Passive sniffing

In passive sniffing (when you have hub in your network infrastructure) all you have to do is putting your NIC card in promiscuous mode through which you will get all the packets in to your PC.

Practical No 1: Keeping our NIC card in promiscuous mode.

Step 1:

Open your terminal window

Step 2:

Find out your NIC card interface name by executing ifconfig

```
eth0: flags=4163<UP, BROADCAST, RUNNING, MULTICAST>  mtu 1500

        inet 192.168.0.117  netmask 255.255.255.0  broadcast 192.168.0.255

        inet6 fe80::a00:27ff:fe52:cb4f  prefixlen 64  scopeid 0x20<link>

        ether 08:00:27:52:cb:4f  txqueuelen 1000  (Ethernet)

        RX packets 133  bytes 17526 (17.1 KiB)

        RX errors 0  dropped 0  overruns 0  frame 0

        TX packets 26  bytes 2373 (2.3 KiB)

        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 3:

Execute the following command to turn on Promiscuous mode on the interface you have selected.

Syntax: ifconfig <interface name> promisc

Ex: ifconfig eth0 promisc

See the command output

```
root@kali:~# ifconfig eth0 promisc

root@kali:~#
```

Done setting up promiscuous mode.

If you want to test your device is in promiscuous mode or not. You can try executing netstat –i command this is before promiscuous mode

```
Kernel Interface table

Iface     MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg

eth0     1500     124     0     0 0          26     0     0     0 BMRU

lo     65536     160     0     0 0         160     0     0     0 LRU
```

if you see P flag for your interface which means you are promiscuous see the below output.

```
Kernel Interface table

Iface     MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg

eth0     1500     191     0     0 0          26     0     0     0 BMPRU

lo     65536     197     0     0 0         197     0     0     0 LRU
```

look at BMRU and BMPRU when you enable promiscuous mode P comes when you disable it, it disappears.

Practical 2: Disabling Promiscuous mode on NIC card

Step 1:

Open your terminal windows

Step 2:

Find out NIC card interface name by executing ifconfig

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500

        inet 192.168.0.117  netmask 255.255.255.0  broadcast 192.168.0.255

        inet6 fe80::a00:27ff:fe52:cb4f  prefixlen 64  scopeid 0x20<link>

        ether 08:00:27:52:cb:4f  txqueuelen 1000  (Ethernet)

        RX packets 133  bytes 17526 (17.1 KiB)

        RX errors 0  dropped 0  overruns 0  frame 0

        TX packets 26  bytes 2373 (2.3 KiB)

        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 3:

Execute the following command to get rid of promiscuous mode

Syntax: ifconfig <interface name> -promisc

Example: ***root@kali:~# ifconfig eth0 -promisc***

```
root@kali:~#
```

you can execute the same netstat –i to figure out it is there or not.

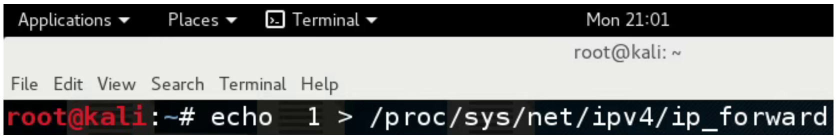
Active Sniffing Practicals.

Practical No2: MITM attack with ARP Poisoning Technique (Unsecured protocols are vulnerable to this attack).

Step1: Open a Blank Terminal

Step2: Execute the following command

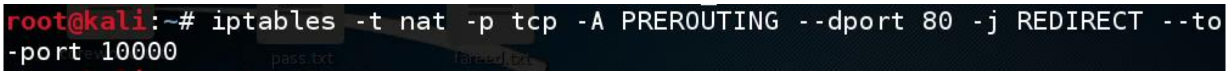
echo 1 > /proc/sys/net/ipv4/ip_forward



