

Practical – 3

Aim: Understand packet capturing tool Wireshark or Ettercap and analysis of those packets.

- **Ettercap**
 - Ettercap stands for Ethernet Capture. Ettercap is a comprehensive suite for man in the middle attacks.
 - It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.
 - Type of active and passive attacks.
 1. **Active attack:** In this kind of attack, The Attacker attempt to alter system resources or destroy the data. Attacker can be changing the data and etc.
 2. **Passive attack:** In this kind of attack, Attacker attempt to gain information from the system and don't destroy the information. This attack is kind of monitoring and recognition the target.
- 1. **Active Attack:**
 - I. Spoofing.
 - II. Denial-of-service attack.
 - III. Man in the middle.
 - IV. ARP poisoning.
 - V. Overflow(s).
- 2. **Passive Attack:**
 - I. Port Scanners. II. Idle Scan.

I. Spoofing

A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware or bypasses access controls. There are several different types of spoofing attacks that malicious parties can use to accomplish this. Some of the most common methods include IP address spoofing attacks, ARP spoofing attacks and DNS server spoofing attacks.

II. Ettercap can work with these four models:

1. IP-based: Filtered packets by IP address.
2. MAC-based: Filtered packets by MAC address.
3. ARP-based: It is very useful for sniffing packets between two hosts on a Switched network.
4. PublicARP-based: It is very useful for sniffing packets from a user to all hosts.

III. Packets Filtering by IP address and ARP poisoning.

Step 1: Change the value in /proc/sys/net/ipv4/ip_forward from 0 to 1 for Interception.

```
root@divyang:~# cat /proc/sys/net/ipv4/ip_forward
0
root@divyang:~# echo 1 >> /proc/sys/net/ipv4/ip_forward
root@divyang:~# cat /proc/sys/net/ipv4/ip_forward
1
root@divyang:~#
```

Step 2: Change the ipchains rules as shown in figure.

First run the command or go to the root>etc>etter.conf then modify and save the changes.

```
root@divyang:~# gedit /etc/etter.conf
```

Before Changing in ipchains we found below statements.

```
#-----
#   Linux
#-----
# if you use ipchains:
#   #redir_command_on = "ipchains -A input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"
#   #redir_command_off = "ipchains -D input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"
```

We have to remove the # as shown in figure from the both highlighted statements.

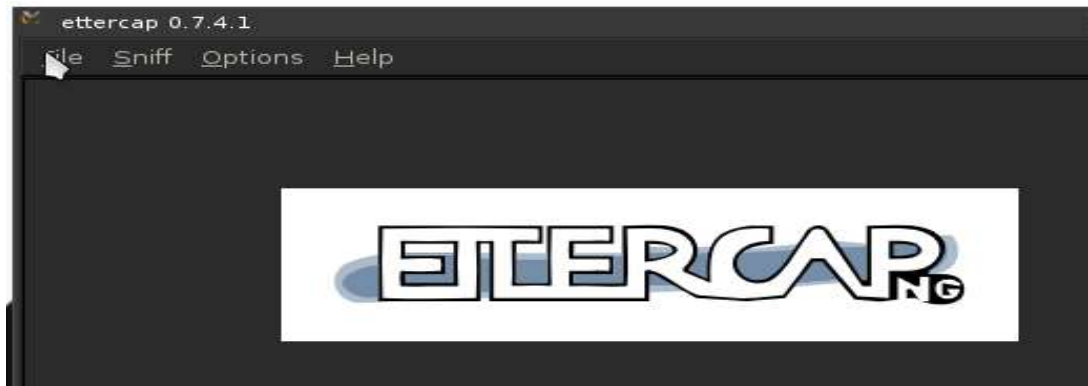
```
#-----
#   Linux
#-----
# if you use ipchains:
redir_command_on = "ipchains -A input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"
redir_command_off = "ipchains -D input -i %iface -p tcp -s 0/0 -d 0/0 %port -j REDIRECT %rport"
```

