# Perform a Basic Vulnerability Scan on PC

## 1. Tool Used: Nmap

Due to issues with Kali Linux and OpenVAS, I performed the vulnerability assessment using **Nmap**, a powerful open-source network scanning tool.

## 2. Scan Target

- **Target IP:** 10.1.41.73
- **Environment:** Local/Private network
- **Objective:** Identify open ports, services, and vulnerabilities on the system.

## 3. Scan Commands Used

**1. nmap -sV 10.1.41.73**

To Detect open ports and service versions

**2. nmap --script smb-vuln-ms17-010 -p445 10.1.41.73**

To Check for SMB vulnerability (EternalBlue)

**3. nmap --script mysql-vuln-cve2012-2122 -p3306 10.1.41.73**

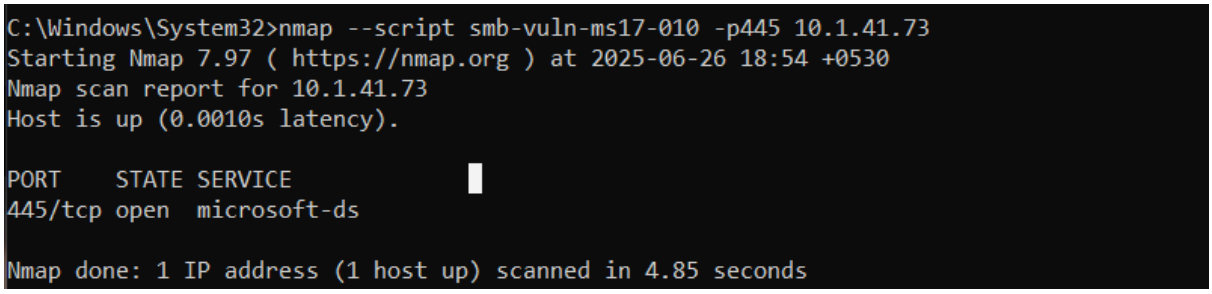
To Detect MySQL authentication bypass

**4. nmap --script http-title,http-enum -p8000,8089 10.1.41.73**

Enumerate exposed web services

## 4. Detected Vulnerabilities

### a) SMB Vulnerability Check (Port 445)




- **Script Run:** smb-vuln-ms17-010
- **Result:** No output confirming the vulnerability.

- **Severity:** Medium (needs deeper testing)
- **Fix:** Ensure the system is patched against MS17-010 (EternalBlue).

### b) MySQL Unauthorized Access (Port 3306)

```
C:\Windows\System32>nmap --script mysql-vuln-cve2012-2122 -p3306 10.1.41.73
Starting Nmap 7.97 ( https://nmap.org ) at 2025-06-26 18:55 +0530
Nmap scan report for 10.1.41.73
Host is up (0.0010s latency).

PORT     STATE SERVICE
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 3.85 seconds

C:\Windows\System32>mysql -h 10.1.41.73 -u root
'mysql' is not recognized as an internal or external command,
operable program or batch file.
```

- **Script Run:** mysql-vuln-cve2012-2122
- **Result:** Scan did not confirm vulnerability.
- **Attempted Manual Access:** mysql -h 10.1.41.73 -u root — command failed (no client installed).
- **Severity:** Low (access denied)
- **Fix:** Keep strong root passwords, disable remote root login, use skip-networking if remote access is not required.

### c) HTTP & Splunk Exposure (Port 8000, 8089)

```
C:\Windows\System32>nmap --script http-title,http-enum -p8000,8089 10.1.41.73
Starting Nmap 7.97 ( https://nmap.org ) at 2025-06-26 18:57 +0530
Nmap scan report for 10.1.41.73
Host is up (0.0019s latency).

PORT     STATE SERVICE
8000/tcp open  http-alt
| http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_Requested resource was http://10.1.41.73:8000/en-US/account/login?return_to=%2Fen-US%2F
| http-enum:
|_  /robots.txt: Robots file
8089/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 5.78 seconds
```

- **Finding:** Login portal detected at /en-US/account/login
- **Exposure:** Web panel available on a public IP may lead to:
    - Brute-force login attacks
    - Exposure of Splunk logs/configs
- **Fix:**
    - Enable HTTPS-only access

- Restrict IP ranges via firewall
- Set strong passwords
- Enable 2FA if supported

```
C:\Windows\System32>nmap -sV 10.1.41.73
Starting Nmap 7.97 ( https://nmap.org ) at 2025-06-26 18:52 +0530
Nmap scan report for 10.1.41.73
Host is up (0.00014s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE         VERSION
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
3306/tcp  open  mysql           MySQL (unauthorized)
8000/tcp  open  http            Splunkd httpd
8089/tcp  open  ssl/http        Splunkd httpd
55555/tcp open  unknown
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.73 seconds
```

**Reason for Using Nmap Instead of OpenVAS**

OpenVAS was originally intended for this assignment. However, due to issues with the Kali Linux VM and the expiration of the Essentials trial, i opted to use **Nmap** with relevant vulnerability detection scripts as an effective alternative.