```
root@kali:~# echo  1 > /proc/sys/net/ipv4/ip_forward
```

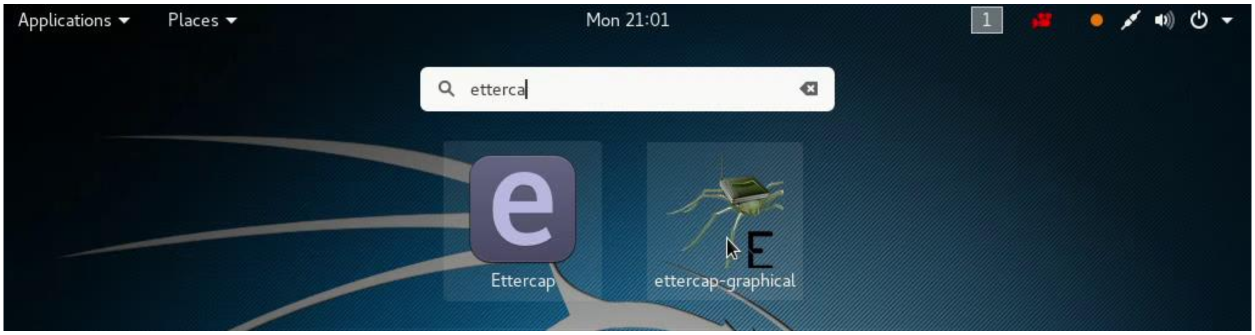
Then execute this command

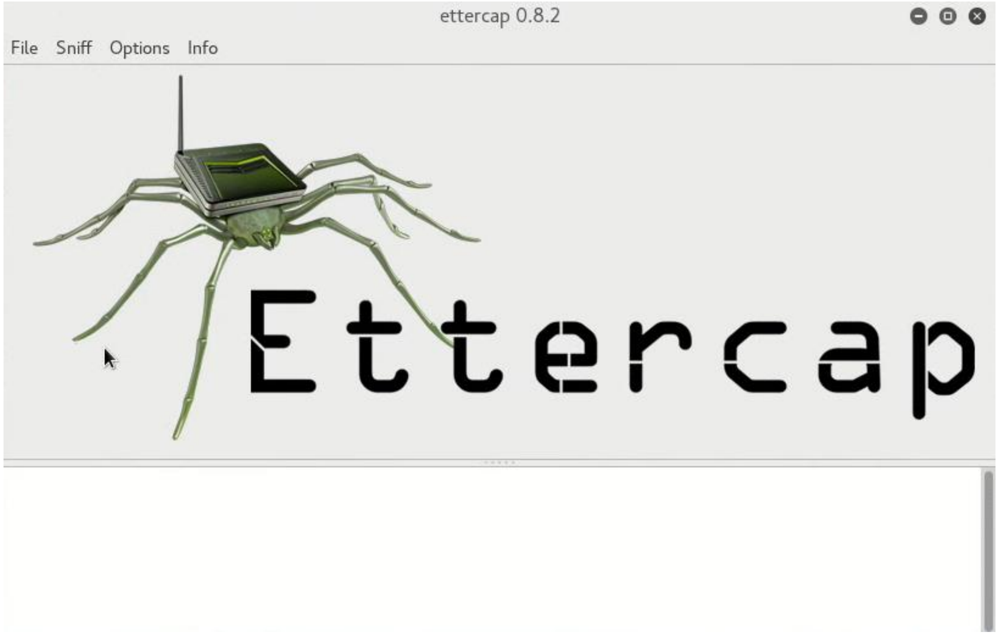
Iiptables –t nat –p tcp –A PREROUTING --dport 80 –j REDIRECT --to-port 10000



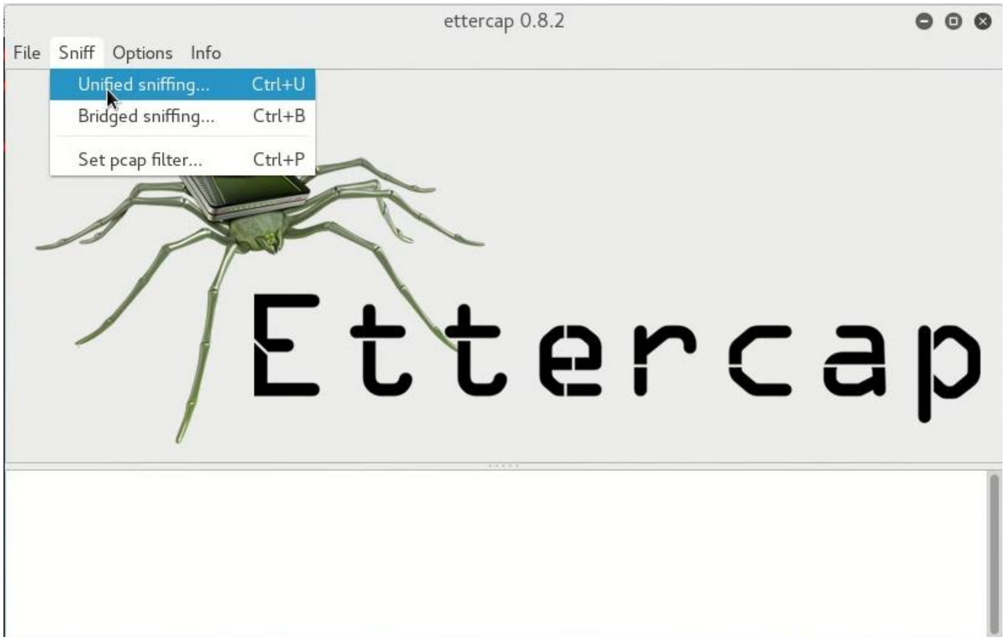
```
root@kali:~# iptables -t nat -p tcp -A PREROUTING --dport 80 -j REDIRECT --to
-port 10000
```

Step3: Open ettercap-graphical tool from the menu. Or from applications -> sniffing and Spoofing -> ettercap-graphical or by searching like this

