UPES
UNIVERSITY OF TOMORROW

IT APP. SEC. LAB FILE

To- Dr. Gopal Rawat

Name- Dhairya Jain
Sap ID- 500105432
Batch- CSF-B1

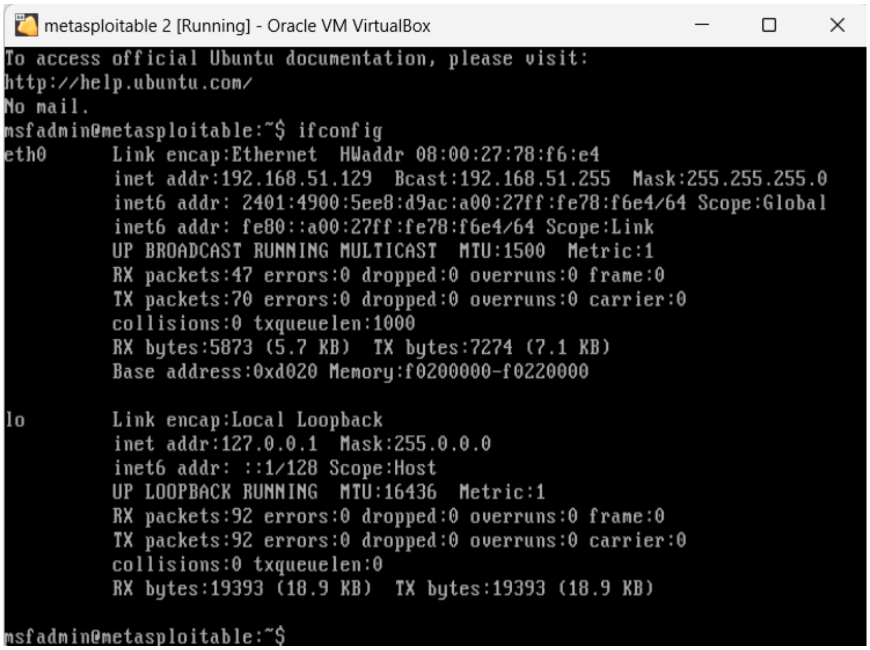
AIM- ***ARP poisoning***

To do the following:

- Demonstrate ARP poisoning and spoofing on
- Perform under low, medium, and high security scenario DVWA.
- demo.testfire site
- testphpvulweb site

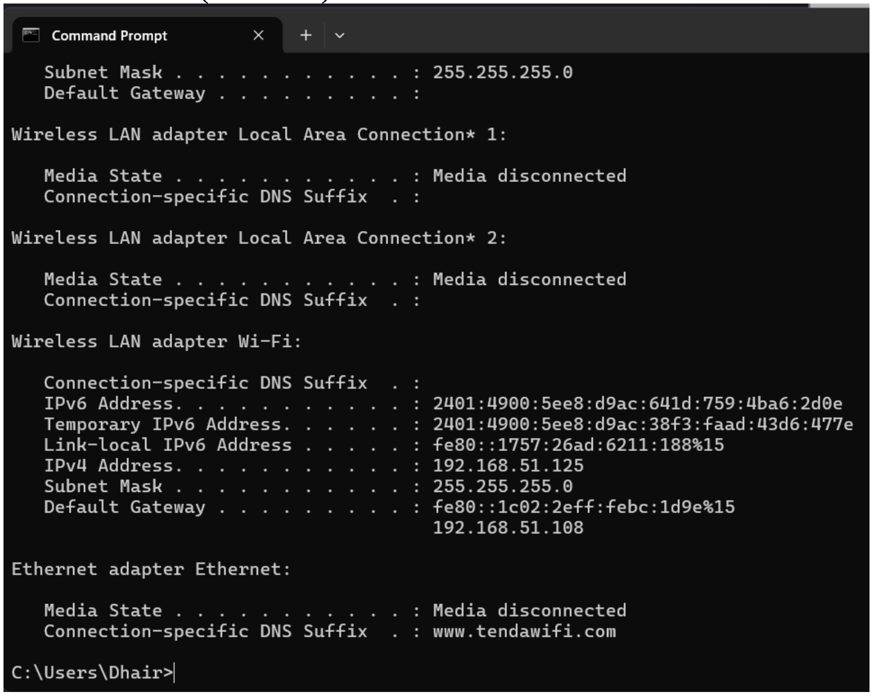
Finding IP Address of all machines

Server machine (metasploitable 2)



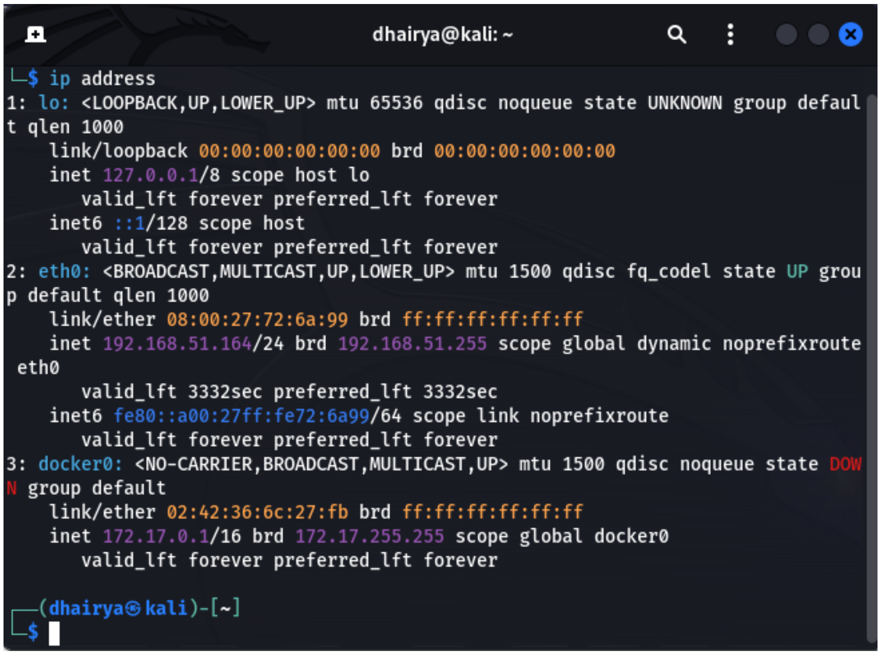
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:78:f6:e4
          inet addr:192.168.51.129  Bcast:192.168.51.255  Mask:255.255.255.0
          inet6 addr: 2401:4900:5ee8:d9ac:a00:27ff:fe78:f6e4/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe78:f6e4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:47 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5873 (5.7 KB)  TX bytes:7274 (7.1 KB)
          Base address:0xd020 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:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

Victim machine (Windows)



```
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:5ee8:d9ac:641d:759:4ba6:2d0e
   Temporary IPv6 Address. . . . . . : 2401:4900:5ee8:d9ac:38f3:faad:43d6:477e
   Link-local IPv6 Address . . . . . : fe80::1757:26ad:6211:188%15
   IPv4 Address. . . . . . . . . . . : 192.168.51.125
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1c02:2eff:febc:1d9e%15
                                       192.168.51.108

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : www.tendawifi.com

C:\Users\Dhair>
```

Kali machine

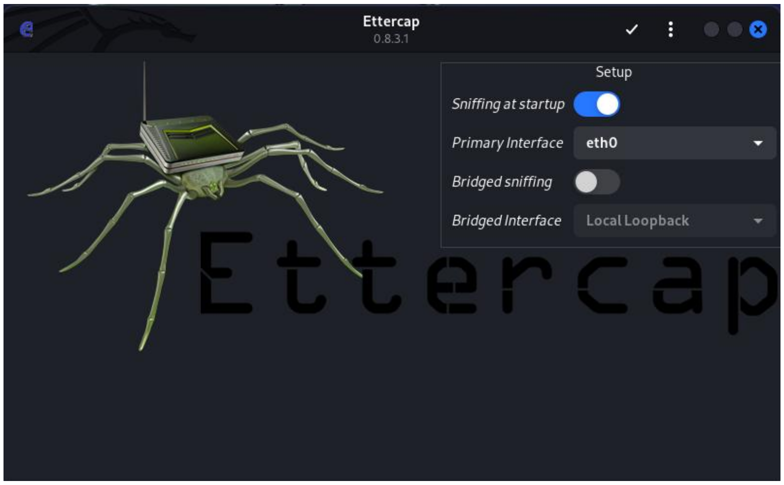


```
└─$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP grou
p default qlen 1000
    link/ether 08:00:27:72:6a:99 brd ff:ff:ff:ff:ff:ff
    inet 192.168.51.164/24 brd 192.168.51.255 scope global dynamic noprefixroute
 eth0
       valid_lft 3332sec preferred_lft 3332sec
    inet6 fe80::a00:27ff:fe72:6a99/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOW
N group default
    link/ether 02:42:36:6c:27:fb brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever

┌──(dhairya㉿kali)-[~]
└─$ 
```

