CAP 791: SECURING NETWORK AND IT INFRASTRUCTURE

CA1- PRACTICAL

Due Date: 29/08/2022

SET- A

1. Rahul is trying to scan a network using the ping command, but he is not able to do so. What could be the possible reason for that? Also, suggest the solution for the same and show its' implementation on your system (capture the screenshots and generate a report).

2. How to find out the password using Wireshark? Explain

3. What are the various methodologies used for scanning? Demonstrate any 2 on your system.

SET-B

1. Using the nmap scanning tool, perform the following tasks:

    a) Scan the UDP ports of the live host

    b) Check the operating system being used on the targeted system

    c) Check whether ports 23 and 143 are open on the targeted system

2. Demonstrate how you can check the version and Operating system individually of the targeted system through scanning.

3. What are the various techniques using which your data can be stolen?

SET- C

1. Nisha is trying to scan the network and she only wants to check whether TCP ports are open on the target system or not. How can she get the desired information? Show its' implementation and capture the screenshots.

2. What is the use of the aggressive scan? Demonstrate and share its' screenshots through the report.

3. How can you check whether the email you have received is sent by the person you know or is sent by a fake person? Demonstrate it on your system.

SET-D

1. What is network scanning? What type of information can be retrieved through scanning? Show any 2 ways using which we can gather the information about the targeted system. Use Wireshark for packet capturing.

2. How can you discover the various services running on the target system?

3. What is the significance of Stealth scan (sS) and IDLE/IPID Header scan (sN). How can you perform the same?

Note:

List out complete instructions, and place appropriate screenshots to support your answers.