ASSIGNMENT-5

USING ARP SPOOFING TO POISON NETWORK AND DETECT USING WIRESHAK

Subject Name:	Cryptography and Network Security
Subject Code:	CS6008
Module:	4

Name:	Sreeratcha B
Reg. No:	2019103585
Date:	06-06-2022

Aim: Using ARP spoofing to poison network and detect using Wireshark.

Tools involved:

- Kali Linux VM
- Ettercap
- Wireshark

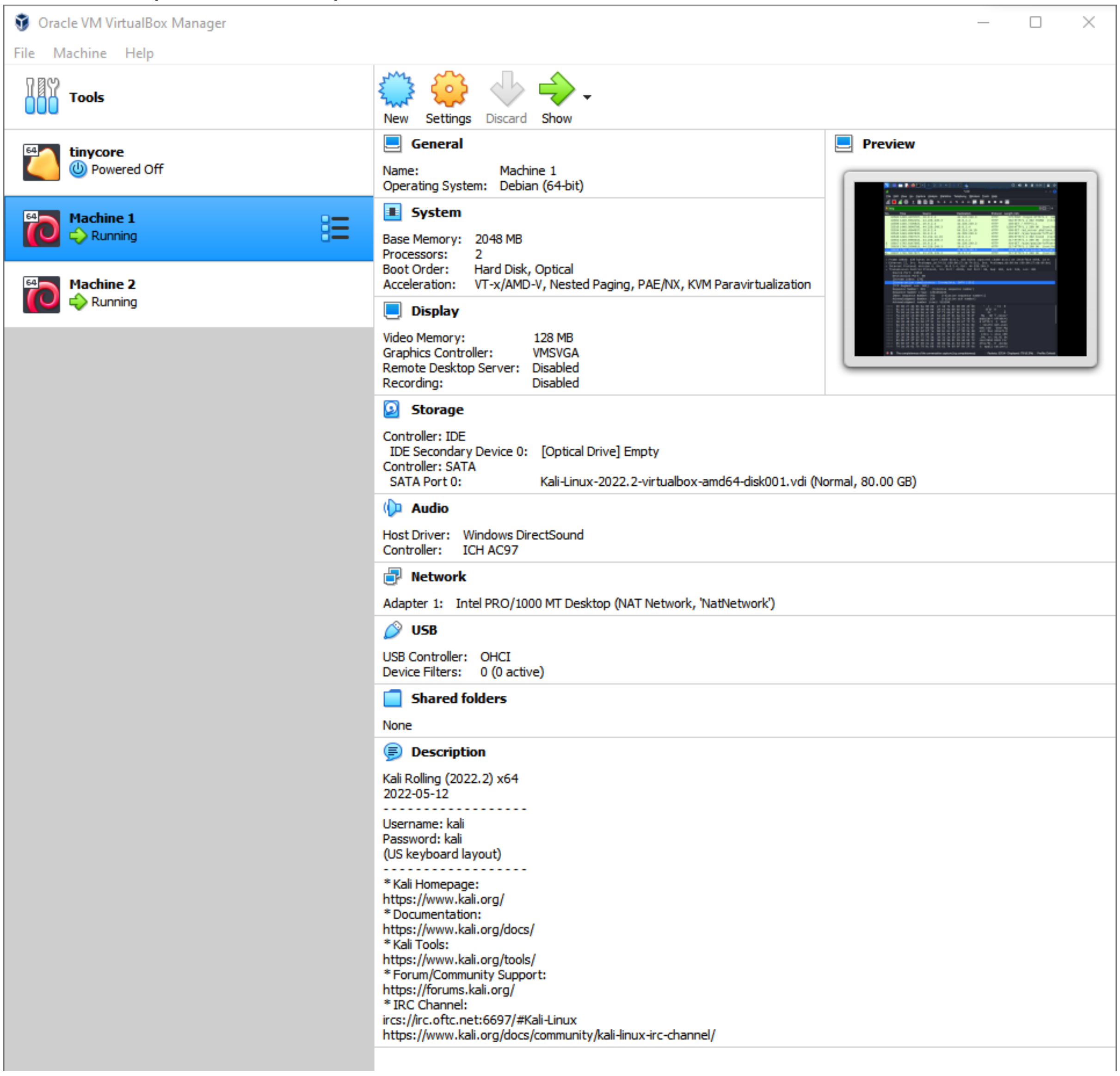
Problem Description:
Address Resolution Protocol (ARP) is a protocol that enables network communications to reach a specific device on the network. ARP translates Internet Protocol (IP) addresses to a Media Access Control (MAC) address, and vice versa. Most commonly, devices use ARP to contact the router or gateway that enables them to connect to the Internet.
Hosts maintain an ARP cache, a mapping table between IP addresses and MAC addresses, and use it to connect to destinations on the network. If the host doesn't know the MAC address for a certain IP address, it sends out an ARP request packet, asking other machines on the network for the matching MAC address.
The ARP protocol was not designed for security, so it does not verify that a response to an ARP request really comes from an authorized party. It also lets hosts accept ARP responses even if they never sent out a request. This is a weak point in the ARP protocol, which opens the door to ARP spoofing attacks.

Input: The user visits any http link and enters credentials.

Output: Username and password.

Screenshots:
Two Kali Linux machines are used to do ARP spoofing.
One machine act as the attacker and the other one is the user.

Attacker (Machine-1)



tinycore
Powered Off
Machine 1
Running
Machine 2
Running

General

Name: Machine 1
Operating System: Debian (64-bit)

System

Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Kali-Linux-2022.2-virtualbox-amd64-disk001.vdi (Normal, 80.00 GB)

Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT Network, 'NatNetwork')

USB

USB Controller: OHCI
Device Filters: 0 (0 active)

