CYSE 450- Ethical Hacking and Penetration Testing

Assignment-3

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
- 2. Metasploitable2(Source: https://sourceforge.net/projects/metasploitable/files/Metasploitable2/)
- 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 (For this task, you can use any browser of your actual computer)

- 1. Go to we.archive.org and in the search box type www.Microsoft.com and hit Enter
- Gather and write in brief information about the updated made between January 1 till current date. <u>Take the screenshot of the result.</u>

	· Collections	Explore more than 8 www.microsoft.con Changes	33 billion web pages saved ov Summary Site Map 0, 1996 and January 28	• URLs	
Saved 2		etween October 2	0, 1990 and January 20,	2024.	
J01 2002 2003 2004 2005 2006 2007 2008	2009 2010 201	11 2012 2013	2014 2015 2016 2017	2018 2019 2020 20	21 2022 2023 <mark>2024</mark>
•					•
JAN	FEB		MAR	APR	
1 2 3 4 5 6	1	2 3	1 2	1 2 3 4	5 6
7 8 9 10 11 12 13 4	5 6 7 8	3 9 10 3	4 5 6 7 8 9	7 8 9 10 11	12 13
14 15 16 17 18 19 20 1	1 12 13 14 1	5 16 17 10	11 12 13 14 15 16	14 15 16 17 18	19 20
21 22 23 24 25 26 27 11	8 19 20 21 2	2 23 24 17	18 19 20 21 22 23	21 22 23 24 25	26 27
28 29 30 31 23	5 26 27 28 2	9 24	25 26 27 28 29 30	28 29 30	
		31			

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?

For task 3, I cannot find any current information. The information available seems to be from the early 2000s and there isn't an option to create an account so I can access updated information on this site.



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.

File Machine Help		
Tools		
Ubuntu		
Kali Linux		
Metasploitable2		
Windows XP		
🔅 Kali Linux - Settings	_	o x
General	Network	
System	Adapter 1 Adapter 2 Adapter 3 Adapter 4	
Display	Enable Network Adapter	
Storage	Attached to: Bridged Adapter	
(Audio	Name: Intel(R) WI-FI 6E AX211 160MHZ	~
Network		
Serial Ports		
USB		
Shared Folders		
User Interface		
	OK Cancel	Help

Tools	
Ubuntu Dowered Off	
Kali Linux	
Metasploitable2	8
Windows XP	
🙀 Metasploitable2 - Settings	– 🗆 X
General	Network
System	Adapter 1 Adapter 2 Adapter 3 Adapter 4
Display	Enable Network Adapter
Storage	Attached to: Bridged Adapter
Audio	Name: Intel(R) Wi-Fi 6E AX211 160MHz
Network	Auvaliceu
Serial Ports	
USB	
Shared Folders	
User Interface	
	OK Cancel Help

File Machine Help						
Tools						
Ubuntu 🕑 Powered Off						
Kali Linux						
Metasploitable2						
Windows XP						
🙀 Windows XP - Settings					- 0	×
General	Network					
System	Adapter 1 Adapter 2	Adapter 3 Ad	lapter 4			
Display	Enable Network Adapte	er				
Storage	Attached to:	Bridged Adapter	~			
Audio	Name:	Intel(R) Wi-Fi 6E AX	211 160MHz			<u>~</u>
Network						
Serial Ports						
USB						
Shared Folders						
User Interface						
			ОК	Cancel	Help	

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.

-(stuhow44®showa006)-[~]

└_\$ ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 192.168.0.252 netmask 255.255.255.0 broadcast 192.168.0.255 inet6 fe80::a00:27ff:fe5b:16d4 prefixlen 64 scopeid 0×20<link> inet6 2600:8805:1931:d300:a00:27ff:fe5b:16d4 prefixlen 64 scopeid 0×0<global> inet6 2600:8805:1931:d300:2e2:a70b:740e:f7e9 prefixlen 64 scopeid 0×0<global> ether 08:00:27:5b:16:d4 txqueuelen 1000 (Ethernet) RX packets 257 bytes 43675 (42.6 KiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 272 bytes 34127 (33.3 KiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536 inet 127.0.0.1 netmask 255.0.0.0 inet6 ::1 prefixlen 128 scopeid 0×10<host> loop txqueuelen 1000 (Local Loopback) RX packets 4 bytes 240 (240.0 B) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 4 bytes 240 (240.0 B) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