Preforming ARP poisoning and spoofing

Setting up Ettercap

- Start Ettercap- graphical on kali machine and enter root password



Setup

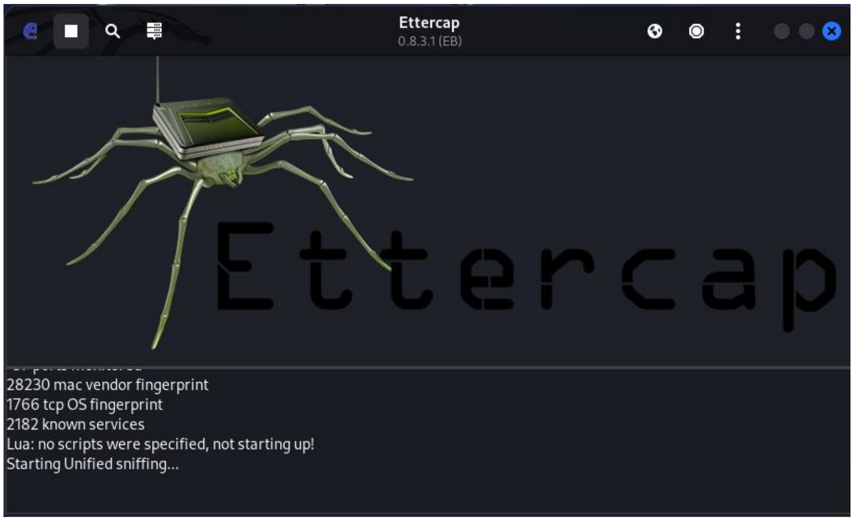
Sniffing at startup: on

Primary Interface: eth0

Bridged sniffing: off

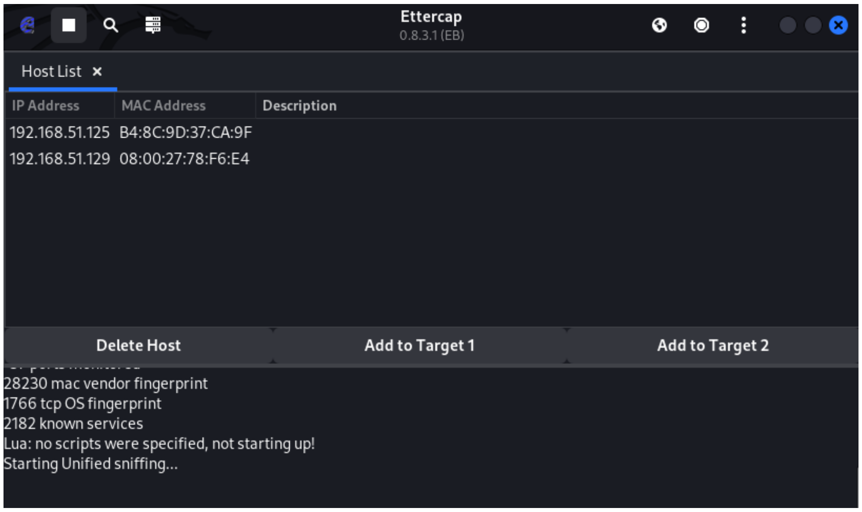
Bridged Interface: Local Loopback

- Now click on tick option on the right top side



```
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

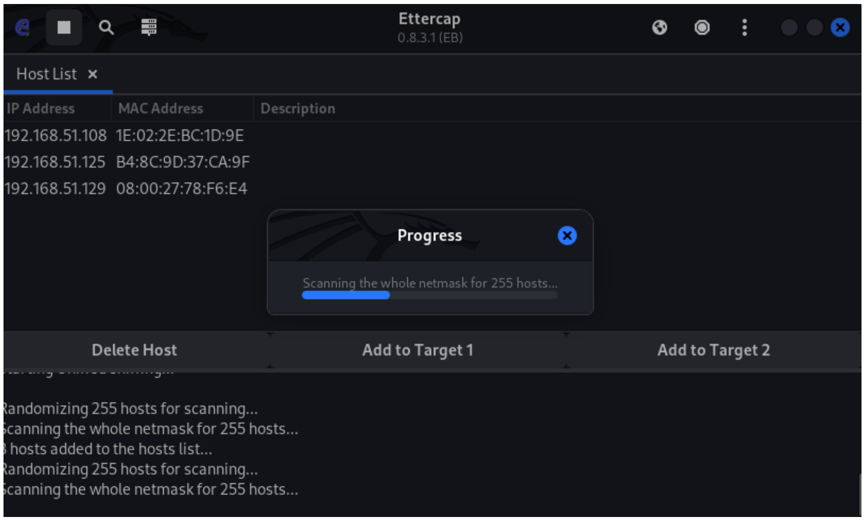
- Now click on 3 dots and choose host option and go to host list



IP Address	MAC Address	Description
192.168.51.125	B4:8C:9D:37:CA:9F	
192.168.51.129	08:00:27:78:F6:E4	

```
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

- Now again click on 3 dots and go to host and select scan for hosts

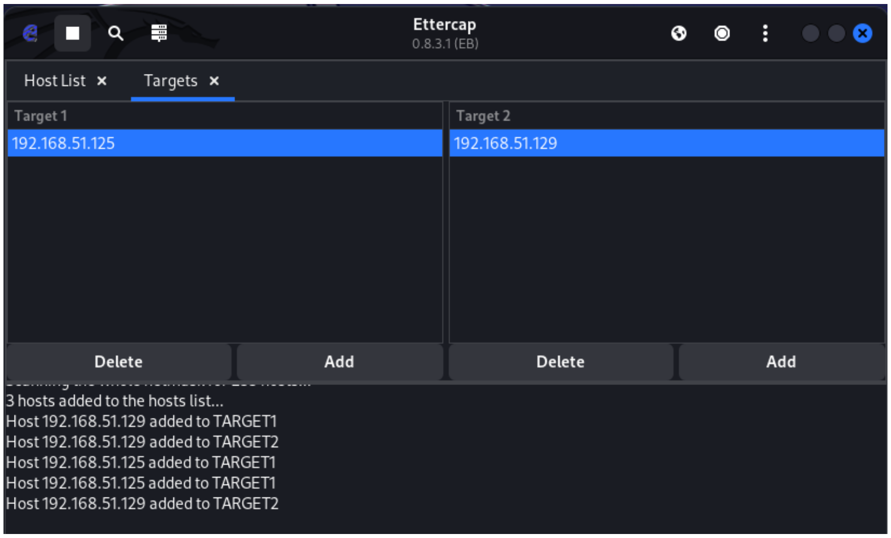


IP Address	MAC Address	Description
192.168.51.108	1E:02:2E:BC:1D:9E	
192.168.51.125	B4:8C:9D:37:CA:9F	
192.168.51.129	08:00:27:78:F6:E4	

Scanning the whole netmask for 255 hosts...

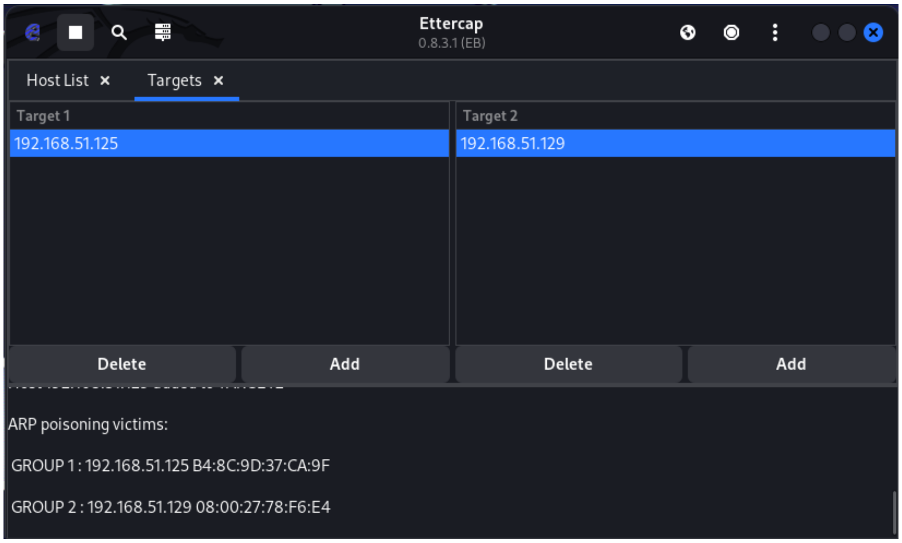
```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
```

- Now add victim machine IP address as target one and server machine IP address as target two



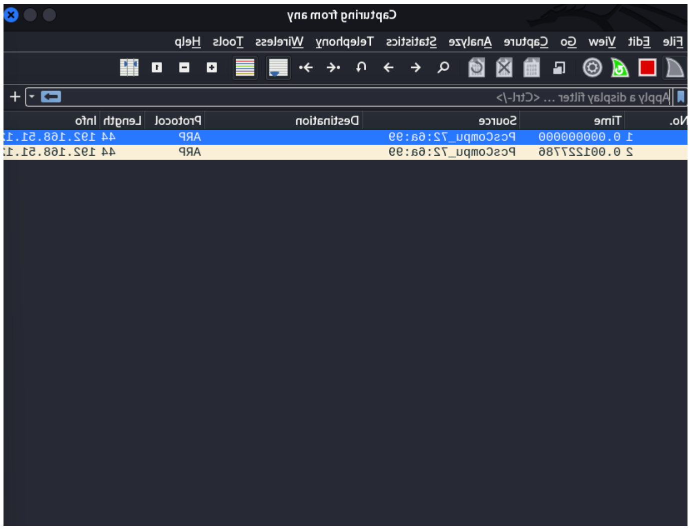
```
3 hosts added to the hosts list...
Host 192.168.51.129 added to TARGET1
Host 192.168.51.129 added to TARGET2
Host 192.168.51.125 added to TARGET1
Host 192.168.51.125 added to TARGET1
Host 192.168.51.129 added to TARGET2
```

- Now click on MITM menu and select ARP poisoning and select sniff remote connections to start ARP poisoning and sniffing packets



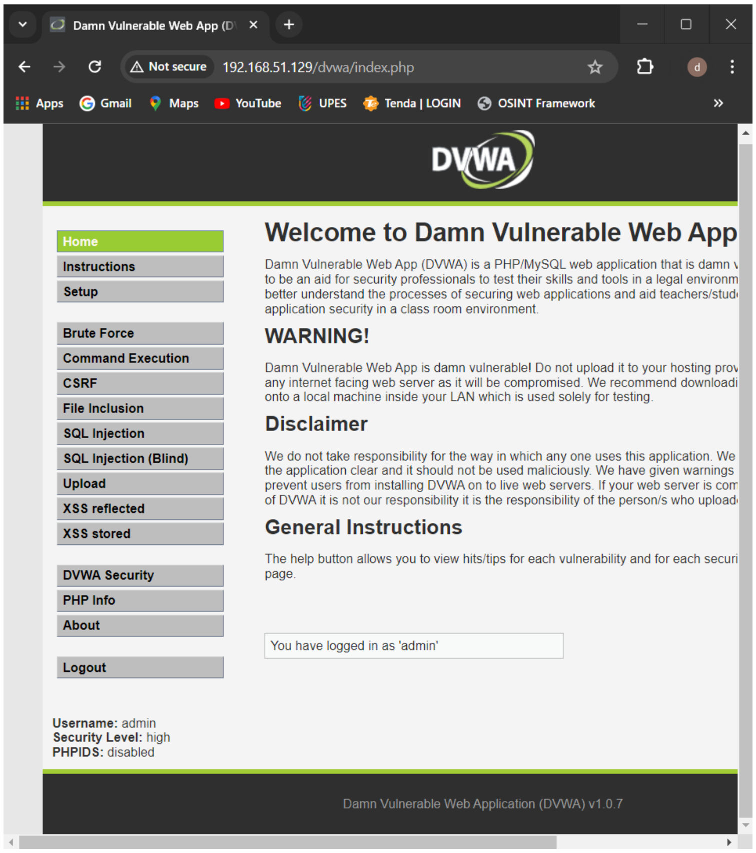
```
ARP poisoning victims:

 GROUP 1 : 192.168.51.125 B4:8C:9D:37:CA:9F

 GROUP 2 : 192.168.51.129 08:00:27:78:F6:E4
```