Step 3: Launch Ettercap using the command

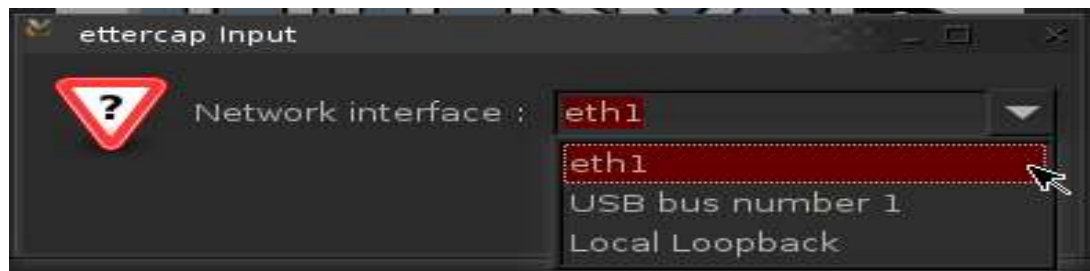
root@divyang:~# ettercap -G.

We can also launch it using following steps which are shown in the Figure.





Step 4: Click “Sniff->Unified Sniffing”. It will list the available network interface as shown below. Choosing the interface on which we want to use for ARP Poisoning.



Once we have chosen the interface the following window will open:



Step 5: Scan for Hosts by clicking “Hosts->Scan for Host” It will start to scan the hosts present in the network.



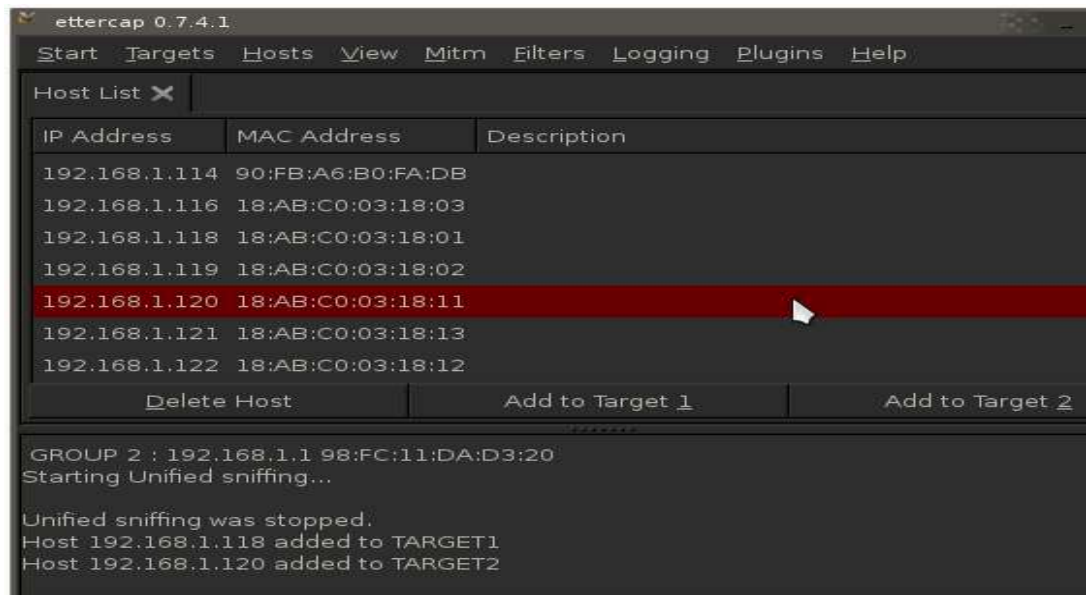
Once it is completed, click “Hosts->Host List”. It will list the available hosts in the LAN as follows:



Step 6: The next step is to add the target list for performing the ARP poisoning.

Now among the list, selected “192.168.1.118” and clicked on “Add to Target 1” and selected “192.168.1.120” and clicked on “Add to Target 2”.

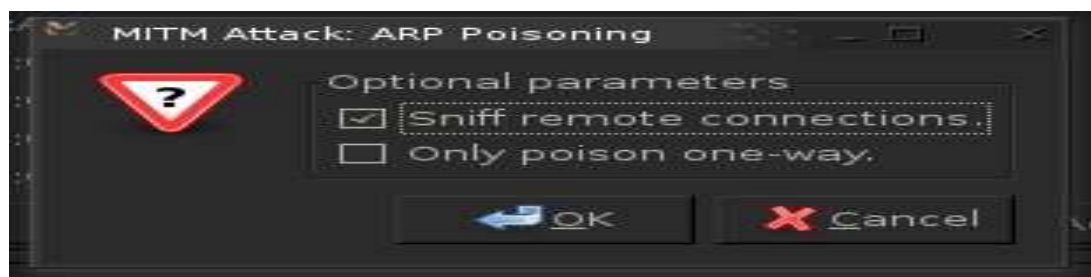
In which **TARGET1** act as Victim and **TARGET2** act server.



