Department of Information Technology

Academic Year: 2022-23 **Semester: V**
Class / Branch: TE IT
Subject: Security Lab (SL)
Subject Lab Incharge: Prof. Apeksha Mohite

EXPERIMENT NO. 3B

Aim: To study analysis of network packets by sing open source sniffing tools like tcpdump and Wireshark in promiscuous and non-promiscuous mode.

Theory :
tcpdump is a common packet analyzer that runs under the command line. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. It is available under most of the Linux/Unix based operating systems. tcpdump also gives us a option to save captured packets in a file for future analysis. It saves the file in a pcap format, that can be viewed by tcpdump command.

Installing tcpdump:
 # sudo apt-get install tcpdump

TCP message flow

1. Connection initialization
(1) Client will send a packet with SYN flag is set and random number(R1) included in the sequence number field.
(2) Server will send a packet with SYN flag and ACK flags are set. sequence number field will contain a new random number(R2) and acknowledgement number field will contain clients sequence number +1 (R1+1).(Which is the next sequence number server is expecting from the client)
(3) Client will acknowledge servers SYN packet by sending a packet with ACK flag is set and acknowledge number field with R2+1. (Which is the next sequence number client is expecting from the server)

2. Load
Payloads will travel both the directions of the TCP connection after the connection initialization. All the packets will set the ACK flag, PSH, URG flags may or may not be set.

3. Termination
TCP connection is normally terminating using a special procedure where each side independently closes its end of the link. It normally begins with one of the application processes signaling to its TCP layer that the session is no longer needed. That device sends a message with FIN flag set to tell the other device that it wants to end the connection, which then get acknowledged. When the responding device is ready, it too sends a FIN, after waiting a period of time for the ACK to be received, the session is closed.
Running tcpdump :

tcpdump -D : display all available interfaces
tcpdump -i wlo1 : capture traffic at the interface "wlo1"
tcpdump -i any : capture traffic at any interface
tcpdump -i wlo1 port 80 : capture traffic at the interface "wlo1" on port 80
tcpdump -i wlo1 -c 5 : capture 5 packets at the interface "wlo1"
tcpdump -i wlo1 tcp : capture only tcp traffic at interface "wlo1"
tcpdump -i wlo1 src 192.168.43.169: capture traffic at interface "wlo1" with source IP 192.168.43.169

To capture only TCP SYN packets:
sudo tcpdump -i wlo1 "tcp[tcpflags] & (tcp-syn) != 0" >/home/apsit/Desktop/syn.txt

Wireshark:
Wireshark is a free application that allows you to capture and view the data traveling back and forth on your network, providing the ability to drill down and read the contents of each packet – filtered to meet your specific needs. It is commonly utilized to troubleshoot network problems as well as to develop and test software. This open-source protocol analyzer is widely accepted as the industry standard, winning its fair share of awards over the years.

Wireshark has a rich feature set which includes the following:
- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis
- Standard three-pane packet browser
- Multi-platform: Runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many others
- Captured network data can be browsed via a GUI, or via the TTY-mode Tshark utility

Installing wireshark :

 # sudo apt-get install wireshark

Promiscuous and non promiscuous mode:
Promiscuous mode is often used to monitor network activity. Promiscuous modeis the opposite of non-promiscuous mode. When a data packet is transmitted innon-promiscuous mode, all the LAN devices "listen to" the data to determine if the network address included in the data packet is theirs.

"Promiscuous mode" on both WiFi and Ethernet means having the card accept packets on the current network, even if they're sent to a different MAC address.
" Non-Promiscuous mode" is WiFi-specific and means having the card accept packets for any network, without having to be associated to it.

Conclusion:
Sometimes a network service is just not behaving the way it should. And the log files do not help you either. Packet sniffing is useful to analyze the data during the transmission in the network . Sniffing tools like tcpdump and Wireshark are useful to implement it. It can be used for network traffic monitoring, traffic analysis, troubleshooting and other useful purposes. Packet sniffers can capture things like passwords and usernames or other sensitive information.