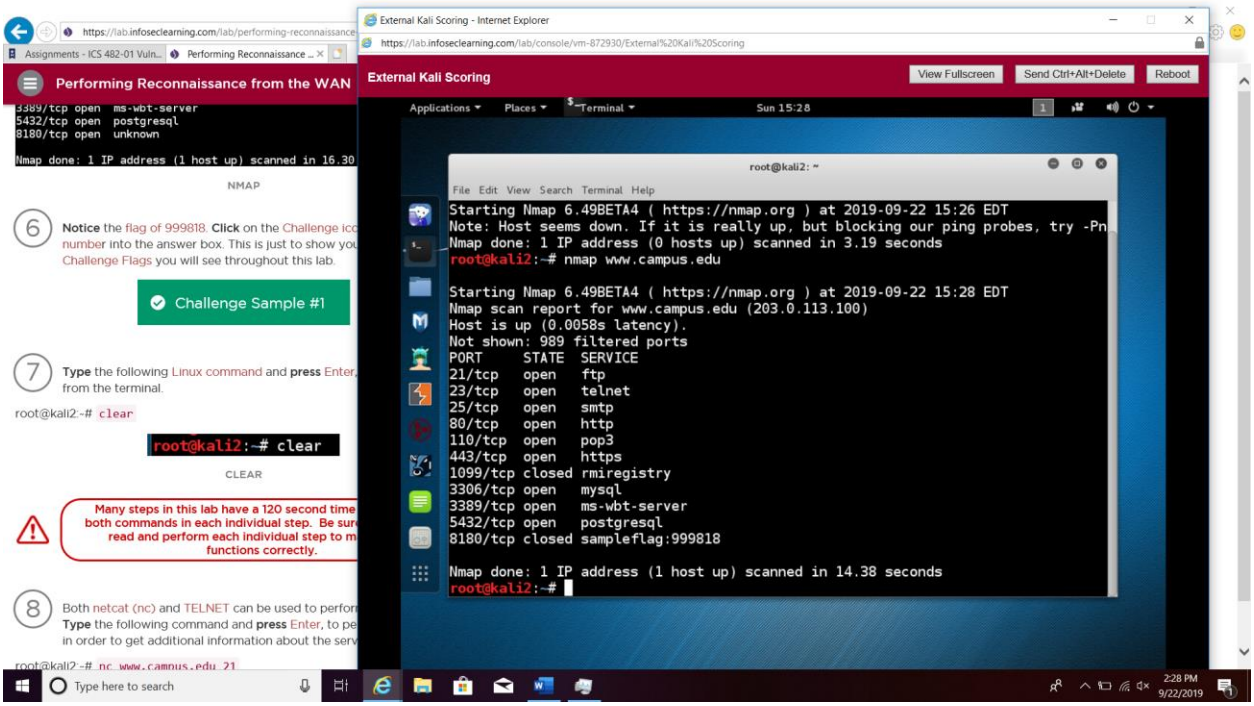
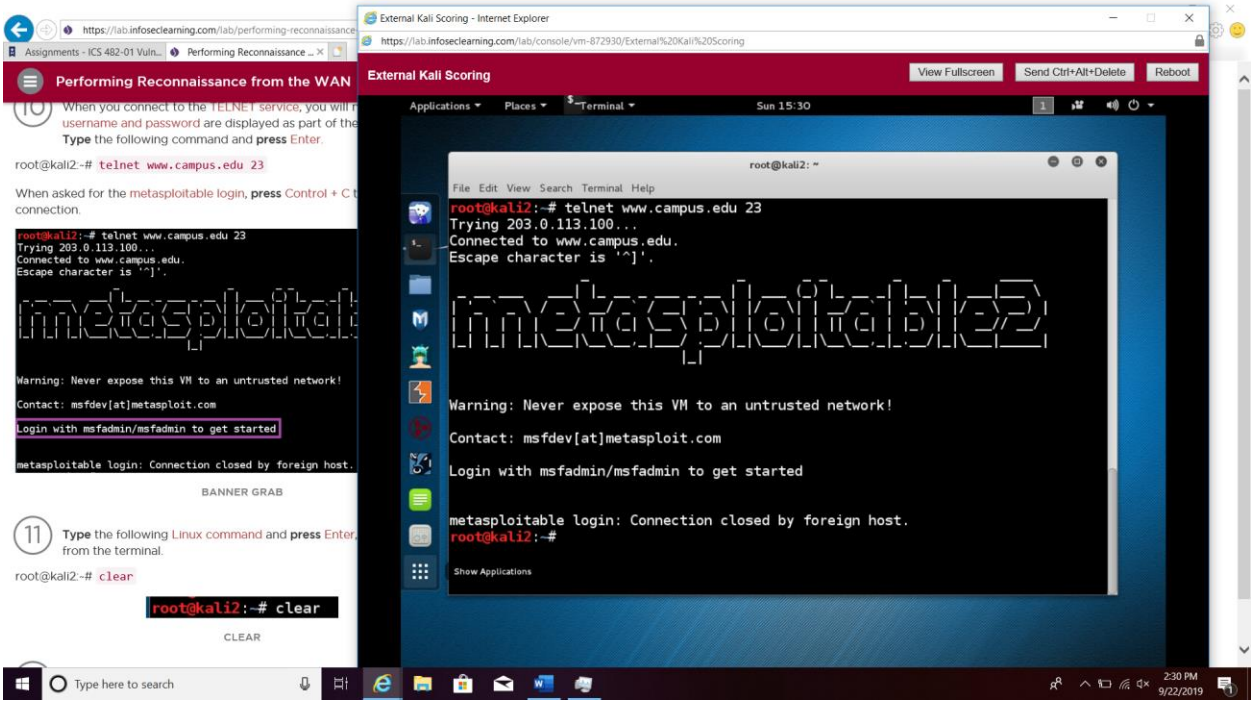
Ryan Brodsky