- Now start wire shark



```
No.  Time          Source              Destination   Protocol  Length  Info
1    0.000000000   PcsCompu_72:6a:99                 ARP       44      192.168.51.1
2    0.001227786   PcsCompu_72:6a:99                 ARP       44      192.168.51.1
```

- Now on windows machine open dvwa



Welcome to Damn Vulnerable Web App

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn v
to be an aid for security professionals to test their skills and tools in a legal environm
better understand the processes of securing web applications and aid teachers/stud
application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting prov
any internet facing web server as it will be compromised. We recommend downloadi
onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We
the application clear and it should not be used maliciously. We have given warnings
prevent users from installing DVWA on to live web servers. If your web server is com
of DVWA it is not our responsibility it is the responsibility of the person/s who upload

General Instructions

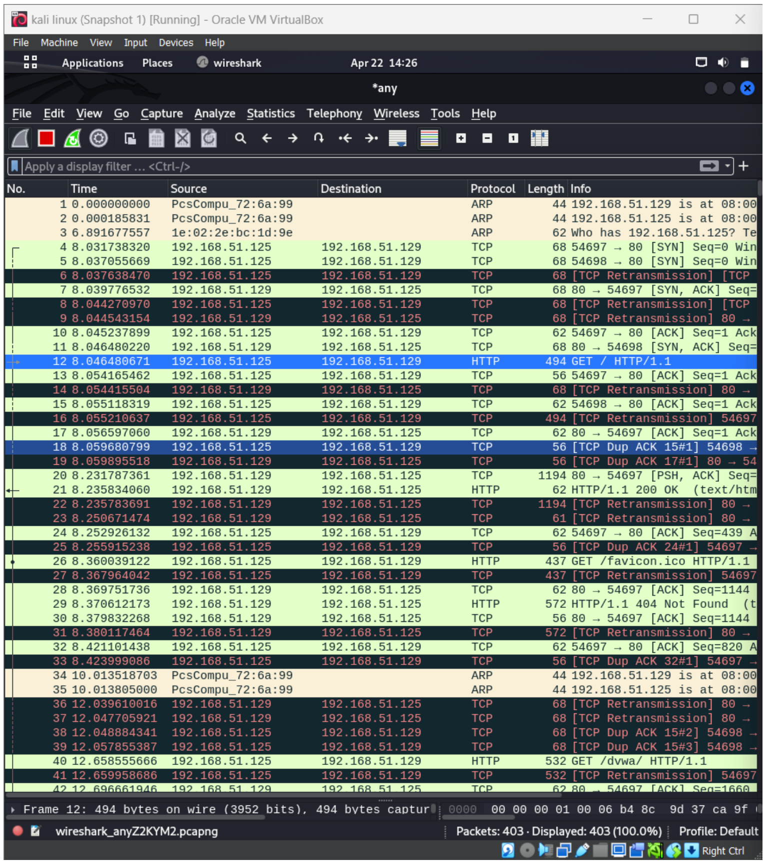
The help button allows you to view hits/tips for each vulnerability and for each securi
page.

You have logged in as 'admin'

Username: admin
Security Level: high
PHPIDS: disabled

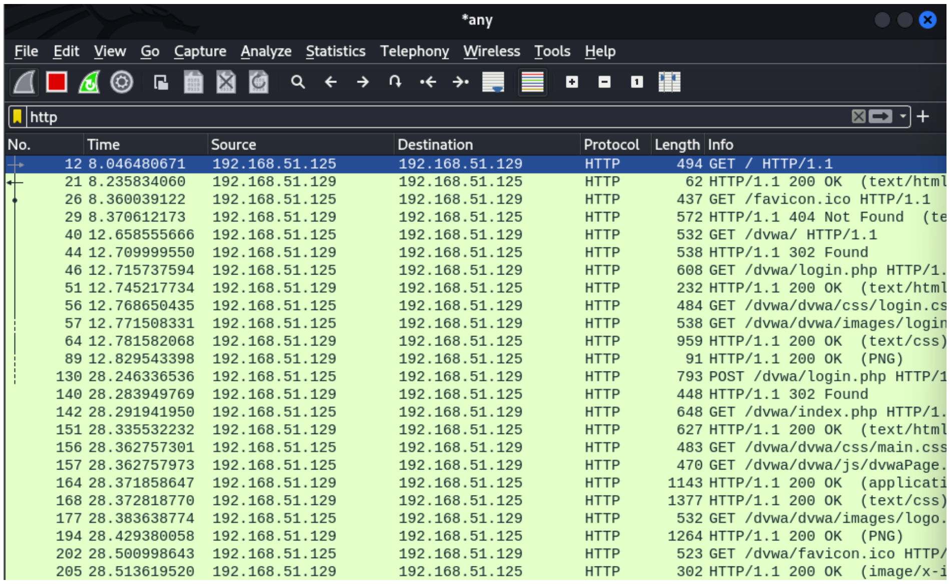
Damn Vulnerable Web Application (DVWA) v1.0.7

- Now go to wire shark all the packets from victim machine to server machine is going via kali machine


kali linux (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places wireshark
Apr 22 14:26
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Right Ctrl

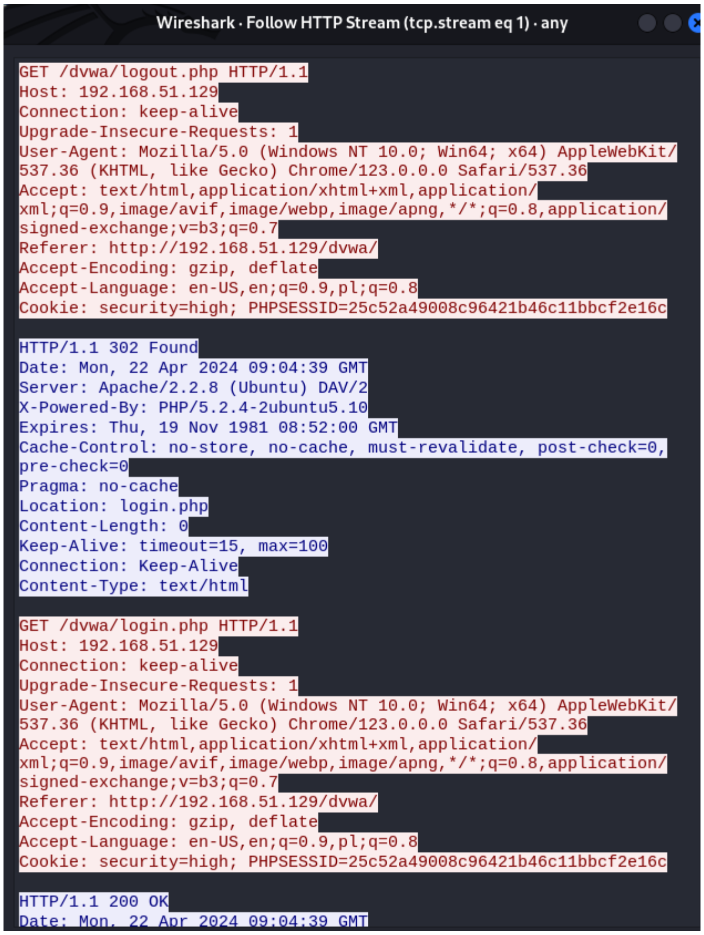
```
No.  Time          Source              Destination      Protocol Length Info
   1 0.000000000   PcsCompu_72:6a:99                    ARP        44 192.168.51.129 is at 08:00
   2 0.000185831   PcsCompu_72:6a:99                    ARP        44 192.168.51.125 is at 08:00
   3 6.891677557   1e:02:2e:bc:1d:9e                    ARP        62 Who has 192.168.51.125? Te
   4 8.031738320   192.168.51.125      192.168.51.129   TCP        68 54697 → 80 [SYN] Seq=0 Win
   5 8.037055669   192.168.51.125      192.168.51.129   TCP        68 54698 → 80 [SYN] Seq=0 Win
   6 8.037638470   192.168.51.125      192.168.51.129   TCP        68 [TCP Retransmission] [TCP
   7 8.039776532   192.168.51.129      192.168.51.125   TCP        68 80 → 54697 [SYN, ACK] Seq=
   8 8.044270970   192.168.51.125      192.168.51.129   TCP        68 [TCP Retransmission] [TCP
   9 8.044543154   192.168.51.129      192.168.51.125   TCP        68 [TCP Retransmission] 80 →
  10 8.045237899   192.168.51.125      192.168.51.129   TCP        62 54697 → 80 [ACK] Seq=1 Ack
  11 8.046480220   192.168.51.129      192.168.51.125   TCP        68 80 → 54698 [SYN, ACK] Seq=
  12 8.046480671   192.168.51.125      192.168.51.129   HTTP      494 GET / HTTP/1.1
  13 8.054165462   192.168.51.125      192.168.51.129   TCP        56 54697 → 80 [ACK] Seq=1 Ack
  14 8.054415504   192.168.51.129      192.168.51.125   TCP        68 [TCP Retransmission] 80 →
  15 8.055118319   192.168.51.125      192.168.51.129   TCP        62 54698 → 80 [ACK] Seq=1 Ack
  16 8.055210637   192.168.51.125      192.168.51.129   TCP       494 [TCP Retransmission] 54697
  17 8.056597060   192.168.51.129      192.168.51.125   TCP        62 80 → 54697 [ACK] Seq=1 Ack
  18 8.059680799   192.168.51.125      192.168.51.129   TCP        56 [TCP Dup ACK 15#1] 54698 →
  19 8.059895518   192.168.51.129      192.168.51.125   TCP        56 [TCP Dup ACK 17#1] 80 → 54
  20 8.231787361   192.168.51.129      192.168.51.125   TCP      1194 80 → 54697 [PSH, ACK] Seq=
  21 8.235834060   192.168.51.129      192.168.51.125   HTTP       62 HTTP/1.1 200 OK  (text/htm
  22 8.235783691   192.168.51.129      192.168.51.125   TCP      1194 [TCP Retransmission] 80 →
  23 8.250671474   192.168.51.129      192.168.51.125   TCP        61 [TCP Retransmission] 80 →
  24 8.252926132   192.168.51.125      192.168.51.129   TCP        62 54697 → 80 [ACK] Seq=439 A
  25 8.255915238   192.168.51.125      192.168.51.129   TCP        56 [TCP Dup ACK 24#1] 54697 →
  26 8.360039122   192.168.51.125      192.168.51.129   HTTP      437 GET /favicon.ico HTTP/1.1
  27 8.367964042   192.168.51.125      192.168.51.129   TCP       437 [TCP Retransmission] 54697
  28 8.369751736   192.168.51.129      192.168.51.125   TCP        62 80 → 54697 [ACK] Seq=1144
  29 8.370612173   192.168.51.129      192.168.51.125   HTTP      572 HTTP/1.1 404 Not Found  (t
  30 8.379832268   192.168.51.129      192.168.51.125   TCP        56 80 → 54697 [ACK] Seq=1144
  31 8.380117464   192.168.51.129      192.168.51.125   TCP       572 [TCP Retransmission] 80 →
  32 8.421101438   192.168.51.125      192.168.51.129   TCP        62 54697 → 80 [ACK] Seq=820 A
  33 8.423999086   192.168.51.125      192.168.51.129   TCP        56 [TCP Dup ACK 32#1] 54697 →
  34 10.013518703  PcsCompu_72:6a:99                    ARP        44 192.168.51.129 is at 08:00
  35 10.013805000  PcsCompu_72:6a:99                    ARP        44 192.168.51.125 is at 08:00
  36 12.039610016  192.168.51.129      192.168.51.125   TCP        68 [TCP Retransmission] 80 →
  37 12.047705921  192.168.51.129      192.168.51.125   TCP        68 [TCP Retransmission] 80 →
  38 12.048884341  192.168.51.125      192.168.51.129   TCP        68 [TCP Dup ACK 15#2] 54698 →
  39 12.057855387  192.168.51.125      192.168.51.129   TCP        68 [TCP Dup ACK 15#3] 54698 →
  40 12.658555666  192.168.51.125      192.168.51.129   HTTP      532 GET /dvwa/ HTTP/1.1
  41 12.659958686  192.168.51.125      192.168.51.129   TCP       532 [TCP Retransmission] 54697
  42 12.696661946  192.168.51.129      192.168.51.125   TCP        62 80 → 54697 [ACK] Seq=1660

› Frame 12: 494 bytes on wire (3952 bits), 494 bytes captur   0000  00 00 00 01 00 06 b4 8c  9d 37 ca 9f
wireshark_anyZ2KYM2.pcapng          Packets: 403 · Displayed: 403 (100.0%)   Profile: Default
```