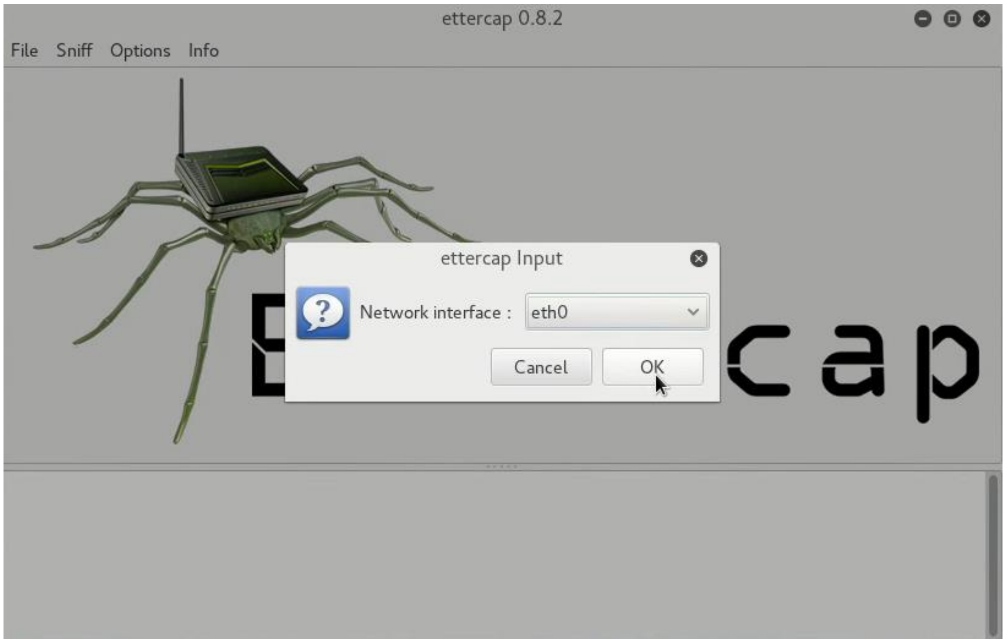




Step 4: Click on sniff menu and select unified sniffing

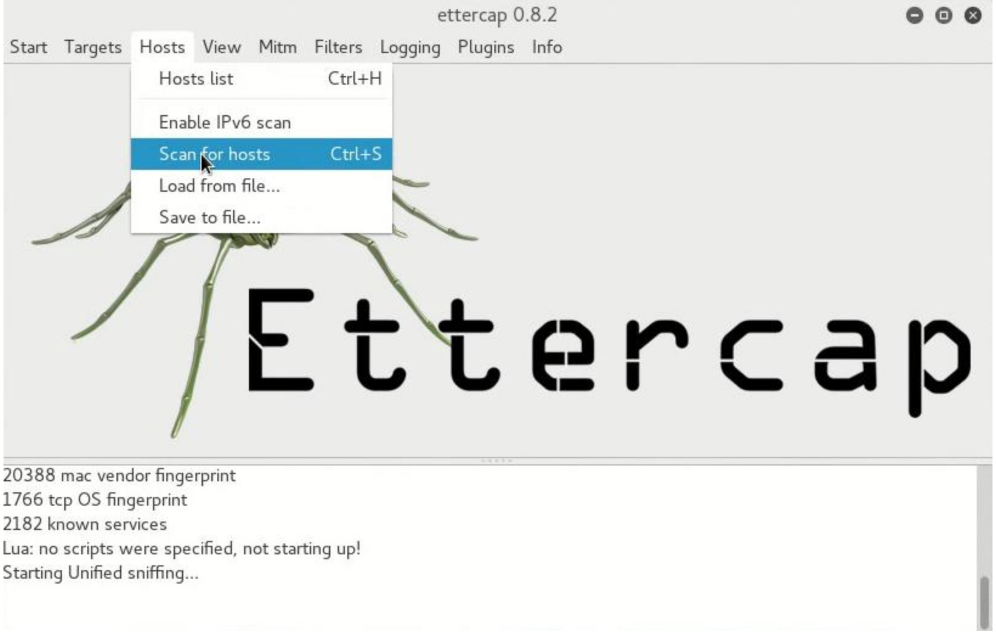

ettercap 0.8.2
File
Sniff
Options
Info
Unified sniffing... Ctrl+U
Bridged sniffing... Ctrl+B
Set pcap filter... Ctrl+P
Ettercap

Step 5: In the ettercap input box select the interface you want to sniff, and click ok.

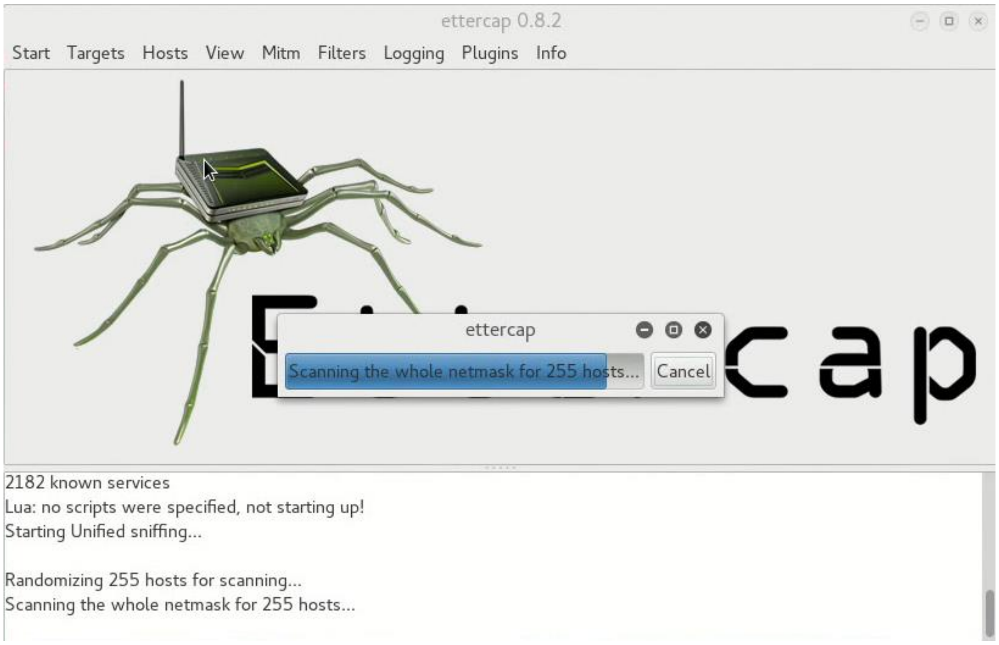


Network interface : eth0

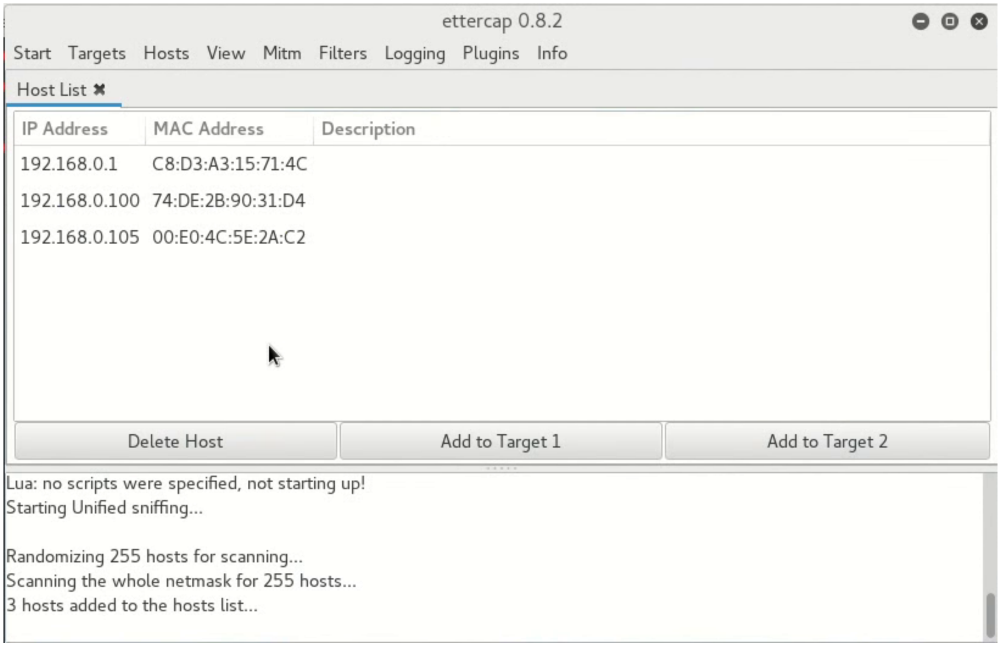
Step 6: Click on “hosts” menu and select “scan for hosts”.