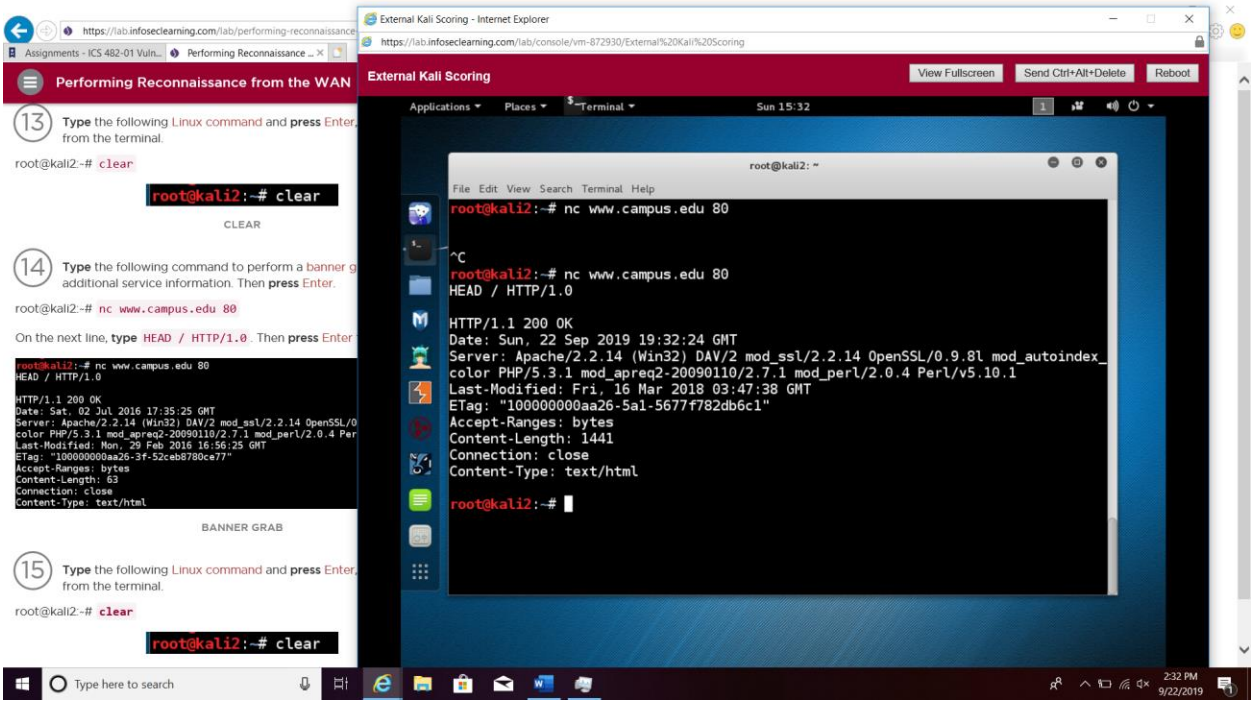
9/22/19

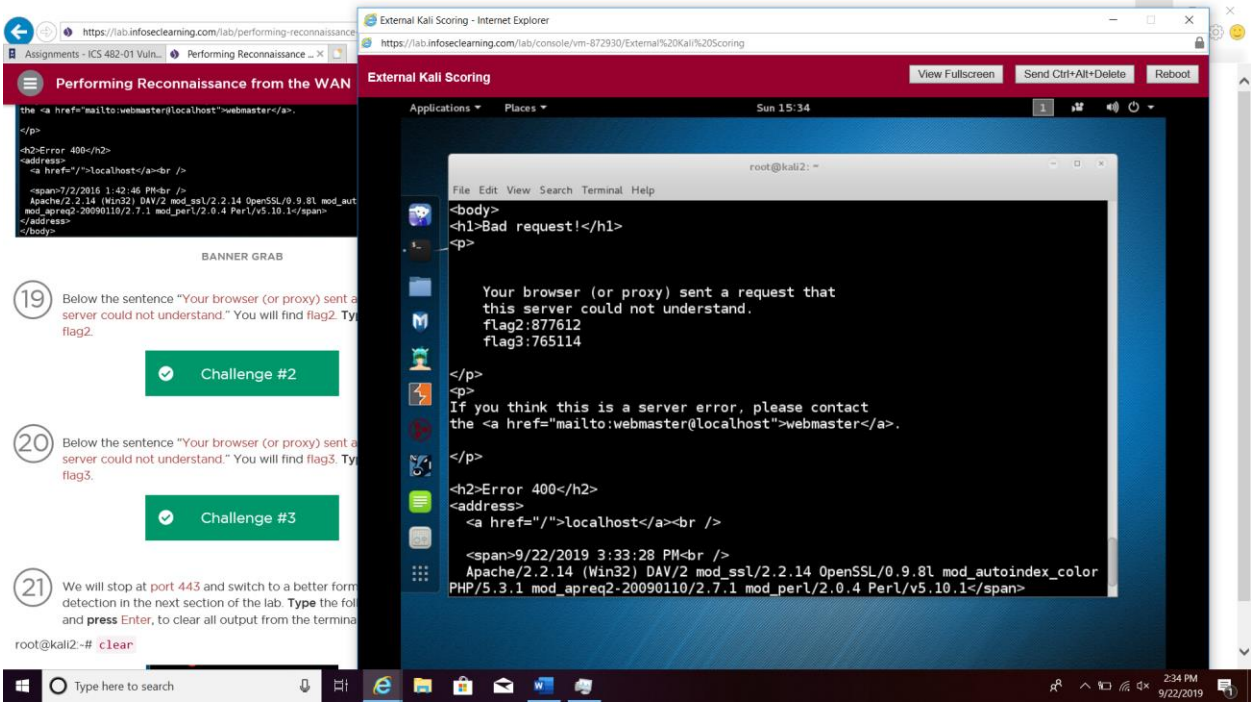
ICS 482

InfoSec Lab: Performing Reconnaissance from the WAN






Performing Reconnaissance from the WAN
13 Type the following Linux command and press Enter, from the terminal.
root@kali2:~# clear
root@kali2:~# clear
CLEAR
14 Type the following command to perform a banner g 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
color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Per