Step 7: Now select “Mitm->Arp Poisoning” as follows:



The following dialog box was appears. Select “Sniff Remote Connection” and click “ok”:



Step 8: Then click “Start->Start Sniffing as follows:

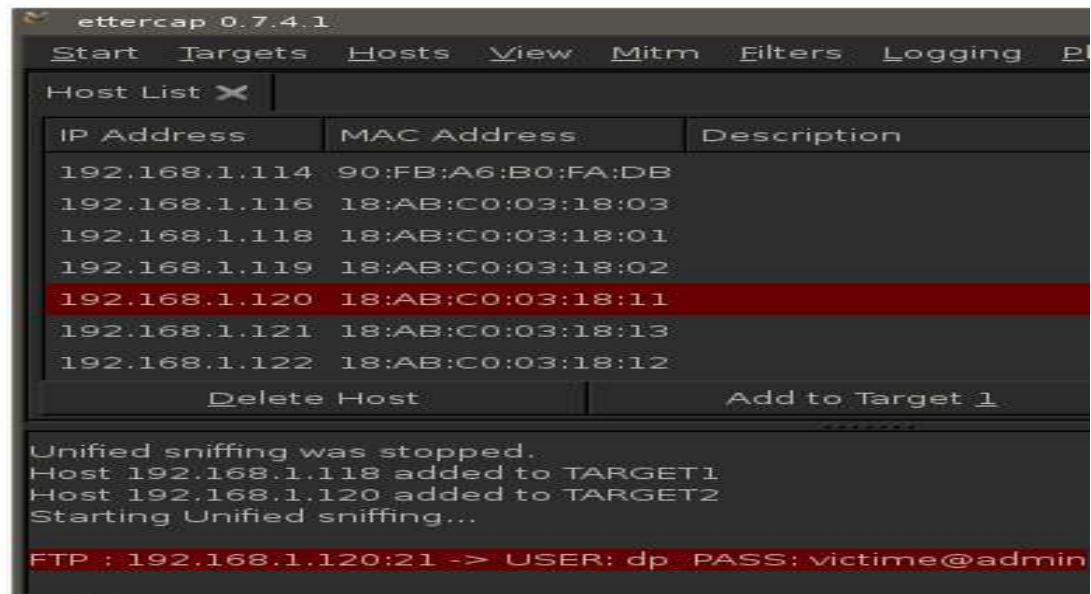


Step 9: Now from the victim machine we are tried to logon into ftp server which are already created.

```
C:\WINDOWS\system32\cmd.exe - ftp 192.168.1.120

C:\Documents and Settings\dp>ftp 192.168.1.120
Connected to 192.168.1.120.
220 Microsoft FTP Service
User (192.168.1.120:(none)): dp
331 Password required for dp.
Password:
230 User dp logged in.
ftp>
```

Step 10: Now in the attacker’s machine checked the Ettercap window and it shows the User Name and Password by which victim access the ftp server.



- **Wireshark**

- Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.
- The following are some of the many features Wireshark provides:
 - Available for UNIX and Windows.
 - Capture live packet data from a network interface.
 - Open files containing packet data captured with tcpdump/WinDump, Wireshark, and a number of other packet capture programs.
 - Import packets from text files containing hex dumps of packet data.
 - Display packets with very detailed protocol information.
 - Save packet data captured.
 - Export some or all packets in a number of capture file formats.
 - Filter packets on many criteria.
 - Search for packets on many criteria.
 - Colorize packet display based on filters.
 - Create various statistics etc.
- Capture ftp traffic using wireshark from a network interface.

