scan of the target on port 25.

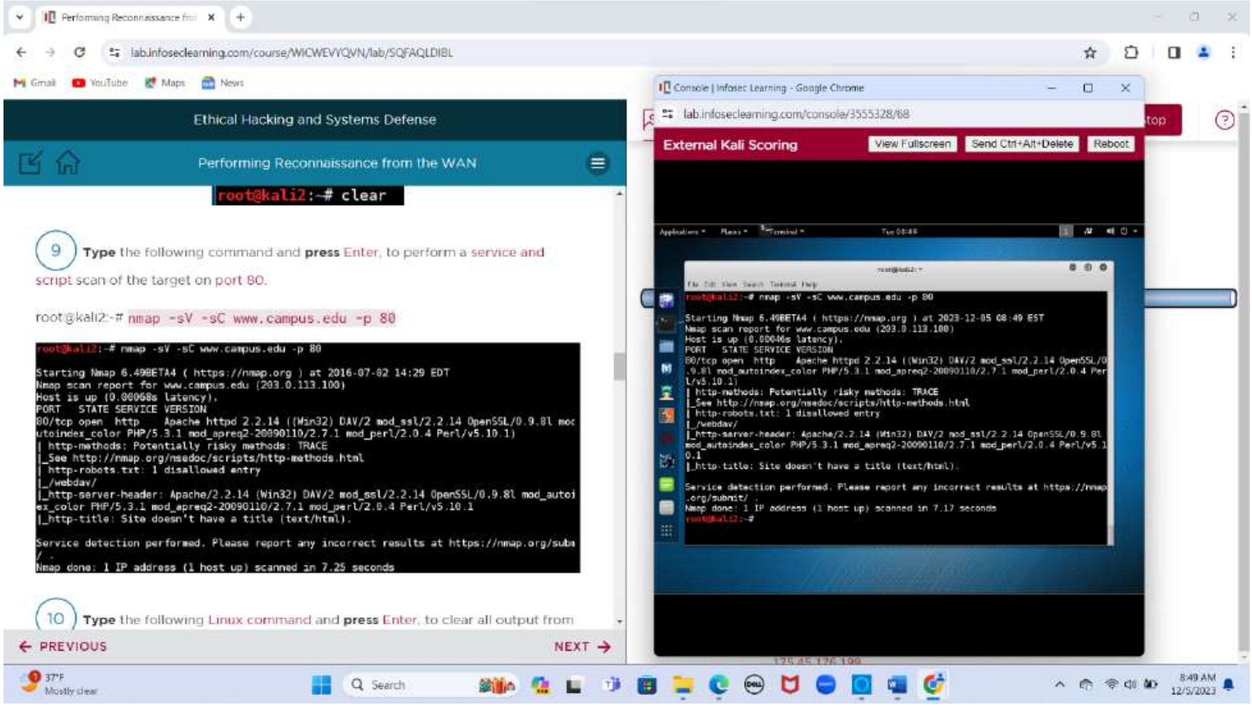
root@kali2:~# `nmap -sV -sC www.campus.edu -p 25`

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 25

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-07-02 14:18 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00053s latency).
PORT   STATE SERVICE VERSION
25/tcp open  smtp    hMailServer smtpd
| smtp-commands: SERVER, SIZE 20480000, AUTH LOGIN,
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
Service Info: Host: SERVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 14.64 seconds
```

8 Type the following Linux command and press Enter, to clear all output from the terminal.

```
NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
NSE: Starting runlevel 2 (of 2) scan.
Read from /usr/bin/../share/nmap: nmap-payloads nmap-service-probes nmap-service
s.
Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 138.28 seconds
root@kali2:~# nmap -sV -sC www.campus.edu -p 25

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-12-05 08:47 EST
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00044s latency).
PORT   STATE SERVICE VERSION
25/tcp open  smtp    hMailServer smtpd
| smtp-commands: SERVER, SIZE 20480000, AUTH LOGIN,
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
Service Info: Host: SERVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.60 seconds
root@kali2:~#
```

Nmap port 80:


Performing Reconnaissance fro
lab.infosecleaming.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
Console | Infosec Learning - Google Chrome
lab.infosecleaming.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
PREVIOUS
NEXT
37°F
Mostly clear
Search
8:49 AM
12/5/2023

```
root@kali2:~# clear
```

9 **Type** the following command and **press** Enter, to perform a service and script scan of the target on port 80.

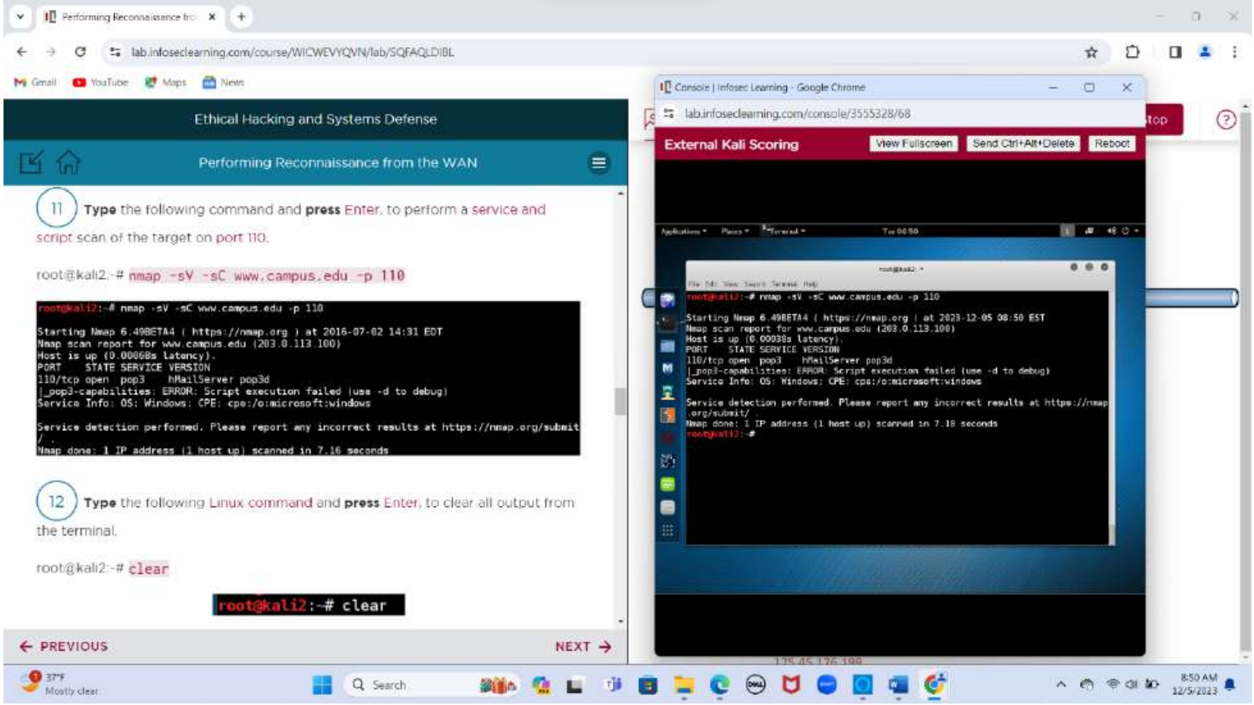
root@kali2:~# `nmap -sV -sC www.campus.edu -p 80`

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 80

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-07-02 14:29 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00068s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.14 ((Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l moc
utoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
| http-methods: Potentially risky methods: TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
| http-robots.txt: 1 disallowed entry
|_/webdav/
|_http-server-header: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoi
ex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
|_http-title: Site doesn't have a title (text/html).

Service detection performed. Please report any incorrect results at https://nmap.org/subm
/ .
Nmap done: 1 IP address (1 host up) scanned in 7.25 seconds
```

10 **Type** the following Linux command and **press** Enter, to clear all output from

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 80

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-12-05 08:49 EST
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00046s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.14 ((Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0
.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Per
l/v5.10.1)
| http-methods: Potentially risky methods: TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
| http-robots.txt: 1 disallowed entry
|_/webdav/
|_http-server-header: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l
mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.1
0.1
|_http-title: Site doesn't have a title (text/html).