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
BANNER GRAB
15 Type the following Linux command and press Enter, from the terminal.
root@kali2:~# clear
root@kali2:~# clear
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
root@kali2: ~
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:~#
Type here to search
2:32 PM
9/22/2019

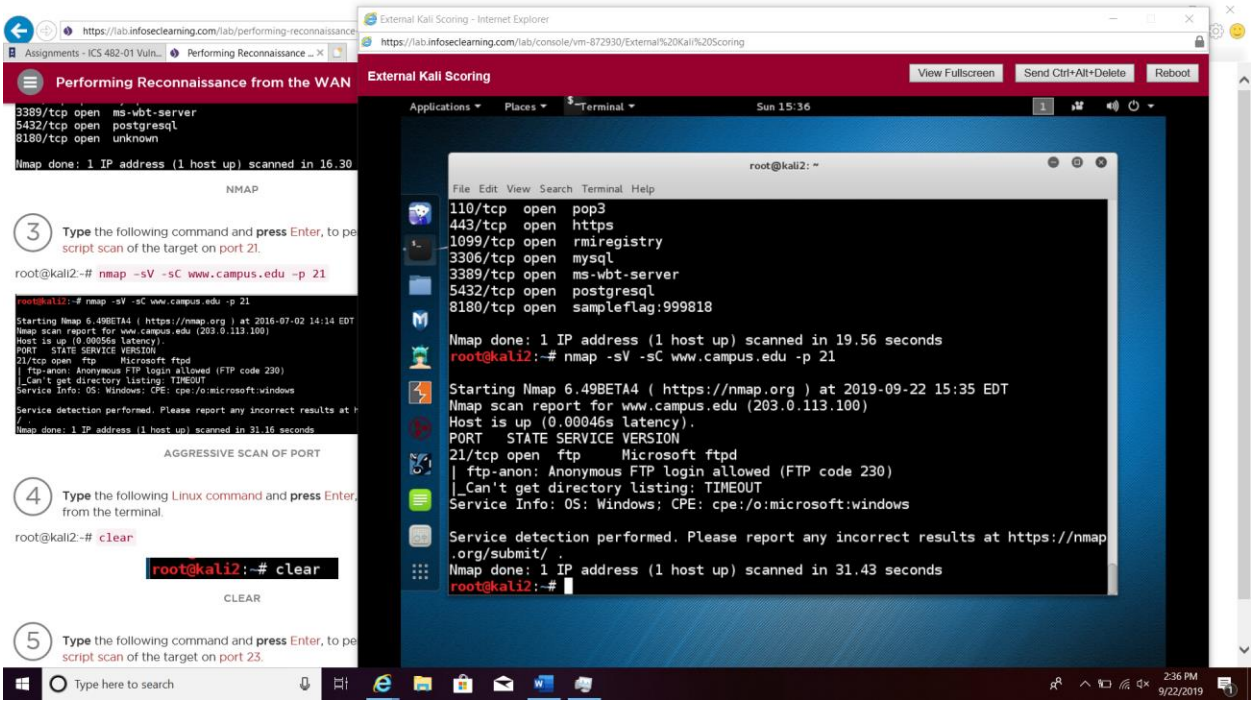

Performing Reconnaissance from the WAN
the webmaster.