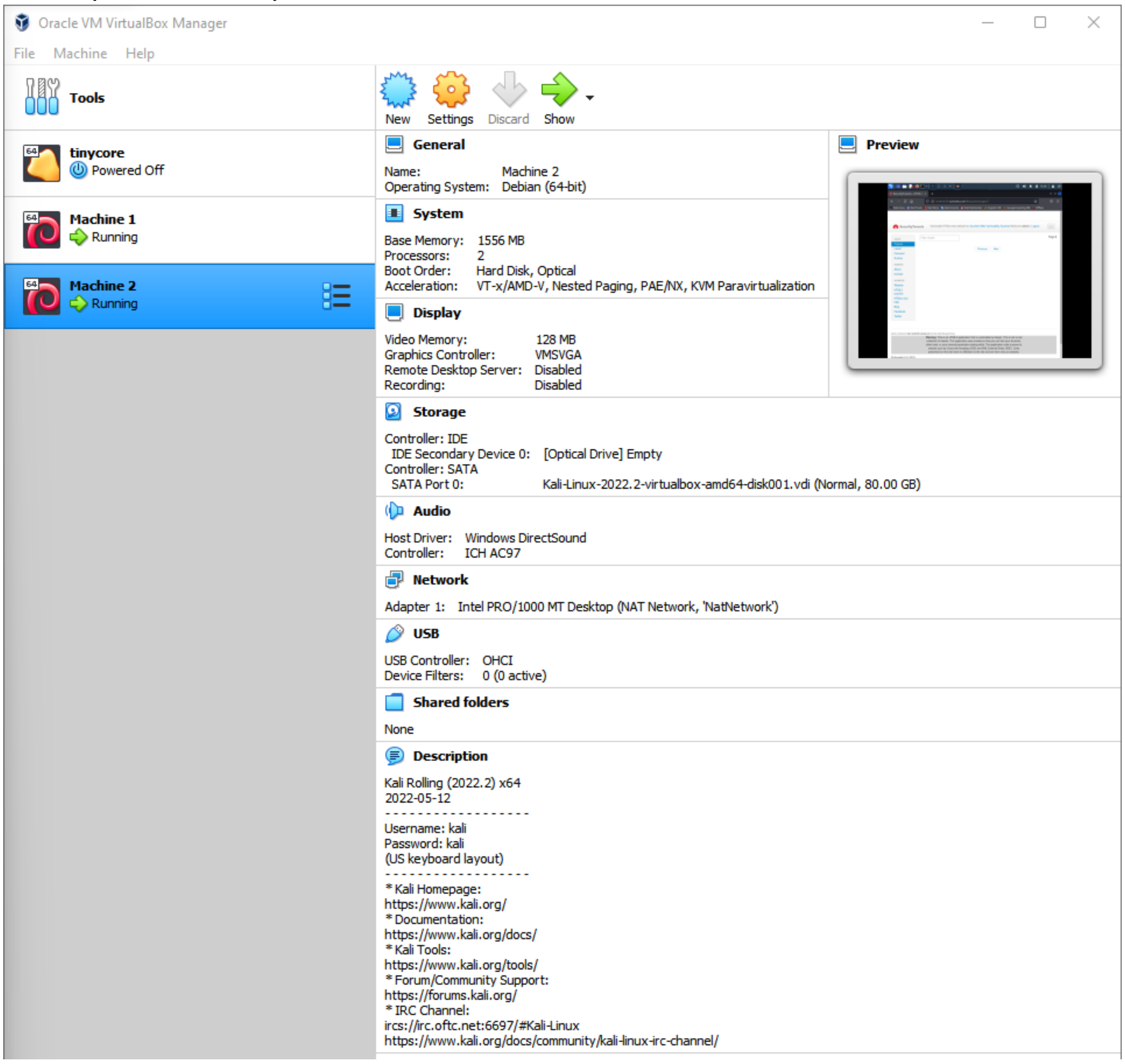
Shared folders

None

Description

```
Kali Rolling (2022.2) x64
2022-05-12
-------------------
Username: kali
Password: kali
(US keyboard layout)
-------------------
* Kali Homepage:
https://www.kali.org/
* Documentation:
https://www.kali.org/docs/
* Kali Tools:
https://www.kali.org/tools/
* Forum/Community Support:
https://forums.kali.org/
* IRC Channel:
ircs://irc.oftc.net:6697/#Kali-Linux
https://www.kali.org/docs/community/kali-linux-irc-channel/
```

User (Machine-2)



General

Name: Machine 2
Operating System: Debian (64-bit)

System

Base Memory: 1556 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Kali-Linux-2022.2-virtualbox-amd64-disk001.vdi (Normal, 80.00 GB)

Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT Network, 'NatNetwork')

USB

USB Controller: OHCI
Device Filters: 0 (0 active)