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.17 seconds
root@kali2:~#
```

Nmap port 110:


Performing Reconnaissance fro
lab.infosecleaming.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
Console | Infosec Learning - Google Chrome
lab.infosecleaming.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
PREVIOUS
NEXT
37°F
Mostly clear
Search
8:50 AM
12/5/2023

11 **Type** the following command and **press** Enter, to perform a service and script scan of the target on port 110.

root@kali2:~# `nmap -sV -sC www.campus.edu -p 110`

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 110

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-07-02 14:31 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00068s latency).
PORT    STATE SERVICE VERSION
110/tcp open  pop3    hMailServer pop3d
|_pop3-capabilities: ERROR: Script execution failed (use -d to debug)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 7.16 seconds
```

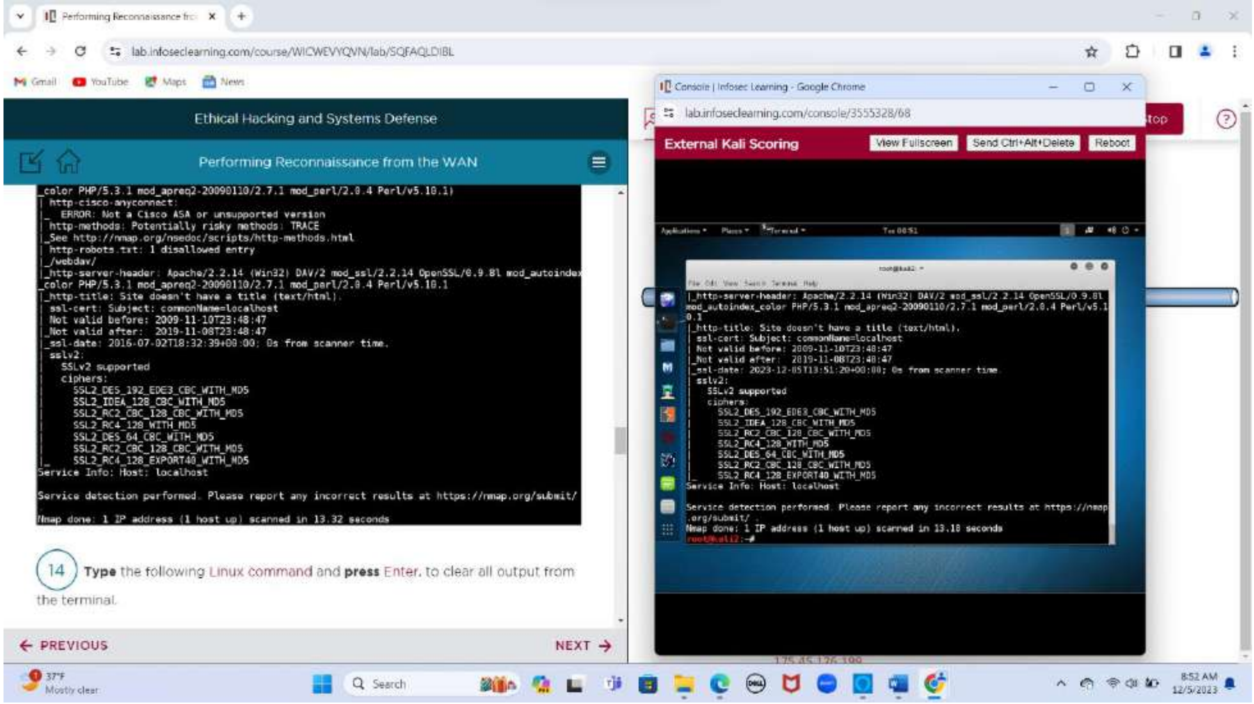
12 **Type** the following Linux command and **press** Enter, to clear all output from the terminal.

root@kali2:~# `clear`

```
root@kali2:~# clear
```

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 110

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-12-05 08:50 EST
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00038s latency).
PORT    STATE SERVICE VERSION
110/tcp open  pop3    hMailServer pop3d
|_pop3-capabilities: ERROR: Script execution failed (use -d to debug)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.18 seconds
root@kali2:~#
```

Nmap port 443:

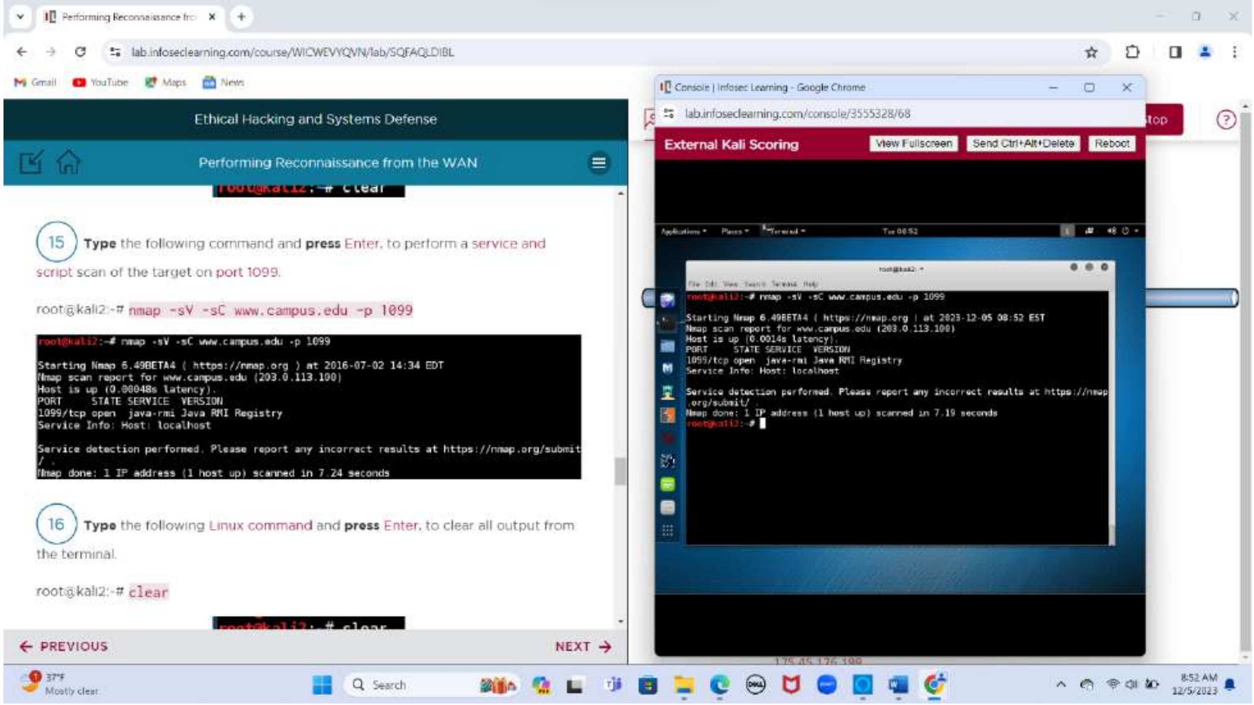

Performing Reconnaissance fro
lab.infosecLearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
Console | Infosec Learning - Google Chrome
lab.infosecLearning.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
← PREVIOUS
NEXT →
37°F
Mostly clear
Search
8:52 AM
12/5/2023

```
_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
| http-cisco-anyconnect:
|_  ERROR: Not a Cisco ASA or unsupported version
| http-methods: Potentially risky methods: TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
| http-robots.txt: 1 disallowed entry
|_/webdav/
|_http-server-header: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex
_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_ssl-date: 2016-07-02T18:32:39+00:00; 0s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_IDEA_128_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
Service Info: Host: localhost

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 13.32 seconds
```

14 **Type** the following Linux command and **press** Enter, to clear all output from the terminal.