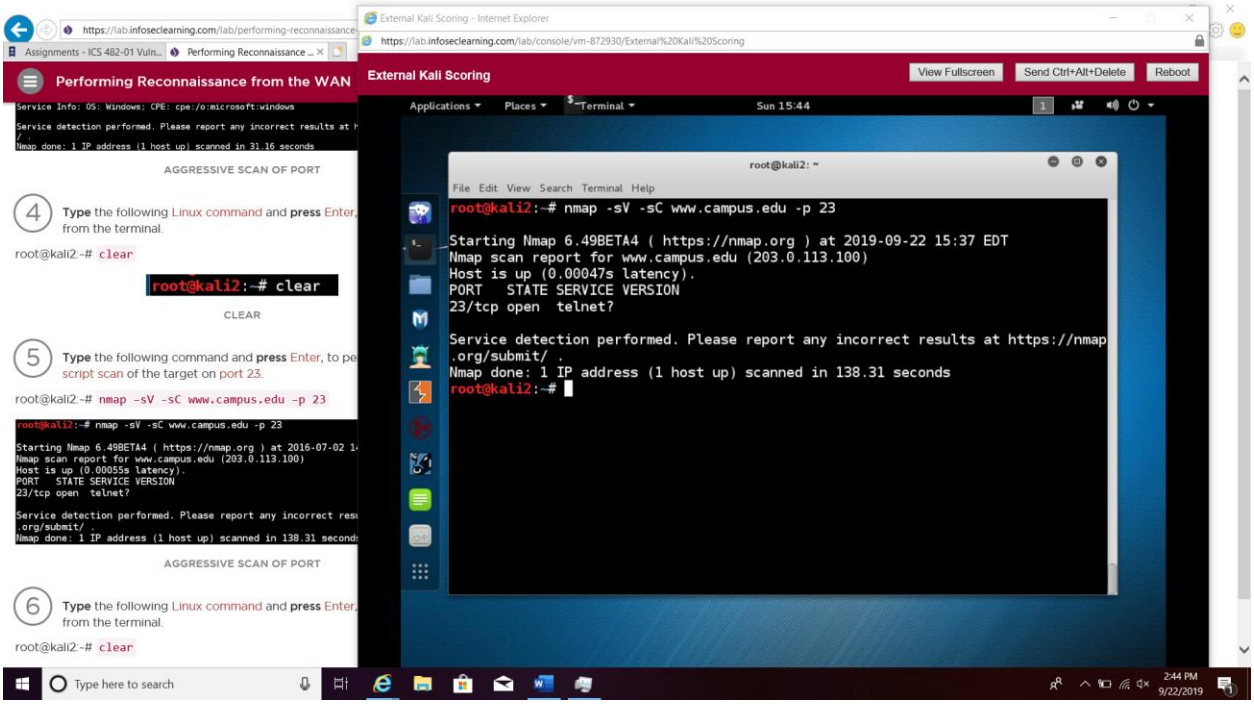
<h2>Error 400</h2>
<address>
localhost
7/2/2016 1:42:46 PM
Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_aut
mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
</address>
</body>
BANNER GRAB
19 Below the sentence "Your browser (or proxy) sent a server could not understand." You will find flag2. Ty flag2.
Challenge #2
20 Below the sentence "Your browser (or proxy) sent a server could not understand." You will find flag3. Ty 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 fol and press Enter, to clear all output from the termina
root@kali2:~# clear
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
Sun 15:34
root@kali2: ~
File Edit View Search Terminal Help
<body>
<h1>Bad request!</h1>

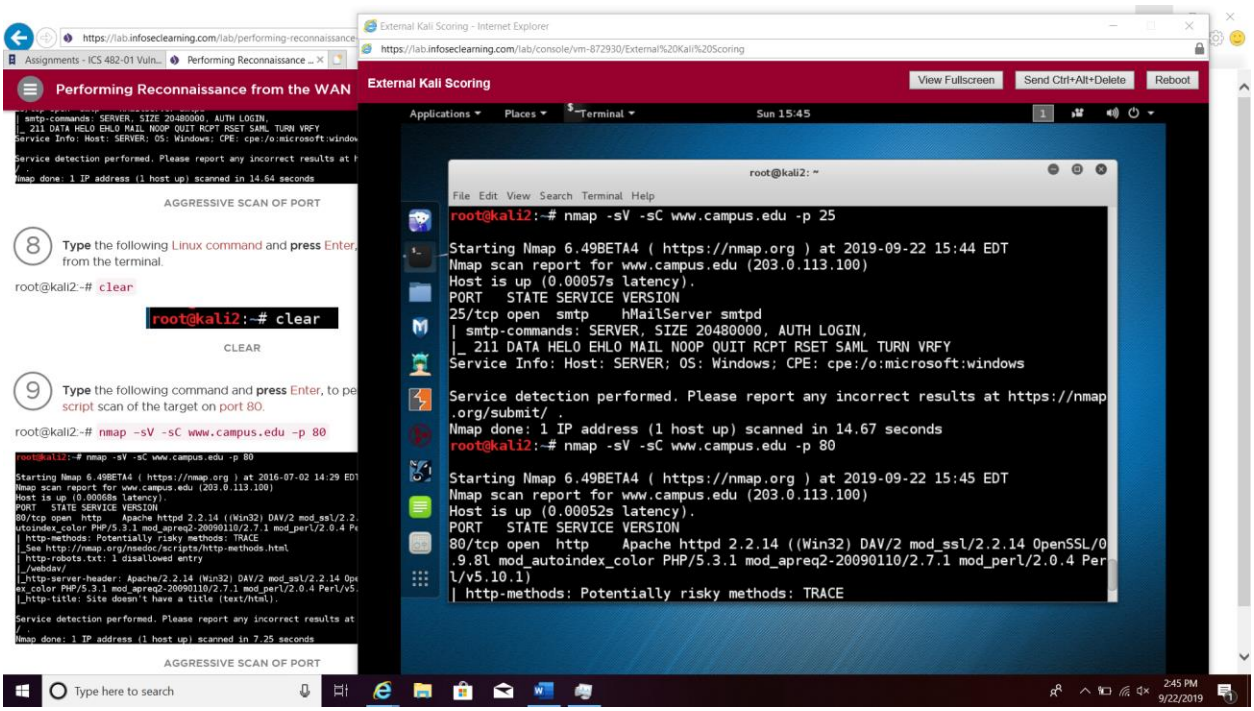
Your browser (or proxy) sent a request that
this server could not understand.
flag2:877612
flag3:765114

