Module 4: Case Study: Enumeration

Problem Statement:

As a cyber security professional working with EcoFusion Nexus, your objective is to perform network enumeration on a designated target network. You'll employ various tools to uncover open ports, services, and vulnerabilities. The target represents a corporate network, and your mission is to gather valuable information that can help improve its security posture.

Objective:

The objective is to develop practical skills in network enumeration by conducting a comprehensive ethical hacking exercise. Students will use a combination of tools, including Nmap, smbclient, enum4linux, theHarvester, and Nessus, to identify open ports, Windows SMB service details, email addresses, and potential security vulnerabilities in a target network or system.

Tasks to be Performed:

1. **Network Discovery:** Identify a target network or system for your assignment. This can be a virtual lab environment, a specific IP address range, or a predefined network.

2. **Scanning with Nmap:**

   - Use Nmap to perform an initial network scan. Identify open ports and running services on the target network/system.

   - Document the results of your Nmap scan and identify any potential targets for further enumeration.

3. **SMB Enumeration with smbclient and enum4linux:**

   - Based on the Nmap results, focus on the SMB service. Use smbclient to connect to SMB shares and enum4linux to gather information about the target's Windows environment.

   - Enumerate shares, users, groups, and other valuable information related to the SMB service.

4. Email Enumeration with theHarvester:

- Utilize theHarvester to search for email addresses and associated information related to the target network or organization.
- Document the email addresses and any other relevant information you discover.

5. Vulnerability Scanning with Nessus:

- Perform a vulnerability scan on the target network/system to identify potential security vulnerabilities.
- Document the vulnerabilities, their severity, and any recommendations provided by Nessus.

Note: Ensure that you have proper authorization to perform network enumeration 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