CYBER SECURITY LAB ASSIGNMENT 1
DIAGNOSTIC AND TROUBLESHOOTING TCP/IP COMMANDS
ASSIGNMENT WEIGHTAGE: 05 MARKS

All of the following questions are based on assuming you are on a Windows 10/11 Internet Enabled PC:

1. Using appropriate command, find out the IP address/es, Default Gateway IP address, Subnet Mask, Primary DNS Server IP address, DHCP Server IP address (if any), MAC address and NIC Card Description of your PC. Identify each IP address shown as an IPv4 or an IPv6 IP address.
2. Determine, using appropriate command, whether your Device is having IP level connectivity with the machine hosting www.yahoo.com.
3. Based on above exercise 2, determine : a) The % packet loss b) The Average RTT
4. Identify the IP address and its type (4 or 6) for www.yahoo.com based on the results obtained in 2.
5. Find out the IPv4 address of the machine hosting www.bata.com
6. Find out the IPv6 address of the machine hosting www.bata.com
7. Construct and execute a command to continuously bombard www.bata.com with ICMP echo request messages. The bombarding should stop only with manual intervention.
8. Identify the host name of the machine whose IPv4 address is 27.123.43.205 using appropriate command.
9. Determine, using appropriate command, whether your Device is having IP level connectivity with the machine hosting www.yahoo.com. You are restricted to using up-to sending test packets two times only.
10. What is the default size of the test packet in exercise 2? Now override the default packet size to 128 bytes and repeat the same exercise of 2.
11. Check whether it is possible to reach the website of 'PGP glass' without fragmentation.
12. Determine, using appropriate command, whether it is possible from your Device to have IP level connectivity with the machine hosting www.yahoo.com using IPv4 only.
13. Determine, using appropriate command, whether it is possible from your Device to have IP level connectivity with the machine hosting www.bata.com using IPv6 only.
14. Find out whether it is possible to reach www.bata.com from your machine within 3 hops only.
15. Assuming you are in LAN, using appropriate command, find out the MAC address of your neighbor's PC remotely, without invoking any command on his/her PC or asking your neighbor.
16. Check whether it is possible to reach Indian Railways Website within 8 hops.
17. Using nslookup command, find out the IP address of the Indian Railways Website. Find out the IP address of the DNS server which gave you this reply. Also identify whether the reply was authoritative or not.
18. Repeat exercise 17 using Google's DNS server.
19. Display all active TCP connections in your PC using appropriate command.
20. Display the hostname of your PC using an appropriate command.

-x-x-x-x-x-

CYBER SECURITY LAB ASSIGNMENT 2
INSTALLING, OPERATING AND TRAFFIC ANALYSIS USING WIRESHARK
ASSIGNMENT WEIGHTAGE: 05 MARKS

All of the following questions are based on assuming you are on a Windows 10/11 Internet Enabled PC:

1) Install Wireshark in Windows 10/11.
2) Demonstrate how live traffic can be captured (either through wired or wireless interface, as per your device/laptop configuration)
3) Demonstrate how live ICMP traffic can be captured. (Hint: Use Ping)
4) Demonstrate how to view only ICMP traffic, assuming all traffic types are being captured.
5) Demonstrate how to capture only ICMP traffic.
6) Identify the source and destination IP address, and the ICMP Message Code number of the request and reply messages.
7) Demonstrate how passwords can be cracked for http /non https sites.

-x-x-x-x-x-

CYBER SECURITY LAB ASSIGNMENT 3
INSTALLING, OPERATING AND ANALYSIS USING Angry IP Scanner
ASSIGNMENT WEIGHTAGE: 05 MARKS

All of the following questions are based on assuming you are on a Windows 10/11 Internet Enabled PC:

1) Download Angry IP scanner in Windows 10/11.
2) Start your Mobile Hotspot and connect your device in which Angry IP scanner is installed. Also connect a couple of devices /your friend's device with the same hot spot. Now start Angry IP scanner in Live host finding mode. Verify whether the devices discovered by Angry IP scanner tally with the actual devices connected to the hotspot. Use the IP address of the devices for the verification. You may tally this using ipconfig/all command on the respective devices and the IP addresses of the live hosts displayed by Angry IP scanner.
3) Install Apache Web Server in your device and in your friend's device, considering above scenario in 2. Start Apache Web Server in both the devices. Verify whether Angry IP scanner is able to detect the above Apache Web Services hosted on your device and your friend's device. Mention the IP address and port number on which these services were found to be hosted.

-x-x-x-x-x-

CYBER SECURITY LAB ASSIGNMENT 4
INSTALLING, OPERATING AND ANALYSIS USING NMAP
ASSIGNMENT WEIGHTAGE: 05 MARKS

All of the following questions are based on assuming you are on a Windows 10/11 Internet Enabled PC:

1. Connect your laptop with your mobile hotspot and request your 2-3 friends also to get connected to your mobile hotspot. Now, perform a Ping Scan using Nmap and verify whether your and your friends IP addresses are being listed as active IPs in the result. Apart

from yours and your friends IPs, are there any other active IPs being shown? If yes, find out which are they.