loitablee [Running] - Oracle VM VirtualBox

ccess official Ubuntu documentation, please visit: ://help.ubuntu.com/ ail. dmin@metasploitable:~\$ ifconfig Link encap:Ethernet HWaddr 08:00:27:e2:34:ef inet addr:192.168.0.188 Bcast:192.168.0.255 Mask:255.25 inet6 addr: fe80::a00:27ff:fee2:34ef/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:3236 errors:0 dropped:0 overruns:0 frame:0 TX packets:178 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:480660 (469.3 KB) TX bytes:25115 (24.5 KB) Base address:0xd020 Memory:f0200000-f0220000 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:16436 Metric:1 RX packets:555 errors:0 dropped:0 overruns:0 frame:0 TX packets:555 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:246349 (240.5 KB) TX bytes:246349 (240.5 KB)



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.

---(stuhow44@showa006)-[~]

```
-s host www.amazon.com
www.amazon.com is an alias for tp.47cf2c8c9-frontier.amazon.com.
tp.47cf2c8c9-frontier.amazon.com is an alias for d3ag4hukkh62yn.cloudfront.net.
d3ag4hukkh62vn.cloudfront.net has address 3.162.98.201
d3ag4hukkh62yn.cloudfront.net has IPv6 address 2600:9000:244d:2200:7:49a5:5fd3:b641
d3ag4hukkh62yn.cloudfront.net has IPv6 address 2600:9000:244d:3400:7:49a5:5fd3:b641
d3ag4hukkh62yn.cloudfront.net has IPv6 address 2600:9000:244d:6200:7:49a5:5fd3:b641
d3ag4hukkh62yn.cloudfront.net has IPv6 address 2600:9000:244d:2a00:7:49a5:5fd3:b641
d3ag4hukkh62yn.cloudfront.net has IPv6 address 2600:9000:244d:c600:7:49a5:5fd3:b641
d3ag4hukkh62yn.cloudfront.net has IPv6 address 2600:9000:244d:2800:7:49a5:5fd3:b641
d3ag4hukkh62yn.cloudfront.net has IPv6 address 2600:9000:244d:a600:7:49a5:5fd3:b641
d3ag4hukkh62yn.cloudfront.net has IPv6 address 2600:9000:244d:4200:7:49a5:5fd3:b641
 --(stuhow44@showa006)-[~]
L-$ dig www.amazon.com
; <>> DiG 9.18.12-1-Debian <<>> www.amazon.com
;; global options: +cmd
;; Got answer:
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
:: QUESTION SECTION:
; www.amazon.com.
                                      IN
                                             A
;; ANSWER SECTION:
                                      CNAME
                                              tp.47cf2c8c9-frontier.amazon.com.
www.amazon.com.
                      1000
                              IN
tp.47cf2c8c9-frontier.amazon.com. 25 IN CNAME d3ag4hukkh62yn.cloudfront.net.
d3ag4hukkh62yn.cloudfront.net. 25 IN A
                                             18.160.49.8
;; Query time: 15 msec
;; SERVER: 68.105.28.11#53(68.105.28.11) (UDP)
;; WHEN: Sun Jan 28 19:00:56 EST 2024
:: MSG SIZE rcvd: 138
```

(stuhow44@ showa006)-[~]
- s nost -t ns www.amazon.com
www.amazon.com is an alias for tp.47cf2c8c9-frontier.amazon.com.
tp.47cf2c8c9-frontier.amazon.com is an alias for d3ag4hukkh62yn.cloudfront.net.
d3ag4hukkh62yn.cloudfront.net name server ns-824.awsdns-39.net.
d3ag4hukkh62yn.cloudfront.net name server ns-1144.awsdns-15.org.
d3ag4hukkh62yn.cloudfront.net name server ns-130.awsdns-16.com.
d3ag4hukkh62yn.cloudfront.net name server ns-2021.awsdns-60.co.uk.

Host is live because you can see information about its IP address.