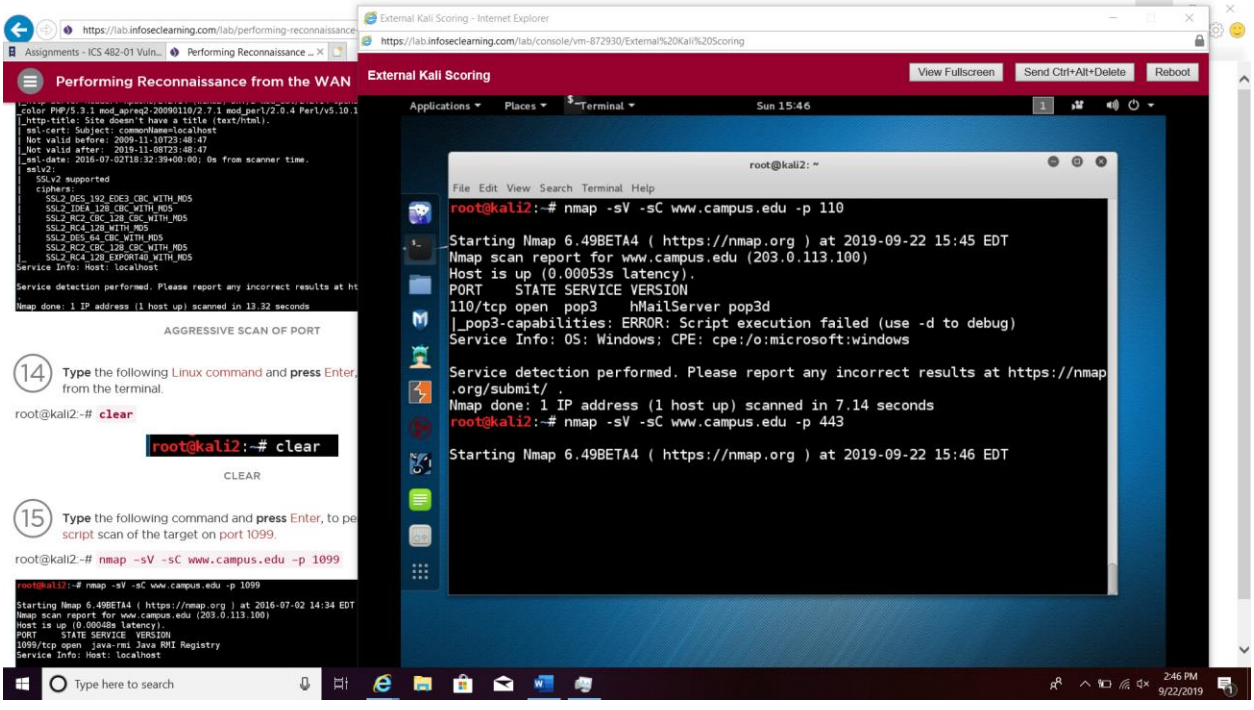
If you think this is a server error, please contact
the webmaster.

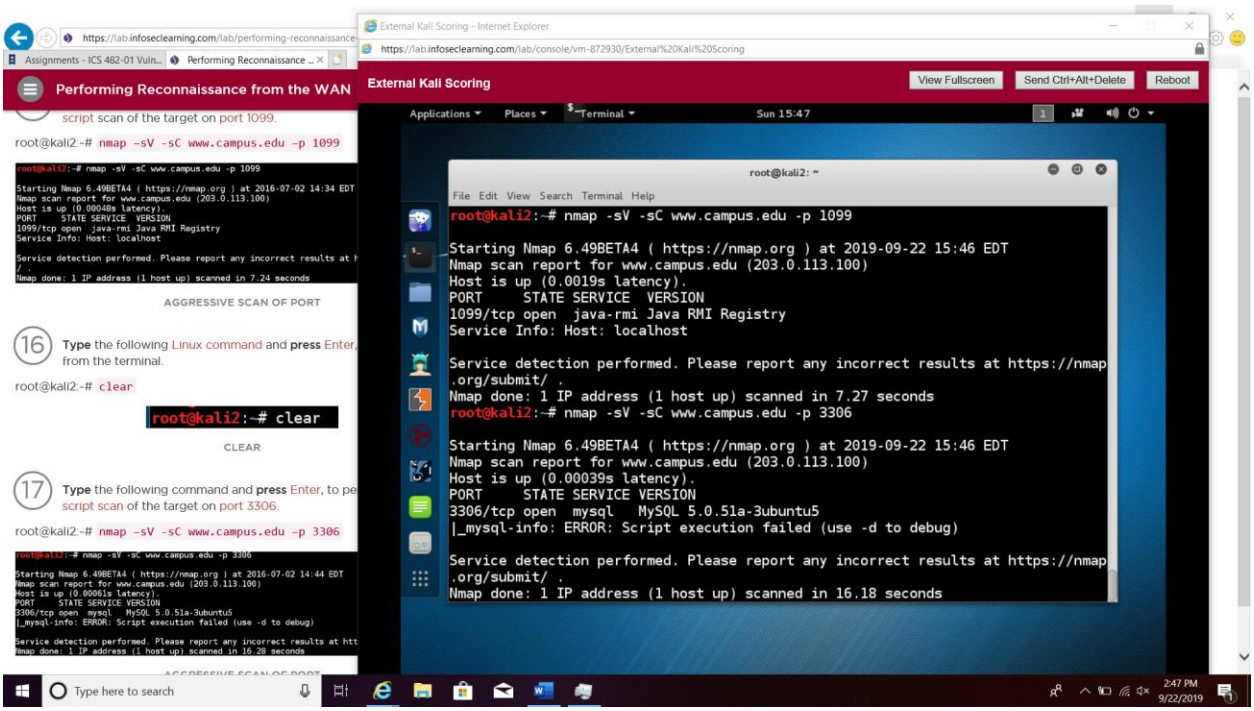
<h2>Error 400</h2>
<address>
localhost
9/22/2019 3:33:28 PM
Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color
PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
Type here to search
2:34 PM
9/22/2019

