PS-4

TCPDUMP

Tcpdump, like wireshark and many other sniffers, is usually used to capture packets and analyze network protocols. The network card of a computer drops packets if the packets are not addressed to the system. However in the promiscuous mode, the network card forwards all packets reaching the card to the operating system so that tcpdump can capture them, regardless of their (MAC) addresses. Using tcpdump in the promiscuous mode can exam all traffic through the interface, extract sensitive information and thereby sniffer the network. For example, if Computer A and a few other computers are inter-connected by a hub, which broadcasts packets it receives to all connected computers, Computer A in the promiscuous mode will be able to capture all packets going through the hub. A computer not in the promiscuous mode is able to capture packets addressed to itself and its outgoing packets. Root privilege is required to use tcpdump for sniffing

Capture Packets using TCPDUMP

Install TCPDUMP `apt-get install tcpdump`

Start Capturing `# tcpdump`

Write capture t file `tcpdump -i eth0 -w capture.pcap`

After generating the .pcap file using **tcpdump** we can use Wireshark GUI tool to analyze traffic. But there are few things that might be important to know. [11]

Time format

Change the Date-Time format in WireShark from *View -> Time Display Format*

- Time shift

The way Wireshark display time stamps can be confusing at first. If you are analyzing tcp packets compared some other sever log, you need to co-relate the time stamps and for that its important to understand how to correctly shift the time of the packets.

Open the Capture file using Wireshark

To view the PCAP file, launch Wireshark, select **File**, click **Open** and browse to the file's location -- probably a network share or a local directory to which you copied the file from the original system.

Now, you have Wireshark's search, filtering and analysis power at your disposal in a helpful graphical interface.

TCPDUMP Tutorial

https://github.com/Samsar4/Ethical-Hacking-Labs/blob/master/11-Bonus/TCPDump-Tutorial.md

Practice Questions

1. Filter the TCPDUMP for TCP UDP and HTTP messages.
2. Can you locate the 3-way handshaking protocol for a TCP connection
3. Did the TCP connection terminate
4. What was the source of the connection
5. Was there any packets with the insecure http protocol
6. If yes, find the source ip and destination IP of the http connection
7. What are the client and server port numbers used in first full TCP three-way handshake? (low number first then high number)
8. Was there any DNS packet, find the source and destination of the DNS packet
9. what tcpdump command will enable you to read from the capture and show the output contents in Hex and ASCII?