Wireshark packet analyser Tool

Aim: Study of packet sniffer tools Wireshark:- a. Observe performance in promiscuous as well as non-promiscuous mode. b. Show the packets can be traced based on different filters.

Objective: To observe the performance in promiscuous; non-promiscuous mode; to find the packets based on different filters.

Outcomes: The learner will be able to:- Identify different packets moving in/out of network using packet sniffer for network analysis.

Course outcome: CO3

Theory:

What is Wireshark?

- Wireshark is a network packet analyser.
- A network packet analyser will try to capture network packets and tries to display that packet data as detailed as possible.
- Wireshark is available for free, is open source, and is one of the best packet analysers available today.
- A packet sniffer, sometimes referred to as a network all the packets of data that pass-through a given network interface.
- By placing a packet sniffer on a network in promiscuous mode, a Malicious intruder can capture and analyse all the network traffic.

What is the promiscuous mode in Wireshark?

- In computer networking, promiscuous mode is a mode of operation, as well as a security, monitoring and administration technique.
- In promiscuous mode, a network device, such as an adapter on a host system, can intercept and read in its entirety each network packet that arrives.
- This mode applies to both a wired network interface card and wireless NIC. In both cases, it causes the controller to pass all traffic it receives to the central processing unit instead of just the frames it is specifically programmed to receive.
- This enables a network monitoring tool to examine the content of the transmission for potential threats.

Steps to enable promiscuous mode in Wireshark:

1. Click on **Edit > Preferences > Capture**.

2. You'll see the preference "**Capture packets in promiscuous mode**".

3. If that is checked, which is Wireshark's default, Wireshark will put the adapter into promiscuous mode for you when you start capturing.

4. If the adapter was not already in promiscuous mode, then Wireshark will switch it back when you stop capturing.

5. So yes, Wireshark does this automatically, if you haven't disabled this preference.

What is non-promiscuous mode in Wireshark?

- If the interface is not running in promiscuous mode, it won't see any traffic that isn't intended to be seen by your machine.
- It will see broadcast packets, and multicast packets sent to a multicast MAC address the interface is set up to receive.

What are the steps to enable non-promiscuous mode in Wireshark?

1. Click on **Edit > Preferences > Capture**.

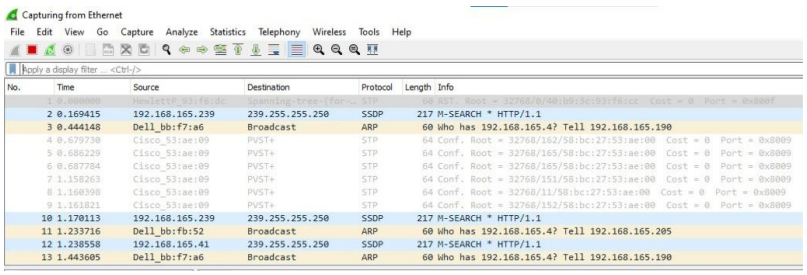
2. You'll see the preference "**Capture packets in promiscuous mode**".

3. If that is checked, which is Wireshark's default, Wireshark will put the adapter into promiscuous mode for you when you start capturing.

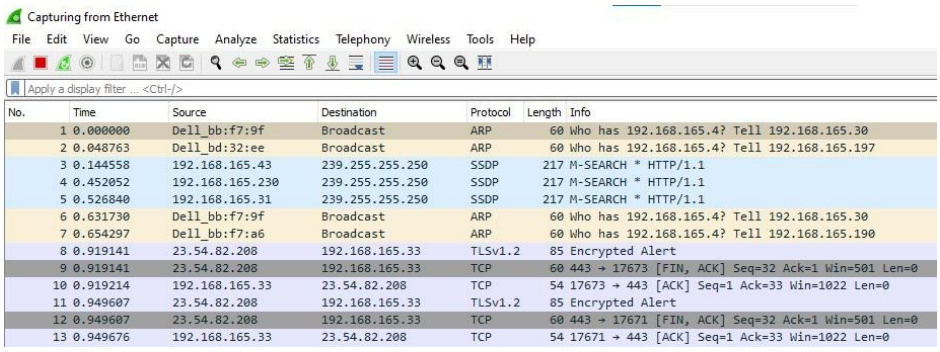
4. Uncheck that option to disable the promiscuous mode in Wireshark.

