

CYSE 450- Ethical Hacking and Penetration Testing

Assignment-3

Total:100 Points

Please complete all the tasks and submit the screenshot for each along with the respective step number in a word or pdf file.

You may refer to the examples demonstrated during the class or go to help/manual page to learn about the commands usage for nmap, dig and, host (using -h)

Task-A: [30 points] Install the following Virtual Machines to complete your lab and submit the screenshots for the IP address displayed in the terminal after using ifconfig (in Linux VM)/ipconfig (in Windows VM) command for all these machines:

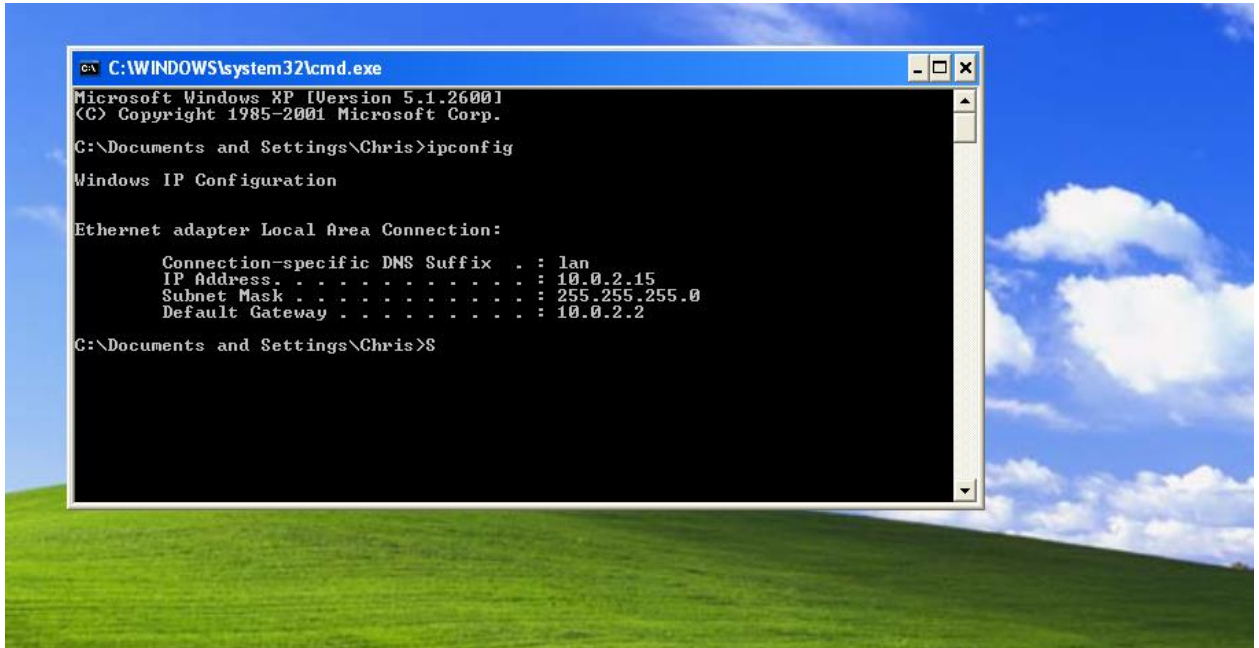
1. Kali Linux

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe3e:fc54 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:3e:fc:54 txqueuelen 1000 (Ethernet)
    RX packets 1 bytes 590 (590.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19 bytes 2822 (2.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