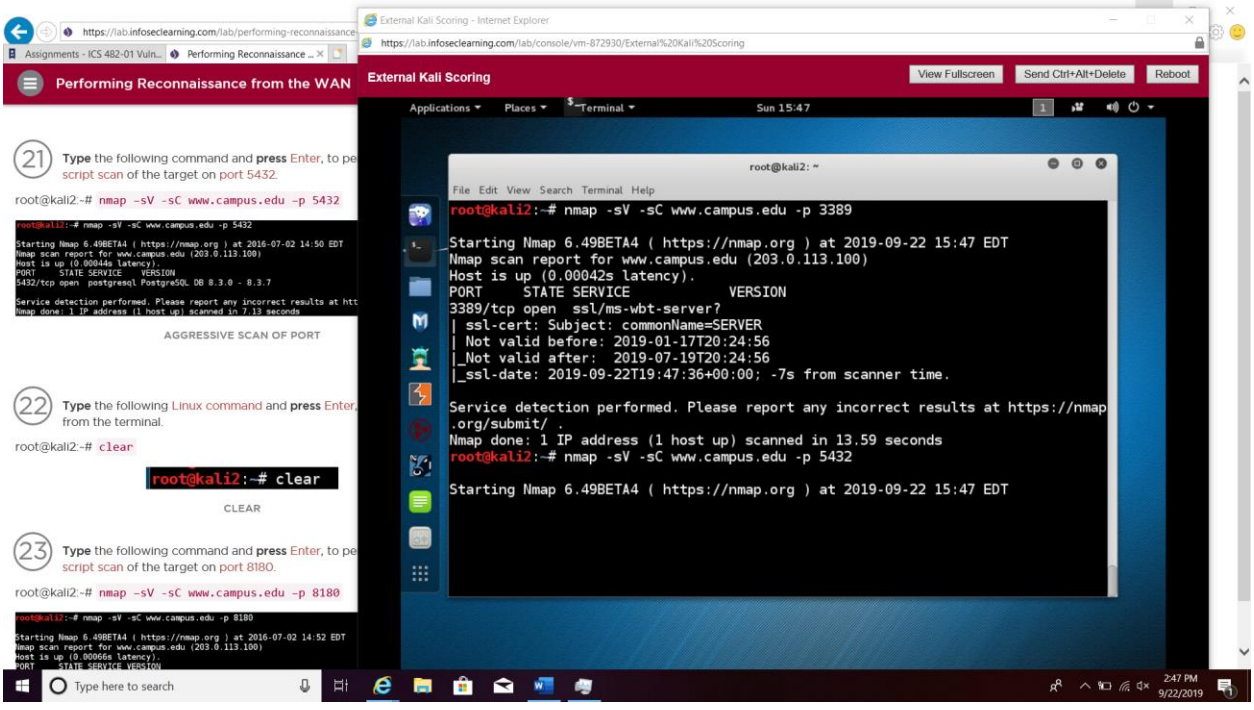

Performing Reconnaissance from the WAN
3389/tcp open ms-wbt-server
5432/tcp open postgresql
8180/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 16.30
NMAP
3 Type the following command and press Enter, to pe
script scan of the target on port 21.
root@kali2:~# nmap -sV -sC www.campus.edu -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 h
/ .
Nmap done: 1 IP address (1 host up) scanned in 31.16 seconds
AGGRESSIVE SCAN OF PORT
4 Type the following Linux command and press Enter,
from the terminal.
root@kali2:~# clear
root@kali2:~# clear
CLEAR
5 Type the following command and press Enter, to pe
script scan of the target on port 23.
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 15:36
root@kali2: ~
File Edit View Search Terminal Help
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 19.56 seconds
root@kali2:~# nmap -sV -sC www.campus.edu -p 21
Starting Nmap 6.49BETA4 (https://nmap.org) at 2019-09-22 15:35 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00046s 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 31.43 seconds
root@kali2:~#
Type here to search
2:36 PM
9/22/2019

