

Ryan Brodsky

ICS 482

9/16/19

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

9 Notice the sample flag of 999818. Click on the Challenge the flag number into the answer box. This is just to show capture Challenge Flags you will see throughout this lab.

Challenge Sample #1

Challenge #2

10 Type the following command and press Enter, so your system has an IP Address.

```
root@kali2:~# ifconfig eth0 0.0.0.0 up
root@kali2:~# ifconfig eth0 0.0.0.0
```

IFCONFIG

11 Type the following command and press Enter, to verify the address is listed for eth0.

```
root@kali2:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:9a:bc:c1
          inet6 addr: fe80::20c:29ff:fe9a:bec1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Met
          RX packets:943 errors:0 dropped:0 overruns:0 c
          TX packets:58 errors:0 dropped:0 overruns:0 c
          collisions:0 txqueuelen:1000
          RX bytes:85927 (83.9 KiB)  TX bytes:8595 (8.3
```

19 Click the Red button to stop the Wireshark capture.

CLICK STOP

20 Close Wireshark by selecting File and then click Quit.

21 When asked, Do you want to save the captured packets? If quitting?, click Quit without Saving.

Internal Kali Scoring - Microsoft Edge

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

Internal Kali Scoring

Applications Places Terminal Mon 14:44

```
root@kali2:~# cat ip3.txt
eth0      Link encap:Ethernet  HWaddr 00:0c:29:9a:bc: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:7439 errors:0 dropped:0 overruns:0 frame:0
          TX packets:49 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:827225 (807.8 KiB)  TX bytes:8005 (7.8 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
          flag:123457
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1200 (1.1 KiB)  TX bytes:1200 (1.1 KiB)

root@kali2:~#
```

Internal Kali Scoring

Applications Places Wireshark Mon 14:49

*eth0 [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
7	1.086107000	Vmware_Be:4e:0e	Broadcast	RARP	60	Who is 00:50:56:8e:4e:0e? Tell 00:50:56:8e:4e:0e
8	1.321542000	Vmware_Be:4e:0e	Broadcast	ARP	60	Who has 203.0.113.254? Tell 203.0.113.100
9	1.321551000	Vmware_Be:4e:0e	Broadcast	ARP	60	Who has 203.0.113.254? Tell 203.0.113.100
10	2.321544000	Vmware_Be:4e:0e	Broadcast	ARP	60	Who has 203.0.113.254? Tell 203.0.113.100
11	2.321554000	Vmware_Be:4e:0e	Broadcast	ARP	60	Who has 203.0.113.254? Tell 203.0.113.100
12	3.332298000	Vmware_Be:4e:0e	Broadcast	ARP	60	Who has 203.0.113.254? Tell 203.0.113.100
13	3.332309000	Vmware_Be:4e:0e	Broadcast	ARP	60	Who has 203.0.113.254? Tell 203.0.113.100
14	3.543470000	192.168.1.10	192.168.1.20	DNS	93	Standard query response 0xbef Server failure
15	4.342394000	Vmware_Be:4e:0e	Broadcast	ARP	60	Who has 203.0.113.254? Tell 203.0.113.100
16	4.342405000	Vmware_Be:4e:0e	Broadcast	ARP	60	Who has 203.0.113.254? Tell 203.0.113.100
17	5.368758000	Vmware_Be:4e:0e	Broadcast	ARP	60	Who has 203.0.113.254? Tell 203.0.113.100

Frame 1: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 0
Ethernet II, Src: Vmware_02:47:be (00:50:56:02:47:be), Dst: Vmware_02:47:c0 (00:50:56:02:47:c0)
Internet Protocol Version 4, Src: 192.168.1.20 (192.168.1.20), Dst: 192.168.1.10 (192.168.1.10)
User Datagram Protocol, Src Port: 61010 (61010), Dst Port: 53 (53)
Domain Name System (query)

0000 00 50 56 02 47 c0 00 50 56 02 47 be 00 00 45 00 .PV.G..P.V.G...E.
0010 00 4f 09 bf 00 00 80 11 ad 70 c0 a8 01 14 c0 a8 ..O.....p.....
0020 01 0a ee 52 00 35 00 3b 40 aa be 8f 01 00 00 01 ...R.S.:@.....
0030 00 00 00 00 00 00 03 76 31 80 0a 76 ef 72 74 65v 10.vorte
0040 78 2d 77 69 6e 04 6d 61 74 61 09 6d 69 63 72 6f x-win.de to micro

File: "tmp/wireshark-prgcap_eth0-2..." Packets: 72 - Displayed: 72 (100.0%) Dropped: 0 (0.0%) Profile: Default

Metropolitan State University

Week 4: Information/Intelligence

Enumerating Hosts Using Wireshark, Windows,...

https://lab.infoseclearning.com/lab/enumerating-hosts-using-wireshark-windows-vm-849134/internal-kali%20kali%20scoring

Enumerating Hosts Using Wireshark, Windows,...