```
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```


ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
ettercap
Scanning the whole netmask for 255 hosts...
Cancel

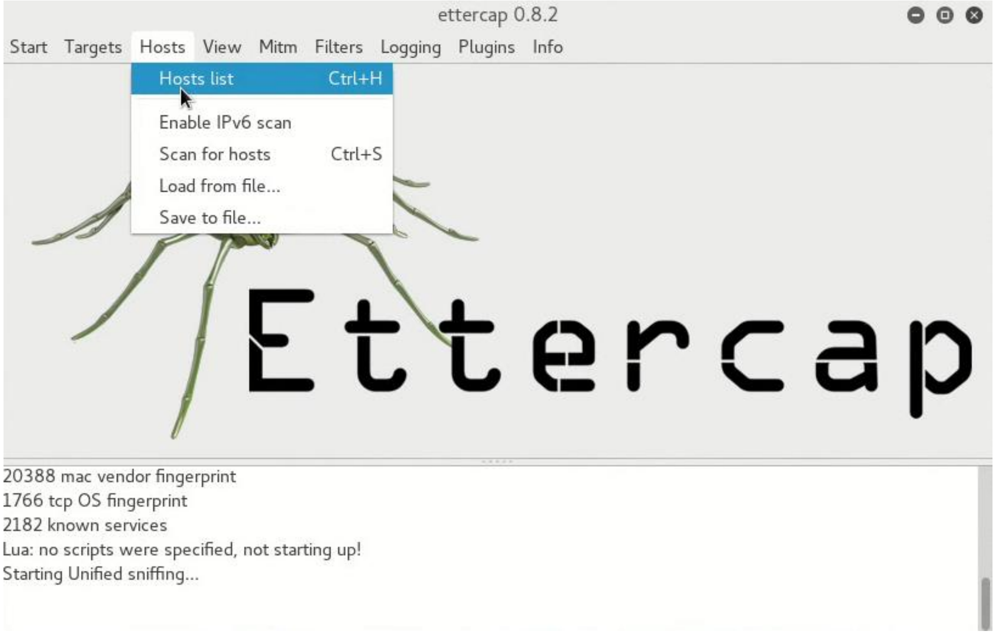
```
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
```



IP Address	MAC Address	Description
192.168.0.1	C8:D3:A3:15:71:4C	
192.168.0.100	74:DE:2B:90:31:D4	
192.168.0.105	00:E0:4C:5E:2A:C2	

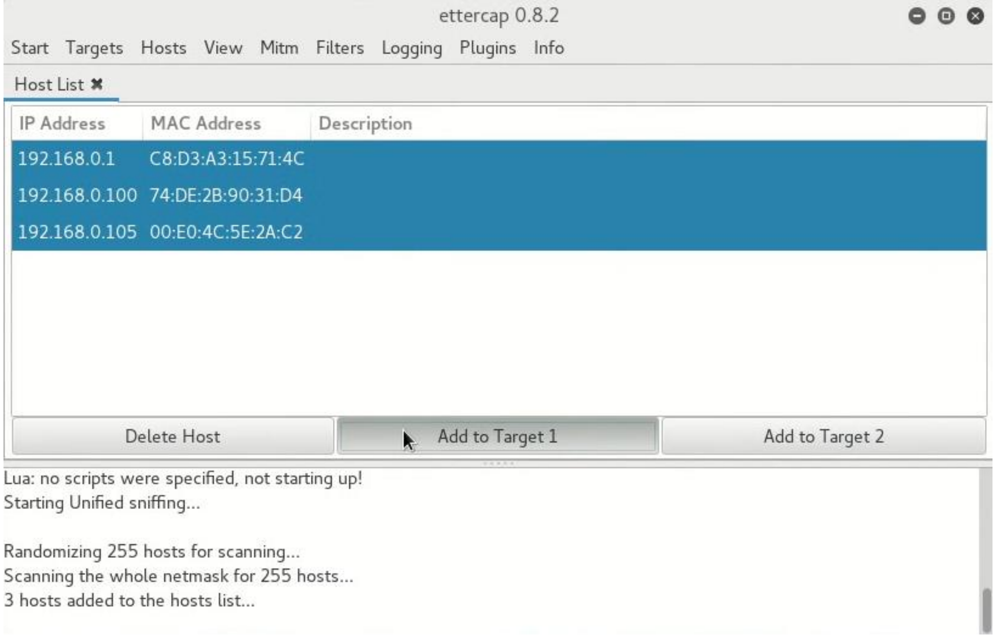
```
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

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

Step 7: Then again select “hosts list” for “hosts” menu.