```
|_http-server-header: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l
mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.1
0.1
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_ssl-date: 2023-12-05T13:51:20+00:00; 0s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_IDEA_128_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
Service Info: Host: localhost

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds
root@kali2:~#
```

Nmap port 1099:


Performing Reconnaissance fro
lab.infosecLearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
Console | Infosec Learning - Google Chrome
lab.infosecLearning.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
← PREVIOUS
NEXT →
37°F
Mostly clear
Search
8:52 AM
12/5/2023

```
root@kali2:~# clear
```

15 **Type** the following command and **press** Enter, to perform a service and script scan of the target on port 1099.

root@kali2:~# `nmap -sV -sC www.campus.edu -p 1099`

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 1099

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-07-02 14:34 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00048s latency).
PORT     STATE SERVICE  VERSION
1099/tcp open  java-rmi Java RMI Registry
Service Info: Host: localhost

Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 7.24 seconds
```

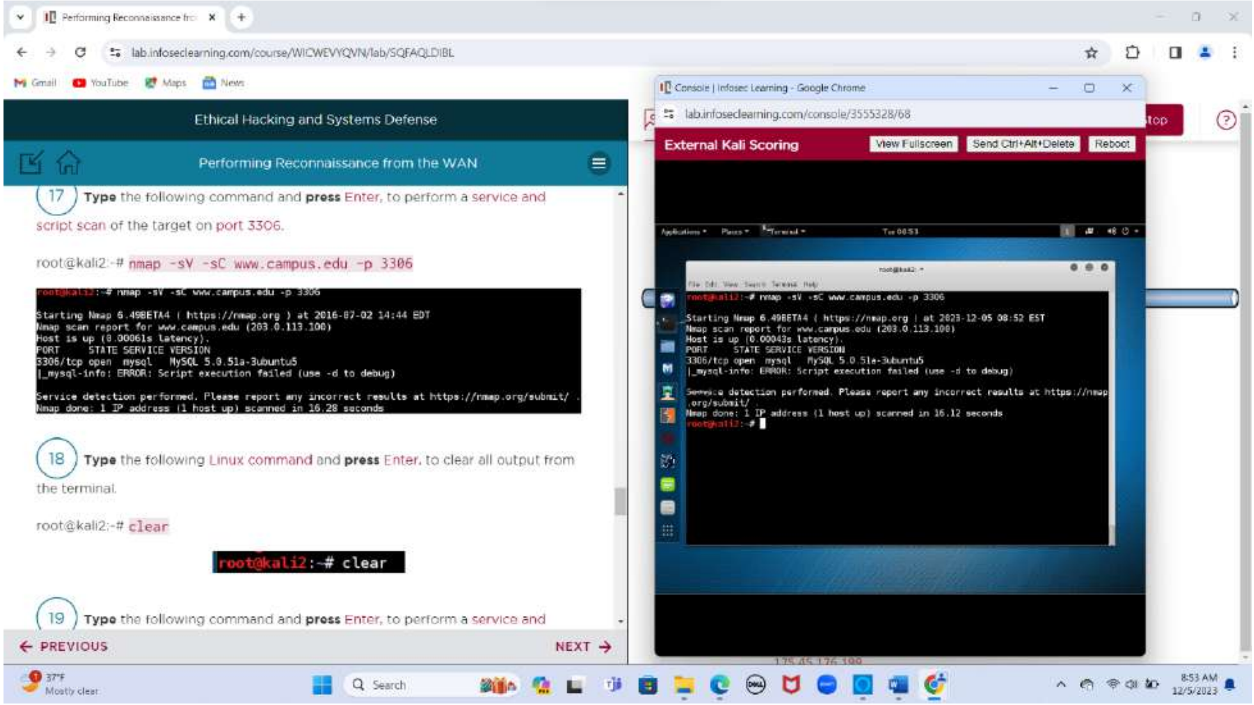
16 **Type** the following Linux command and **press** Enter, to clear all output from the terminal.

root@kali2:~# `clear`

```
root@kali2:~# clear
```

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 1099

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-12-05 08:52 EST
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.0014s latency).
PORT     STATE SERVICE  VERSION
1099/tcp open  java-rmi Java RMI Registry
Service Info: Host: localhost

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.19 seconds
root@kali2:~#
```

Nmap port 3306:


Performing Reconnaissance fro
lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
PREVIOUS
NEXT
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Terminal
Tue 08:53
37°F
Mostly clear
Search
8:53 AM
12/5/2023

17 **Type** the following command and **press** Enter, to perform a service and script scan of the target on port 3306.

```
root@kali2:-# nmap -sV -sC www.campus.edu -p 3306
```

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 3306

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-07-02 14:44 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00061s latency).
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.0.51a-3ubuntu5
|_mysql-info: ERROR: Script execution failed (use -d to debug)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.28 seconds
```

18 **Type** the following Linux command and **press** Enter, to clear all output from the terminal.

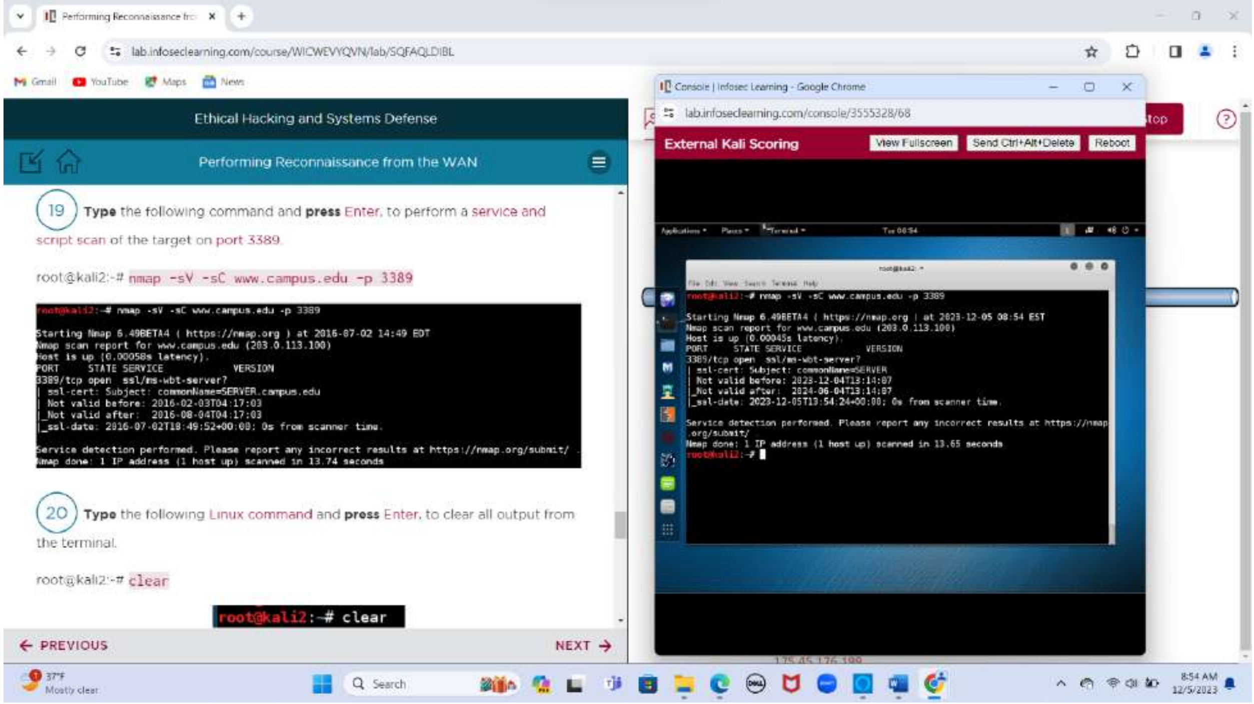
```
root@kali2:-# clear
```

```
root@kali2:~# clear
```

