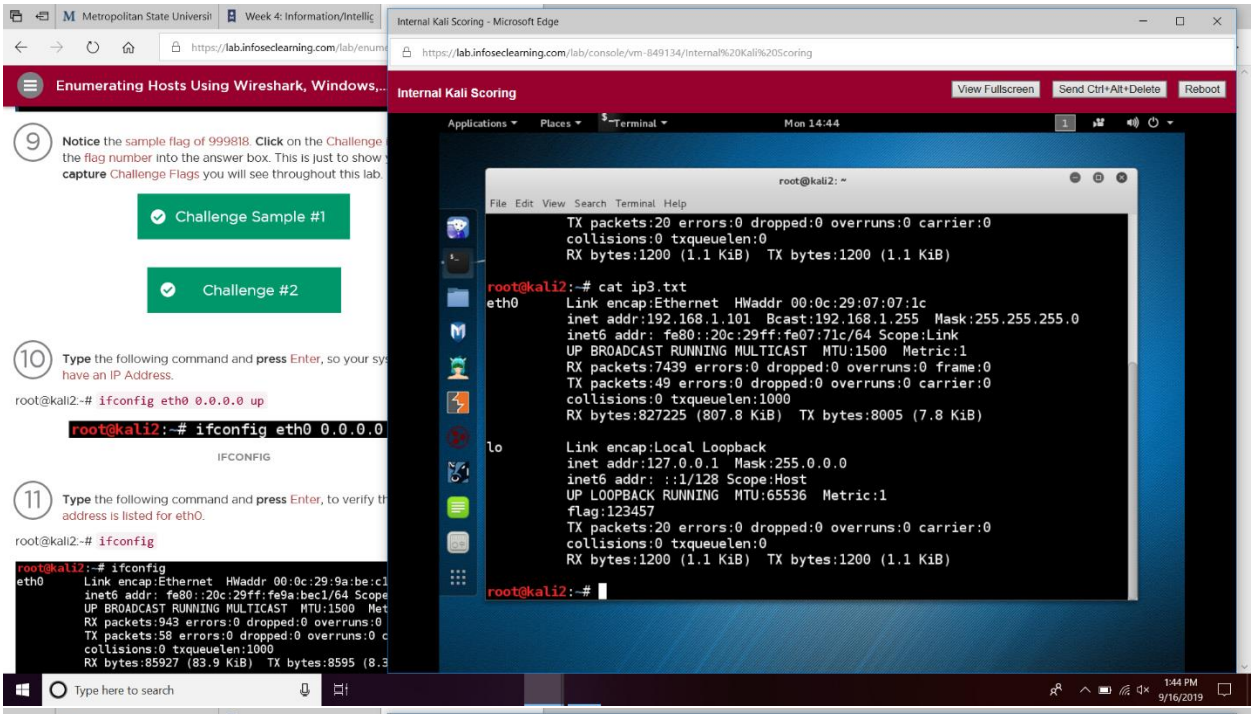
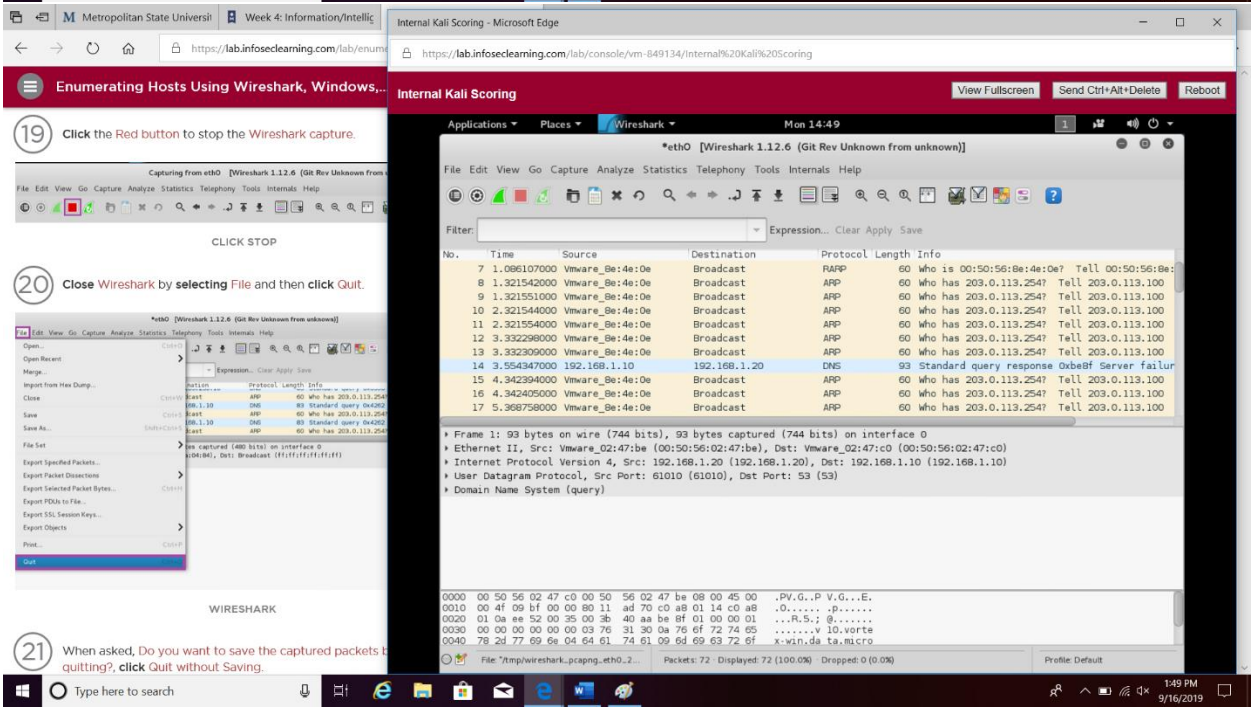
Ryan Brodsky