- Now search for http packets on wire shark


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

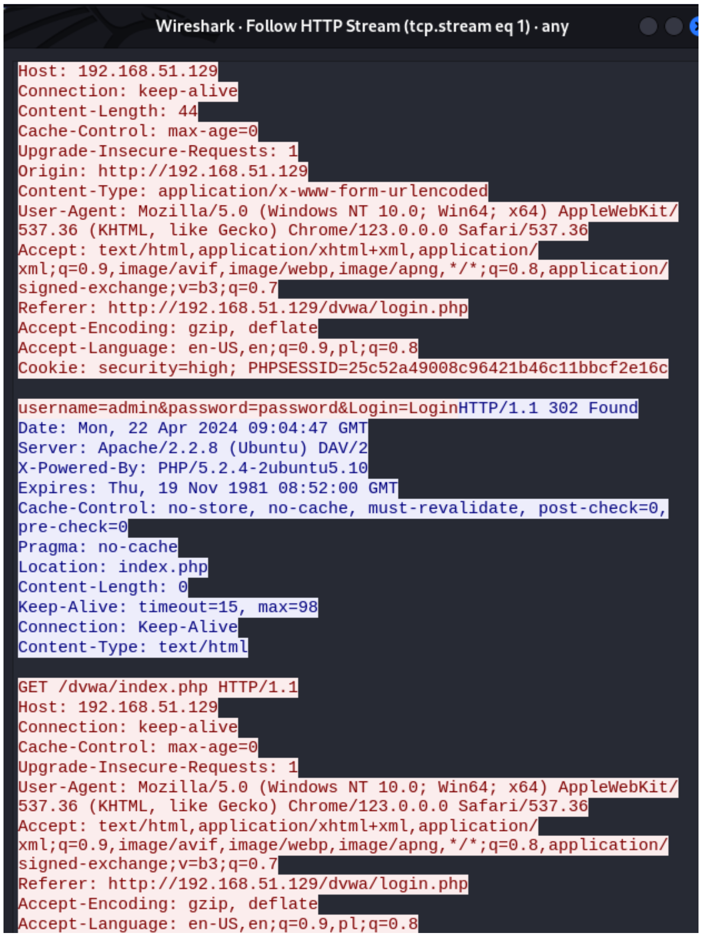
```
No.     Time          Source          Destination     Protocol Length Info
     12 8.046480671   192.168.51.125  192.168.51.129  HTTP      494 GET / HTTP/1.1
     21 8.235834060   192.168.51.129  192.168.51.125  HTTP       62 HTTP/1.1 200 OK  (text/html
     26 8.360039122   192.168.51.125  192.168.51.129  HTTP      437 GET /favicon.ico HTTP/1.1
     29 8.370612173   192.168.51.129  192.168.51.125  HTTP      572 HTTP/1.1 404 Not Found  (te
     40 12.658555666  192.168.51.125  192.168.51.129  HTTP      532 GET /dvwa/ HTTP/1.1
     44 12.709999550  192.168.51.129  192.168.51.125  HTTP      538 HTTP/1.1 302 Found
     46 12.715737594  192.168.51.125  192.168.51.129  HTTP      608 GET /dvwa/login.php HTTP/1.
     51 12.745217734  192.168.51.129  192.168.51.125  HTTP      232 HTTP/1.1 200 OK  (text/html
     56 12.768650435  192.168.51.125  192.168.51.129  HTTP      484 GET /dvwa/dvwa/css/login.cs
     57 12.771508331  192.168.51.125  192.168.51.129  HTTP      538 GET /dvwa/dvwa/images/login
     64 12.781582068  192.168.51.129  192.168.51.125  HTTP      959 HTTP/1.1 200 OK  (text/css)
     89 12.829543398  192.168.51.129  192.168.51.125  HTTP       91 HTTP/1.1 200 OK  (PNG)
    130 28.246336536  192.168.51.125  192.168.51.129  HTTP      793 POST /dvwa/login.php HTTP/1
    140 28.283949769  192.168.51.129  192.168.51.125  HTTP      448 HTTP/1.1 302 Found
    142 28.291941950  192.168.51.125  192.168.51.129  HTTP      648 GET /dvwa/index.php HTTP/1.
    151 28.335532232  192.168.51.129  192.168.51.125  HTTP      627 HTTP/1.1 200 OK  (text/html
    156 28.362757301  192.168.51.125  192.168.51.129  HTTP      483 GET /dvwa/dvwa/css/main.css
    157 28.362757973  192.168.51.125  192.168.51.129  HTTP      470 GET /dvwa/dvwa/js/dvwaPage.
    164 28.371858647  192.168.51.129  192.168.51.125  HTTP     1143 HTTP/1.1 200 OK  (applicati
    168 28.372818770  192.168.51.129  192.168.51.125  HTTP     1377 HTTP/1.1 200 OK  (text/css)
    177 28.383638774  192.168.51.125  192.168.51.129  HTTP      532 GET /dvwa/dvwa/images/logo.
    194 28.429380058  192.168.51.129  192.168.51.125  HTTP     1264 HTTP/1.1 200 OK  (PNG)
    202 28.500998643  192.168.51.125  192.168.51.129  HTTP      523 GET /dvwa/favicon.ico HTTP/
    205 28.513619520  192.168.51.129  192.168.51.125  HTTP      302 HTTP/1.1 200 OK  (image/x-i
```

- To get mere information follow http packets
- I am following packet of login page to find username password and other details