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)

(stuhow44@showa006)-[~] dnsenum www.amazon.com dnsenum VERSION:1.2.6					
www.amazon.com					
Host's addresses:					
d3ag4hukkh62yn.cloudfront.net.	10	IN	А	3.162.118.164	
Name Servers:					
ns-1144.awsdns-15.org. ns-130.awsdns-16.com. ns-2021.awsdns-60.co.uk. ns-824.awsdns-39.net.	27013 27214 27020 27130	IN IN IN IN	A A A A	205.251.196.120 205.251.192.130 205.251.199.229 205.251.195.56	
Hail (MX) Servers:					
Trying Zone Transfers and getting Bind V					
Trying Zone Transfer for www.amazon.com o AXFR record query failed: corrupt packet	on ns-114	4.awsd	ns-15.org		
Trying Zone Transfer for www.amazon.com o AXFR record query failed: corrupt packet	on ns-202	1.awsd	ns-60.co.	uk	
Trying Zone Transfer for www.amazon.com (AXFR record query failed: corrupt packet	on ns-130	.awsdn:	s-16.com		
Trying Zone Transfer for www.amazon.com (AXFR record query failed: corrupt packet	on ns-824	.awsdn	s-39.net		
Brute forcing with /usr/share/dnsenum/dn					

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]

```
nmap -PE -sn 192.168.0.188
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-28 21:02 EST
Nmap scan report for 192.168.0.188
Host is up (0.0010s latency).
MAC Address: 08:00:27:E2:34:EF (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 11.29 seconds
nmap -PE -sn 192.168.0.188 -- reason
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-28 21:03 EST
Nmap scan report for 192.168.0.188
Host is up, received arp-response (0.00066s latency).
MAC Address: 08:00:27:E2:34:EF (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 11.20 seconds
nmap -PE -sn 192.168.0.188 -- reason -- disable-arp-ping
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-28 21:04 EST
Nmap scan report for 192.168.0.188
Host is up, received echo-reply ttl 64 (0.0012s latency).
MAC Address: 08:00:27:E2:34:EF (Oracle VirtualBox Virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 11.20 seconds
```

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)