Shared folders

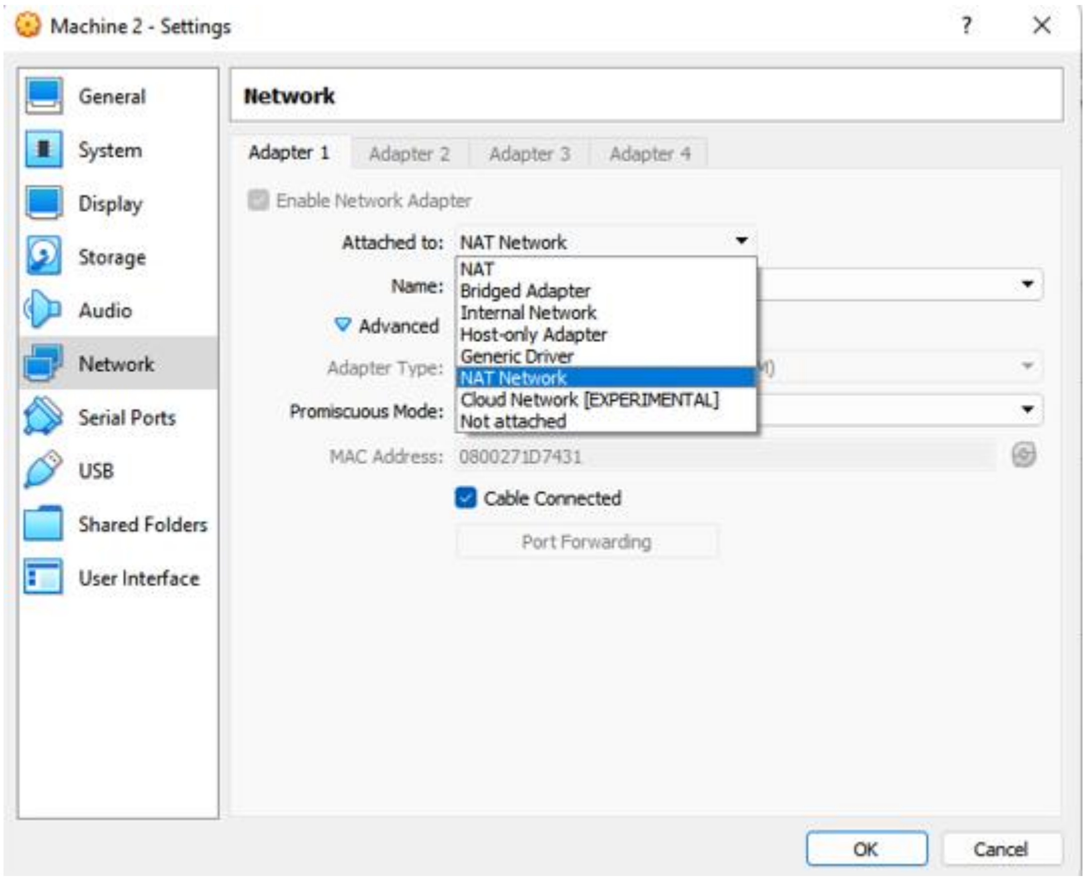
None

Description

Kali Rolling (2022.2) x64
2022-05-12

Username: kali
Password: kali
(US keyboard layout)
----
* Kali Homepage:
https://www.kali.org/
* Documentation:
https://www.kali.org/docs/
* Kali Tools:
https://www.kali.org/tools/
* Forum/Community Support:
https://forums.kali.org/
* IRC Channel:
ircs://irc.oftc.net:6697/#Kali-Linux
https://www.kali.org/docs/community/kali-linux-irc-channel/

NAT network is used.



Machine 2 - Settings

Network

Adapter 1

Enable Network Adapter

Attached to: NAT Network

Name:

Adapter Type:

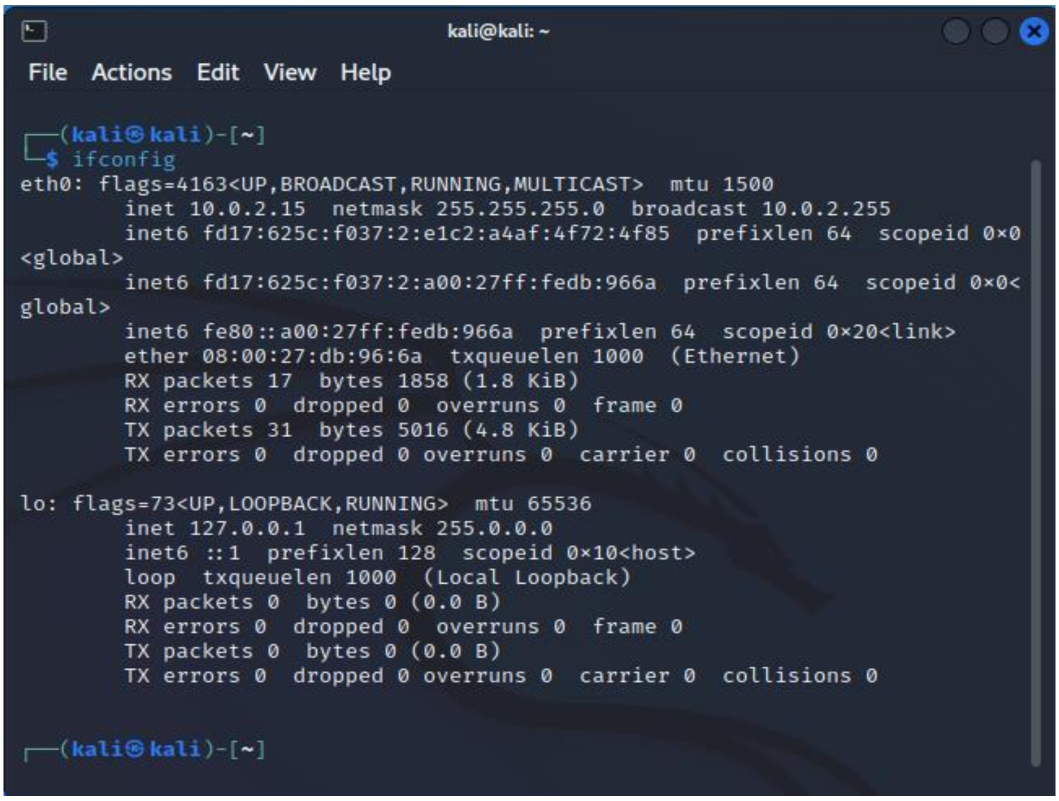
Promiscuous Mode:

MAC Address: 0800271D7431

Cable Connected

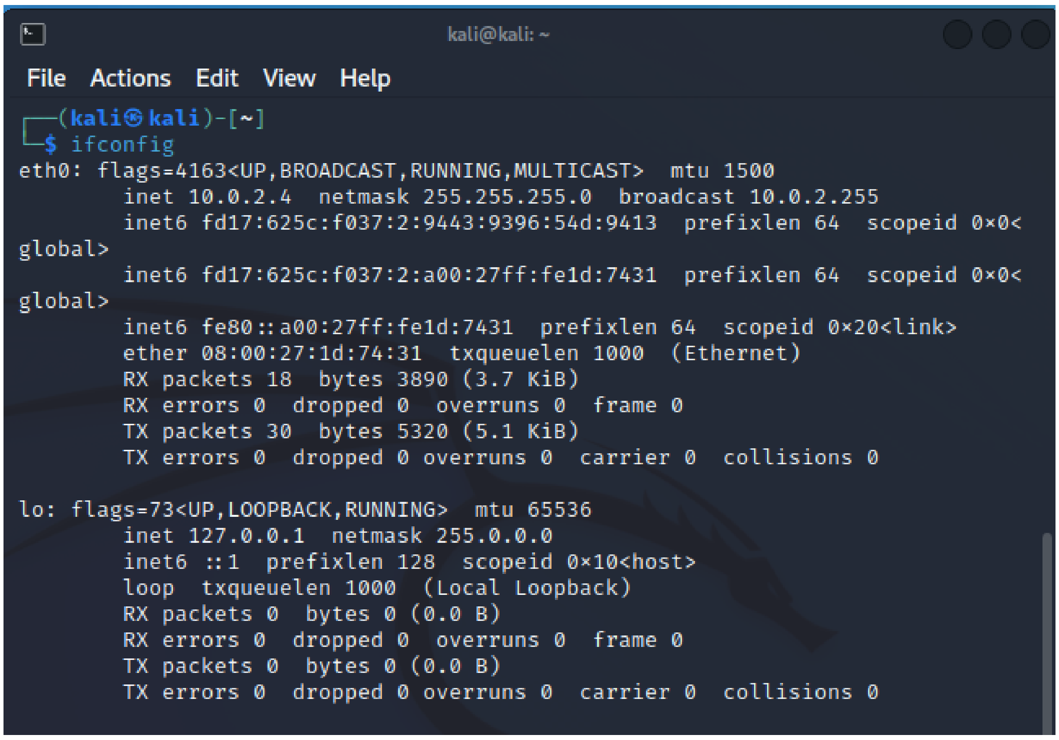
Using the ifconfig command we can view the IP address, mac address and default gateway.

