IP LAB EXPERIMENT – 2 [CYS 2022 - 2024] 09-10-2022

(Note: Total 25 marks for this lab assignment which includes 20 marks + 5 marks for your report)

For each of the following steps describe your results, give the syntax of the command you used, and, where appropriate, the output produced. Include screen captures as needed in your output. Be sure to label your results carefully and organize your results in the order of steps as given here and answer each question in your report.

1. Understand PING and document it, then answer the following question: (3 marks)
   a. Use ping on google.com and document your results on the output you received. [Find the IP address, Time to live value, and round trip time value from the results you got].
   b. By default, ping will send 4 packets to check the details, here you have to send 8 packets to check the output over google.com. Explain what the purpose of this doing is.
   c. Ping your local host. Explain what the purpose
   is.Reference: https://linux.die.net/man/8/ping
2. Read the Unix manual page for traceroute OR help for tracert. Experiment with the various options. Describe the three things that you found most useful in the result. (2 marks)
   Answer the following question:
   a. Try tracert over google.com
   b. Type tracert -d google.com
      1. How many hops is your machine away from google.com? (Attach the output in the lab report)
      2. Wait for a while and execute the same command again. Is the output the same as the first time? Observe and compare the difference and explain the reason.
3. You have to read about NETSTAT from the manual page or help before answering the belowquestions: (1 mark)
   a . Use netstat to display information about the routing table.
   b. Use netstat to display about ethernet statistics.
   Reference: https://man7.org/linux/man-pages/man8/netstat.8.html
4. What is the purpose of NSLOOKUP ? Answer the following questions below: (3 marks)
   a. Use nslookup to find out the internet address of the domain amrita.edu.

b. What is the mail exchanger for the domain google.com.

c. What is the name server for amrita.edu.

Reference: http://linux.math.tifr.res.in/manuals/man/nslookup.html

5. What are ARP and RARP? Answer the following questions below: (3 marks)

a. Use arp command to find the gateway address and host systems hardware address.

b. How do you find the arp entries for a particular interface?

c. How do delete an arp entry?

d. How do you add and arp entry in arpcache?

Reference: https://man7.org/linux/man-pages/man8/arp.8.html

6. Read about TCPDUMP tool [use manual page]. Answer the questions below: (1 marks)

a. Using tcpdump, get the information about the general incoming network traffic with names.

b. Using tcpdump, get the information about the general incoming network traffic with ip address on specific interface.

Reference : https://www.tcpdump.org/manpages/tcpdump.1.html

7. Use Wireshark (Latest version) to solve the below scenarios: (7 Marks)
Use Evidence.pcapng as evidence [Provided in Teams] file to answer the below questions.

1. You, as a SOC analyst noted that someone try to send information (**PING**) to unknown IP address and you are suspecting some malicious information might transferred in it. Analyze the log file.

a. Find the data transferred.

b. Find the source and destination IP of that log.

c. Find the Data length (Bytes) and verify the checksum status on destination.

2. Now you have found that some kind of file is been downloaded by insider in **unencrypted web traffic**. Your task is to

a. Find the name and type of file.

b. Export that file from that web traffic, then analyze the file for any secret information.

c. Find the hostname in which the file is stored.

3. Based upon their activities, auditing team has started investigation against them and found that the insider passed some **sensitive information via call** to someone. The traffic is been captured.

a. Analyze the traffic and find those conversations and extract the sensitive information in it.

b. Find the call-ID when the status of the call is ringing.

4. On further investigation, you have a suspect on some wireless device communications. List out the **Bluetooth devices communications** from this traffic and find the details about native Bluetooth adapter.

a. Analyze the captured **WPA handshake** from this traffic and report in detail about it toyour administrator.

b. Geo locate all the endpoint of wireless devices.

c. Analyze the **protocol level information transfer** between wireless devices.

Tutorial link : https://www.youtube.com/watch?v=R5-dzWJzzEw&list=PLib7LoYR5PuA52bv7pjkRZ-5Dj1697h4x

Wireshark Download link : https://www.wireshark.org/download.html