ICS 482

9/16/19

InfoSec Lab: Enumerating Hosts Using Wireshark, Windows, and Linux Commands





Enumerating Hosts Using Wireshark, Windows,...

RESOLV.CONF

27 **Type** the following command to view the IP Address configuration in the file

root@kali2:~# `cat /etc/resolv.conf.backup1`

```
root@kali2:~# cat  /etc/resolv.conf.backup1
# Generated by NetworkManager
search localdomain
nameserver 172.16.200.2
```

RESOLV.CONF

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

Challenge #3

29 **Type** the following command and **press** Enter, to set the DNS server.

root@kali2:~# `echo nameserver 192.168.1.10 > /etc/resolv.conf`

```
root@kali2:~# echo nameserver 192.168.1.10 > /etc/resolv.conf
```

DNS SERVER

30 **Type** the following command to view the new /etc/resolv.conf file.

root@kali2:~# `cat /etc/resolv.conf`

Internal Kali Scoring - Microsoft Edge

https://lab.infoseclearning.com/lab/console/vm-849134/Internal%20Kali%20Scoring

Internal Kali Scoring — View Fullscreen — Send Ctrl+Alt+Delete

Applications — Places — Terminal — Mon 14:52

root@kali2: ~

File Edit View Search Terminal Help

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:38 errors:0 dropped:0 overruns:0 frame:0
          TX packets:38 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2942 (2.8 KiB)  TX bytes:2942 (2.8 KiB)

root@kali2:~# ifconfig eth0 192.168.1.101 netmask 255.255.255.0
root@kali2:~# route add default gw 192.168.1.254
root@kali2:~# cp /etc/resolv.conf /etc/resolv.conf.backup1
root@kali2:~# cat /etc/resolv.conf.backup1
# Generated by NetworkManager
search localdomain
nameserver 172.16.200.2

root@kali2:~# cat /etc/resolv.conf.backup2
# Generated by NetworkManager
search localdomain
nameserver 172.16.200.2
flag:334451
root@kali2:~#
```

Type here to search — 1:52 PM 9/16/2019

Enumerating Hosts Using Wireshark, Windows,...

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

Challenge #3

29 **Type** the following command and **press** Enter, to set the DNS server.

root@kali2:~# `echo nameserver 192.168.1.10 > /etc/resolv.conf`