Machine-1



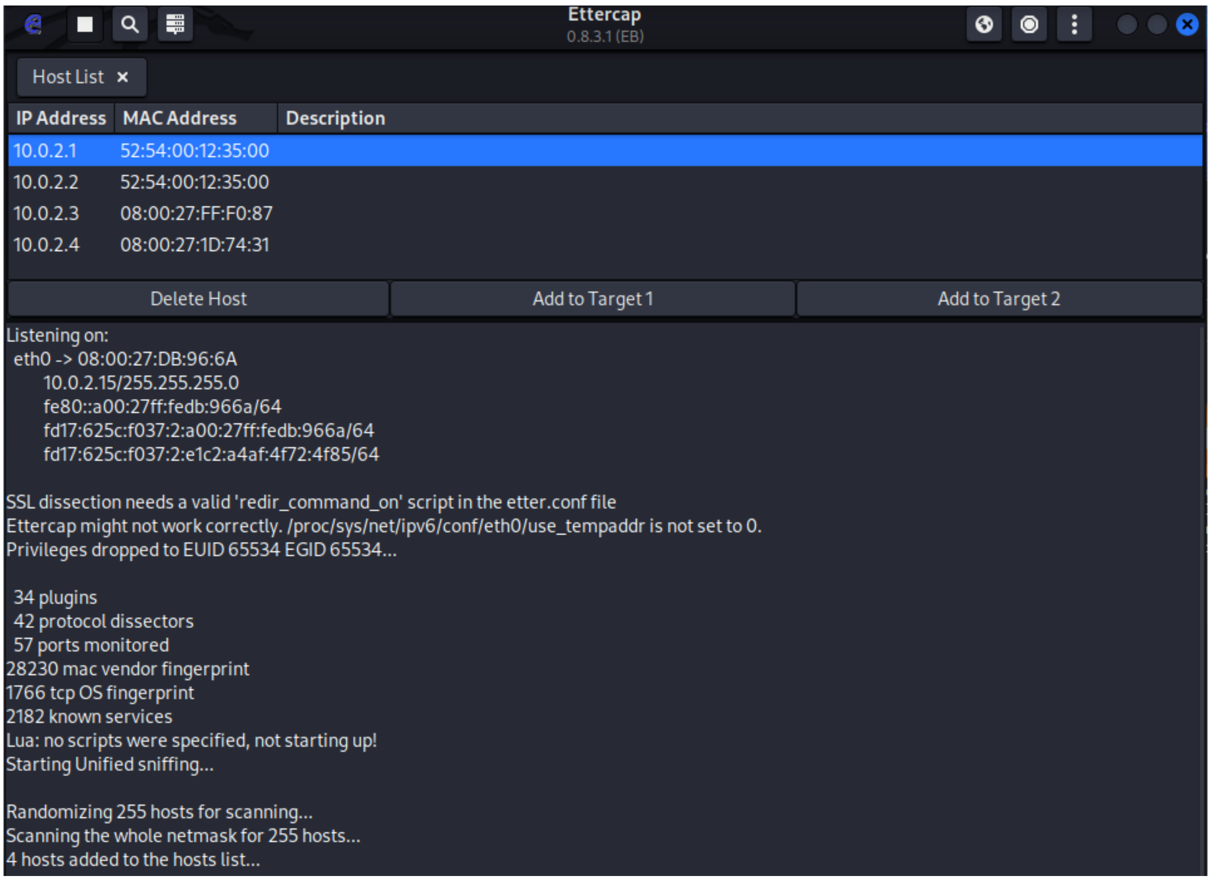
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fd17:625c:f037:2:e1c2:a4af:4f72:4f85  prefixlen 64  scopeid 0x0
<global>
        inet6 fd17:625c:f037:2:a00:27ff:fedb:966a  prefixlen 64  scopeid 0x0<
global>
        inet6 fe80::a00:27ff:fedb:966a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:db:96:6a  txqueuelen 1000  (Ethernet)
        RX packets 17  bytes 1858 (1.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 31  bytes 5016 (4.8 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 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


┌──(kali㉿kali)-[~]
```

Machine-2



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fd17:625c:f037:2:9443:9396:54d:9413  prefixlen 64  scopeid 0x0<
global>
        inet6 fd17:625c:f037:2:a00:27ff:fe1d:7431  prefixlen 64  scopeid 0x0<
global>
        inet6 fe80::a00:27ff:fe1d:7431  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1d:74:31  txqueuelen 1000  (Ethernet)
        RX packets 18  bytes 3890 (3.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30  bytes 5320 (5.1 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 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
```

Ettercap software is used to do ARP Spoofing. This software is used to scan and display the list of hosts and perform poisoning.