(10019 SHOWAU90)-	~	
-# nmap -PE -sn 192.	168.0.224 reason disable-arp-ping packet-trace	
Starting Nmap 7.93 (https://nmap.org) at 2024-01-28 22:01 EST	
SENT (0.0500s) ICMP	192.168.0.252 > 192.168.0.224 Echo request (type=8/code=0) id=32259 seq=0] IP [ttl=37 id=6	55144 iplen=28]
RCVD (0.0546s) ICMP	192.168.0.224 > 192.168.0.252 Echo reply (type=0/code=0) id=32259 seq=0] IP [ttl=128 id=20	01 iplen=28]
NSOCK INFO [0.1250s]	nsock_iod_new2(): nsock_iod_new (IOD #1)	
NSOCK INFO [0.1250s]	<pre>nsock_connect_udp(): UDP connection requested to 2001:578:3f:1::30:53 (IOD #1) EID 8</pre>	
NSOCK INFO [0.1250s]	nsock_read(): Read request from IOD #1 [2001:578:3f:1::30:53] (timeout: -1ms) EID 18	
NSOCK INFO [0.1250s]	nsock_iod_new2(): nsock_iod_new (IOD #2)	
NSOCK INFO [0.1250s]	nsock_connect_udp(): UDP connection requested to 2001:578:3f::30:53 (IOD #2) EID 24	
NSOCK INFO [0.1260s]	nsock_read(): Read request from IOD #2 [2001:578:3f::30:53] (timeout: -1ms) EID 34	
NSOCK INFO [0.1260s]	nsock_iod_new2(): nsock_iod_new (IOD #3)	
NSOCK INFO [0.12605]	nsock_connect_udp(): UDP connection requested to 68.105.28.12:53 (IOD #3) EID 40	
NSOCK INFO [0.1260s]	nsock_read(): Read request from IOD #3 [68.105.28.12:53] (timeout: -1ms) EID 50	
NSOCK INFO [0.1260s]	nsock_iod_new2(): nsock_iod_new (IOD #4)	
NSOCK INFO [0.1260s]	nsock_connect_udp(): UDP connection requested to 68.105.29.11:53 (IOD #4) EID 56	
NSOCK INFO [0.1260s]	nsock_read(): Read request from IOD #4 [68.105.29.11:53] (timeout: -1ms) EID 66	
NSOCK INFO [0.1260s]	nsock_lod_new2(): nsock_lod_new (IOD #5)	
NSOCK INFO [0.1260s]	nsock_connect_udp(): UDP connection requested to 68.105.28.11:53 (IOD #5) EID 72	
NSOCK INFO [0.1260s]	nsock_read(): Read request from 100 #5 [68.105.28.11:53] (timeout: -1ms) EID 82	
NSOCK INFO [0.1260s]	hsock_write(): write request for 44 bytes to 10D #1 EID 91 [2001:578:3f:1::30:53]	
NSOCK INFO [0.1260s]	nsock_trace_nangler_callback(): Callback: CONNECT SUCCESS for EID 8 [2001:5/8:3f:1::30:53	
NSOCK INFO [0.12605]	nsock_trace_handler_callback(): Callback: WkIte_SOCCESS for EID 91 [2001:578:31:1::30:53]	
NSOCK INFO [0.12605]	nsock_trace_nangler_callback(): Callback: CONNECT SUCCESS For EID 24 [2001:5/8:3f::30:53]	
NSOCK INFO [0.12605]	HSOCK_trace_nancter_callback(): Callback: CONNECT SUCCESS FOR ELD 40 [68.105.28.12:53]	
NSOCK INFO [0.12605]	nsock_trace_nanuler_callback(): Callback: CONNECT SUCCESS FOR ELD 56 [68.105.29.11:53]	
NSOCK INFO [0.12605]	HSOCK_trate Handler_cattback(): Cattback: Conwect Soccess for ED 72 [68.105.28.11:53]	
NSOCK INFO [2.03005]	H_{reck} write(), write request for 44 bytes to 100 #1 EID 99 [2001:578:37:11:30:53]	
NSOCK INFO [2.03005]	hsock_triate_inducter_cattback(). Cattback: WAIE SUCCESS TOT EID 99 [2001:3/8:31:1::30:53]	
NSOCK INFO [5.63705]	$r_{1} = r_{1} = r_{1$	
NSOCK INFO [8 14805]	sock write(): Write request for 44 bytes to TOD #2 FD 115 [2001:578:35 -: 30:33]	
NSOCK INFO [8 14805]	r_{1} r_{2} r_{1} r_{2} r_{2	
NSOCK INFO [11.15405]	I sock write(): Write request for 44 bytes to TOD #3 FD 123 [68 105 28 12:53]	
NSOCK INFO [11.15405	nsock_trace handler callback(): Callback: WRITE SUCCESS for FID 123 [68 105 28 12:53]	
NSOCK INFO [11.17105	nsock trace handler callback(): Callback: READ SUCCESS for FID 50 [68.105.28.12:53]	ovtes):
NSOCK INFO [11.17105	nsock read(): Read request from IOD #3 [68.105.28.12:53] (timeout: -1ms) FID 130	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
NSOCK INFO [11.17105	nsock iod delete(): nsock iod delete (IOD #1)	
NSOCK INFO [11.17105	nevent delete(): nevent delete on event #18 (type READ)	
NSOCK INFO [11.1710s	nsock iod delete(): nsock iod delete (IOD #2)	
NSOCK INFO [11.1710s	nevent delete(): nevent delete on event #34 (type READ)	
NSOCK INFO [11.1710s	nsock_iod_delete(): nsock_iod_delete (IOD #3)	
NSOCK INFO [11.17105	nevent delete(): nevent delete on event #130 (type READ)	
NSOCK INFO [11.17105	nsock iod delete(): nsock iod delete (IOD #4)	
NSOCK INFO [11.1710s]	nevent_delete(): nevent_delete on event #66 (type READ)	
NSOCK INFO [11.17105]	nsock_iod_delete(): nsock_iod_delete (IOD #5)	
NSOCK INFO [11.17105	nevent_delete(): nevent_delete on event #82 (type READ)	
Nan Cor	192.168.0.224	
Host is up, received	ecno-reply ttl 128 (0.0048s latency).	
Address: 00.44.2	C:E2:07 (Oracle VirtualBox virtual NZ)	
Nmap done: 1 IP addre	ess (1 host up) scanned in 11.18 seconds	