**TCPDUMP LAB**

**Lab Objective** – Learn to capture packets using tcpdump.

**Lab Purpose** – Tcpdump is a tool that is similar to Wireshark but without the GUI. It allows the user to display TCP/IP and other packets being transmitted or received over a network.

**Lab Tool** – Kali Linux.

**Lab Walkthrough** –

TASK 1

* Tcpdump is already installed in kali linux by default. First we use the command “tcpdump –version” and then tcpdump –help. Respectively with each command we get to know the version of tcpdump we are running and the available commands we can use.  
  A screenshot of a computer screen

  Description automatically generated
* In order to start the packet capture we need to first select an interface. In simpler words interface can be your wifi or ethernet connection. Type the command “tcpdump -D”  
  A screenshot of a computer program

  Description automatically generated
* We can slelect the eth0 interface by using the command “tcpdump -I eth0”, furthermore we can add -c 5 to the command which will hence capture only 5 packets. So the final command would be tcpdump -I eth0 -c 5. (Use the command in root)  
  A screenshot of a computer program

  Description automatically generated
* In case youre interested in adding the MAC Adresses as well, then add the -e to the above command. That is tcpdump -e -I eth0 -c 5  
  A computer screen shot of a computer code

  Description automatically generated

TASK 2

* Using the verbose option in the command for packet capture is recommended since it provides us with extra data integrity information like Time to Live, total length, etc. All we need to do is add a -v parameter. Below you can see the difference between both commands. The above one uses a verbose option and the down one doesn’t.   
  A screenshot of a computer

  Description automatically generated
* Some other commands can be :  
  tcpdump -n “udp and dst port 53” This command will help you pickup DNS Requests.
* Tcpdump port 443 This command can help capture packets only related to port 443. Replace 443 with anyport number you want.

There are tons of other ways to use the tcpdump. Here a link to help you out. <https://docs.netgate.com/pfsense/en/latest/diagnostics/packetcapture/tcpdump.html>

TASK 3

* To print each packet in ASCII code, we need to use “-A” parameter. This next command is an example of using grep with tcpdump to help it only display information we deem to be important.
* tcpdump -n -i eth0 -A | grep -e “POST”
* This command will begin gathering all packets using tcpdump, and we then use grep to find and display all POST requests to us. This is an example of how tcpdump can be used in a creative fashion to display detailed information about the network.  
  A computer screen shot of a computer code

  Description automatically generated

TASK 4

* We can save our captured file as well. We need to add a -w and a filename with the extension .pcap at the end.
* Tcpdump -I eth0 -c 5 -w sess.pcap  
  A screenshot of a computer screen

  Description automatically generated

**Lab Conclusion:**

* In this lab, the objective was to learn packet capturing using tcpdump, a command-line tool on Kali Linux. The walkthrough included tasks such as checking the tcpdump version, selecting a network interface, capturing packets with various options (e.g., limiting the number of packets, including MAC addresses), and using verbose options for additional information like Time to Live and total length.
* The lab also covered specific commands for capturing DNS requests, filtering packets related to a specific port, and printing each packet in ASCII code. Additionally, it demonstrated the use of grep with tcpdump to selectively display information, showcasing the creative ways tcpdump can provide detailed insights into network activity.
* Furthermore, the lab highlighted the capability to save captured packets into a file using the -w option, enabling users to analyze and review the captured data later. Overall, the hands-on exercises in this lab aimed to enhance understanding and proficiency in using tcpdump for packet analysis on a network.