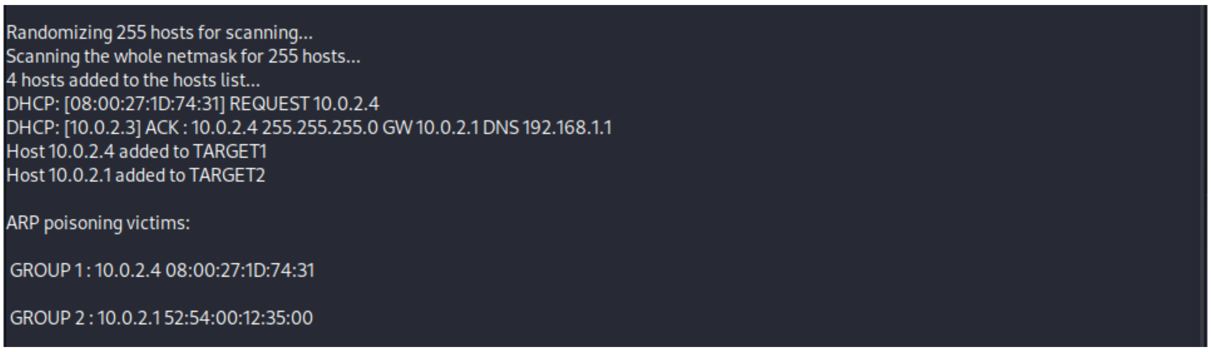
IP Address	MAC Address	Description
10.0.2.1	52:54:00:12:35:00	
10.0.2.2	52:54:00:12:35:00	
10.0.2.3	08:00:27:FF:F0:87	
10.0.2.4	08:00:27:1D:74:31	

```
Listening on:
 eth0 -> 08:00:27:DB:96:6A
      10.0.2.15/255.255.255.0
      fe80::a00:27ff:fedb:966a/64
      fd17:625c:f037:2:a00:27ff:fedb:966a/64
      fd17:625c:f037:2:e1c2:a4af:4f72:4f85/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

 34 plugins
 42 protocol dissectors
 57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
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...
```

IP address of machine-1: 10.0.2.15
MAC address: Ends with 6a
IP address of machine-2: 10.0.2.4
MAC address: Ends with 31
IP address of router: 10.0.2.1
MAC address: Ends with 00

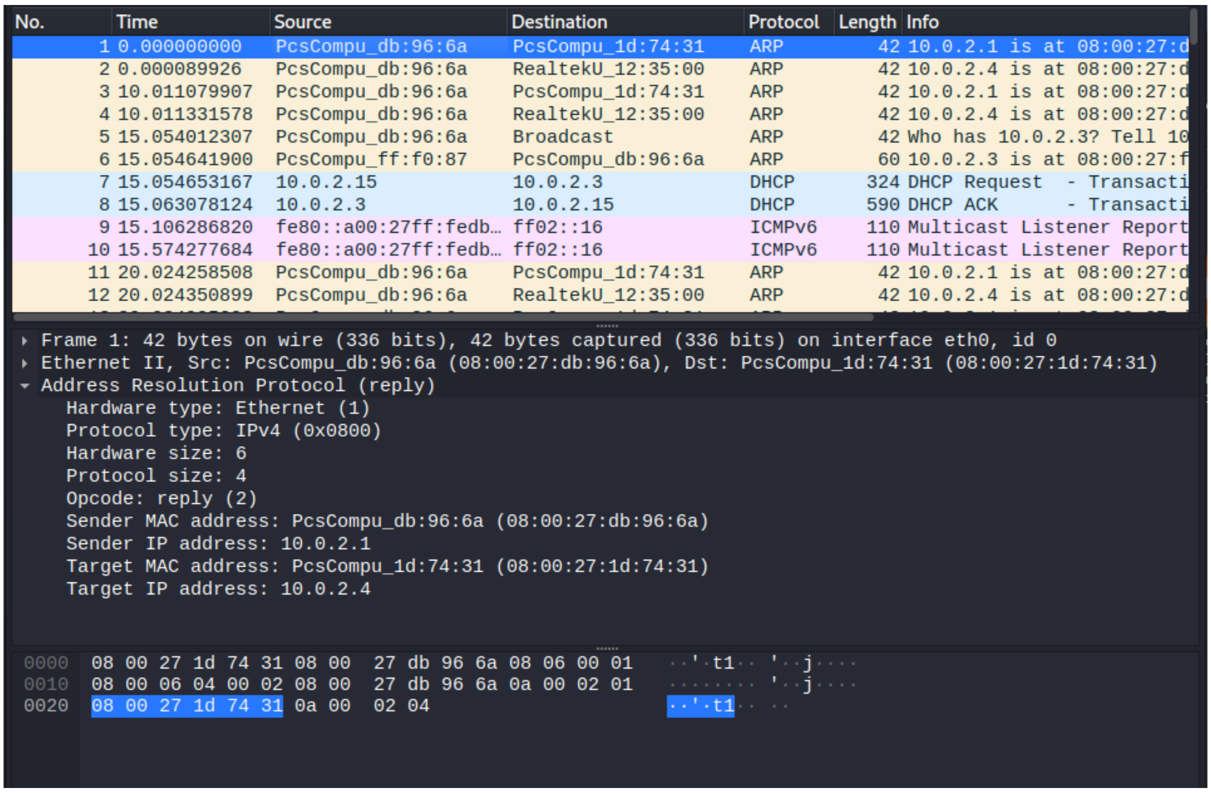
In the Ettercap the user on which attack is performed is added to target-1 and the router is added to target-2.

ARP poisoning can be performed on a button click using Ettercap.