Step 1: Launch wireshark using the command

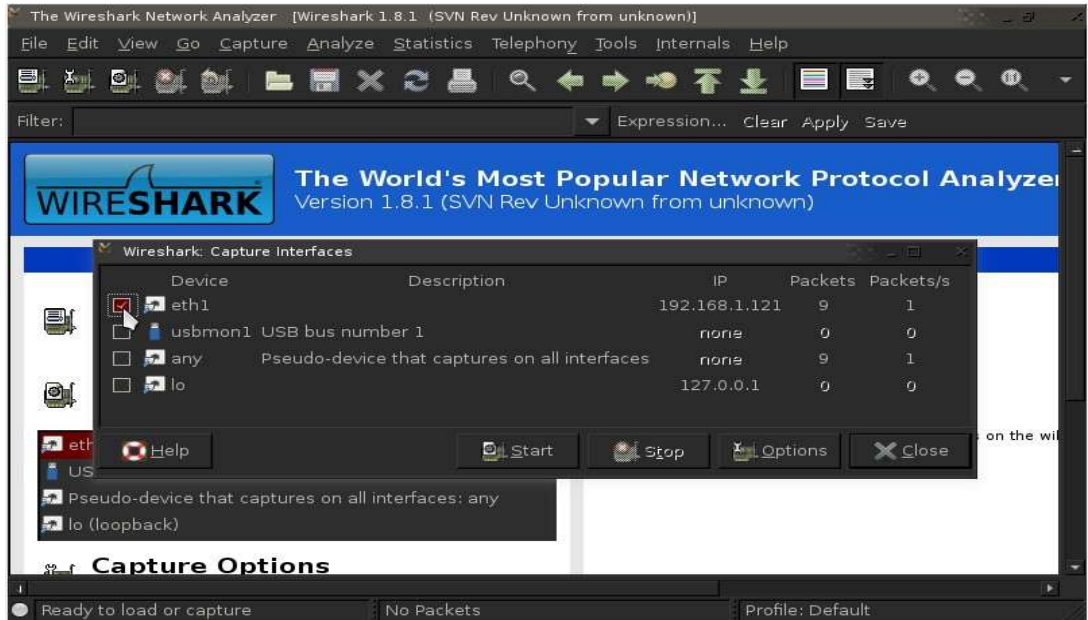
```
root@divyang:~# wireshark
```

We can also launch it using following steps which are shown in the Figure.

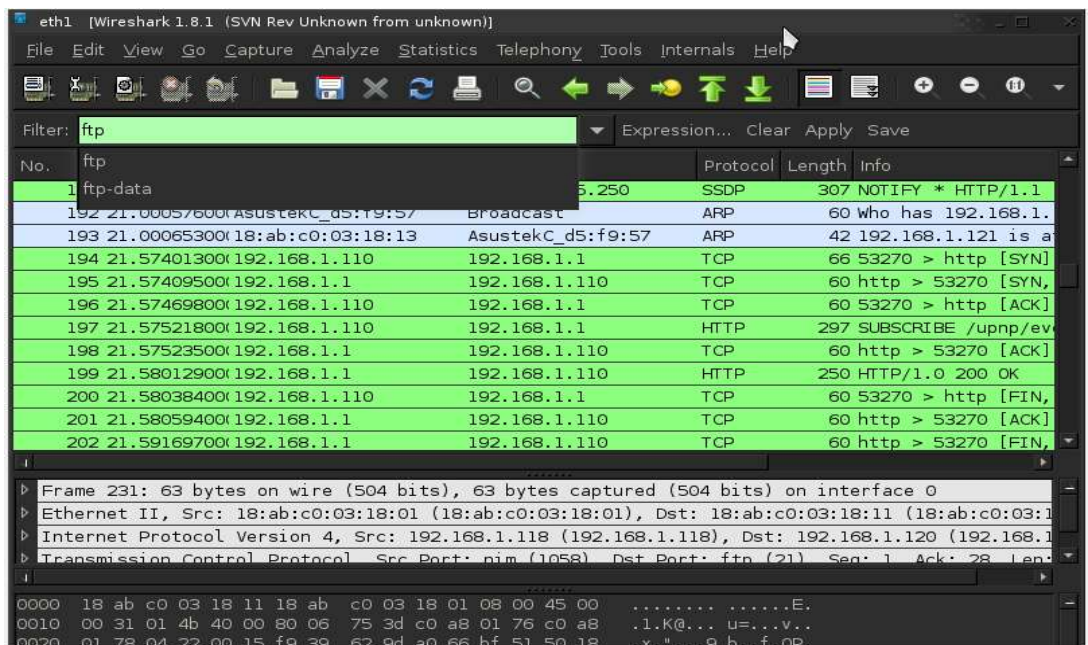


Step 2: Capture The Interface by clicking “ Capture->Interface ”

It will list the available network interface as shown below. Choosing the interface on which we want to capture the packets and click on Start.