```
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

Check and confirm that your target ip and the router ip appearing on the list. If yes select the target ip address and click on add to target 1 or 2

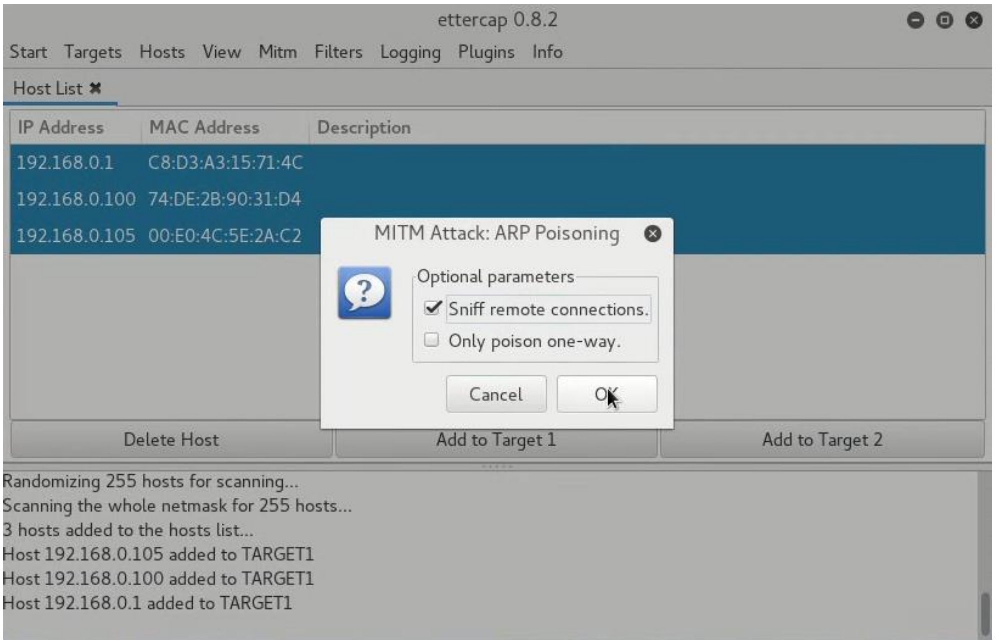


IP Address	MAC Address	Description
192.168.0.1	C8:D3:A3:15:71:4C	
192.168.0.100	74:DE:2B:90:31:D4	
192.168.0.105	00:E0:4C:5E:2A:C2	

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

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

If not repeat step 6 and 7 again

Step 8: Now select “ARP poisoning” from “MITM” menu and check the box for “sniff remote connections only” and click ok.


ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List
MITM Attack: ARP Poisoning
Cancel
OK
Delete Host
Add to Target 1
Add to Target 2

IP Address	MAC Address	Description
192.168.0.1	C8:D3:A3:15:71:4C	
192.168.0.100	74:DE:2B:90:31:D4	
192.168.0.105	00:E0:4C:5E:2A:C2	

Optional parameters

☑ Sniff remote connections.

□ Only poison one-way.

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Host 192.168.0.105 added to TARGET1
Host 192.168.0.100 added to TARGET1
Host 192.168.0.1 added to TARGET1
```

Step 9: Then click on start menu and select start sniffing.

If you follow the steps correctly you will start seeing the victim’s authentication credentials on the ettercap screen.

Practical 3: MITM attack with ARP Poisoning Technique (We are going to remove the SSL security from the secured websites using this method).

Step1: Open a Blank Terminal

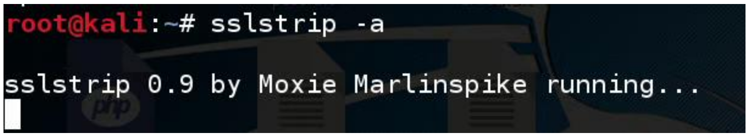
Step2: Execute the following commands

echo 1 > /proc/sys/net/ipv4/ip_forward

iptables –t nat –p tcp –A PREROUTING --dport 80 –j REDIRECT --to-port 10000

Finally execute

sslstrip -a



```
root@kali:~# sslstrip -a

sslstrip 0.9 by Moxie Marlinspike running...
```

Step3: Open ettercap-graphical tool from the menu. Or from applications -> sniffing and Spoofing -> ettercap-graphical

Step 4: Click on sniff menu and select unified sniffing

Step 5: In the ettercap input box select the interface you want to sniff, and click ok.

Step 6: Click on “hosts” menu and select “scan for hosts”.

Step 7: Then again select “hosts list” for “hosts” menu.

Check and confirm that your target ip and the router ip appearing on the list. If not repeat step 6 and 7 again

Step 8: Now select “ARP poisoning” from “MITM” menu and check the box for “sniff remote connections only” and click ok.

Step 9: Then click on start menu and select start sniffing.

If you follow the steps correctly you will start seeing the victim’s authentication credentials on the ettercap screen.

Network Monitoring Tools

Practical No 4: Driftnet

Driftnet is an image sniffer,

Unlike wireshark and ettercap, while you sniffing if you start your driftnet it can show you what images the targets are watching that’s a specialty of the driftnet tool

To use driftnet execute the following command in your terminal while you do sniffing (if you run it without sniffing it will show you the images opened by you only)

```
driftnet –i eth0 –vv
```

The above command will open a small black color box in your kali Linux just maximize it so that you can get more images at once, if the MITM was successful you will start seeing the images of the victim web browsers.

Practical No 5: Darkstat

Darkstat is a pure and free software based network monitoring tool. This tool has capability of showing graphs of the network usage in live for the periods of last 60 secs, 60 mins, etc;

It can also show you how many packets sent and received by a pc also.

To initiate Darkstat just execute the below given command in your command prompt.