2. In continuation of above exercise, now tell any of your connected friends to start XAMPP services or start Apache Web Server (install it if not installed). Now launch a complete TCP scan for the whole subnet and identify which services have been hosted on which devices.
3. Repeat the above exercise 2 for a TCP stealth scan.
4. Repeat the above exercise 2 for a UDP scan.
5. Repeat the above exercise 2 for an OS scan.
6. Perform a ping scan for specified hosts from a file.
7. Perform a generalized scan on scanme.nmap.org

-x-x-x-x-x-

CYBER SECURITY LAB ASSIGNMENT 5
Digital Forensics: Data Recovery Using RECUVA File Recovery Tool
ASSIGNMENT WEIGHTAGE: 05 MARKS

All of the following questions are based on assuming you are on a Windows 10/11 Internet Enabled PC:

1. Visit the following link:

https://www.ccleaner.com/recuva/download/standard

(NOTE: YOU ARE FREE TO USE ANY OTHER SIMILAR TOOL INSTEAD OF RECUVA)

This will download the recuva windows installation file rcsetup154.exe which is of around 25 MB.

Now, click on the above file and installation of Recuva will start.It may take around 5-10 minutes.

After successful installation, you will find its desktop icon on your desktop.

Now, delete any (non-important) image file like <file_name>.jpg from your PC. So,it will be now stored in recycle bin. Now, go to recycle bin and delete the above file from there. System will ask a question like whether you want to permanently delete this file? Select Yes. So the file will be now deleted from recycle bin also. Verify by visiting the original location of the file as well as recycle bin whether the file has been actually deleted.

Now, start the Revuca utility. It will ask you which file type you are looking for. Select "pictures".
It will also ask you any specific file path you would like to provide for searching. (like my documents, downloads, etc.) Select the option "Everywhere in the PC".

Then, a dialog box will appear where there will be an unchecked check box with the option "Deep Scan". Check the check box and go ahead. Now, Recuva will start searching your

file. It may take typically at least 15-20 minutes. After the scan is over, recuva will give you a thumbnail preview of various image files which it has recovered. File names will necessarily be the same as your original file. However, by seeing the thumbnail preview, you will be able to identify your file. Click on it and then you will be able to recover your file. It is possible that at this last stage, the software asks for "payment". Do not go for payment. If you are able to view your file in the thumbnail preview, it means recuva has successfully recovered your file.

Repeat the above exercise for different file types like docx, xlsx, pdf, mp3, located at different file locations like my documents, downloads, my pictures, etc.

KINDLY NOTE THAT YOU NEED TO SELECT ONLY NON IMPORTANT/DUMMY files!

2. Now, delete any of the above recovered files using a file shredding utility like fileshredder (https://www.fileshredder.org/). Verify whether you are able to recover the shredded files using Recuva after deleting using file shredder.

   NOTE: You are free to use any other file shredding tool instead of the above tool

-x-x-x-x-x-

CYBER SECURITY LAB ASSIGNMENT 6
Digital Forensics: Autopsy Sleuthkit
ASSIGNMENT WEIGHTAGE: 05 MARKS

All of the following questions are based on assuming you are on a Windows 10/11 Internet Enabled PC:

1. Install Autopsy Sleuthkit using the following link: https://www.sleuthkit.org/autopsy/download.php
2. Demonstrate how the given tool can be used to detect files with deceptive extensions.
3. Demonstrate how the given tool can be used to perform keyword search through given files where keywords are of the type IP address and URL/Email address.

-x-x-x-x-x-

CYBER SECURITY LAB ASSIGNMENT 7
Firewalls
ASSIGNMENT WEIGHTAGE: 05 MARKS

All of the following questions are based on assuming you are on a Windows 10/11 Internet Enabled PC:

1. Use Windows In-built Firewalls and demonstrate how a given URL can be blocked by configuring appropriate rules.

CYBER SECURITY LAB ASSIGNMENT 8
Password Cracking using John the Ripper
ASSIGNMENT WEIGHTAGE: 05 MARKS

All of the following questions are based on assuming you are on a Windows 10/11 Internet Enabled PC:

1. **Install John the Ripper in Ubuntu (For Kali Linux it is inbuilt) using the following command:**
   sudo apt-get install john-the-ripper OR sudo apt-get install john
2. Demonstrate how to use the single crack mode for password cracking.
3. Demonstrate how to use the word list mode for password cracking.
4. Demonstrate how to use the incremental mode for password cracking.

-x-x-x-x-x-

CYBER SECURITY LAB ASSIGNMENT 9
Online Vulnerability Scanner Tools
ASSIGNMENT WEIGHTAGE: 05 MARKS

All of the following questions are based on assuming you are on a Windows 10/11 Internet Enabled PC:

1. Perform online vulnerability scanning using following online vulnerability scanners:
   https://pentest-tools.com/website-vulnerability-scanning/website-scanner
   https://www.immuniweb.com/websec/

   You may try out different types of URLs like .com. .gov.in, .org, .ac.in, etc. on above links. They will produce a vulnerability report. Create a report of all vulnerabilities listed from different online tools of above. You may keep the data set (the list of URLS to be scanned) the same for all of the above online tools. Mention in the report your findings regarding which vulnerabilities were common and which ones were relatively uncommon.

NOTE: If you have already submitted the above report on the link shared in group, kindly ignore this assignment.

-x-x-x-x-x-