As soon we clicked on start it started capturing the packets on selected interface and shows as the follow.



Step 3: Now from the victim machine we are tried to logon into ftp server which are already created.

```

C:\WINDOWS\system32\cmd.exe - ftp 192.168.1.120

C:\Documents and Settings\dp>ftp 192.168.1.120
Connected to 192.168.1.120.
220 Microsoft FTP Service
User <192.168.1.120:(none)>: dp
331 Password required for dp.
Password:
230 User dp logged in.
ftp>

```

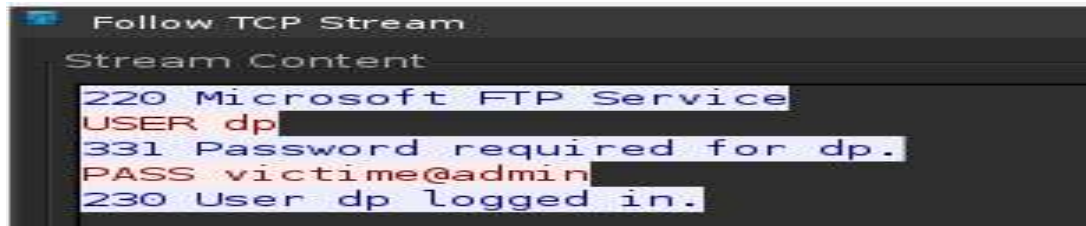
Step 4: Now in the attacker's machine we stop the capturing and filtering the packets by filter section in which we are trying to filter FTP Packets as shown in screen shot.

No.	Time	Source	Destination	Protocol	Length	Info
126	18.57301600	192.168.1.118	192.168.1.120	FTP	60	Request: QUIT
127	18.57486400	192.168.1.120	192.168.1.118	FTP	61	Response: 221
207	22.43388500	192.168.1.120	192.168.1.118	FTP	81	Response: 220 Microsc
231	27.51577300	192.168.1.118	192.168.1.120	FTP	63	Request: USER dp
232	27.51661800	192.168.1.120	192.168.1.118	FTP	85	Response: 331 Passwor
274	34.27596000	192.168.1.118	192.168.1.120	FTP	74	Request: PASS victime
275	34.27760300	192.168.1.120	192.168.1.118	FTP	78	Response: 230 User dp

Step 5: Check the FTP Packets by Right click on a packet and selecting “Follow TCP Stream”.

No.	Time	Source	Destination	Protocol	Length	Info
204	22.43148900	192.168.1.118	192.168.1.120	TCP	62	nim > ftp [SYN] Seq=6
205	22.43211800	192.168.1.120	192.168.1.118	TCP	62	ftp > nim [SYN, ACK]
206	22.43281200	192.168.1.118	192.168.1.120	TCP	60	ftp > nim [ACK] Seq=1
207	22.43388500	192.168.1.120	192.168.1.118	TCP	60	nim > ftp [ACK] Seq=1
231	27.51577300	192.168.1.118	192.168.1.120	FTP	63	Request: USER dp
232	27.51661800	192.168.1.120	192.168.1.118	FTP	85	Response: 331 Passwor
233	27.71088800	192.168.1.118	192.168.1.120	FTP	85	Request: PASS victime
274	34.27596000	192.168.1.118	192.168.1.120	FTP	74	Request: PASS victime
275	34.27760300	192.168.1.120	192.168.1.118	FTP	78	Response: 230 User dp
276	34.42000500	192.168.1.118	192.168.1.120	FTP	78	Request: QUIT

Step 6: In the packet we found Name and Password by which victim access the ftp server.



```
Follow TCP Stream
Stream Content
220 Microsoft FTP Service
USER dp
331 Password required for dp.
PASS victime@admin
230 User dp logged in.
```