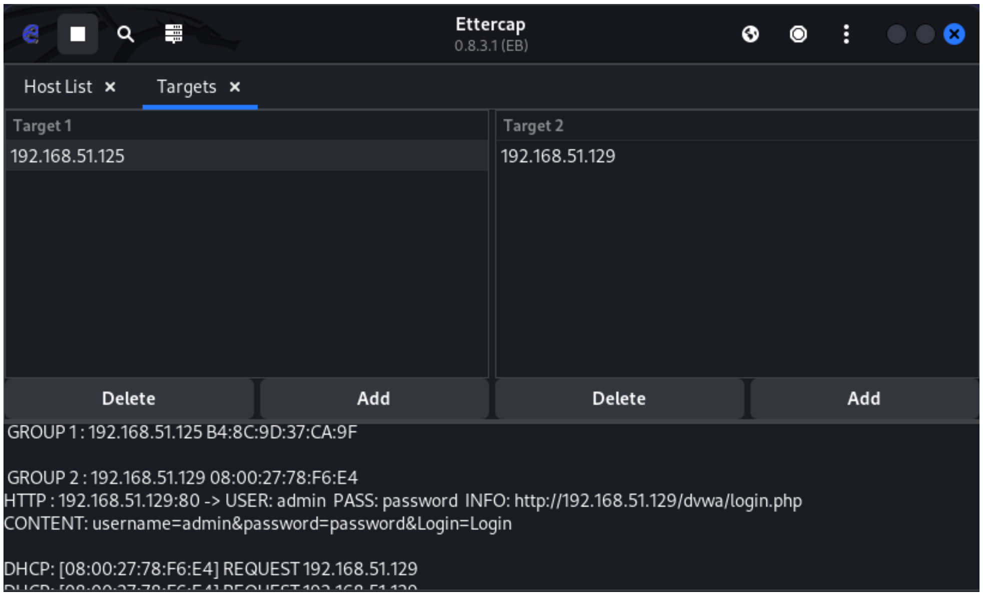
```
GET /dvwa/logout.php HTTP/1.1
Host: 192.168.51.129
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/
xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.7
Referer: http://192.168.51.129/dvwa/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,pl;q=0.8
Cookie: security=high; PHPSESSID=25c52a49008c96421b46c11bbcf2e16c

HTTP/1.1 302 Found
Date: Mon, 22 Apr 2024 09:04:39 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
Connection: Keep-Alive
Content-Type: text/html

GET /dvwa/login.php HTTP/1.1
Host: 192.168.51.129
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/
xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.7
Referer: http://192.168.51.129/dvwa/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,pl;q=0.8
Cookie: security=high; PHPSESSID=25c52a49008c96421b46c11bbcf2e16c

HTTP/1.1 200 OK
Date: Mon, 22 Apr 2024 09:04:39 GMT
```

- Since dvwa is an HTTP site so it is not secured and using get method for login form so we can see details by following http packets



```
Host: 192.168.51.129
Connection: keep-alive
Content-Length: 44
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.51.129
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/
xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.7
Referer: http://192.168.51.129/dvwa/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,pl;q=0.8
Cookie: security=high; PHPSESSID=25c52a49008c96421b46c11bbcf2e16c

username=admin&password=password&Login=LoginHTTP/1.1 302 Found
Date: Mon, 22 Apr 2024 09:04:47 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: index.php
Content-Length: 0
Keep-Alive: timeout=15, max=98
Connection: Keep-Alive
Content-Type: text/html

GET /dvwa/index.php HTTP/1.1
Host: 192.168.51.129
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/
xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.7
Referer: http://192.168.51.129/dvwa/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,pl;q=0.8
```

- And we also get username and password on etter cap also



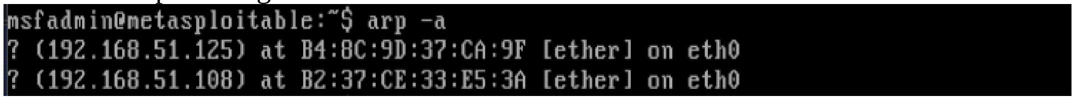
Target 1: 192.168.51.125

Target 2: 192.168.51.129

```
GROUP 1 : 192.168.51.125 B4:8C:9D:37:CA:9F

GROUP 2 : 192.168.51.129 08:00:27:78:F6:E4
HTTP : 192.168.51.129:80 -> USER: admin  PASS: password  INFO: http://192.168.51.129/dvwa/login.php
CONTENT: username=admin&password=password&Login=Login

DHCP: [08:00:27:78:F6:E4] REQUEST 192.168.51.129
DHCP: [08:00:27:78:F6:E4] REQUEST 192.168.51.129
```

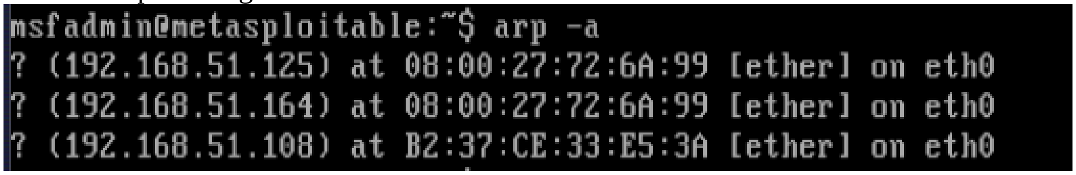
- We can check ARP poisoning by using command arp -a on meta and windows

Meta
Before ARP poisoning



```
msfadmin@metasploitable:~$ arp -a
? (192.168.51.125) at B4:8C:9D:37:CA:9F [ether] on eth0
? (192.168.51.108) at B2:37:CE:33:E5:3A [ether] on eth0
```

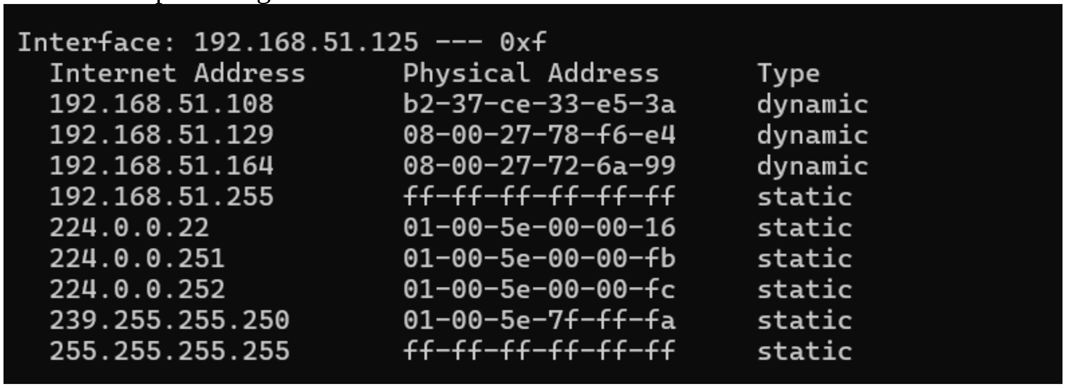
After ARP poisoning



```
msfadmin@metasploitable:~$ arp -a
? (192.168.51.125) at 08:00:27:72:6A:99 [ether] on eth0
? (192.168.51.164) at 08:00:27:72:6A:99 [ether] on eth0
? (192.168.51.108) at B2:37:CE:33:E5:3A [ether] on eth0
```

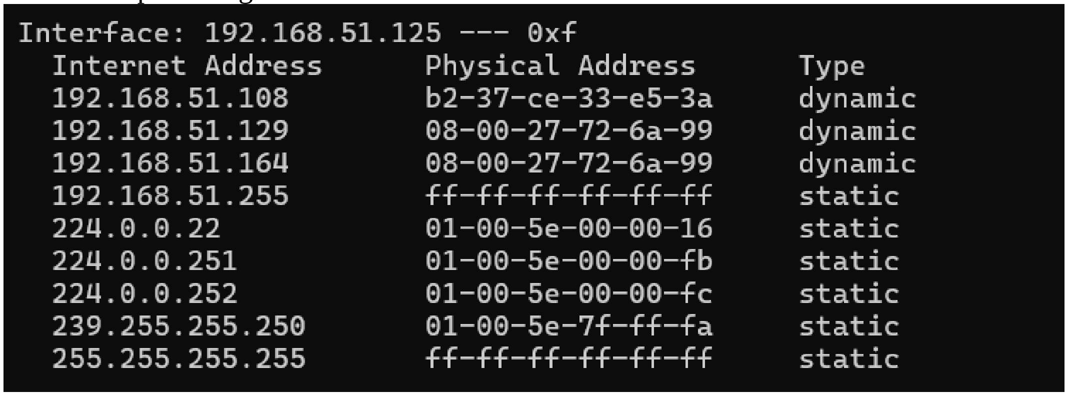
We can see that the mac address of kali and windows is same which means that the arp table has been poisoned

Windows
Before ARP poisoning



```
Interface: 192.168.51.125 --- 0xf
  Internet Address      Physical Address      Type
  192.168.51.108        b2-37-ce-33-e5-3a     dynamic
  192.168.51.129        08-00-27-78-f6-e4     dynamic
  192.168.51.164        08-00-27-72-6a-99     dynamic
  192.168.51.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

After ARP poisoning

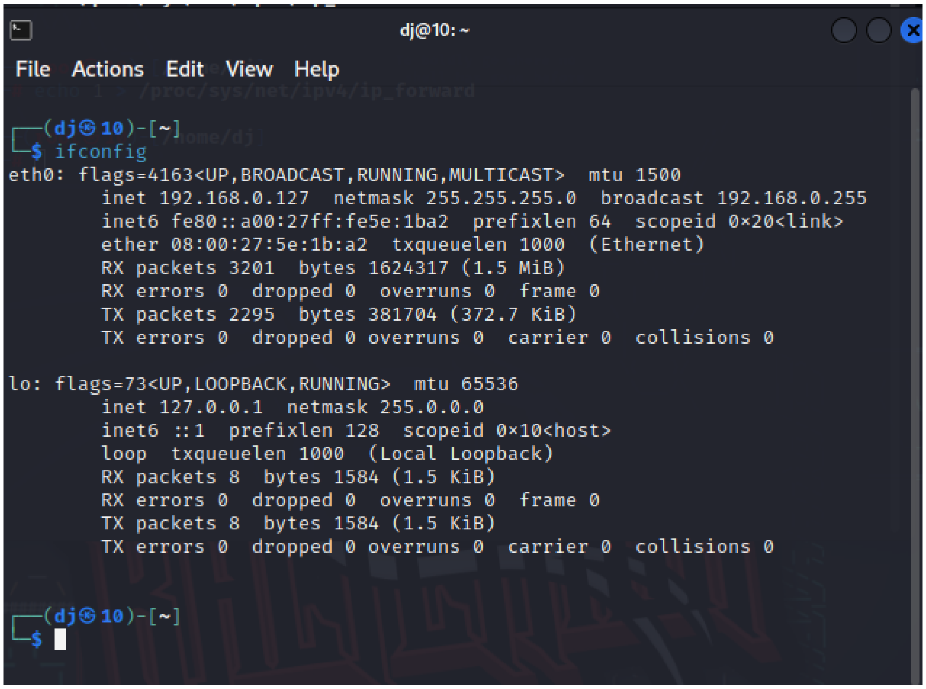