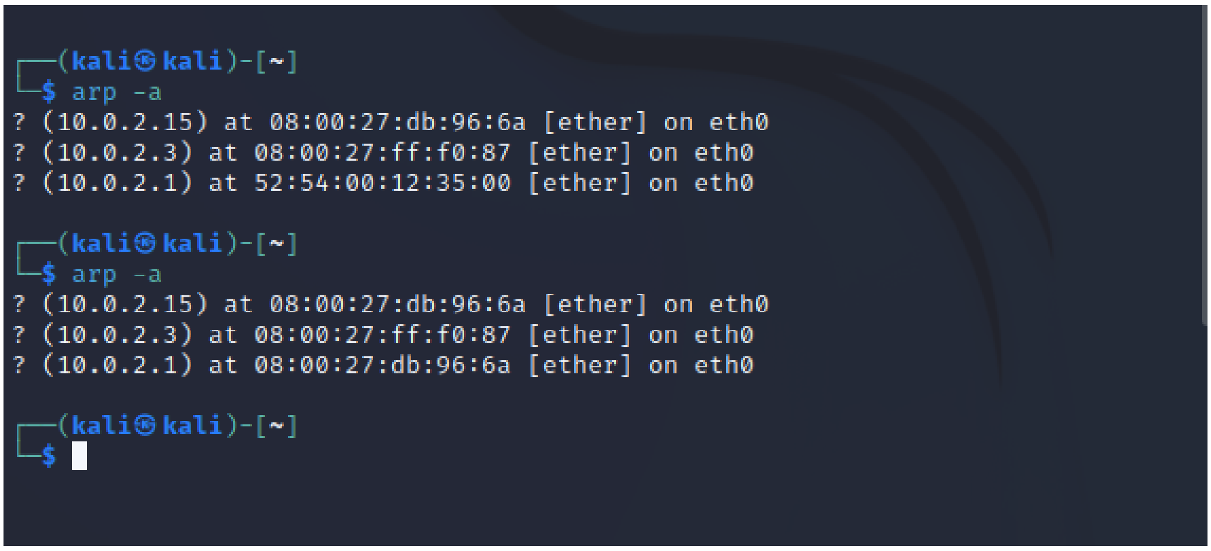
```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
DHCP: [08:00:27:1D:74:31] REQUEST 10.0.2.4
DHCP: [10.0.2.3] ACK : 10.0.2.4 255.255.255.0 GW 10.0.2.1 DNS 192.168.1.1
Host 10.0.2.4 added to TARGET1
Host 10.0.2.1 added to TARGET2

ARP poisoning victims:

 GROUP 1 : 10.0.2.4 08:00:27:1D:74:31

 GROUP 2 : 10.0.2.1 52:54:00:12:35:00
```

We can see the traffic getting directed to attacker’s machine.



```
No.  Time          Source                  Destination        Protocol Length Info
   1 0.000000000   PcsCompu_db:96:6a       PcsCompu_1d:74:31  ARP          42 10.0.2.1 is at 08:00:27:d
   2 0.000089926   PcsCompu_db:96:6a       RealtekU_12:35:00  ARP          42 10.0.2.4 is at 08:00:27:d
   3 10.011079907  PcsCompu_db:96:6a       PcsCompu_1d:74:31  ARP          42 10.0.2.1 is at 08:00:27:d
   4 10.011331578  PcsCompu_db:96:6a       RealtekU_12:35:00  ARP          42 10.0.2.4 is at 08:00:27:d
   5 15.054012307  PcsCompu_db:96:6a       Broadcast          ARP          42 Who has 10.0.2.3? Tell 10
   6 15.054641900  PcsCompu_ff:f0:87       PcsCompu_db:96:6a  ARP          60 10.0.2.3 is at 08:00:27:f
   7 15.054653167  10.0.2.15               10.0.2.3           DHCP        324 DHCP Request  - Transacti
   8 15.063078124  10.0.2.3                10.0.2.15          DHCP        590 DHCP ACK      - Transacti
   9 15.106286820  fe80::a00:27ff:fedb…    ff02::16           ICMPv6      110 Multicast Listener Report
  10 15.574277684  fe80::a00:27ff:fedb…    ff02::16           ICMPv6      110 Multicast Listener Report
  11 20.024258508  PcsCompu_db:96:6a       PcsCompu_1d:74:31  ARP          42 10.0.2.1 is at 08:00:27:d
  12 20.024350899  PcsCompu_db:96:6a       RealtekU_12:35:00  ARP          42 10.0.2.4 is at 08:00:27:d

▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_db:96:6a (08:00:27:db:96:6a), Dst: PcsCompu_1d:74:31 (08:00:27:1d:74:31)
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: PcsCompu_db:96:6a (08:00:27:db:96:6a)
    Sender IP address: 10.0.2.1
    Target MAC address: PcsCompu_1d:74:31 (08:00:27:1d:74:31)
    Target IP address: 10.0.2.4

0000  08 00 27 1d 74 31 08 00  27 db 96 6a 08 06 00 01   ··'·t1·· '··j····
0010  08 00 06 04 00 02 08 00  27 db 96 6a 0a 00 02 01   ········ '··j····
0020  08 00 27 1d 74 31 0a 00  02 04                     ··'·t1·· ··
```

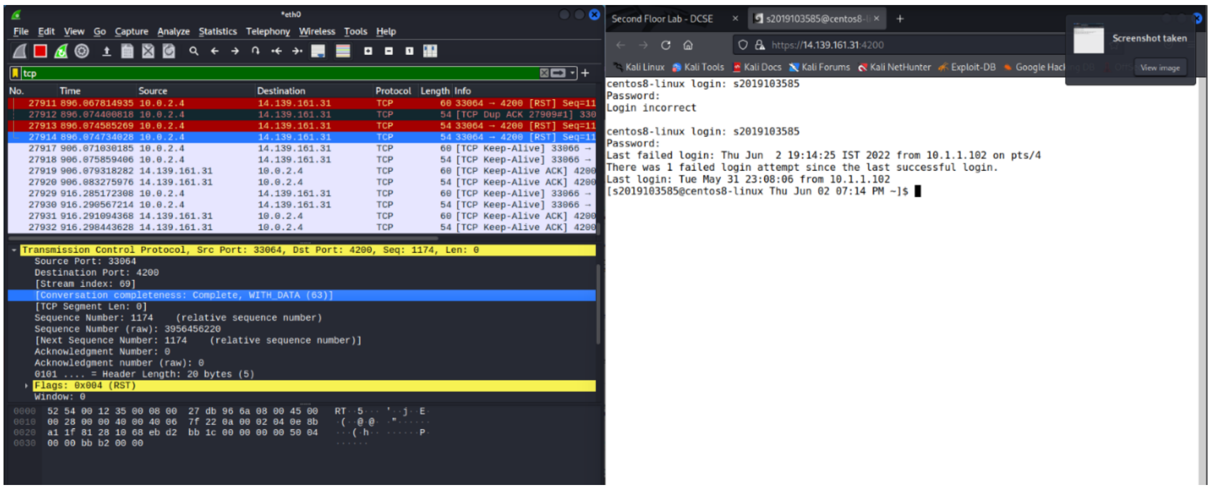
After poisoning we can observe that the ARP cache has mapped the router’s IP address with the MAC address of the attacker’s machine. In this way the ARP cache is poisoned.



```
┌──(kali㉿kali)-[~]
└─$ arp -a
? (10.0.2.15) at 08:00:27:db:96:6a [ether] on eth0
? (10.0.2.3) at 08:00:27:ff:f0:87 [ether] on eth0
? (10.0.2.1) at 52:54:00:12:35:00 [ether] on eth0

┌──(kali㉿kali)-[~]
└─$ arp -a
? (10.0.2.15) at 08:00:27:db:96:6a [ether] on eth0
? (10.0.2.3) at 08:00:27:ff:f0:87 [ether] on eth0
? (10.0.2.1) at 08:00:27:db:96:6a [ether] on eth0

┌──(kali㉿kali)-[~]
└─$ 
```

Example-1

We can see the user accessing the server in their machine. Since it’s a https link we can’t read the username and password.