19 **Type** the following command and **press** Enter, to perform a service and

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 3306

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-12-05 08:52 EST
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00043s latency).
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.0.51a-3ubuntu5
|_mysql-info: ERROR: Script execution failed (use -d to debug)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.12 seconds
root@kali2:~# 
```

Nmap port 3389:


Performing Reconnaissance fro
lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
PREVIOUS
NEXT
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Terminal
Tue 08:54
37°F
Mostly clear
Search
8:54 AM
12/5/2023

19 **Type** the following command and **press** Enter, to perform a service and script scan of the target on port 3389.

```
root@kali2:-# nmap -sV -sC www.campus.edu -p 3389
```

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 3389

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-07-02 14:49 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00058s latency).
PORT     STATE SERVICE           VERSION
3389/tcp open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=SERVER.campus.edu
| Not valid before: 2016-02-03T04:17:03
|_Not valid after:  2016-08-04T04:17:03
|_ssl-date: 2016-07-02T18:49:52+00:00; 0s from scanner time.

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.74 seconds
```

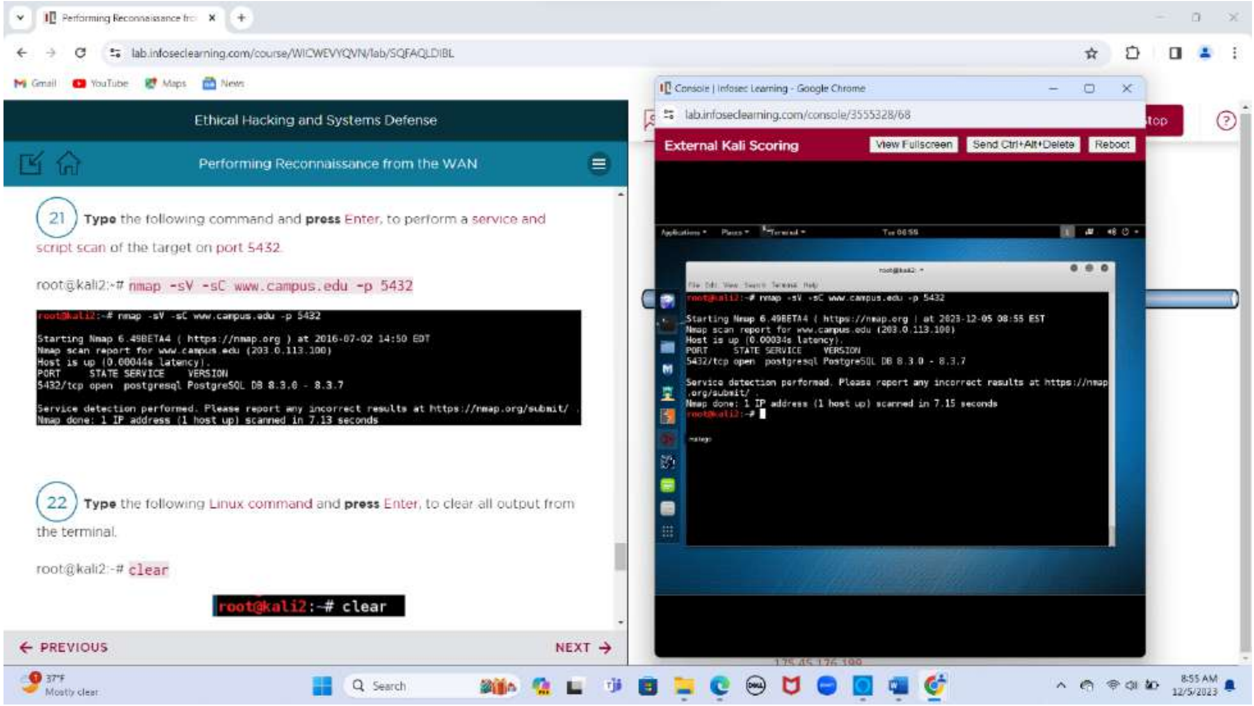
20 **Type** the following Linux command and **press** Enter, to clear all output from the terminal.

```
root@kali2:-# clear
```

```
root@kali2:~# clear
```

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 3389

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-12-05 08:54 EST
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00045s latency).
PORT     STATE SERVICE           VERSION
3389/tcp open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=SERVER
| Not valid before: 2023-12-04T13:14:07
|_Not valid after:  2024-06-04T13:14:07
|_ssl-date: 2023-12-05T13:54:24+00:00; 0s from scanner time.

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.65 seconds
root@kali2:~# 
```

Nmap port 5432:


Performing Reconnaissance fro
lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
PREVIOUS
NEXT
37°F
Mostly clear
Search
8:55 AM
12/5/2023

Ethical Hacking and Systems Defense

Performing Reconnaissance from the WAN

21 **Type** the following command and **press** Enter, to perform a service and script scan of the target on port 5432.

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 5432
```