```
root@kali2:~# echo nameserver 192.168.1.10 > /etc/resolv.conf
```

DNS SERVER

30 **Type** the following command to view the new /etc/resolv.conf file.

root@kali2:~# `cat /etc/resolv.conf`

```
root@kali2:~# cat /etc/resolv.conf
nameserver 8.8.8.8
```

DNS SERVER

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

Challenge #4

Internal Kali Scoring - Microsoft Edge

https://lab.infoseclearning.com/lab/console/vm-849134/Internal%20Kali%20Scoring

Internal Kali Scoring — View Fullscreen — Send Ctrl+Alt+Delete

Applications — Places — Terminal — Mon 14:56

root@kali2: ~

File Edit View Search Terminal Help

```
host.conf                 postgresql-common   X11
hostname                  ppp                 xdg
hosts                     profile             xml
hosts.allow               profile.d           xpdf
hosts.deny                protocols           xprobe2
iceweasel                 proxychains.conf    zsh
root@kali2:/etc# cd ..
root@kali2:/# ls
0     dev   initrd.img  live-build  mnt   root  srv  usr
bin   etc   lib         lost+found  opt   run   sys  var
boot  home  lib64       media       proc  sbin  tmp  vmlinuz
root@kali2:/# cd root
root@kali2:~# ls
armitage              Downloads  sampleflag.txt
armitage150813.tgz    flag5.txt  Templates
bad.exe               hi.txt     test.txt
bye.txt               ip2.txt    Videos
capture.cap           ip3.txt    VMwareTools-10.0.6-3560309.tar.gz
Desktop               Music      vmware-tools-distrib
Documents             Pictures
root@kali2:~# cat /etc/resolv.flag
flag:888999
root@kali2:~#
```

Type here to search — 1:56 PM 9/16/2019

techniques from the previous steps.

Challenge #4

32 **Type** the following command and **press** Enter, to verify that the correct IPv4 address is listed for eth0.

root@kali2:~# `ifconfig`

```
root@kali2:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:9a:be:c1
          inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe9a:bec1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:906 errors:0 dropped:0 overruns:0 frame:0
          TX packets:56 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:82563 (80.6 KiB)  TX bytes:8475 (8.2 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:22 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1358 (1.3 KiB)  TX bytes:1358 (1.3 KiB)
```

IFCONFIG

BACK NEXT

Internal Kali Scoring - Microsoft Edge

https://lab.infoseclearning.com/lab/console/vm-849134/Internal%20Kali%20Scoring

Internal Kali Scoring — View Fullscreen — Send Ctrl+Alt+Delete

Applications — Places — Terminal — Mon 14:57

root@kali2: ~

File Edit View Search Terminal Help

```
root@kali2:~# cat /etc/resolv.flag
flag:888999
root@kali2:~# ifcongfig
bash: ifcongfig: command not found
root@kali2:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:8e:e9:ae
          inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe8e:e9ae/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1760 errors:0 dropped:0 overruns:0 frame:0
          TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:112908 (110.2 KiB)  TX bytes:16001 (15.6 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:38 errors:0 dropped:0 overruns:0 frame:0
          TX packets:38 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2942 (2.8 KiB)  TX bytes:2942 (2.8 KiB)

root@kali2:~#
```

Type here to search — 1:57 PM 9/16/2019

```
administrator  Disk           Home Directo
opt            Disk
tmp            Disk           oh noes!
The command completed successfully.
```

NET VIEW COMMAND

Challenge #5

Challenge #6

12 Attempt to enumerate the IP and MAC Address of the machine na server. **Type** the following command, then **press** Enter.

C:\Windows\System32> `nbtstat -a server`

