Information Security
Assignment 1

Note: Submission will result 0 and non submission will result -1 marks

Question 1:

You are a security intern at "VulnScan Analytics." A client has provided a system for a non-intrusive security assessment. Your task is strictly to perform reconnaissance and vulnerability scanning to identify potential security weaknesses. You are **explicitly prohibited** from attempting to **exploit** any found vulnerabilities (e.g., no password guessing, no exploitation, no using msfconsole). Your role is to find and report, not to penetrate.

Lab Setup & Tools

Virtualization Software: Oracle VirtualBox / VMware.
Attacking Machine: any Linux OS preferred, search for required tools.
Target Machine: Download one of the following from VulnHub:
Meow (Very Easy)
Kioptrix: Level 1 (Easy)
Suggested Tools: You are encouraged to use any tool available on Kali Linux or through apt that is designed for reconnaissance and scanning. This includes, but is **not limited** to:

1. netdiscover , nmap , arp-scan (Network Discovery)
2. nikto , gobuster , dirb , whatweb (Web Assessment)
3. enum4linux , smbclient (SMB Assessment)
4. nuclei (Modern Vulnerability Scanner)

Your own custom Bash scripts.

Tasks

1. URL of the vulnerable machine you used
   Test your lab network configuration so vulnerable and attacker machines are accessible to each other. The best way is to ping each other.
2. **Network Discovery**
   a. Use at least one tool (e.g., netdiscover , arp-scan) to identify the IP address of the target VM.

b. Provide a screenshot of the command and its output.

3. **Service Enumeration & Analysis**

   Perform a comprehensive scan of the target using nmap .

Your scan must use flags for service version detection (-sV), default scripts (-sC), and OS detection (-O). Scanning all ports (-p-) is recommended for a better grade.
Provide a screenshot of your full nmap command and its output.
Analysis Table: Create a table summarizing your findings. | Port | Protocol | Service | Version | Key Finding (from NSE scripts) | | :--- | :--- | :--- | :--- | :--- | | 22 | tcp | ssh | OpenSSH 4.3p2 | Protocol 2.0 only | | 80 | tcp | http | Apache httpd 2.2.8 | |

4. **Focused Vulnerability Scanning**

   Based on your findings from Task 3, perform two additional, focused scans using tools other than or in addition to nmap and nikto .

Examples:
If a web server (port 80/443) is found, use gobuster or dirb to find hidden directories. AND use whatweb to identify web technologies.
If SMB (port 445) is found, use smbclient to list shares or enum4linux to enumerate information.
Use a modern scanner like nuclei to check for common vulnerabilities.
For each scan:
Provide a screenshot of the command and its output.
Write one sentence explaining what the scan was designed to find.

Question 2:

1. Read about ETW (event tracers for windows). What you understand about its architecture(max 4 lines).

2. Read about Getprocaddress() and Getmodulehandle() of Microsoft Windows API