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

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

Generated by NetworkManager
search localdomain
nameserver 172.16.200.2

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

Type here to search

Metropolitan State University

Week 4: Information/Intelligence

Enumerating Hosts Using Wireshark, Windows,...

https://lab.infoseclearning.com/lab/enumerating-hosts-using-wireshark-windows-vm-849134/internal-kali%20kali%20scoring

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

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-kali%20kali%20scoring

Internal Kali Scoring

View Fullscreen Send Ctrl+Alt+Delete

Applications Places Terminal Mon 14:52

File Edit View Search Terminal Help

root@kali2: ~

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:~#

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
(Leapop) res Music vmware-tools-distrib
Desktop Pictures
Documents Public

root@kali2:~# cat /etc/resolv.flag

flag:888999

root@kali2:~#

Type here to search

Metropolitan State University

Week 4: Information/Intelligence

Enumerating Hosts Using Wireshark, Windows,...

https://lab.infoseclearning.com/lab/enumerating-hosts-using-wireshark-windows-vm-849134/internal-kali%20kali%20scoring

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

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

Metropolitan State University Week 4: Information/Intelligence Enumerating Hosts Using Wireshark, Windows, and Linux

Enumerating Hosts Using Wireshark, Windows, and Linux

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:bc:c1
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe9a:bc1/64 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:1350 (1.3 KiB) TX bytes:1350 (1.3 KiB)
```

IFCONFIG

Internal Kali Scoring - Microsoft Edge

Internal Kali Scoring

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

```
flag:888999
root@kali2:~# ifconfig
bash: ifconfig: 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:~#

Metropolitan State University Week 4: Information/Intelligence Enumerating Hosts Using Wireshark, Windows, and Linux

Enumerating Hosts Using Wireshark, Windows, and Linux

Challenge #5

Challenge #6

12 Attempt to enumerate the IP and MAC Address of the machine name 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
CAMPIUS              <00>                GROUP               Registered
```

Internal Windows 10 Scoring - Microsoft Edge

Internal Windows 10 Scoring

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>
```


Enumerating Hosts Using Wireshark, Windows,...

13 Attempt to enumerate the IP and MAC Address of the machine named 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
  
```

Internal Windows 10 Scoring - Microsoft Edge

Internal Windows 10 Scoring

View Fullscreen Send Ctrl+Alt+Delete Rob

Administrator: cmd - Shortcut

```

CAMPUS <1B>  UNIQUE           Registered
CAMPUS <1D>  UNIQUE           Registered
_<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>

BACK INFOSEC LEARNING NEXT

Enumerating Hosts Using Wireshark, Windows,...

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
-----
192.168.1.10  00:50:56:9a:37:91  Windows 2008
192.168.1.20  00:50:56:9a:d7:a6  Windows Phone
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
  
```

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

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 results 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
-----
192.168.1.10  00:50:56:02:47:c0  Windows 2008
192.168.1.20  00:50:56:02:47:be  Windows Phone
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
msf >
  
```

Metropolitan State University

Week 4: Information/Intelligence

Enumerating Hosts Using Wireshark, Windows,...

Internal Kali Scoring - Microsoft Edge

https://lab.infoseclearning.com/lab/enumerating-hosts-using-wireshark-windows-...

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

4 DISCOVERED HOSTS

Note: Press the STOP button to complete the lab.

BACK

INFOSEC LEARNING

NEXT

Armitage

Armitage View Hosts Attacks Workspaces Help

192.168.1.254 192.168.1.10 192.168.1.30 192.168.1.20

Console X Scan X Scan X

[*] 192.168.1.254:80 lighttpd/1.4.30
[*] Scanned 1 of 1 hosts (100% complete)
[*] I 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 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_hpm13v11
[*] Scanned 1 of 1 hosts (100% complete)
[*] Scan complete in 27.556s
msf auxiliary(ssh_version) >