```
Interface: 192.168.51.125 --- 0xf
  Internet Address      Physical Address      Type
  192.168.51.108        b2-37-ce-33-e5-3a     dynamic
  192.168.51.129        08-00-27-72-6a-99     dynamic
  192.168.51.164        08-00-27-72-6a-99     dynamic
  192.168.51.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

We can see that the mac address of kali and meta is same which means that the arp table has been poisoned

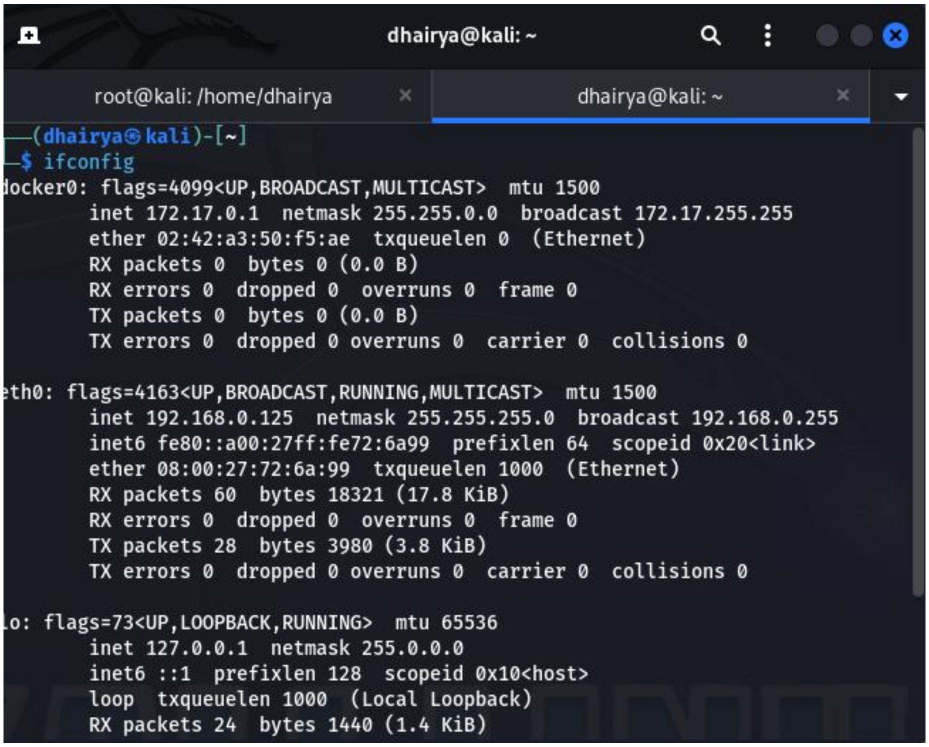
Demo.testfire.net

Victim machine IP Address



```
┌──(dj㉿10)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.127  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe5e:1ba2  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5e:1b:a2  txqueuelen 1000  (Ethernet)
        RX packets 3201  bytes 1624317 (1.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2295  bytes 381704 (372.7 KiB)
        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 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 1584 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 1584 (1.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(dj㉿10)-[~]
└─$ 
```

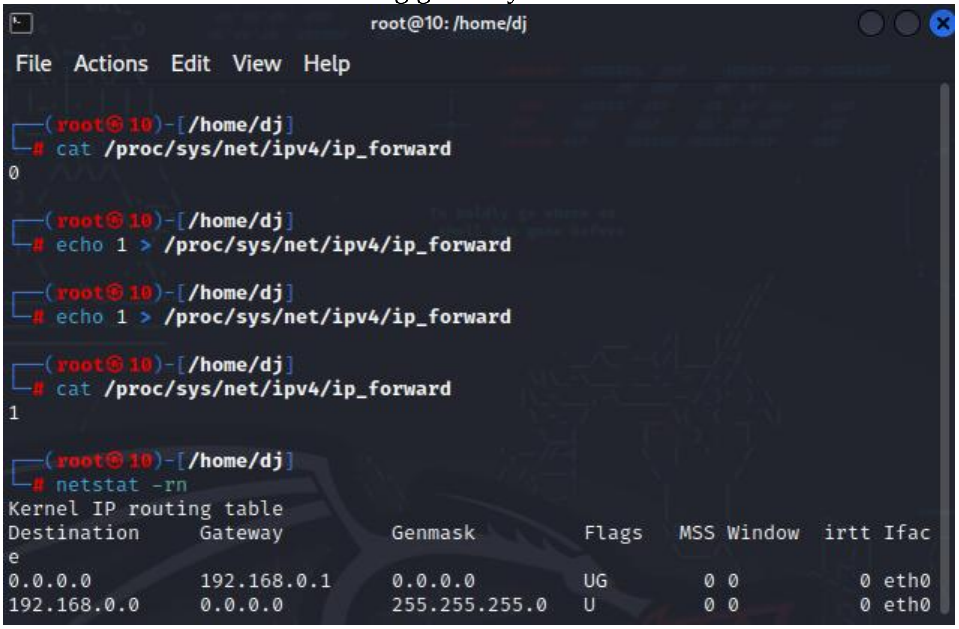
Kali machine IP Address



```
┌──(dhairya㉿kali)-[~]
└─$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:a3:50:f5:ae  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.125  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe72:6a99  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:72:6a:99  txqueuelen 1000  (Ethernet)
        RX packets 60  bytes 18321 (17.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 3980 (3.8 KiB)
        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 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1440 (1.4 KiB)
```

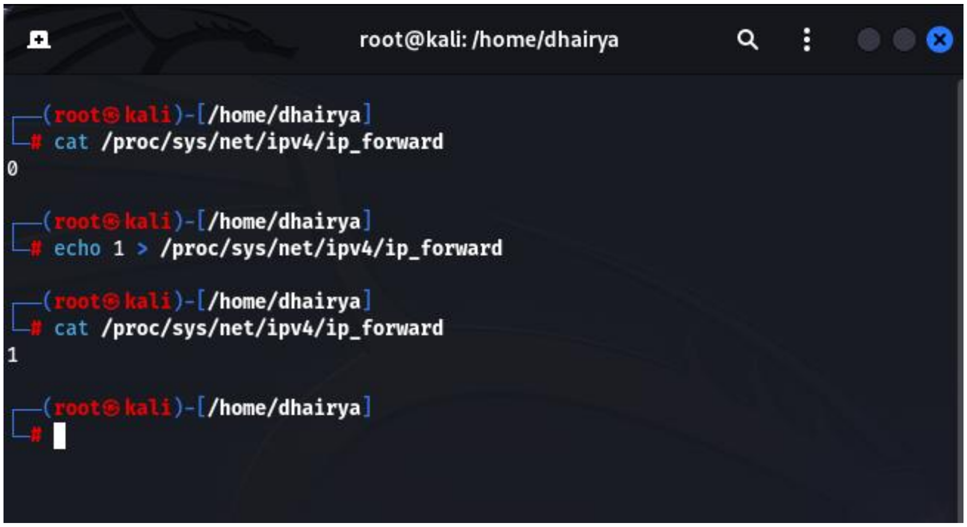
Starting IP forwarding on both machine

Victim machine and also checking gate way IP



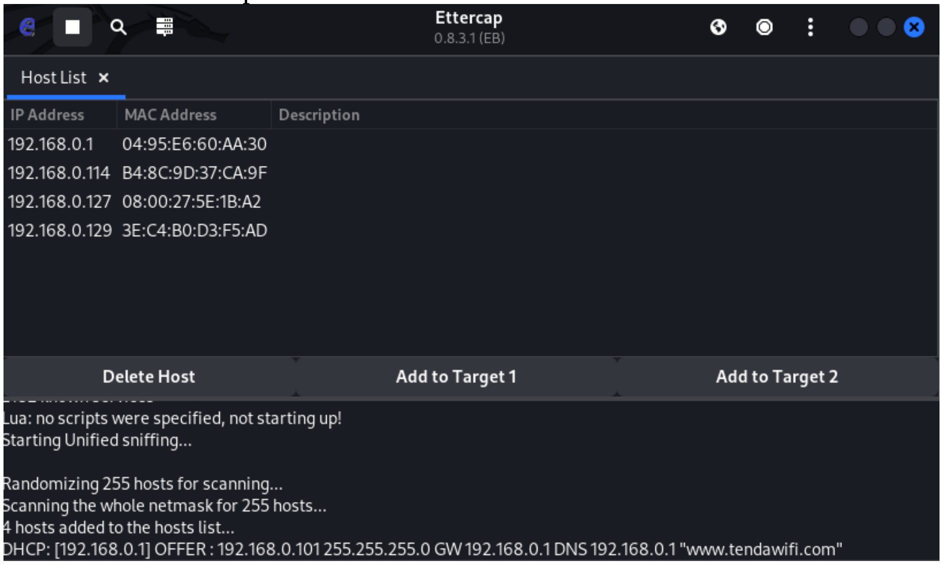
```
┌──(root㉿10)-[/home/dj]
└─# cat /proc/sys/net/ipv4/ip_forward
0

┌──(root㉿10)-[/home/dj]
└─# echo 1 > /proc/sys/net/ipv4/ip_forward

┌──(root㉿10)-[/home/dj]
└─# echo 1 > /proc/sys/net/ipv4/ip_forward

┌──(root㉿10)-[/home/dj]
└─# cat /proc/sys/net/ipv4/ip_forward
1

┌──(root㉿10)-[/home/dj]
└─# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Ifac
e
0.0.0.0         192.168.0.1     0.0.0.0         UG        0 0          0 eth0
192.168.0.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

Kali machine IP address