```
darkstat –i eth0 –b 0.0.0.0
```

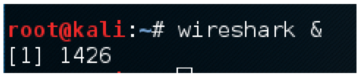
Then open your favorite browser and load http://127.0.0.1:667 to see Darkstat web interface.

Network monitoring using Wireshark

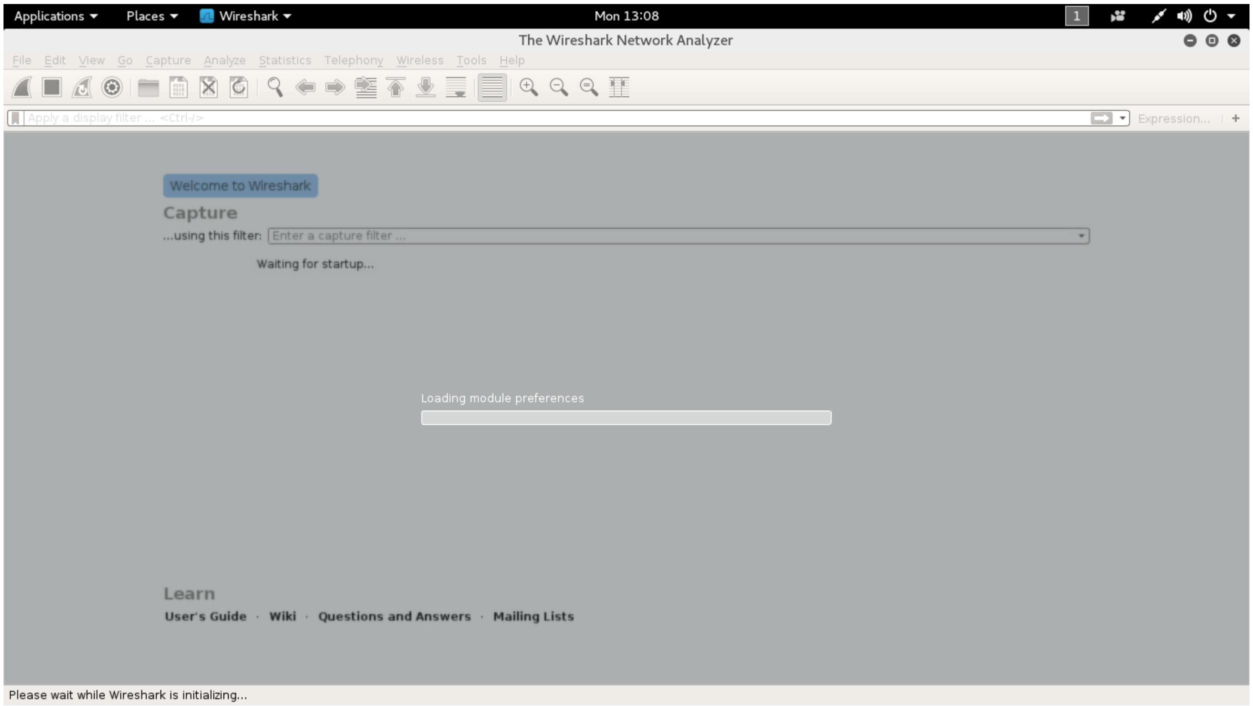
Wireshark: Wireshark is a network protocol analyzer which helps you in observing packets entering or leaving your computer in the real time.

To see wireshark in action just open a blank terminal and type

wireshark &



