Module 3: Case Study: Scanning Networks

Problem Statement:

You are a junior cybersecurity analyst working for a consulting firm specializing in network security assessments. Your team has been tasked with conducting a security assessment on a client's network. Your objectives include host discovery, port scanning, OS discovery, and generating a comprehensive report on the network's vulnerabilities. You must follow ethical and legal guidelines throughout the assessment.

Objective:

Conduct a thorough security assessment on a client's network by performing host discovery, comprehensive port scanning, OS discovery, and generating a detailed report on vulnerabilities. Ensure compliance with ethical and legal guidelines, while also demonstrating the use of network scanning tools like 'ping' and Wireshark.

Tasks to be Performed:

1. **Host Discovery Using the 'ping' Command**: Your first task is to perform host discovery on the client's network using the **'ping'** command. Provide a detailed explanation of the data you can extract from the results and how this helps in the assessment.

2. **Comprehensive Port Scan:** Now, you need to conduct a comprehensive and non-intrusive port scan on the specified target IP address. Outline the steps you would take, including the choice of tools and software. Explain the reasons for using non-intrusive methods.

3. **OS Discovery and Ethical/Legal Considerations:** Perform OS discovery on the network you do not own or manage. Discuss the ethical and legal considerations that security professionals should be aware of and adhere to during this process.

4. **Scanning Beyond IDS and Firewall:** Conduct a scan beyond the Intrusion Detection System (IDS) and Firewall. Provide a report of all the

outcomes, including vulnerabilities and potential risks that may have been missed by these security measures.

5. **Network Scan Using Wireshark:** Create a step-by-step tutorial on how to use Wireshark to carry out a basic network scan. Demonstrate how to locate open ports on a target machine as an example.

6. **Generating a Comprehensive Report:** After completing the tasks mentioned above, generate a comprehensive report summarizing your findings, including vulnerabilities, risks, and recommendations for improving the network's security.

Note: Ensure that you have proper authorization to perform network scanning on the chosen target. Always follow ethical and legal guidelines when conducting security assessments. The target could be any authorized domain or any of the domains from the below list:

1. www.certifiedhacker.com
2. www.moviescope.com
3. www.goodshopping.com
4. Testphp.vulnweb.com
5. Machine IP from your Lab Setup