```
C:\Windows\System32>nbtstat -a server

Ethernet0:
Node IpAddress: [192.168.1.20] Scope Id: []

            NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    SERVER         <00>  UNIQUE      Registered
    CAMPUS         <00>  GROUP       Registered
```

Internal Windows 10 Scoring - Microsoft Edge

https://lab.infoseclearning.com/lab/console/vm-849136/Internal%20Windows%2010%20Scoring

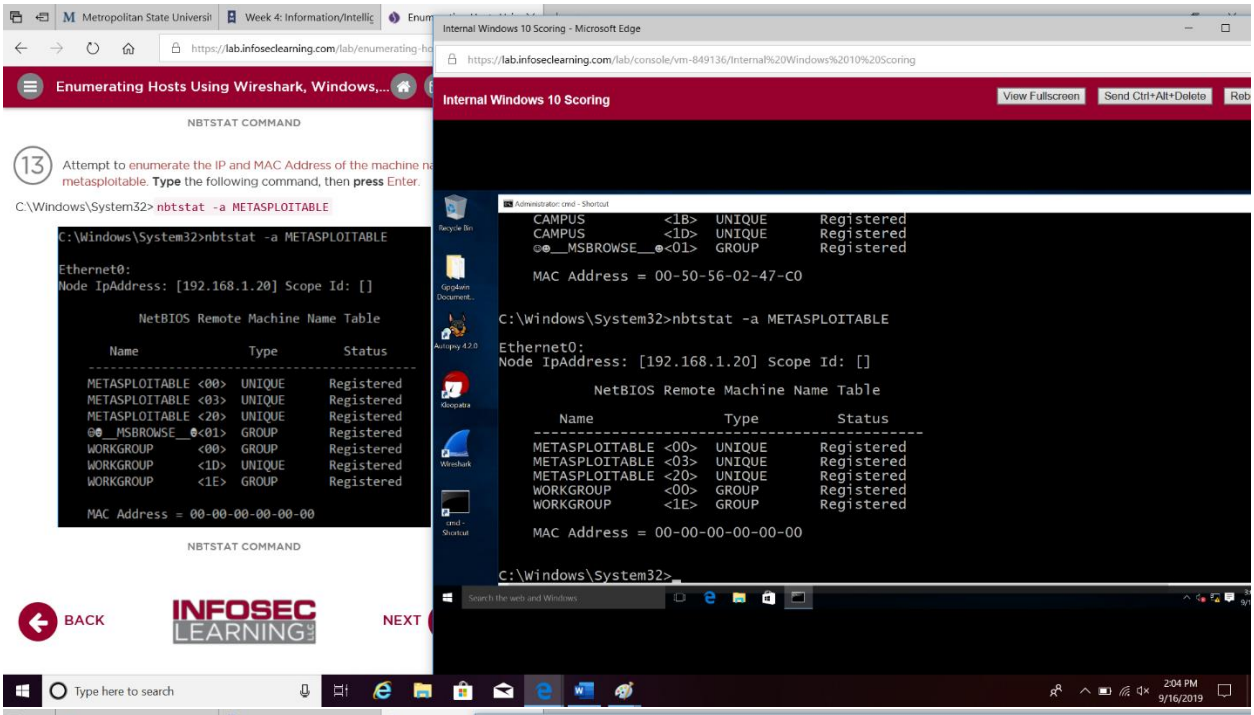
Internal Windows 10 Scoring — View Fullscreen — Send Ctrl+Alt+Delete

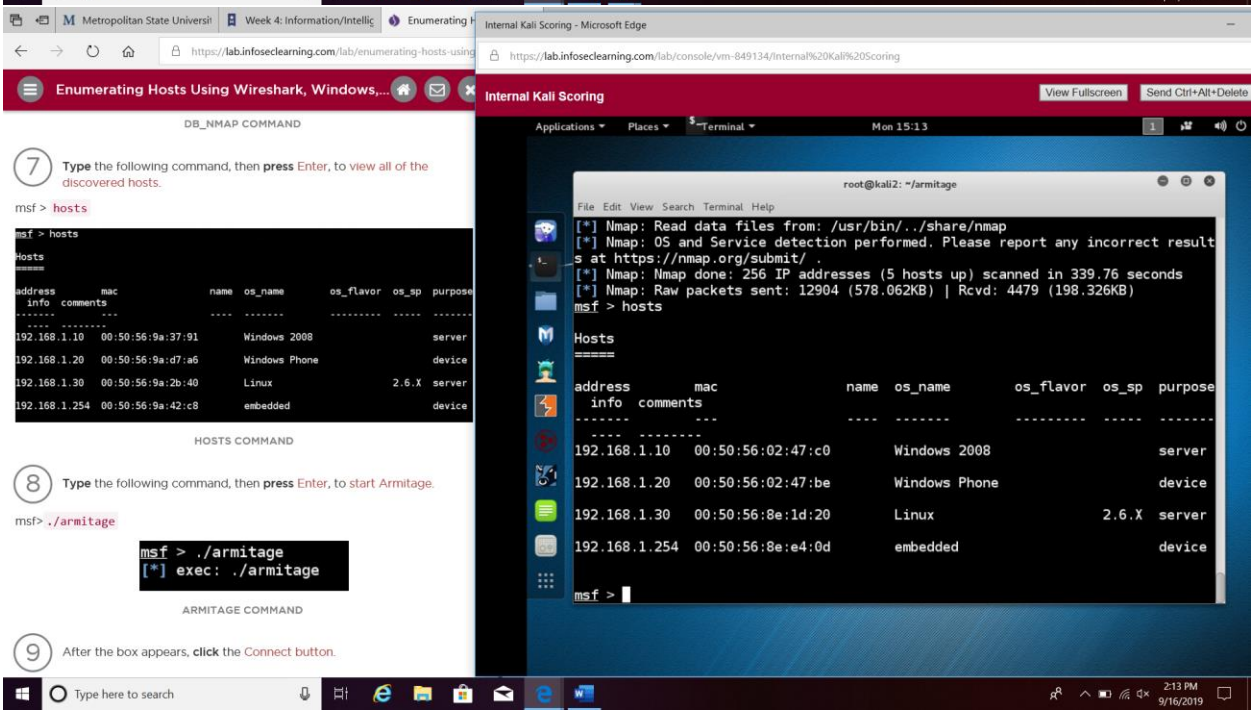
Administrator: cmd - Shortcut

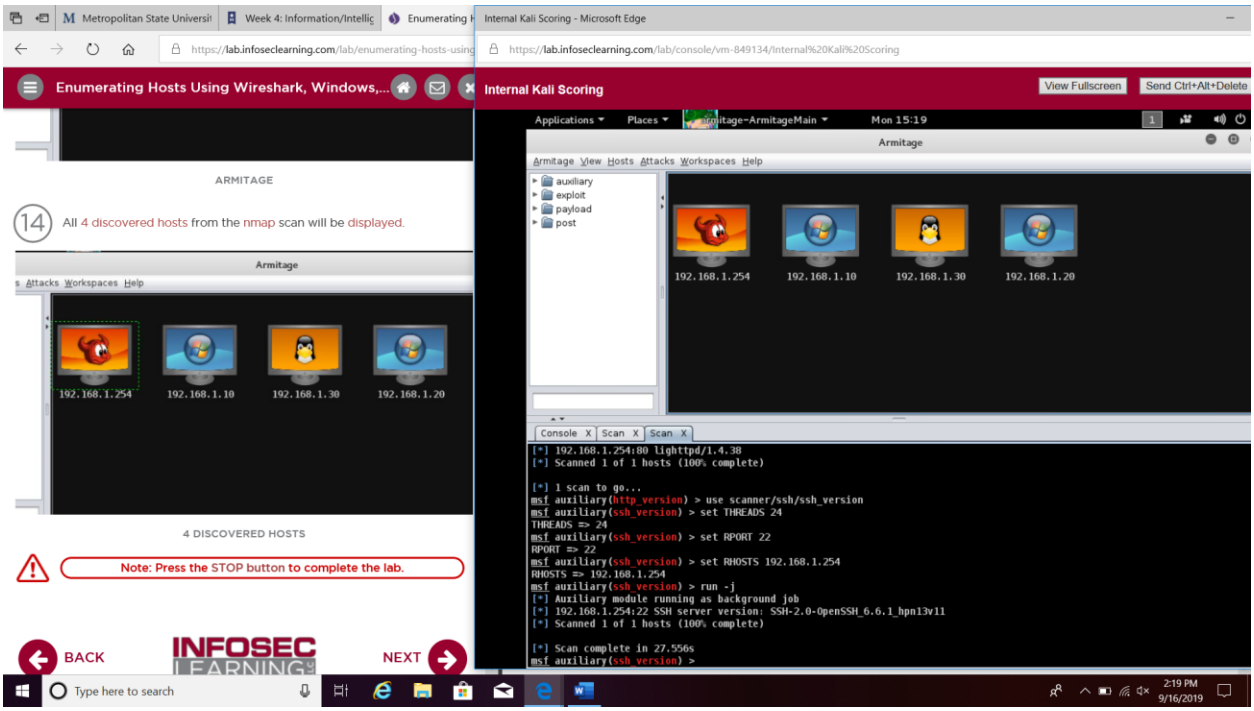
```
Share name  Type  Used as  Comment