```
root@kali:~# wireshark &
[1] 1426
```

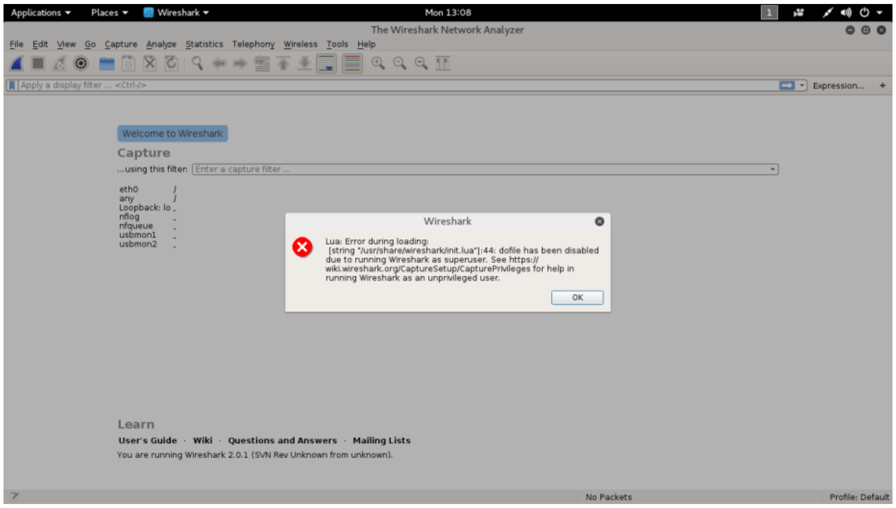

Applications
Places
Wireshark
Mon 13:08
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

Waiting for startup...

Loading module preferences

Please wait while Wireshark is initializing...

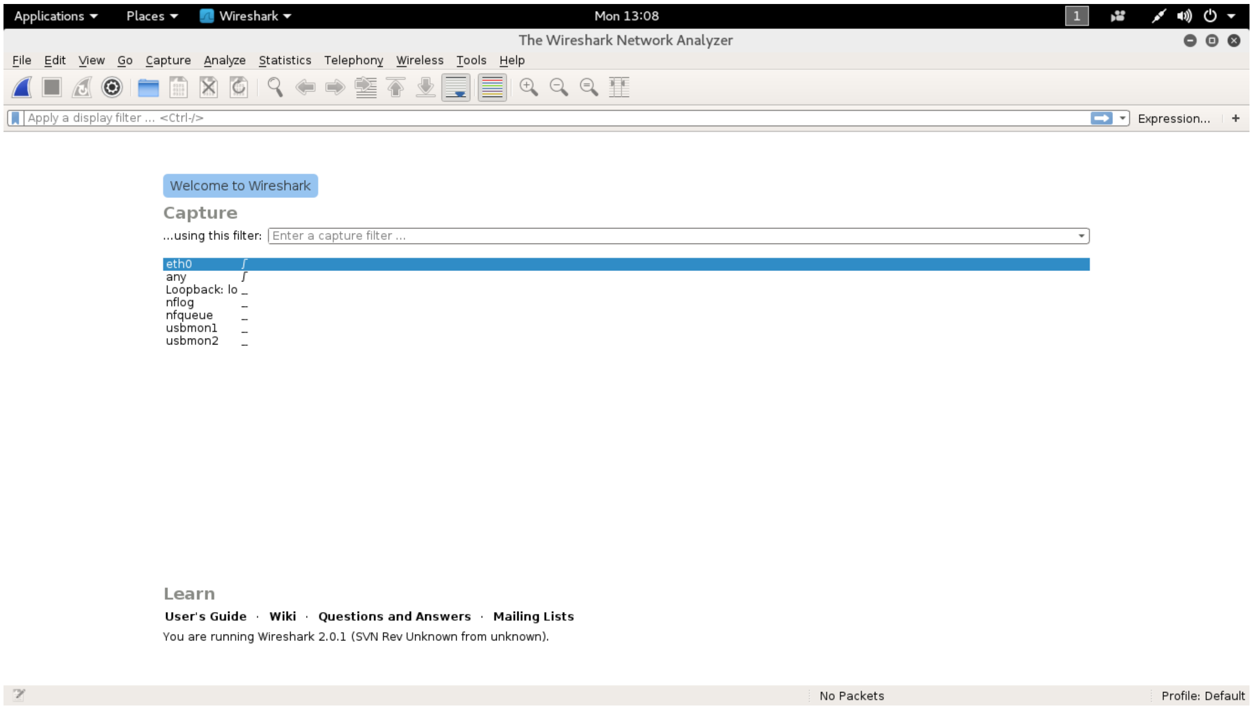
It will give you error telling that you can't use wireshark as root just hit enter so wireshark will load as root user.


Applications
Places
Wireshark
Mon 13:08
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
eth0
any
Loopback: lo
nflog
nfqueue
usbmon1
usbmon2
Wireshark
OK
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
No Packets
Profile: Default

Lua: Error during loading:
 [string "/usr/share/wireshark/init.lua"]:44: dofile has been disabled due to running Wireshark as superuser. See https://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark as an unprivileged user.

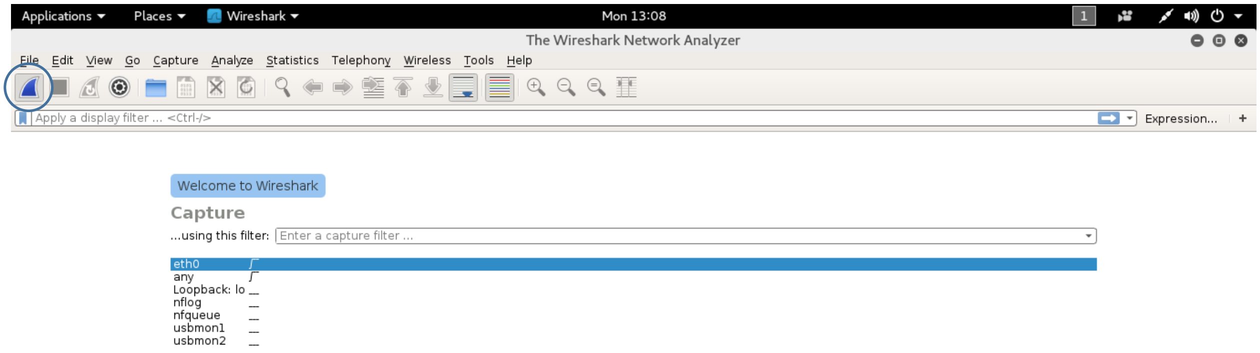
You are running Wireshark 2.0.1 (SVN Rev Unknown from unknown).

When it opens you have to select your interface name Ethernet or Wifi,

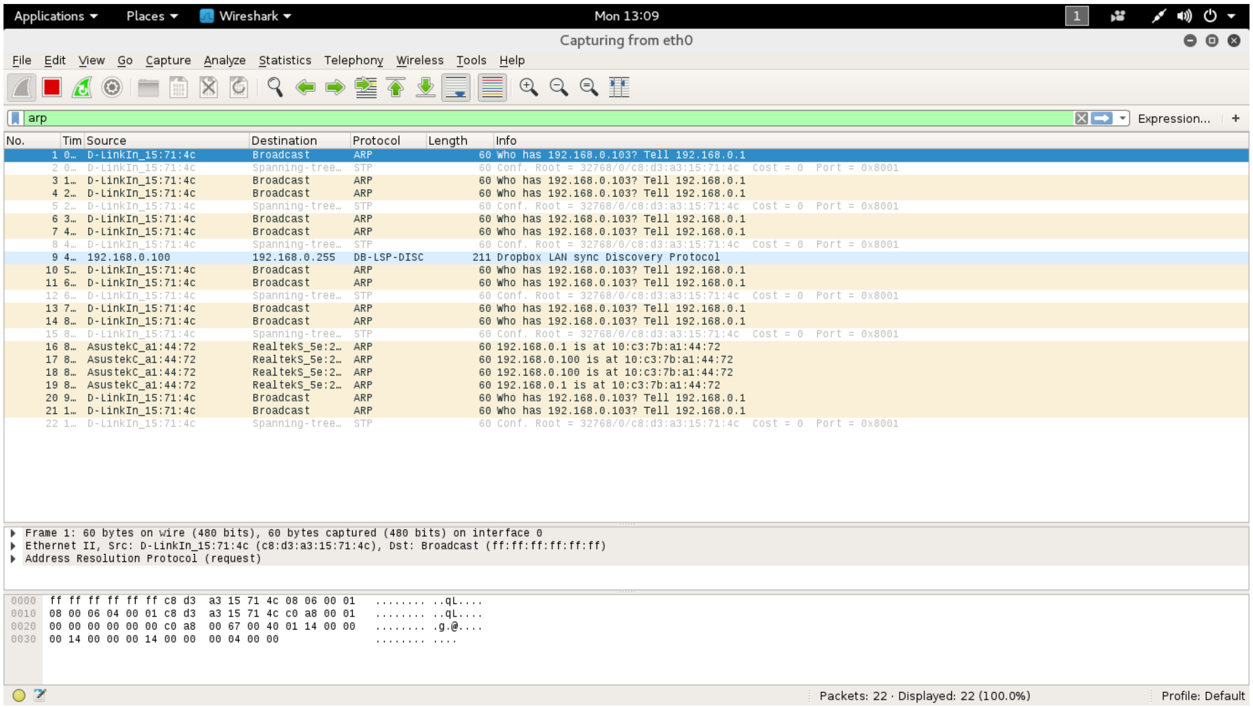

Applications
Places
Wireshark
Mon 13:08
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
eth0
any
Loopback: lo
nflog
nfqueue
usbmon1
usbmon2
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
No Packets
Profile: Default

You are running Wireshark 2.0.1 (SVN Rev Unknown from unknown).

And Click on the blue color fin button here



Immediately it will start showing the incoming and outgoing packets which are coming and leaving your device in live.


Applications
Places
Wireshark
Mon 13:09
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

arp

No.	Tim	Source	Destination	Protocol	Length	Info
1	0…	D-LinkIn_15:71:4c	Broadcast	ARP	60	Who has 192.168.0.103? Tell 192.168.0.1
2	0…	D-LinkIn_15:71:4c	Spanning-tree…	STP	60	Conf. Root = 32768/0/c8:d3:a3:15:71:4c Cost = 0 Port = 0x8001
3	1…	D-LinkIn_15:71:4c	Broadcast	ARP	60	Who has 192.168.0.103? Tell 192.168.0.1
4	2…	D-LinkIn_15:71:4c	Broadcast	ARP	60	Who has 192.168.0.103? Tell 192.168.0.1
5	2…	D-LinkIn_15:71:4c	Spanning-tree…	STP	60	Conf. Root = 32768/0/c8:d3:a3:15:71:4c Cost = 0 Port = 0x8001
6	3…	D-LinkIn_15:71:4c	Broadcast	ARP	60	Who has 192.168.0.103? Tell 192.168.0.1