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 5432

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-07-02 14:50 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00044s latency).
PORT     STATE SERVICE    VERSION
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.13 seconds
```

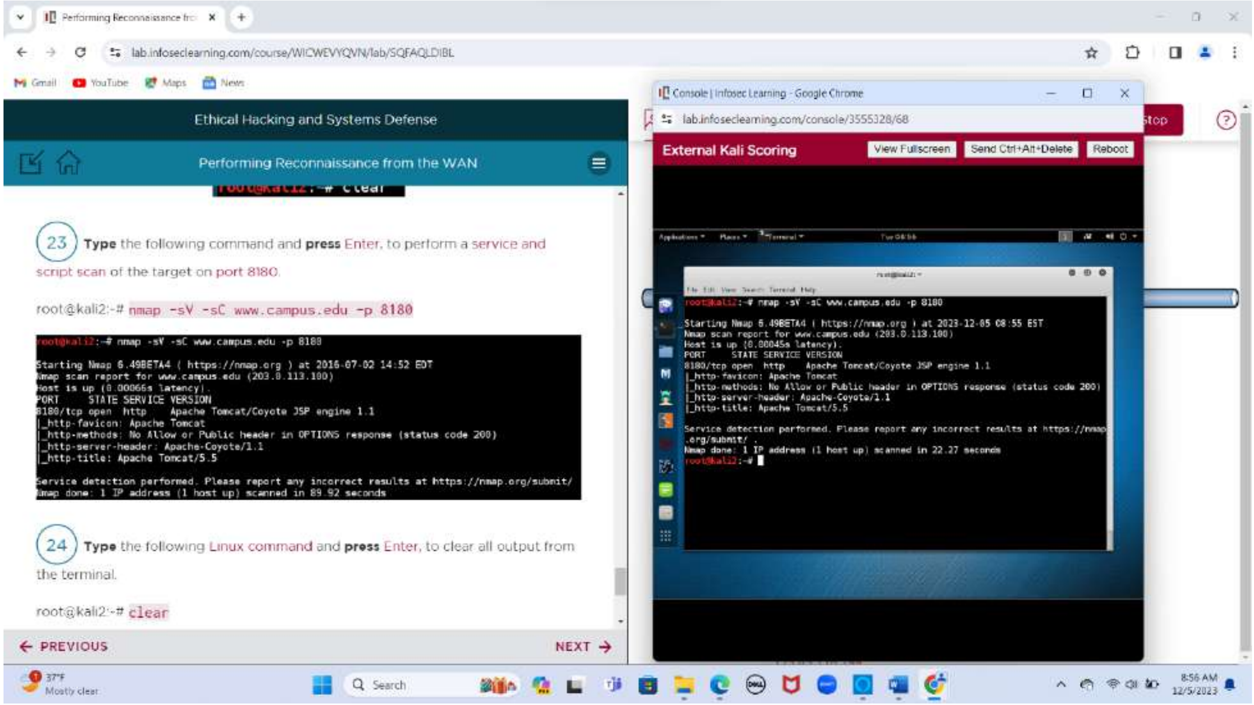
22 **Type** the following Linux command and **press** Enter, to clear all output from the terminal.

```
root@kali2:~# clear
```

```
root@kali2:~# clear
```

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 5432

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-12-05 08:55 EST
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00034s latency).
PORT     STATE SERVICE    VERSION
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.15 seconds
root@kali2:~# 
```

Nmap port 8180:


Performing Reconnaissance fro
lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
PREVIOUS
NEXT
37°F
Mostly clear
Search
8:56 AM
12/5/2023

Ethical Hacking and Systems Defense

Performing Reconnaissance from the WAN

23 **Type** the following command and **press** Enter, to perform a service and script scan of the target on port 8180.

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 8180
```

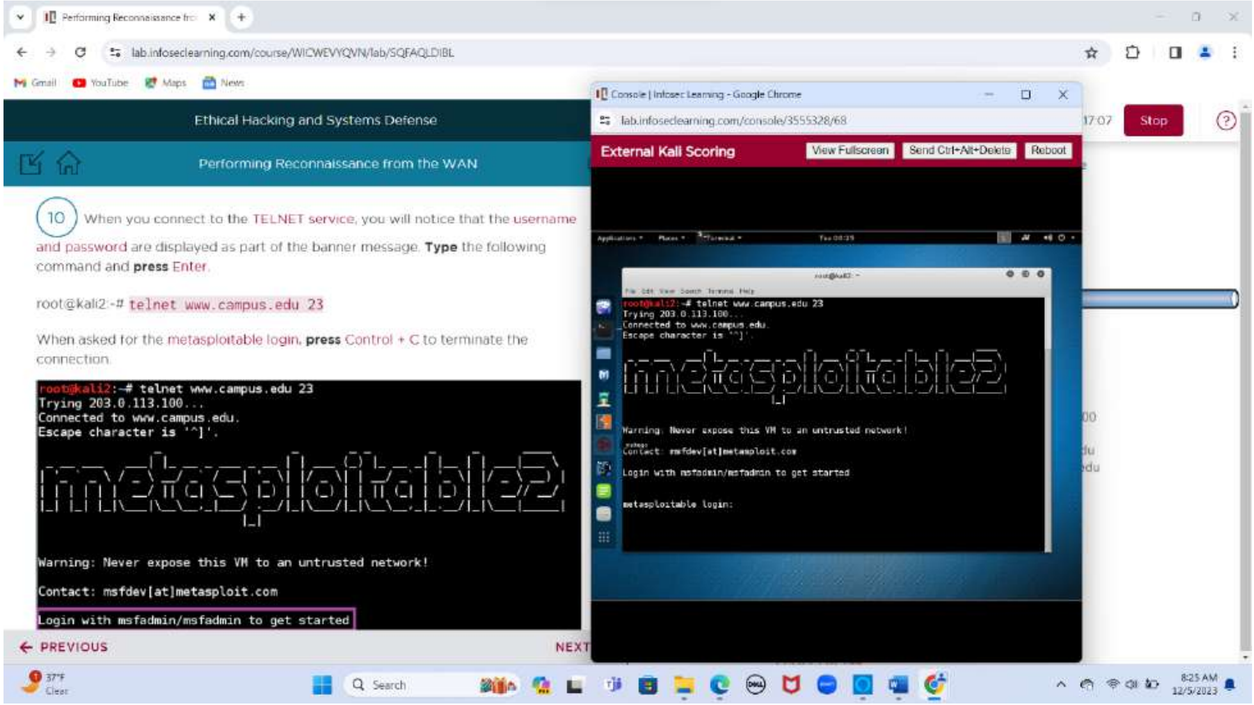
```
root@kali2:~# nmap -sV -sC www.campus.edu -p 8180

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-07-02 14:52 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00066s latency).
PORT     STATE SERVICE VERSION
8180/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 89.92 seconds
```

24 **Type** the following Linux command and **press** Enter, to clear all output from the terminal.

```
root@kali2:~# clear
```

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 8180

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2023-12-05 08:55 EST
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00045s latency).
PORT     STATE SERVICE VERSION
8180/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.27 seconds
root@kali2:~# 
```

Connecting to TELNET:


Performing Reconnaissance fro
lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
17:07
Stop
PREVIOUS
NEXT
37°F
Clear
Search
8:25 AM
12/5/2023

10 When you connect to the TELNET service, you will notice that the username and password are displayed as part of the banner message. **Type** the following command and **press** Enter.

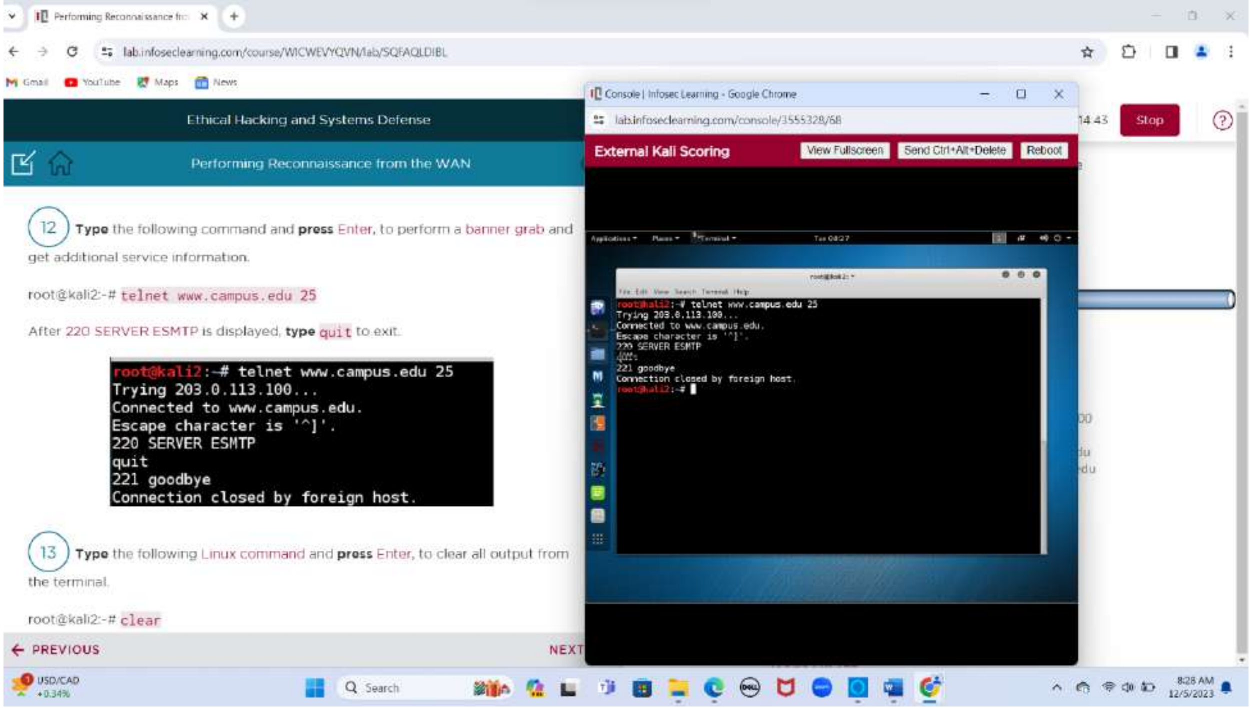
root@kali2:~# `telnet www.campus.edu 23`