-------------------------------------------------------------------------------
flag5       Disk           flag5:571444
flag6       Disk           flag6:333459
share       Disk
The command completed successfully.


C:\Windows\System32>net view concord
Shared resources at concord


Share name  Type  Used as  Comment

-------------------------------------------------------------------------------
flag5       Disk           flag5:571444
flag6       Disk           flag6:333459
share       Disk
The command completed successfully.


C:\Windows\System32>_
```

Search the web and Windows

Type here to search — 2:02 PM 9/16/2019


Metropolitan State Universit
Week 4: Information/Intellig
https://lab.infoseclearning.com/lab/enumerating-ho
Enumerating Hosts Using Wireshark, Windows,...
NBTSTAT COMMAND
13
Attempt to enumerate the IP and MAC Address of the machine na
metasploitable. Type the following command, then press Enter.
C:\Windows\System32> nbtstat -a METASPLOITABLE
C:\Windows\System32>nbtstat -a METASPLOITABLE
Ethernet0:
Node IpAddress: [192.168.1.20] Scope Id: []
NetBIOS Remote Machine Name Table
Name Type Status
METASPLOITABLE <00> UNIQUE Registered
METASPLOITABLE <03> UNIQUE Registered
METASPLOITABLE <20> UNIQUE Registered
@@__MSBROWSE__@<01> GROUP Registered
WORKGROUP <00> GROUP Registered
WORKGROUP <1D> UNIQUE Registered
WORKGROUP <1E> GROUP Registered
MAC Address = 00-00-00-00-00-00
NBTSTAT COMMAND
BACK
INFOSEC LEARNING
NEXT
Internal Windows 10 Scoring - Microsoft Edge
https://lab.infoseclearning.com/lab/console/vm-849136/Internal%20Windows%2010%20Scoring
Internal Windows 10 Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Administrator: cmd - Shortcut
CAMPUS <1B> UNIQUE Registered
CAMPUS <1D> UNIQUE Registered
@@__MSBROWSE__@<01> GROUP Registered
MAC Address = 00-50-56-02-47-C0
C:\Windows\System32>nbtstat -a METASPLOITABLE
Ethernet0:
Node IpAddress: [192.168.1.20] Scope Id: []
NetBIOS Remote Machine Name Table
Name Type Status
METASPLOITABLE <00> UNIQUE Registered
METASPLOITABLE <03> UNIQUE Registered
METASPLOITABLE <20> UNIQUE Registered
WORKGROUP <00> GROUP Registered
WORKGROUP <1E> GROUP Registered
MAC Address = 00-00-00-00-00-00
C:\Windows\System32>
Type here to search
2:04 PM
9/16/2019


Metropolitan State Universit
Week 4: Information/Intellig
Enumerating H
https://lab.infoseclearning.com/lab/enumerating-hosts-using
Enumerating Hosts Using Wireshark, Windows,...
DB_NMAP COMMAND
7
Type the following command, then press Enter, to view all of the
discovered hosts.
msf > hosts
msf > hosts
Hosts
=====
address mac name os_name os_flavor os_sp purpose
info comments
192.168.1.10 00:50:56:9a:37:91 Windows 2008 server
