Capture and Analise Packets

In this lab session we will use tcpdump and wireshark to capture packets. To analise them we will use wireshark.

Packet Capturing using tcpdump

- Go to the ubuntu VM
- use tcpdump command to pacture packets

```
•tcpdump -nn
```

- you will get outputs like following

```
•IP 199.59.148.139.443 > 192.168.1.8.54343: Flags [P.], seq
   53:106,

•ack 1, win 67, options [nop,nop,TS val 854797891 ecr
   376933204],

•length 53
```

- You can try tcpdump with different attributes

```
•tcpdump –nni eth0 host 10.10.10.10

•tcpdump –nni eth0 dst host 10.10.10.10 and tcp

•tcpdump –nni eth0 src net 10.10.10.0/24 and tcp and portrange
   1-1024

•tcpdump –nni eth0 –s0

•tcpdump –nni eth0 not port 22 –s0 –c 1000

•tcpdump –nni eth0 not port 22 and dst host 10.10.10.10 and not
   src net 10.20.30.0/24

•

•-nn = don’t use DNS to resolve IPs and display port no

•-i = interface to watch

•dst = watch only traffic des0ned to a net, host or port

•src = watch only traffic whose src is a net, host or port

•net = specifies network
```

```
•host = specifies host

•port = specifies a port

•proto = protocol ie tcp or udp

•-s0 = seIng samples length to 0 m

•-c = number of packets
```

- You can capture packets and save them to a file

```
•# tcpdump –nni eth0 -w capture.pcap –vv –c 1000

•# tcpdump –nni eth0 –r capture.pcap port 80

•

•-w capture.pcap = save capture packet to capture.pcap

•–vv =  display number of packet captured

•-r capture.pcap = read capt
```

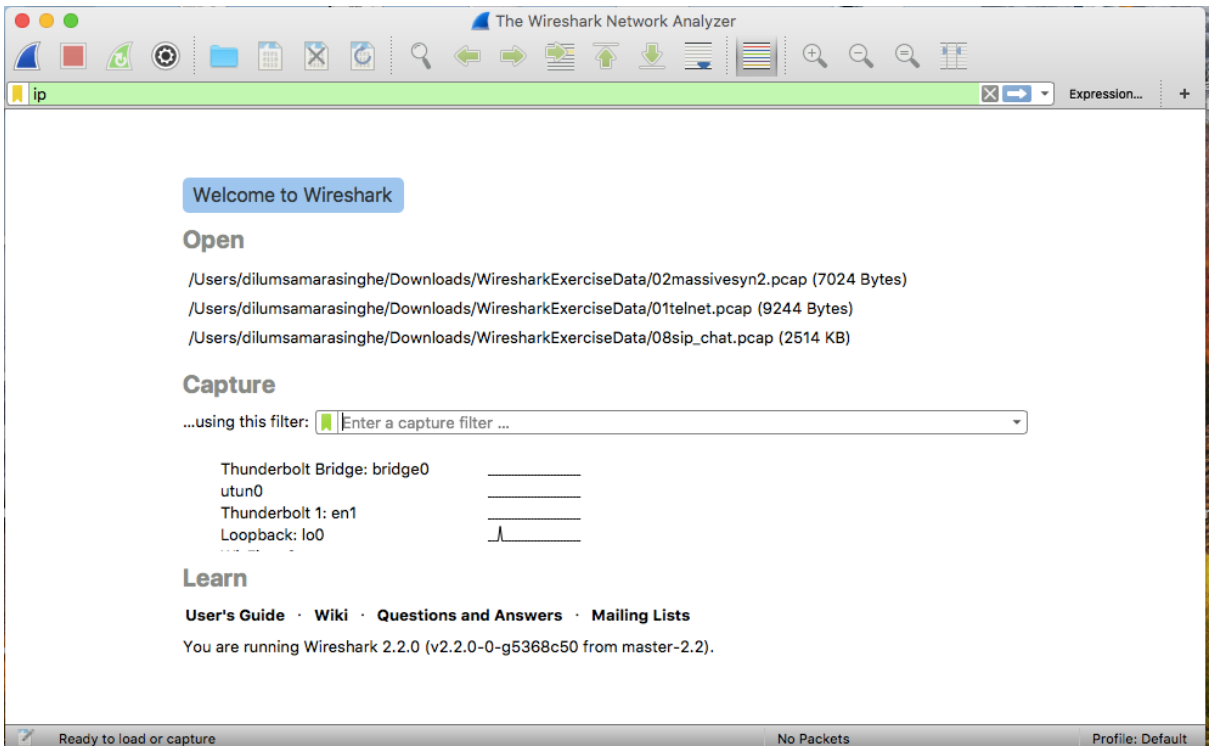
- You can open the created file and see the captured packets

Wireshark

Download wireshark and istall wireshark. Installation is very simple.

Captureing Packets from wireshark

Once you open the wireshark you will get the following interface.



You can select the interface that you want to capture packets clicking on the intarface listed there. Then you can click the **Start Capture** to capture the packets. 

You will see the packets capturing. Click the **Stop Capture** button when you want to stop the capturing. 

You can save the captured packets by clicking **File>Save as...** and Clicking **Save** after you select a Location

You can change the interface and add or remove filter by clicking the **Options** button. 

Filters

Wireshark has lot of filters. Let's try a simple filter. Let's capture only the packets that are usinf ICMP protocol.

You will the filter text field in the wireshark interface. Type **icmp** there and start capturing. You can try different filters.

- **ip.addr == <Your IP address>** [Sets a filter for any packet with 10.0.0.1, as either the source or dest]
- **ip.addr==<Your IP address> && ip.addr==<neighbors IP address>** [sets a conversation filter between the two defined IP addresses]
- **http or dns** [sets a filter to display all http and dns]
- **tcp.port==53** [sets a filter for any TCP packet with 4000 as a source or dest port]
- **http.request** [displays all HTTP GET requests]
- **!(arp or icmp or dns)** [masks out arp, icmp, dns, or whatever other protocols may be background noise. Allowing you to focus on the traffic of interest]

Analysing

Download the sample packet capture files from here. Open them from wireshak to analyse them. Go to **File>Open** and select tha pcap file to be open.

Telnet.pcap

- Wht is the Username and Password?
- What did the User do after log in?

Open the file. Filter all the telnet traffic. Go to Analyse>Follow>TCP Stream.

massivesyn.pcap

- Is this an attack? If so what type of an attack?

Open the file, Go to Statistics>Coversation. Check for the Type of packet, Sourse IP and the duration

chat.dmp

- What are the email addresses of the chatters?
- What were they planning to do?

Open the file. Go to Analyse>Follow>TCP Stream.

ftp.pcap

- What is the IP address of the FTP server and the Client?
- What is the error code 530?

Open the file. Statistics>Coversation. Click TCP. Check the Statistics. Go to Analyse>Follow>TCP Stream

foobar.pcap

- What is the protocol use TCP 6346?
- What could be this scenario?

Open the file. Statistics>Coversation and check for source and destination IP and port. Go to Statistics>Protocol Hierarchy

covertinfo.pcap

- Is this a normal icmp packet?

Open the file. Statistics>Coversation and check for packet length.

sip.pcap

- What is the protocol used for media?
- Can you listen to the phone conversation?

Statistics>Protocol Hierarchy check for UDP protocols. Use Telephony>(Protocol) > Analysis