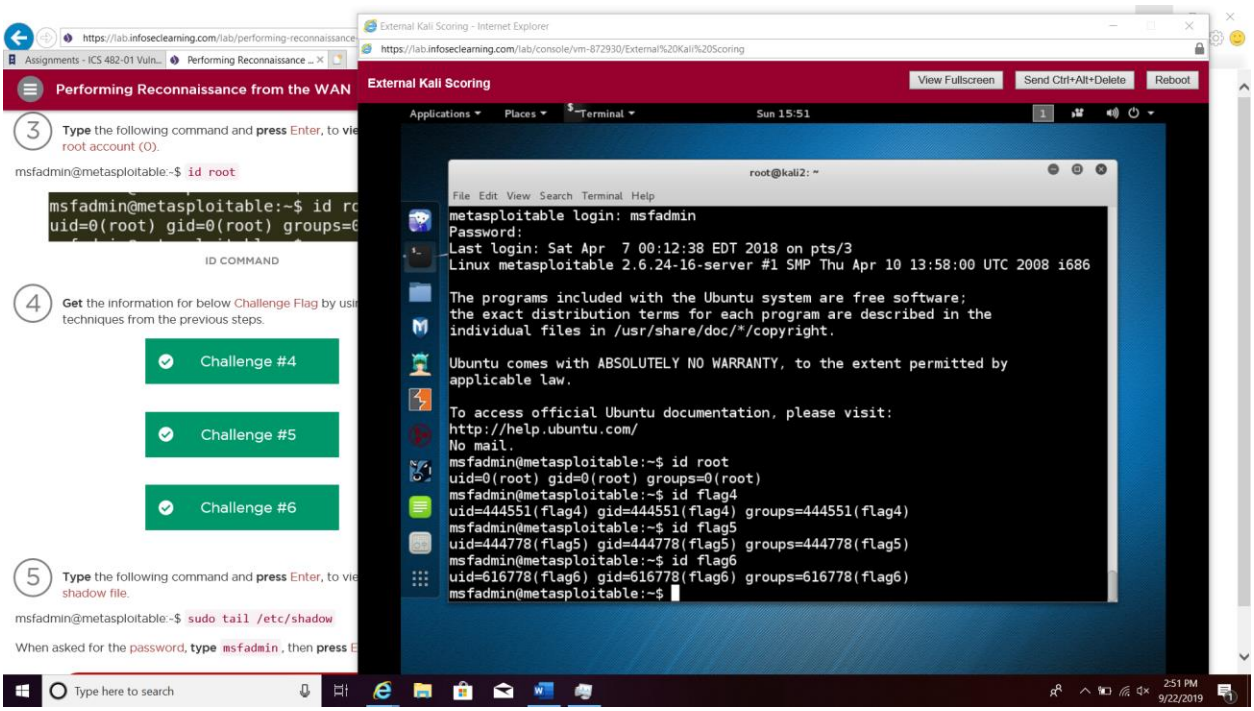

Performing Reconnaissance from the WAN
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at h
/ .
Nmap done: 1 IP address (1 host up) scanned in 31.16 seconds
AGGRESSIVE SCAN OF PORT
4 Type the following Linux command and press Enter,
from the terminal.
root@kali2:~# clear
root@kali2:~# clear
CLEAR
5 Type the following command and press Enter, to pe
script scan of the target on port 23.
root@kali2:~# nmap -sV -sC www.campus.edu -p 23
Starting Nmap 6.49BETA4 (https://nmap.org) at 2016-07-02 1
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00055s latency).
PORT STATE SERVICE VERSION
23/tcp open telnet?
Service detection performed. Please report any incorrect resu
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 138.31 second
AGGRESSIVE SCAN OF PORT
6 Type the following Linux command and press Enter,
from the terminal.
root@kali2:~# clear
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 15:44
root@kali2: ~
File Edit View Search Terminal Help
root@kali2:~# nmap -sV -sC www.campus.edu -p 23
Starting Nmap 6.49BETA4 (https://nmap.org) at 2019-09-22 15:37 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00047s latency).
PORT STATE SERVICE VERSION
23/tcp open telnet?
Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 138.31 seconds
root@kali2:~#
Type here to search
2:44 PM
9/22/2019

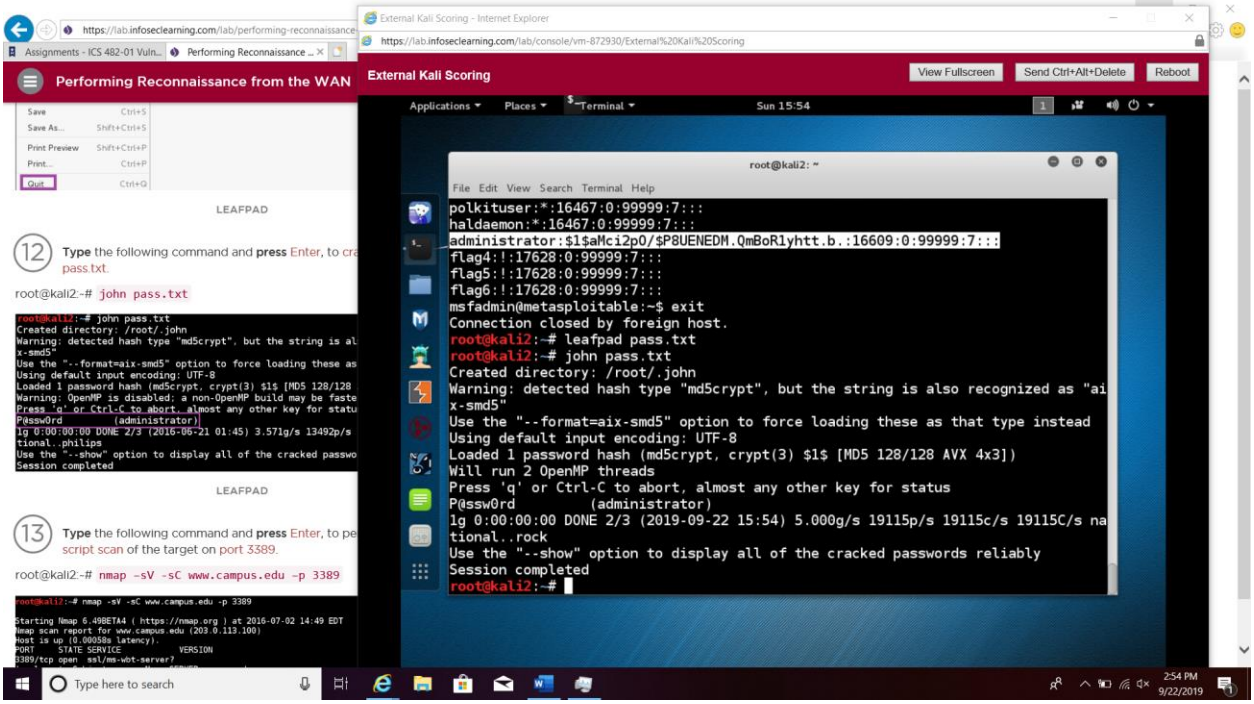

Performing Reconnaissance from the WAN
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Terminal
Sun 15:45
root@kali2: ~
File Edit View Search Terminal Help
root@kali2:~# nmap -sV -sC www.campus.edu -p 25
Starting Nmap 6.49BETA4 (https://nmap.org) at 2019-09-22 15:44 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-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 14.67 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
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 pe script scan of the target on port 80.
root@kali2:~# nmap -sV -sC www.campus.edu -p 80
AGGRESSIVE SCAN OF PORT
Type here to search
2:45 PM
9/22/2019