When asked for the metasploitable login, **press** Control + C to terminate the connection.

```
root@kali2:~# telnet www.campus.edu 23
Trying 203.0.113.100...
Connected to www.campus.edu.
Escape character is '^]'.

metasploitable2

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

```
root@kali2:~# telnet www.campus.edu 23
Trying 203.0.113.100...
Connected to www.campus.edu.
Escape character is '^]'.

metasploitable2

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
```

TELNET banner grab:


Performing Reconnaissance fro
lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
14:43
Stop
PREVIOUS
NEXT
USD/CAD
+0.34%
Search
8:28 AM
12/5/2023

12 **Type** the following command and **press** Enter, to perform a banner grab and get additional service information.

root@kali2:~# `telnet www.campus.edu 25`

After 220 SERVER ESMTP is displayed, **type** `quit` to exit.

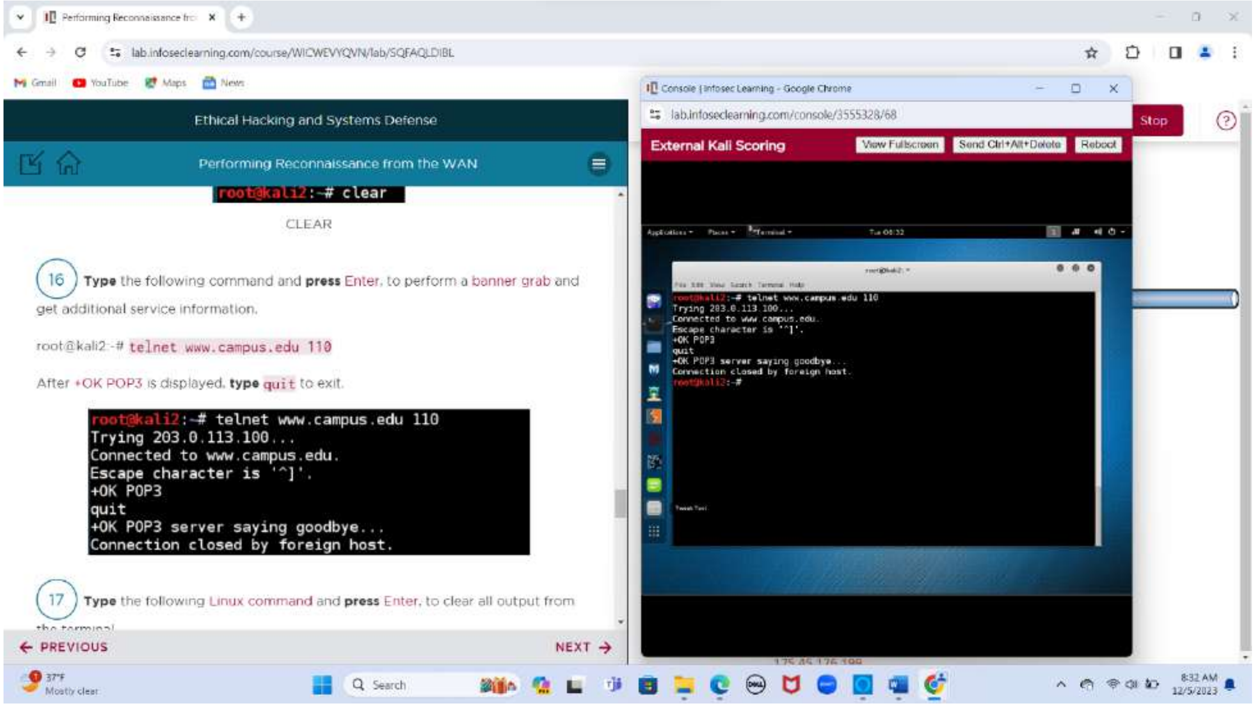
```
root@kali2:~# telnet www.campus.edu 25
Trying 203.0.113.100...
Connected to www.campus.edu.
Escape character is '^]'.
220 SERVER ESMTP
quit
221 goodbye
Connection closed by foreign host.
```

13 **Type** the following Linux command and **press** Enter, to clear all output from the terminal.

root@kali2:~# `clear`

```
root@kali2:~# telnet www.campus.edu 25
Trying 203.0.113.100...
Connected to www.campus.edu.
Escape character is '^]'.
220 SERVER ESMTP
quit
221 goodbye
Connection closed by foreign host.
root@kali2:~# 
```

TELNET 110:


Performing Reconnaissance fro
lab.infosecleaming.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
Console | Infosec Learning - Google Chrome
lab.infosecleaming.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
Applications
Places
Terminal
Tue 08:32
root@kali2: ~
File Edit View Search Terminal Help
PREVIOUS
NEXT
37°F
Mostly clear
Search
8:32 AM
12/5/2023