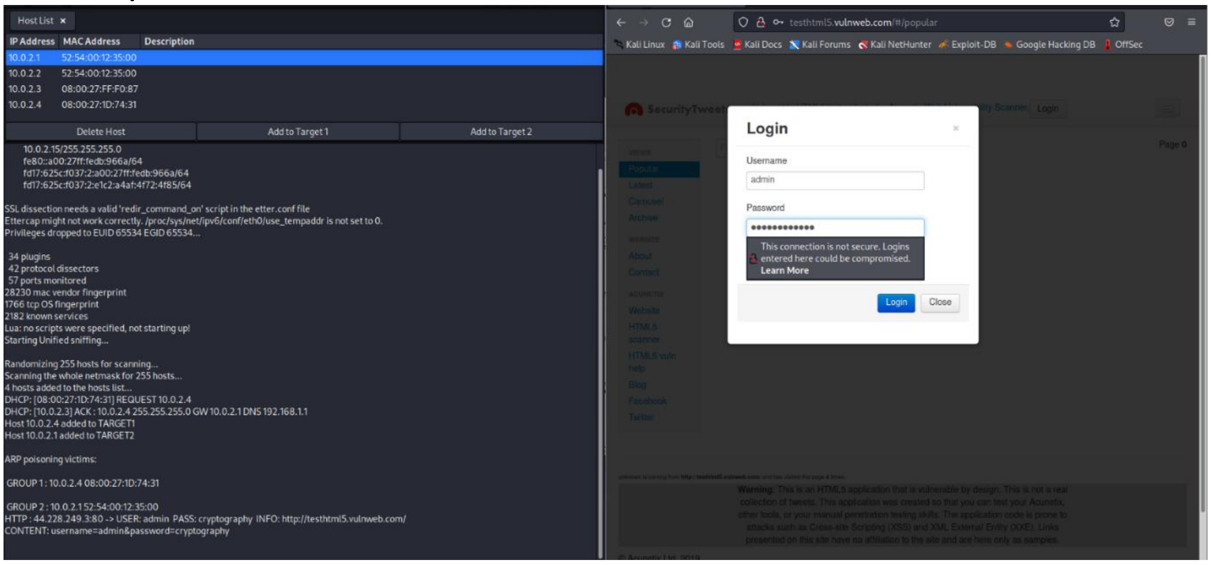
```
No.   Time          Source         Destination    Protocol Length Info
27911 896.067814935 10.0.2.4       14.139.161.31  TCP      60 33064 → 4200 [RST] Seq=11
27912 896.074400818 10.0.2.4       14.139.161.31  TCP      54 [TCP Dup ACK 27909#1] 330
27913 896.074585269 10.0.2.4       14.139.161.31  TCP      54 33064 → 4200 [RST] Seq=11
27914 896.074734028 10.0.2.4       14.139.161.31  TCP      54 33064 → 4200 [RST] Seq=11
27917 906.071030185 10.0.2.4       14.139.161.31  TCP      60 [TCP Keep-Alive] 33066 →
27918 906.075859406 10.0.2.4       14.139.161.31  TCP      54 [TCP Keep-Alive] 33066 →
27919 906.079318282 14.139.161.31  10.0.2.4       TCP      60 [TCP Keep-Alive ACK] 4200
27920 906.083275976 14.139.161.31  10.0.2.4       TCP      54 [TCP Keep-Alive ACK] 4200
27929 916.285172308 10.0.2.4       14.139.161.31  TCP      60 [TCP Keep-Alive] 33066 →
27930 916.290567214 10.0.2.4       14.139.161.31  TCP      54 [TCP Keep-Alive] 33066 →
27931 916.291094368 14.139.161.31  10.0.2.4       TCP      60 [TCP Keep-Alive ACK] 4200
27932 916.298443628 14.139.161.31  10.0.2.4       TCP      54 [TCP Keep-Alive ACK] 4200

▾ Transmission Control Protocol, Src Port: 33064, Dst Port: 4200, Seq: 1174, Len: 0
    Source Port: 33064
    Destination Port: 4200
    [Stream index: 69]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
    Sequence Number: 1174    (relative sequence number)
    Sequence Number (raw): 3956456220
    [Next Sequence Number: 1174    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x004 (RST)
    Window: 0

0000  52 54 00 12 35 00 08 00  27 db 96 6a 08 00 45 00   RT··5···'··j··E·
0010  00 28 00 00 40 00 40 06  7f 22 0a 00 02 04 0e 8b   ·(··@·@··"······
0020  a1 1f 81 28 10 68 eb d2  bb 1c 00 00 00 00 50 04   ···(·h········P·
0030  00 00 bb b2 00 00                                  ······
```

```
centos8-linux login: s2019103585
Password:
Login incorrect

centos8-linux login: s2019103585
Password:
Last failed login: Thu Jun  2 19:14:25 IST 2022 from 10.1.1.102 on pts/4
There was 1 failed login attempt since the last successful login.
Last login: Tue May 31 23:08:06 from 10.1.1.102
[s2019103585@centos8-linux Thu Jun 02 07:14 PM ~]$ 
```