2. Metasploitable2(Source:<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>)

```
msfadmin@metasploitable:~$ ifconfig
-bash: ifconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ee:ac:ff
          inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee:acff/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:34 errors:0 dropped:0 overruns:0 frame:0
          TX packets:63 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4387 (4.2 KB)  TX bytes:6714 (6.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

3. Windows XP or Windows 7 (Refer to the class recording to install this)



Task B: [30 points] Perform passive reconnaissance using archive.org and [netcraft](https://netcraft.com) (For this task, you can use any browser of your actual computer)

Organizations keep updating their websites from time to time. The archive.org website keeps track of all the updates or changes since the website was launched. An attacker can use this website to determine the changes made on the website. An attacker may use this information to conduct various attacks, such as phishing.

1. Go to we.archive.org and in the search box type www.microsoft.com and hit Enter
2. Gather and write in brief information about the updated made between **January 1** till **current date**. Take the screenshot of the result.
3. For this step, open a new tab and go to **www.netcraft.com** and gather information about network like, network domain, network registrar, IPV4 address, and nameserver for www.microsoft.com. write in brief what you analyzed?

Network Domain: **microsoft.com**.

Network Registrar: **MarkMonitor Inc.**

IPV4 address: **23.60.66.20**

Nameserver:

microsoft.com. 14380 IN NS ns1-39.azure-dns.com.

microsoft.com. 14380 IN NS ns2-39.azure-dns.net.

microsoft.com. 14380 IN NS ns3-39.azure-dns.org.

microsoft.com. 14380 IN NS ns4-39.azure-dns.info.

Task C: [40 points] Perform active reconnaissance using attacker Kali Linux and target Metasploitable VM

1. In the settings, change the network adapter to **Bridge** mode for all the Three machines.
2. Open the terminals and execute the correct command to print the IP addresses for all the 3 machines separately (Make sure the IP address should be unique for all the 3 machines).

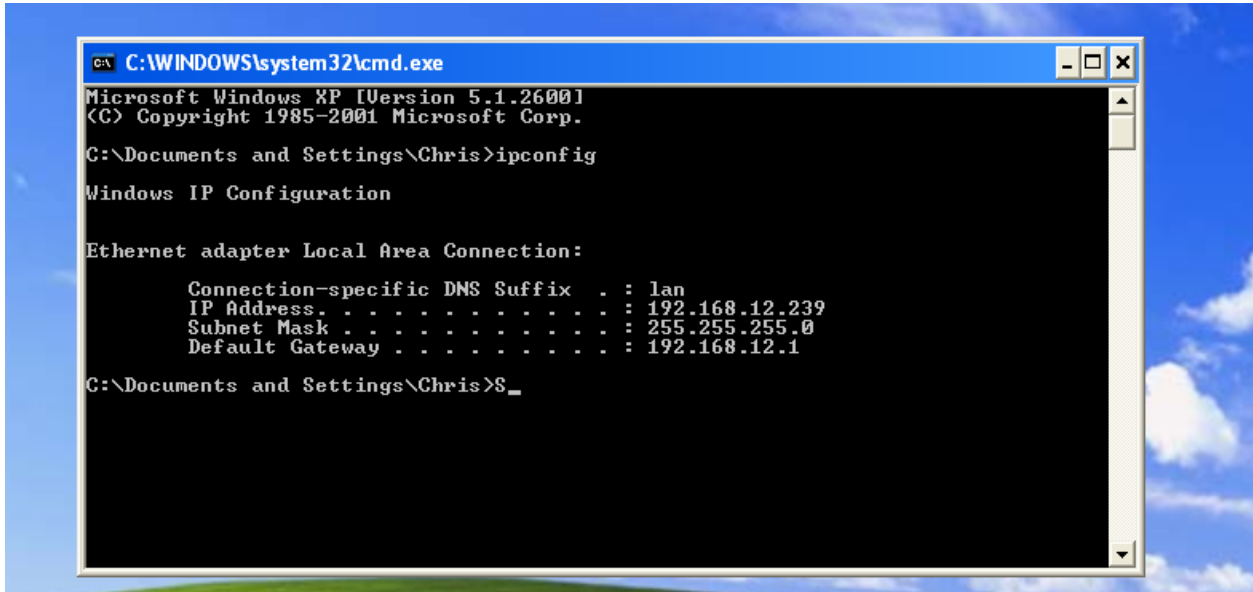
Kali Linux:

```
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.12.164 netmask 255.255.255.0 broadcast 192.168.12.255
    inet6 fe80::a00:27ff:fe3e:fc54 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:3e:fc:54 txqueuelen 1000 (Ethernet)
    RX packets 17 bytes 2151 (2.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 29 bytes 4270 (4.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Metasploitable2:

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ee:ac:ff
          inet addr:192.168.12.136  Bcast:192.168.12.255  Mask:255.255.255.0
          inet6 addr: 2607:fb90:758b:83e6:a00:27ff:feee:acff/64 Scope:Global
          inet6 addr: fe80::a00:27ff:feee:acff/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:61 errors:0 dropped:0 overruns:0 frame:0
          TX packets:81 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6170 (6.0 KB)  TX bytes:8090 (7.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

Windows:



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Chris>ipconfig

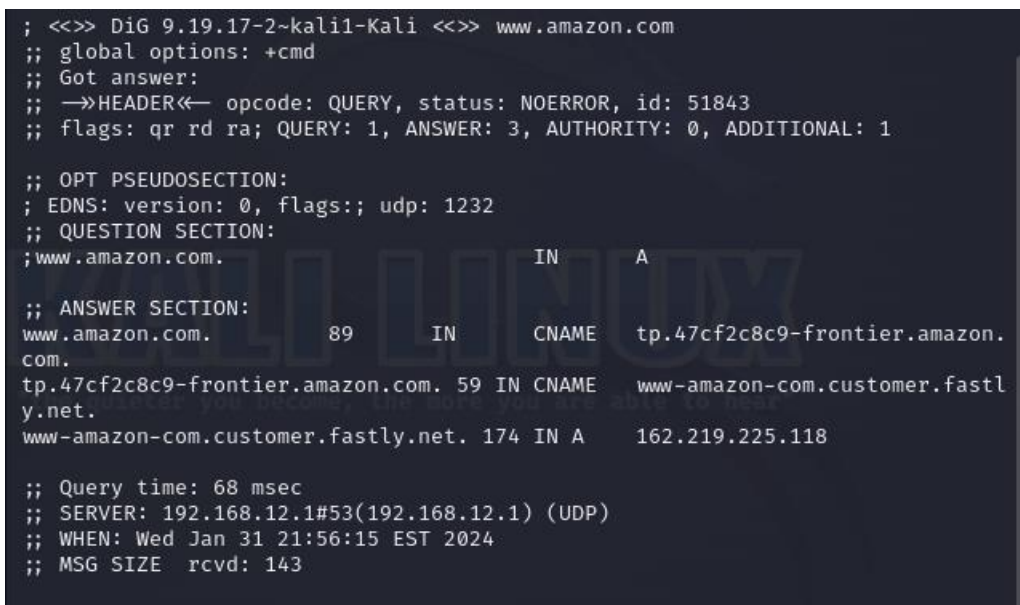
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : lan
    IP Address. . . . . : 192.168.12.239
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.12.1