```
┌──(root㉿kali)-[/home/dhairya]
└─# cat /proc/sys/net/ipv4/ip_forward
0

┌──(root㉿kali)-[/home/dhairya]
└─# echo 1 > /proc/sys/net/ipv4/ip_forward

┌──(root㉿kali)-[/home/dhairya]
└─# cat /proc/sys/net/ipv4/ip_forward
1

┌──(root㉿kali)-[/home/dhairya]
└─# █
```

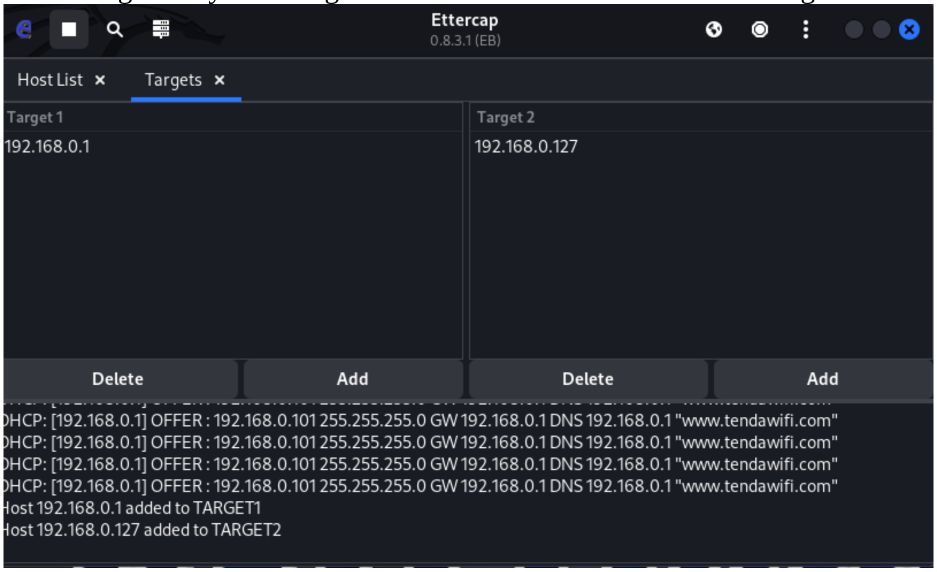
Now turn on Ettercap and scan for host



IP Address	MAC Address	Description
192.168.0.1	04:95:E6:60:AA:30	
192.168.0.114	B4:8C:9D:37:CA:9F	
192.168.0.127	08:00:27:5E:1B:A2	
192.168.0.129	3E:C4:B0:D3:F5:AD	

```
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
DHCP: [192.168.0.1] OFFER : 192.168.0.101 255.255.255.0 GW 192.168.0.1 DNS 192.168.0.1 "www.tendawifi.com"
```

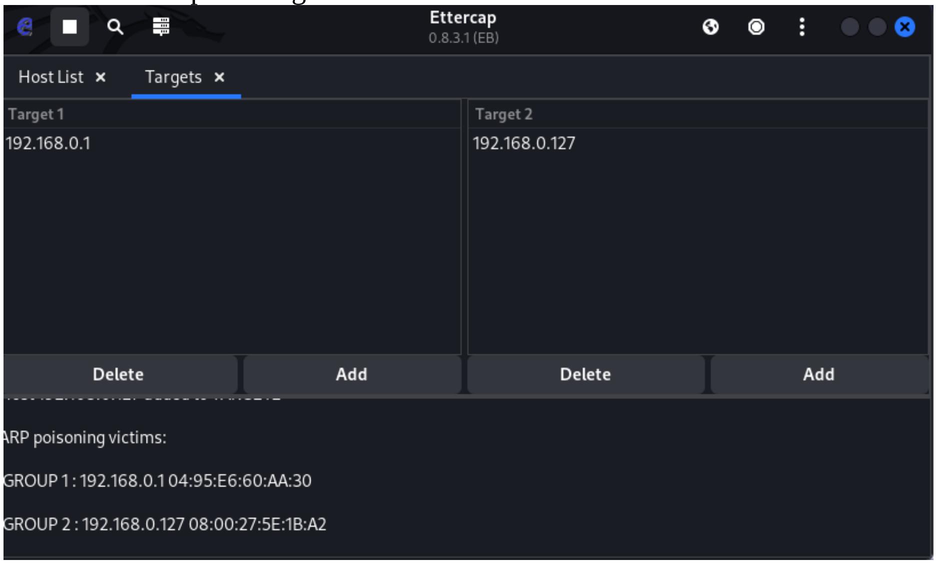
Now add gate way IP to target one and add victim machine IP to target to



Target 1	Target 2
192.168.0.1	192.168.0.127

```
DHCP: [192.168.0.1] OFFER : 192.168.0.101 255.255.255.0 GW 192.168.0.1 DNS 192.168.0.1 "www.tendawifi.com"
DHCP: [192.168.0.1] OFFER : 192.168.0.101 255.255.255.0 GW 192.168.0.1 DNS 192.168.0.1 "www.tendawifi.com"
DHCP: [192.168.0.1] OFFER : 192.168.0.101 255.255.255.0 GW 192.168.0.1 DNS 192.168.0.1 "www.tendawifi.com"
DHCP: [192.168.0.1] OFFER : 192.168.0.101 255.255.255.0 GW 192.168.0.1 DNS 192.168.0.1 "www.tendawifi.com"
Host 192.168.0.1 added to TARGET1
Host 192.168.0.127 added to TARGET2
```

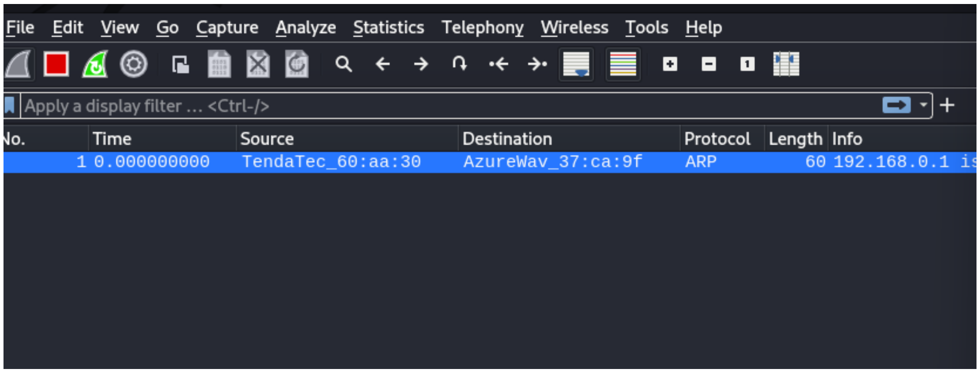
Now start ARP poisoning



Target 1	Target 2
192.168.0.1	192.168.0.127

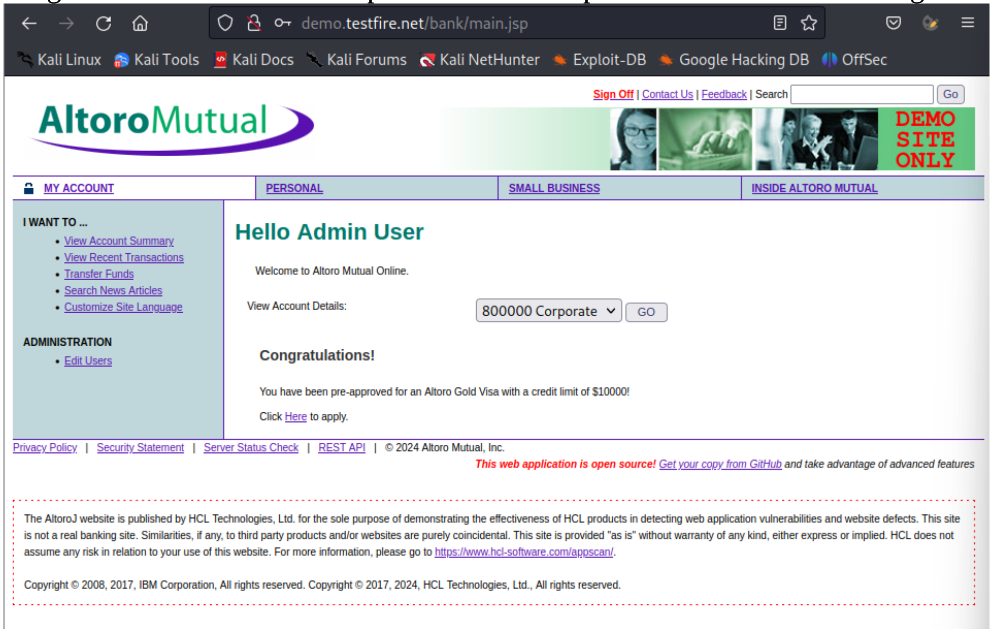
```
ARP poisoning victims:

GROUP 1 : 192.168.0.1 04:95:E6:60:AA:30

GROUP 2 : 192.168.0.127 08:00:27:5E:1B:A2
```

Now start wire shark in kali machine on eth0


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time          Source                Destination           Protocol  Length Info
    1 0.000000000   TendaTec_60:aa:30     AzureWav_37:ca:9f     ARP           60 192.168.0.1 is
```

No go to victim machine and open browser and open demo.testfire.net and log in


demo.testfire.net/bank/main.jsp
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Sign Off | Contact Us | Feedback | Search Go
AltoroMutual
DEMO SITE ONLY
MY ACCOUNT PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.

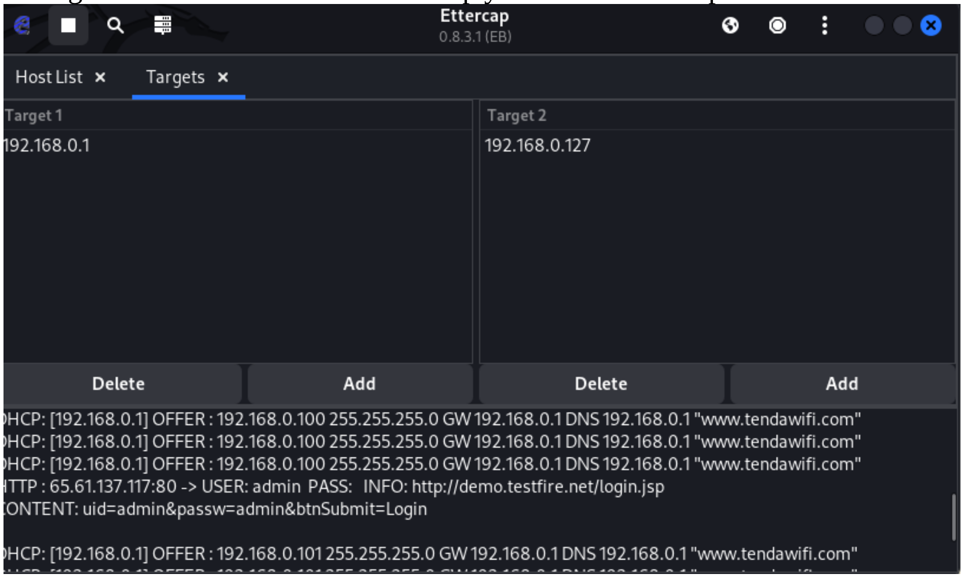
Privacy Policy | Security Statement | Server Status Check | REST API | © 2024 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.

