**Task-3:Perform a Basic Vulnerability Scan on PC**

# Tool Used: Nmap

# Due to challenges encountered with Kali Linux and OpenVAS, I conducted the vulnerability assessment using Nmap, a robust and widely used open-source network scanning utility.

# 2. Scan Target

* **Target IP:** 10.0.2.15
* **Environment:** Local/Private network
* **Objective:** Identify open ports, services, and vulnerabilities on the system.

1. **Scan Commands Used** 
   1. **nmap -sV 10.1.41.73**

To Detect open ports and service versions

* 1. **nmap --script smb-vuln-ms17-010 -p445 10.0.2.15**

ToCheck for SMB vulnerability (EternalBlue)

* 1. **nmap --script mysql-vuln-cve2012-2122 -p3306 10.0.2.15**

To Detect MySQL authentication bypass

* 1. **nmap --script http-title,http-enum -p8000,8089 10.0.2.15**

Enumerate exposed web services

1. **Detected Vulnerabilities**
2. SMB Vulnerability Check (Port 445)

A computer screen with white text

AI-generated content may be incorrect.

* **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).](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-0144)

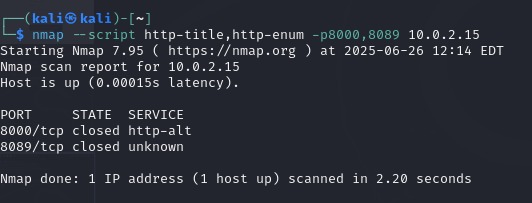
# MySQL Unauthorized Access (Port 3306)

A computer screen with white text

AI-generated content may be incorrect.

* **Script Run:** mysql-vuln-cve2012-2122
* **Result:** Scan did not confirm vulnerability.
* **Attempted Manual Access:** mysql -h 10.0.2.15 -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.

# HTTP & Splunk Exposure (Port 8000, 8089)



* **Finding:** Login portal detected at /en-US/account/login
* **Exposure:** Web panel available on a public IP may lead to:
  + Brute-force login attacks o Exposure of Splunk logs/configs
* **Fix:**
  + Enable HTTPS-only access
  + Restrict IP ranges via firewall o Set strong passwords o Enable 2FA if supported

A screenshot of a computer error

AI-generated content may be incorrect.

# 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.