7	4…	D-LinkIn_15:71:4c	Broadcast	ARP	60	Who has 192.168.0.103? Tell 192.168.0.1
8	4…	D-LinkIn_15:71:4c	Spanning-tree…	STP	60	Conf. Root = 32768/0/c8:d3:a3:15:71:4c Cost = 0 Port = 0x8001
9	4…	192.168.0.100	192.168.0.255	DB-LSP-DISC	211	Dropbox LAN sync Discovery Protocol
10	5…	D-LinkIn_15:71:4c	Broadcast	ARP	60	Who has 192.168.0.103? Tell 192.168.0.1
11	6…	D-LinkIn_15:71:4c	Broadcast	ARP	60	Who has 192.168.0.103? Tell 192.168.0.1
12	6…	D-LinkIn_15:71:4c	Spanning-tree…	STP	60	Conf. Root = 32768/0/c8:d3:a3:15:71:4c Cost = 0 Port = 0x8001
13	7…	D-LinkIn_15:71:4c	Broadcast	ARP	60	Who has 192.168.0.103? Tell 192.168.0.1
14	8…	D-LinkIn_15:71:4c	Broadcast	ARP	60	Who has 192.168.0.103? Tell 192.168.0.1
15	8…	D-LinkIn_15:71:4c	Spanning-tree…	STP	60	Conf. Root = 32768/0/c8:d3:a3:15:71:4c Cost = 0 Port = 0x8001
16	8…	AsustekC_a1:44:72	RealtekS_5e:2…	ARP	60	192.168.0.1 is at 10:c3:7b:a1:44:72
17	8…	AsustekC_a1:44:72	RealtekS_5e:2…	ARP	60	192.168.0.100 is at 10:c3:7b:a1:44:72
18	8…	AsustekC_a1:44:72	RealtekS_5e:2…	ARP	60	192.168.0.100 is at 10:c3:7b:a1:44:72
19	8…	AsustekC_a1:44:72	RealtekS_5e:2…	ARP	60	192.168.0.1 is at 10:c3:7b:a1:44:72
20	9…	D-LinkIn_15:71:4c	Broadcast	ARP	60	Who has 192.168.0.103? Tell 192.168.0.1
21	1…	D-LinkIn_15:71:4c	Broadcast	ARP	60	Who has 192.168.0.103? Tell 192.168.0.1
22	1…	D-LinkIn_15:71:4c	Spanning-tree…	STP	60	Conf. Root = 32768/0/c8:d3:a3:15:71:4c Cost = 0 Port = 0x8001

```
▸ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: D-LinkIn_15:71:4c (c8:d3:a3:15:71:4c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff c8 d3  a3 15 71 4c 08 06 00 01   ........ ..qL....
0010  08 00 06 04 00 01 c8 d3  a3 15 71 4c c0 a8 00 01   ........ ..qL....
0020  00 00 00 00 00 00 c0 a8  00 67 00 40 01 14 00 00   ........ .g.@....
0030  00 14 00 00 00 14 00 00  00 04 00 00               ........ ....
```

Packets: 22 · Displayed: 22 (100.0%)   Profile: Default

Few wireshark filter can be helpful

Any protocol name like http, ftp, smtp, telnet, icmp, udp, dns, arp, etc.

For a particular ip packets

ip.addr == <ip address>

For a particular ip address as a source device.

ip.src_host == <source ip>

For a particular ip address as a destination device.

ip.dst_host == <destination ip>

For a particular port number

tcp.port == <port number>

For comination you can use &&

ip.addr == 192.168.0.1 && http