Example-2

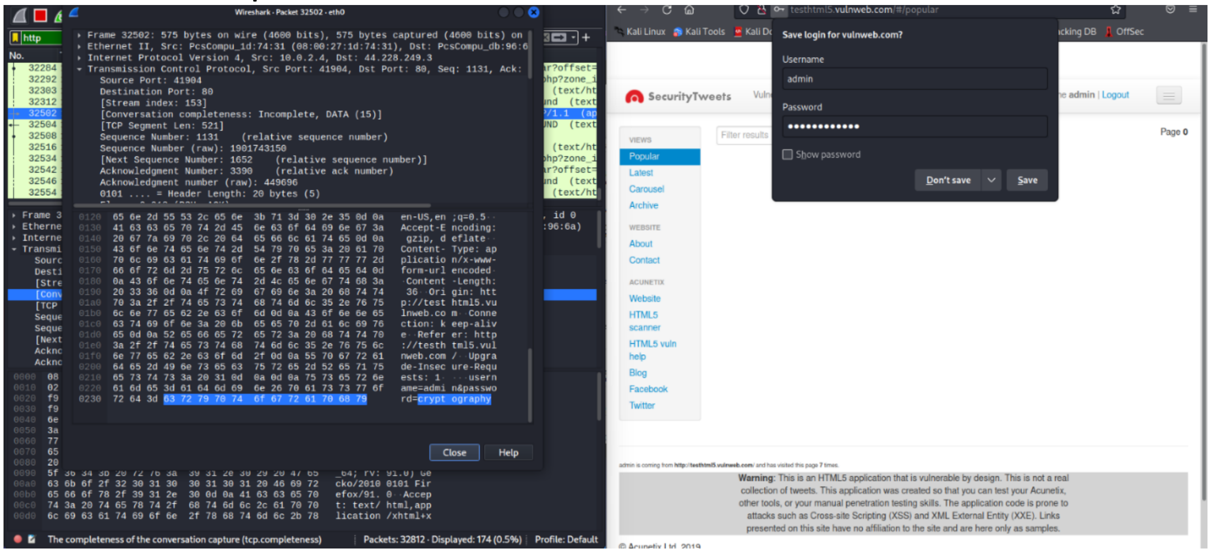
In this example a http site is accessed and the username and password are entered. The attacker can access those since http is not secure.

Ettercap:


Host List
Delete Host
Add to Target 1
Add to Target 2
testhtml5.vulnweb.com/#/popular
Login
Username
admin
Password
This connection is not secure. Logins entered here could be compromised. Learn More
Login
Close

```
IP Address  MAC Address        Description
10.0.2.1    52:54:00:12:35:00
10.0.2.2    52:54:00:12:35:00
10.0.2.3    08:00:27:FF:F0:87
10.0.2.4    08:00:27:1D:74:31

    10.0.2.15/255.255.255.0
    fe80::a00:27ff:fedb:966a/64
    fd17:625c:f037:2:a00:27ff:fedb:966a/64
    fd17:625c:f037:2:e1c2:a4af:4f72:4f85/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

 34 plugins
 42 protocol dissectors
 57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
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: [08:00:27:1D:74:31] REQUEST 10.0.2.4
DHCP: [10.0.2.3] ACK : 10.0.2.4 255.255.255.0 GW 10.0.2.1 DNS 192.168.1.1
Host 10.0.2.4 added to TARGET1
Host 10.0.2.1 added to TARGET2

ARP poisoning victims:

 GROUP 1 : 10.0.2.4 08:00:27:1D:74:31

 GROUP 2 : 10.0.2.1 52:54:00:12:35:00
HTTP : 44.228.249.3:80 -> USER: admin  PASS: cryptography  INFO: http://testhtml5.vulnweb.com/
CONTENT: username=admin&password=cryptography
```

Wireshark output:



```
▸ Frame 32502: 575 bytes on wire (4600 bits), 575 bytes captured (4600 bits) on
▸ Ethernet II, Src: PcsCompu_1d:74:31 (08:00:27:1d:74:31), Dst: PcsCompu_db:96:6
▸ Internet Protocol Version 4, Src: 10.0.2.4, Dst: 44.228.249.3
▾ Transmission Control Protocol, Src Port: 41904, Dst Port: 80, Seq: 1131, Ack:
    Source Port: 41904
    Destination Port: 80
    [Stream index: 153]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 521]
    Sequence Number: 1131    (relative sequence number)
    Sequence Number (raw): 1901743150
    [Next Sequence Number: 1652    (relative sequence number)]
    Acknowledgment Number: 3390    (relative ack number)
    Acknowledgment number (raw): 449696
    0101 .... = Header Length: 20 bytes (5)

0120  65 6e 2d 55 53 2c 65 6e  3b 71 3d 30 2e 35 0d 0a   en-US,en ;q=0.5··
0130  41 63 63 65 70 74 2d 45  6e 63 6f 64 69 6e 67 3a   Accept-E ncoding:
0140  20 67 7a 69 70 2c 20 64  65 66 6c 61 74 65 0d 0a    gzip, d eflate··
0150  43 6f 6e 74 65 6e 74 2d  54 79 70 65 3a 20 61 70   Content- Type: ap
0160  70 6c 69 63 61 74 69 6f  6e 2f 78 2d 77 77 77 2d   plicatio n/x-www-
0170  66 6f 72 6d 2d 75 72 6c  65 6e 63 6f 64 65 64 0d   form-url encoded·
0180  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   ·Content -Length:
0190  20 33 36 0d 0a 4f 72 69  67 69 6e 3a 20 68 74 74    36··Ori gin: htt
01a0  70 3a 2f 2f 74 65 73 74  68 74 6d 6c 35 2e 76 75   p://test html5.vu
01b0  6c 6e 77 65 62 2e 63 6f  6d 0d 0a 43 6f 6e 6e 65   lnweb.co m··Conne
01c0  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
01d0  65 0d 0a 52 65 66 65 72  65 72 3a 20 68 74 74 70   e··Refer er: http
01e0  3a 2f 2f 74 65 73 74 68  74 6d 6c 35 2e 76 75 6c   ://testh tml5.vul
01f0  6e 77 65 62 2e 63 6f 6d  2f 0d 0a 55 70 67 72 61   nweb.com /··Upgra
0200  64 65 2d 49 6e 73 65 63  75 72 65 2d 52 65 71 75   de-Insec ure-Requ
0210  65 73 74 73 3a 20 31 0d  0a 0d 0a 75 73 65 72 6e   ests: 1· ···usern
0220  61 6d 65 3d 61 64 6d 69  6e 26 70 61 73 73 77 6f   ame=admi n&passwo
0230  72 64 3d 63 72 79 70 74  6f 67 72 61 70 68 79      rd=crypt ography
```

Username: admin

Password: cryptography

These are the credentials obtained through poisoning.