```
root@kali2:~# clear
```

CLEAR

16 **Type** the following command and **press** Enter, to perform a banner grab and get additional service information.

root@kali2:~# `telnet www.campus.edu 110`

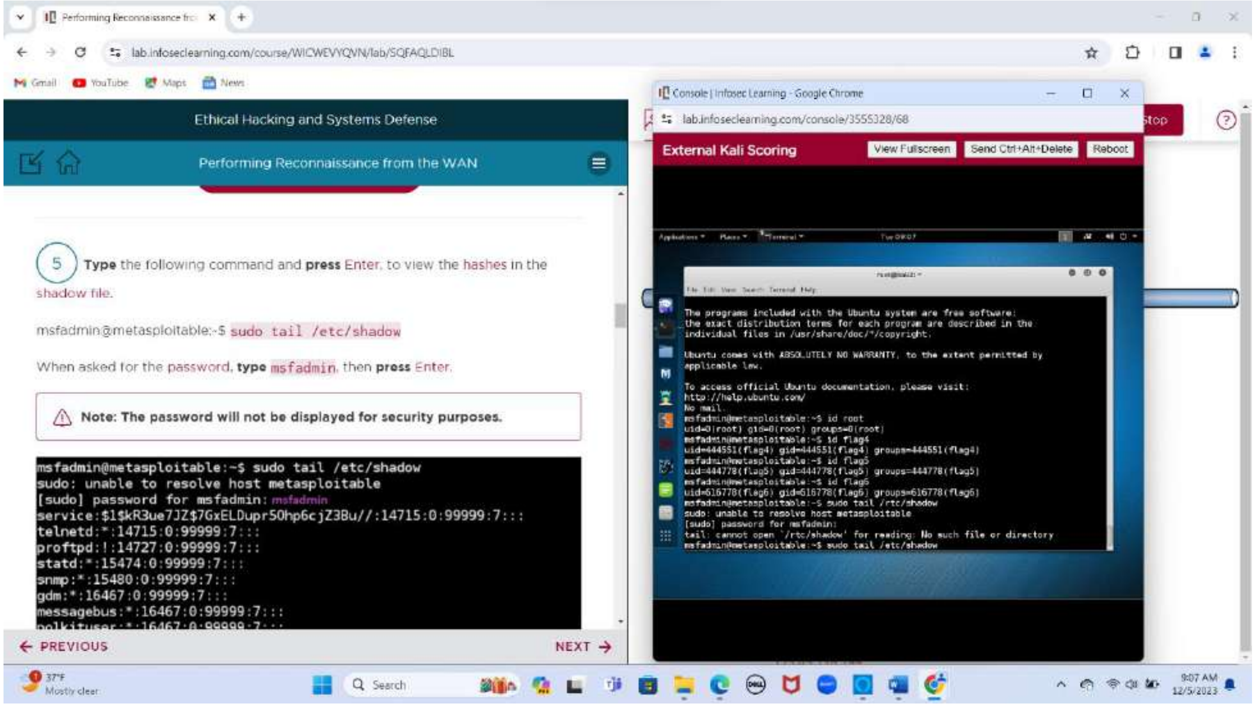
After +OK POP3 is displayed, **type** `quit` to exit.

```
root@kali2:~# telnet www.campus.edu 110
Trying 203.0.113.100...
Connected to www.campus.edu.
Escape character is '^]'.
+OK POP3
quit
+OK POP3 server saying goodbye...
Connection closed by foreign host.
```

17 **Type** the following Linux command and **press** Enter, to clear all output from the terminal.

```
root@kali2:~# telnet www.campus.edu 110
Trying 203.0.113.100...
Connected to www.campus.edu.
Escape character is '^]'.
+OK POP3
quit
+OK POP3 server saying goodbye...
Connection closed by foreign host.
root@kali2:~#
```

Viewing hashes:


Performing Reconnaissance fro
lab.infosecleaming.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
Console | Infosec Learning - Google Chrome
lab.infosecleaming.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
Applications
Places
Terminal
Tue 09:07
root@kali2: ~
File Edit View Search Terminal Help
PREVIOUS
NEXT
37°F
Mostly clear
Search
9:07 AM
12/5/2023

5 **Type** the following command and **press** Enter, to view the hashes in the shadow file.

msfadmin@metasploitable:~$ `sudo tail /etc/shadow`

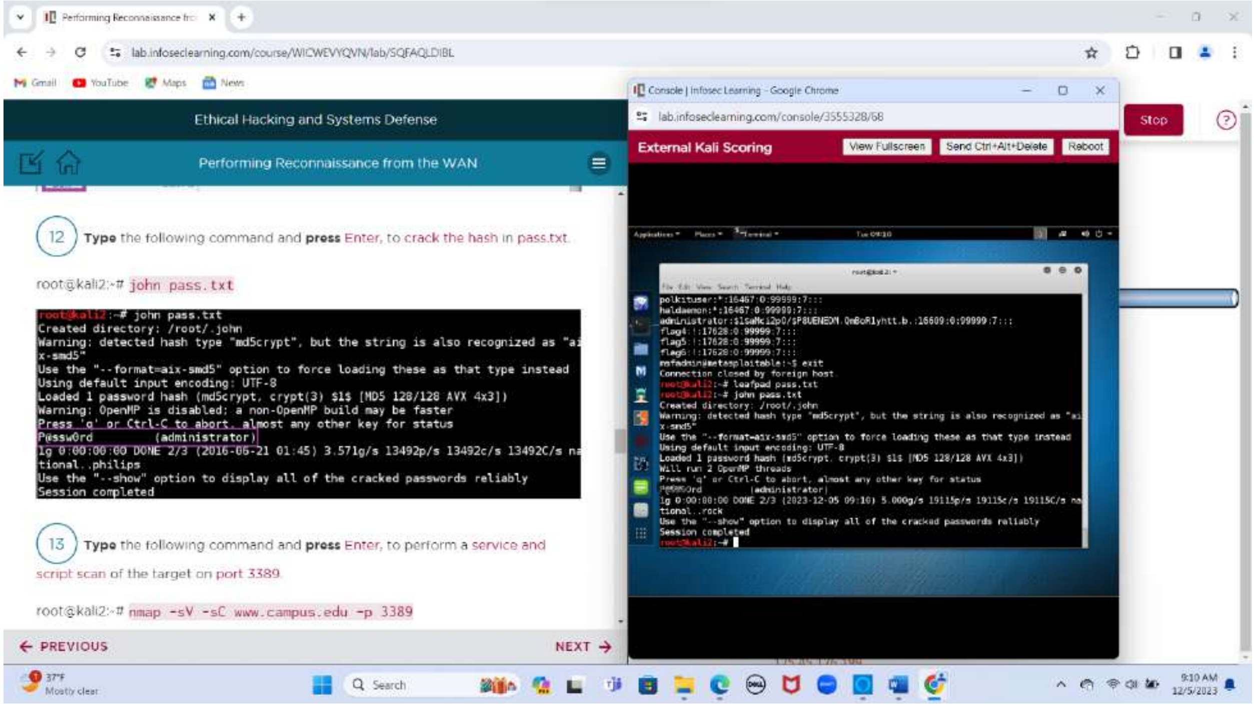
When asked for the password, **type** `msfadmin`, then **press** Enter.

⚠ **Note: The password will not be displayed for security purposes.**

```
msfadmin@metasploitable:~$ sudo tail /etc/shadow
sudo: unable to resolve host metasploitable
[sudo] password for msfadmin: msfadmin
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
snmp:*:15480:0:99999:7:::
gdm:*:16467:0:99999:7:::
messagebus:*:16467:0:99999:7:::
polkituser:*:16467:0:99999:7:::
```