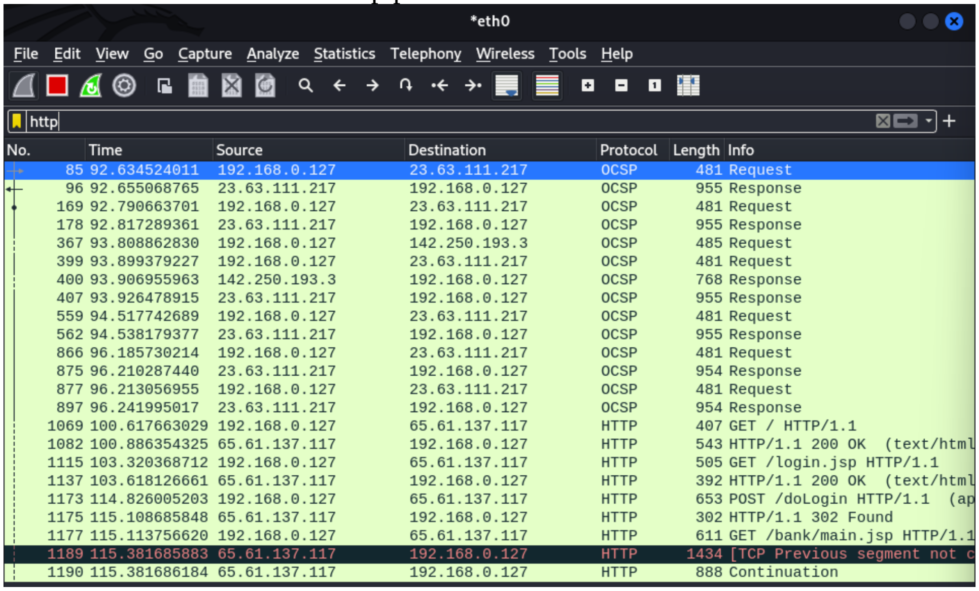
Now go to kali machine and on Ettercap you can see id and password



Target 1	Target 2
192.168.0.1	192.168.0.127

```
)HCP: [192.168.0.1] OFFER : 192.168.0.100 255.255.255.0 GW 192.168.0.1 DNS 192.168.0.1 "www.tendawifi.com"
)HCP: [192.168.0.1] OFFER : 192.168.0.100 255.255.255.0 GW 192.168.0.1 DNS 192.168.0.1 "www.tendawifi.com"
)HCP: [192.168.0.1] OFFER : 192.168.0.100 255.255.255.0 GW 192.168.0.1 DNS 192.168.0.1 "www.tendawifi.com"
ITTP : 65.61.137.117:80 -> USER: admin  PASS:   INFO: http://demo.testfire.net/login.jsp
:ONTENT: uid=admin&passw=admin&btnSubmit=Login

)HCP: [192.168.0.1] OFFER : 192.168.0.101 255.255.255.0 GW 192.168.0.1 DNS 192.168.0.1 "www.tendawifi.com"
```

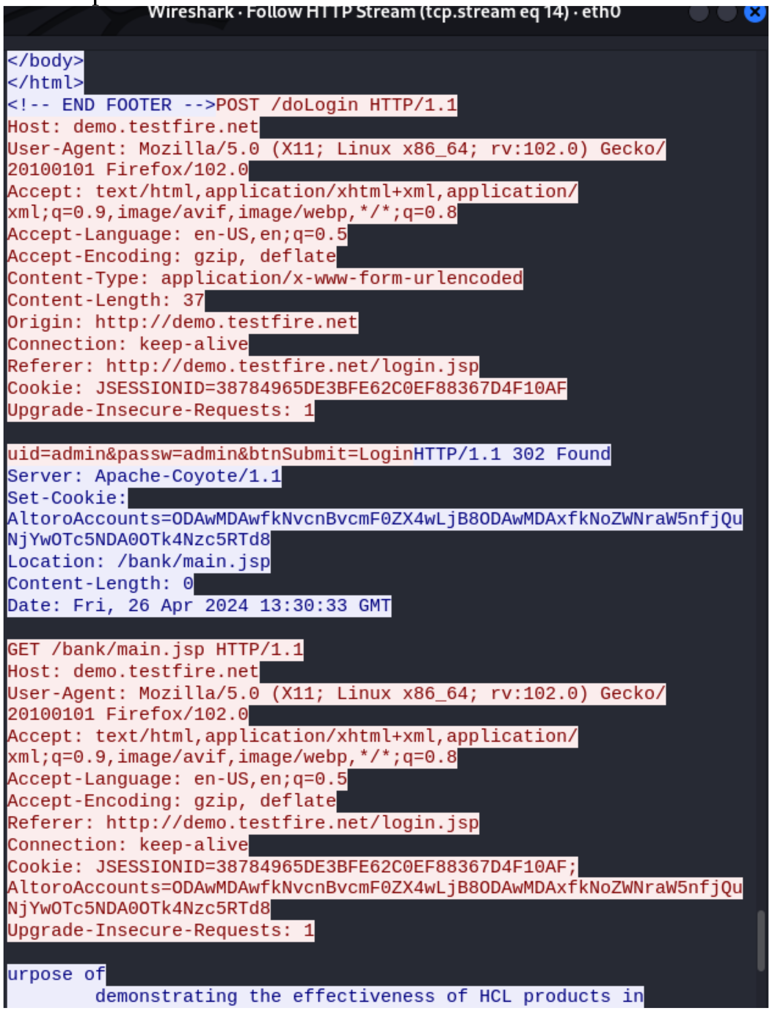
Now Wireshark on filter for http packets


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.   Time            Source          Destination     Protocol Length Info
   85 92.634524011    192.168.0.127   23.63.111.217   OCSP     481 Request
   96 92.655068765    23.63.111.217   192.168.0.127   OCSP     955 Response
  169 92.790663701    192.168.0.127   23.63.111.217   OCSP     481 Request
  178 92.817289361    23.63.111.217   192.168.0.127   OCSP     955 Response
  367 93.808862830    192.168.0.127   142.250.193.3   OCSP     485 Request
  399 93.899379227    192.168.0.127   23.63.111.217   OCSP     481 Request
  400 93.906955963    142.250.193.3   192.168.0.127   OCSP     768 Response
  407 93.926478915    23.63.111.217   192.168.0.127   OCSP     955 Response
  559 94.517742689    192.168.0.127   23.63.111.217   OCSP     481 Request
  562 94.538179377    23.63.111.217   192.168.0.127   OCSP     955 Response
  866 96.185730214    192.168.0.127   23.63.111.217   OCSP     481 Request
  875 96.210287440    23.63.111.217   192.168.0.127   OCSP     954 Response
  877 96.213056955    192.168.0.127   23.63.111.217   OCSP     481 Request
  897 96.241995017    23.63.111.217   192.168.0.127   OCSP     954 Response
 1069 100.617663029   192.168.0.127   65.61.137.117   HTTP     407 GET / HTTP/1.1
 1082 100.886354325   65.61.137.117   192.168.0.127   HTTP     543 HTTP/1.1 200 OK  (text/html
 1115 103.320368712   192.168.0.127   65.61.137.117   HTTP     505 GET /login.jsp HTTP/1.1
 1137 103.618126661   65.61.137.117   192.168.0.127   HTTP     392 HTTP/1.1 200 OK  (text/html
 1173 114.826005203   192.168.0.127   65.61.137.117   HTTP     653 POST /doLogin HTTP/1.1  (ap
 1175 115.108685848   65.61.137.117   192.168.0.127   HTTP     302 HTTP/1.1 302 Found
 1177 115.113756620   192.168.0.127   65.61.137.117   HTTP     611 GET /bank/main.jsp HTTP/1.1
 1189 115.381685883   65.61.137.117   192.168.0.127   HTTP    1434 [TCP Previous segment not c
 1190 115.381686184   65.61.137.117   192.168.0.127   HTTP     888 Continuation
```

Now we can see the http packets now we will follow the login packet since the protocol is http so we can see the packet in clear text



```
</body>
</html>
<!-- END FOOTER -->POST /doLogin HTTP/1.1
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/
20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/
xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Origin: http://demo.testfire.net
Connection: keep-alive
Referer: http://demo.testfire.net/login.jsp
Cookie: JSESSIONID=38784965DE3BFE62C0EF88367D4F10AF
Upgrade-Insecure-Requests: 1

uid=admin&passw=admin&btnSubmit=LoginHTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie:
AltoroAccounts=ODAwMDAwfkNvcnBvcmF0ZX4wLjB8ODAwMDAxfkNoZWNraW5nfjQu
NjYwOTc5NDA0OTk4Nzc5RTd8
Location: /bank/main.jsp
Content-Length: 0
Date: Fri, 26 Apr 2024 13:30:33 GMT

GET /bank/main.jsp HTTP/1.1
Host: demo.testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/
20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/
xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://demo.testfire.net/login.jsp
Connection: keep-alive
Cookie: JSESSIONID=38784965DE3BFE62C0EF88367D4F10AF;
AltoroAccounts=ODAwMDAwfkNvcnBvcmF0ZX4wLjB8ODAwMDAxfkNoZWNraW5nfjQu
NjYwOTc5NDA0OTk4Nzc5RTd8
Upgrade-Insecure-Requests: 1

urpose of
        demonstrating the effectiveness of HCL products in
```