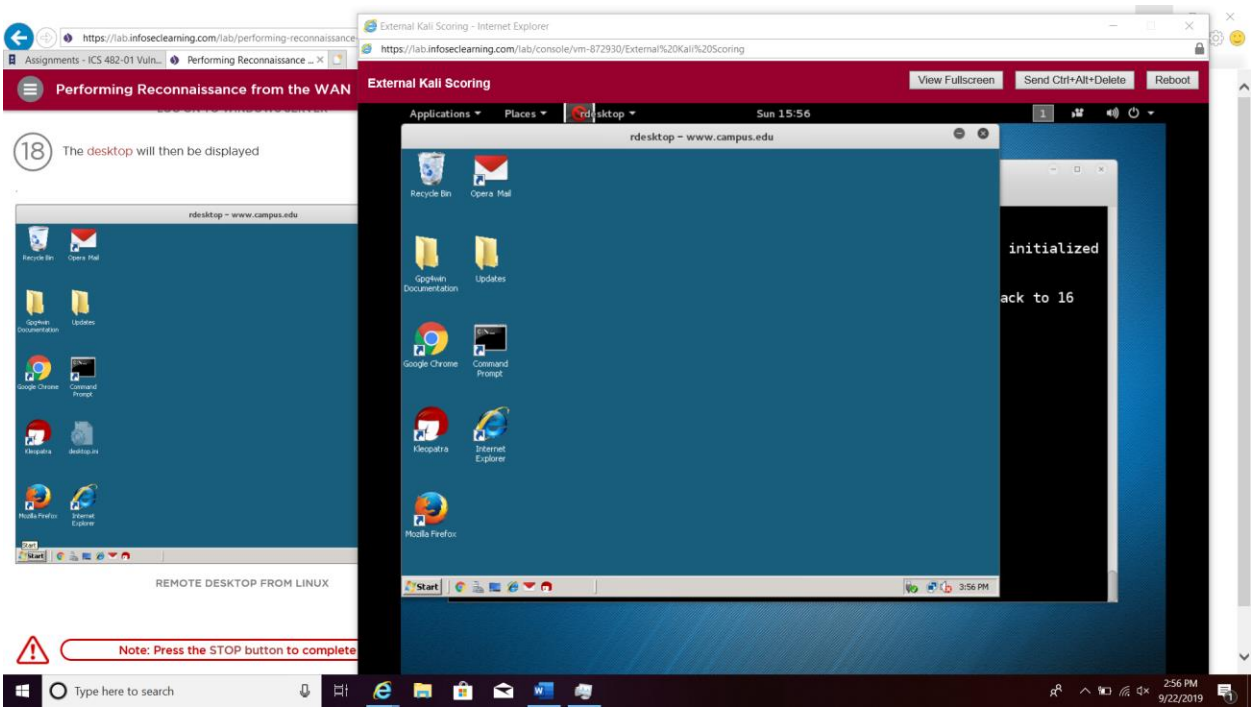

Performing Reconnaissance from the WAN
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Terminal
Sun 15:46
root@kali2: ~
File Edit View Search Terminal Help
root@kali2:~# nmap -sV -sC www.campus.edu -p 110
Starting Nmap 6.49BETA4 (https://nmap.org) at 2019-09-22 15:45 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
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 pe script scan of the target on port 1099.
root@kali2:~# nmap -sV -sC www.campus.edu -p 1099
AGGRESSIVE SCAN OF PORT
Type here to search
2:46 PM
9/22/2019


Performing Reconnaissance from the WAN
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
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
root@kali2:~# clear
AGGRESSIVE SCAN OF PORT
CLEAR


Performing Reconnaissance from the WAN
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
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
root@kali2:~# clear
AGGRESSIVE SCAN OF PORT
CLEAR


Performing Reconnaissance from the WAN
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 15:51
root@kali2: ~
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:~$
Challenge #4
Challenge #5
Challenge #6
msfadmin@metasploitable:~$ sudo tail /etc/shadow
Type here to search
2:51 PM
9/22/2019


Performing Reconnaissance from the WAN
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 15:54
root@kali2: ~
File Edit View Search Terminal Help
polkituser:*:16467:0:99999:7:::
haldaemon:*:16467:0:99999:7:::
administrator:1aMci2pO/$P8UENEDM.QmBoR1yhtt.b.:16609:0:99999:7:::
flag4:!:17628:0:99999:7:::
flag5:!:17628:0:99999:7:::
flag6:!:17628:0:99999:7:::
msfadmin@metasploitable:~$ 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 (2019-09-22 15:54) 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:~#
Save Ctrl+S
Save As... Shift+Ctrl+S
Print Preview Shift+Ctrl+P
Print... Ctrl+P
Quit Ctrl+Q
LEAFPAD
root@kali2:~# john pass.txt
Created directory: /root/.john
Warning: detected hash type "md5crypt", but the string is al
x-smd5"
Use the "--format=aix-smd5" option to force loading these as
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 faste
Press 'q' or Ctrl-C to abort, almost any other key for statu
P@ssw0rd (administrator)
1g 0:00:00:00 DONE 2/3 (2016-06-21 01:45) 3.571g/s 13492p/s
tional..philips
Use the "--show" option to display all of the cracked passwo
Session completed
LEAFPAD
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 (0.00050s latency).
PORT STATE SERVICE VERSION
3389/tcp open ssl/ms-wbt-server?
Type here to search
2:54 PM
9/22/2019


Performing Reconnaissance from the WAN
18 The desktop will then be displayed
REMOTE DESKTOP FROM LINUX
Note: Press the STOP button to complete
External Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Sun 15:56
rdesktop – www.campus.edu
Recycle Bin
Opera Mail
Gpg4win Documentation
Updates
Google Chrome
Command Prompt
Kleopatra
Internet Explorer
Mozilla Firefox
initialized
ack to 16
Start
3:56 PM
Type here to search
2:56 PM
9/22/2019