```
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.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ id root
uid=0(root) gid=0(root) groups=0(root)
msfadmin@metasploitable:~$ id flag4
uid=444551(flag4) gid=444551(flag4) groups=444551(flag4)
msfadmin@metasploitable:~$ id flag5
uid=444778(flag5) gid=444778(flag5) groups=444778(flag5)
msfadmin@metasploitable:~$ id flag6
uid=616778(flag6) gid=616778(flag6) groups=616778(flag6)
msfadmin@metasploitable:~$ sudo tail /rtc/shadow
sudo: unable to resolve host metasploitable
[sudo] password for msfadmin:
tail: cannot open `/rtc/shadow' for reading: No such file or directory
msfadmin@metasploitable:~$ sudo tail /etc/shadow
```

Cracking the hash:



Performing Reconnaissance fro
lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
PREVIOUS
NEXT
37°F
Mostly clear
Search
9:10 AM
12/5/2023

12 **Type** the following command and **press** Enter, to crack the hash in pass.txt.

root@kali2:~# john pass.txt

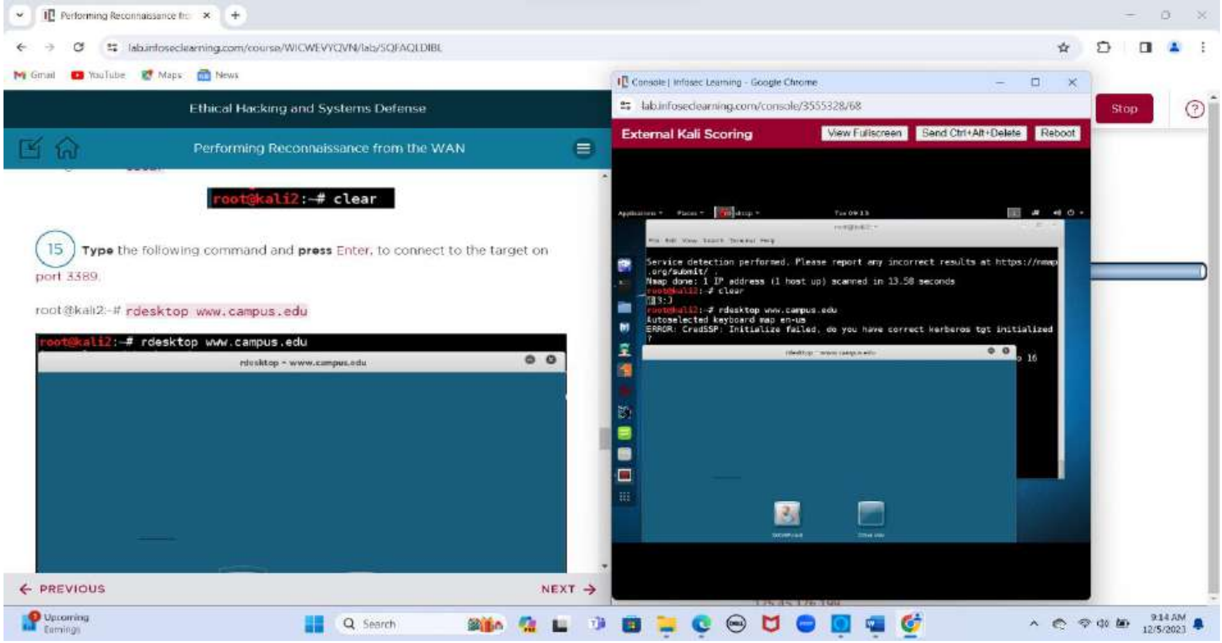
```
root@kali2:~# john pass.txt
Created directory: /root/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "ai
x-smd5"
Use the "--format=aix-smd5" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 128/128 AVX 4x3])
Warning: OpenMP is disabled; a non-OpenMP build may be faster
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd         (administrator)
1g 0:00:00:00 DONE 2/3 (2016-06-21 01:45) 3.571g/s 13492p/s 13492c/s 13492C/s na
tional..philips
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

13 **Type** the following command and **press** Enter, to perform a service and script scan of the target on port 3389.

root@kali2:~# nmap -sV -sC www.campus.edu -p 3389

```
polkituser:*:16467:0:99999:7:::
haldaemon:*:16467:0:99999:7:::
administrator:$1$aMc12p0/$P8UENEDM.QmBoR1yhtt.b.:16609:0:99999:7:::
flag4:!:17628:0:99999:7:::
flag5:!:17628:0:99999:7:::
flag6:!:17628:0:99999:7:::
msfadmin@metasploitable:~$ exit
Connection closed by foreign host.
root@kali2:~# leafpad pass.txt
root@kali2:~# john pass.txt
Created directory: /root/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "ai
x-smd5"
Use the "--format=aix-smd5" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 128/128 AVX 4x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd         (administrator)
1g 0:00:00:00 DONE 2/3 (2023-12-05 09:10) 5.000g/s 19115p/s 19115c/s 19115C/s na
tional..rock
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali2:~#
```

Connecting to target:



Performing Reconnaissance fro
lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
rdesktop - www.campus.edu
PREVIOUS
NEXT
Upcoming
Earnings
Search
9:14 AM
12/5/2023

```
root@kali2:~# clear
```

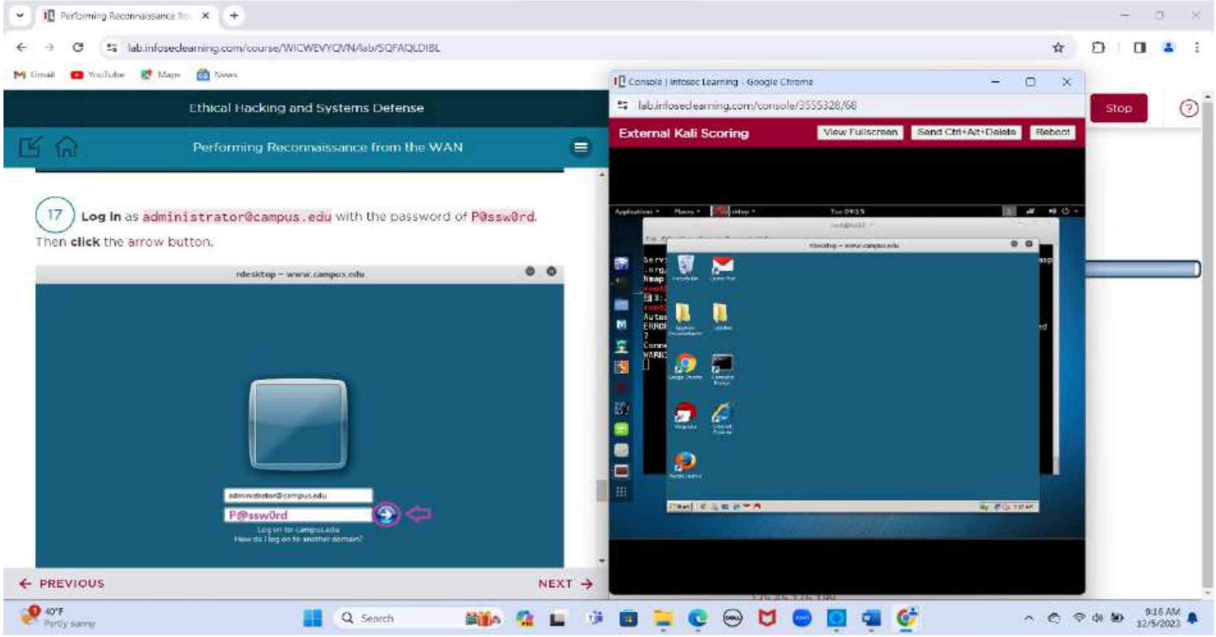
15 **Type** the following command and **press** Enter, to connect to the target on port 3389.

root@kali2:~# rdesktop www.campus.edu

```
root@kali2:~# rdesktop www.campus.edu
```

```
Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.58 seconds
root@kali2:~# clear
3:)
root@kali2:~# rdesktop www.campus.edu
Autoselected keyboard map en-us
ERROR: CredSSP: Initialize failed, do you have correct kerberos tgt initialized
?
```

Login to target:



Performing Reconnaissance fro
lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL
Gmail
YouTube
Maps
News
Ethical Hacking and Systems Defense
Performing Reconnaissance from the WAN
rdesktop – www.campus.edu
administrator@campus.edu
P@ssw0rd
Log on to campus.edu
How do I log on to another domain?
PREVIOUS
NEXT
Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/3555328/68
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Stop
40°F
Partly sunny
Search
9:16 AM
12/5/2023

17 **Log in** as `administrator@campus.edu` with the password of `P@ssw0rd`. Then **click** the arrow button.

This is the last screen before the end of the lab.