192.168.1.20 00:50:56:9a:d7:a6 Windows Phone device
192.168.1.30 00:50:56:9a:2b:40 Linux 2.6.X server
192.168.1.254 00:50:56:9a:42:c8 embedded device
HOSTS COMMAND
8
Type the following command, then press Enter, to start Armitage.
msf> ./armitage
msf > ./armitage
[*] exec: ./armitage
ARMITAGE COMMAND
9
After the box appears, click the Connect button.
Internal Kali Scoring - Microsoft Edge
https://lab.infoseclearning.com/lab/console/vm-849134/Internal%20Kali%20Scoring
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
Applications
Places
Terminal
Mon 15:13
root@kali2: ~/armitage
File Edit View Search Terminal Help
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: OS and Service detection performed. Please report any incorrect result
s at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 256 IP addresses (5 hosts up) scanned in 339.76 seconds
[*] Nmap: Raw packets sent: 12904 (578.062KB) | Rcvd: 4479 (198.326KB)
msf > hosts
Hosts
=====
address mac name os_name os_flavor os_sp purpose
info comments
192.168.1.10 00:50:56:02:47:c0 Windows 2008 server
192.168.1.20 00:50:56:02:47:be Windows Phone device
192.168.1.30 00:50:56:8e:1d:20 Linux 2.6.X server
192.168.1.254 00:50:56:8e:e4:0d embedded device
msf >
Type here to search
2:13 PM
9/16/2019


Metropolitan State Universi
Week 4: Information/Intellig
Enumerating H
Internal Kali Scoring - Microsoft Edge
https://lab.infoseclearning.com/lab/enumerating-hosts-using
https://lab.infoseclearning.com/lab/console/vm-849134/Internal%20Kali%20Scoring
Enumerating Hosts Using Wireshark, Windows,...
Internal Kali Scoring
View Fullscreen
Send Ctrl+Alt+Delete
ARMITAGE
14 All 4 discovered hosts from the nmap scan will be displayed.
Armitage
Attacks Workspaces Help
192.168.1.254
192.168.1.10
192.168.1.30
192.168.1.20
4 DISCOVERED HOSTS
Note: Press the STOP button to complete the lab.
BACK
INFOSEC LEARNING
NEXT
Applications
Places
Mon 15:19
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Console X
Scan X
Scan X
[*] 192.168.1.254:80 lighttpd/1.4.38
[*] Scanned 1 of 1 hosts (100% complete)
[*] 1 scan to go...
msf auxiliary(http_version) > use scanner/ssh/ssh_version
msf auxiliary(ssh_version) > set THREADS 24
THREADS => 24
msf auxiliary(ssh_version) > set RPORT 22
RPORT => 22
msf auxiliary(ssh_version) > set RHOSTS 192.168.1.254
RHOSTS => 192.168.1.254
msf auxiliary(ssh_version) > run -j
[*] Auxiliary module running as background job
[*] 192.168.1.254:22 SSH server version: SSH-2.0-OpenSSH_6.6.1_hpn13v11
[*] Scanned 1 of 1 hosts (100% complete)
[*] Scan complete in 27.556s
msf auxiliary(ssh_version) >
Type here to search
2:19 PM
9/16/2019