C:\Documents and Settings\Chris>S_
```

3. In Kali Linux terminal, execute the command (**host/dig**) to demonstrate whether the host (www.odu.edu or www.amazon.com) is live/UP or not. **Also provide the reason if the host is live /UP by using the option - -reason.**



```
; <<>> DiG 9.19.17-2~kali1-Kali <<>> www.amazon.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 51843
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.amazon.com.                IN      A

;; ANSWER SECTION:
www.amazon.com.                89      IN      CNAME   tp.47cf2c8c9-frontier.amazon.com.
tp.47cf2c8c9-frontier.amazon.com. 59      IN      CNAME   www-amazon-com.customer.fastly.net.
www-amazon-com.customer.fastly.net. 174     IN      A       162.219.225.118

;; Query time: 68 msec
;; SERVER: 192.168.12.1#53(192.168.12.1) (UDP)
;; WHEN: Wed Jan 31 21:56:15 EST 2024
;; MSG SIZE rcvd: 143
```

4. Using terminal in Kali Linux, perform **DNS enumeration** using **dnsenum** command for www.odu.edu or www.google.com (Please refer to the slide for using dnsenum)

```
thedarkone@kali: ~  
File Actions Edit View Help  
(thedarkone@kali)-[~]  
$ dnsenum www.amazon.com  
dnsenum VERSION:1.2.6  
  
----- www.amazon.com -----  
  
Host's addresses:  
-----  
d3ag4hukkh62yn.cloudfront.net.      14      IN      A      3.161.137.148  
  
Name Servers:  
-----  
ns-824.awsdns-39.net.      3567     IN      A      205.251.195.56  
ns-130.awsdns-16.com.      377      IN      A      205.251.192.130  
ns-2021.awsdns-60.co.uk.   3294     IN      A      205.251.199.229  
ns-1144.awsdns-15.org.     2432     IN      A      205.251.196.120
```

5. In kali Linux, perform **ICMP Sweep scan** to gather information about the target machine (Metasploitable Linux) by sending **ICMP echo request** to target machine (using its ip address), using **nmap** command with correct options. Highlight the line indicating whether the ICMP reply has been received or not. [Do not forget to disable the arp-ping]

```
(root@kali)-[~]  
$ nmap -PE -sn 192.168.12.136 --reason --disable-arp-ping --packet-trace  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-31 22:34 EST  
SENT (0.0135s) ICMP [192.168.12.164 > 192.168.12.136 Echo request (type=8/code=0) id=36695 seq=0] IP [ttl=39 id=54245 iplen=28 ]  
RCVD (0.0201s) ICMP [192.168.12.136 > 192.168.12.164 Echo reply (type=0/code=0) id=36695 seq=0] IP [ttl=64 id=48858 iplen=28 ]  
NSOCK INFO [0.0490s] nsock_iod_new2(): nsock_iod_new (IOD #1)  
NSOCK INFO [0.0490s] nsock_connect_udp(): UDP connection requested to fe80::3aa0:67ff:fe7a:add:53 (IOD #1) EID 8  
NSOCK INFO [0.0490s] nsock_read(): Read request from IOD #1 [fe80::3aa0:67ff:fe7a:add:53] (timeout: -1ms) EID 18  
NSOCK INFO [0.0490s] nsock_iod_new2(): nsock_iod_new (IOD #2)  
NSOCK INFO [0.0490s] nsock_connect_udp(): UDP connection requested to 192.168.12.1:53 (IOD #2) EID 24
```

6. In kali Linux, perform **ICMP Sweep scan** to gather information about the target machine (Windows Xp/7) by sending **ICMP echo request**, using **nmap** command with correct options. (Make sure the firewall is turned on in windows machine)

```
(root@kali)-[~]  
# nmap -PE -sn 192.168.12.239 --reason --packet-trace --disable-arp-ping  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-31 22:42 EST  
SENT (0.0115s) ICMP [192.168.12.164 > 192.168.12.239 Echo request (type=8/code=  
SENT (1.0138s) ICMP [192.168.12.164 > 192.168.12.239 Echo request (type=8/code=  
Note: Host seems down. If it is really up, but blocking our ping probes, try -F  
Nmap done: 1 IP address (0 hosts up) scanned in 2.05 seconds
```

```
(root@kali)-[~]  
#
```

Home:

"the quieter you become, the more you are able to hear"