<u>Output:</u>

1. **Packets captured in promiscuous mode:**

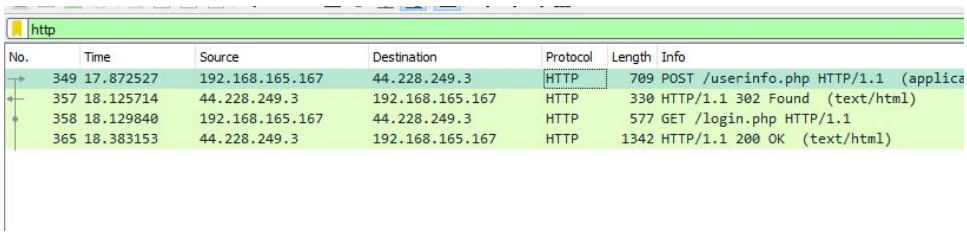


2. **Packets captured in non-promiscuous mode:**



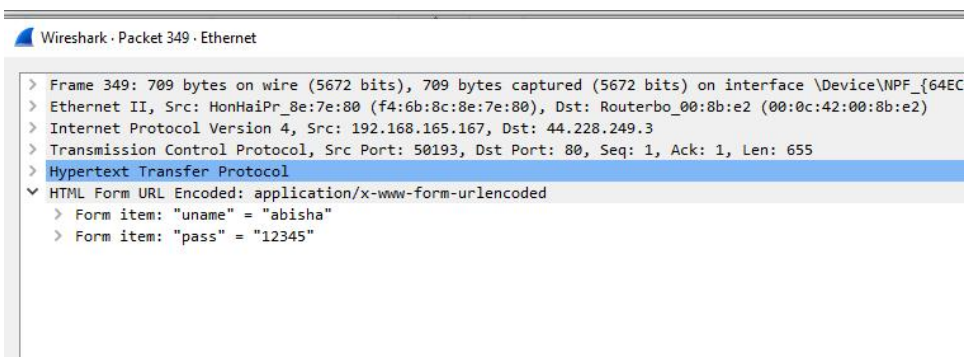
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Dell_bb:f7:9f	Broadcast	ARP	60	Who has 192.168.165.4? Tell 192.168.165.30
2	0.048763	Dell_bd:32:ee	Broadcast	ARP	60	Who has 192.168.165.4? Tell 192.168.165.197
3	0.144558	192.168.165.43	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
4	0.452052	192.168.165.230	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
5	0.526840	192.168.165.31	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
6	0.631730	Dell_bb:f7:9f	Broadcast	ARP	60	Who has 192.168.165.4? Tell 192.168.165.30
7	0.654297	Dell_bb:f7:a6	Broadcast	ARP	60	Who has 192.168.165.4? Tell 192.168.165.190
8	0.919141	23.54.82.208	192.168.165.33	TLSv1.2	85	Encrypted Alert
9	0.919141	23.54.82.208	192.168.165.33	TCP	60	443 → 17673 [FIN, ACK] Seq=32 Ack=1 Win=501 Len=0
10	0.919214	192.168.165.33	23.54.82.208	TCP	54	17673 → 443 [ACK] Seq=1 Ack=33 Win=1022 Len=0
11	0.949607	23.54.82.208	192.168.165.33	TLSv1.2	85	Encrypted Alert
12	0.949607	23.54.82.208	192.168.165.33	TCP	60	443 → 17671 [FIN, ACK] Seq=32 Ack=1 Win=501 Len=0
13	0.949676	192.168.165.33	23.54.82.208	TCP	54	17671 → 443 [ACK] Seq=1 Ack=33 Win=1022 Len=0

3. **Packets captured using filters:**



No.	Time	Source	Destination	Protocol	Length	Info
349	17.872527	192.168.165.167	44.228.249.3	HTTP	709	POST /userinfo.php HTTP/1.1 (applica
357	18.125714	44.228.249.3	192.168.165.167	HTTP	330	HTTP/1.1 302 Found (text/html)
358	18.129840	192.168.165.167	44.228.249.3	HTTP	577	GET /login.php HTTP/1.1
365	18.383153	44.228.249.3	192.168.165.167	HTTP	1342	HTTP/1.1 200 OK (text/html)

4. **User credentials on a vulnerable website captured using Wireshark:**



<u>Conclusion:</u> The different packets moving in and out of network are analysed successfully using packet sniffer.