**Task 3: Perform a Basic Vulnerability Scan on Your PC.**

* **Objective**: Use free tools to identify common vulnerabilities on your computer.
* **Tools**: OpenVAS Community Edition (free vulnerability scanner) or Nessus Essentials.
* **Deliverables**: Vulnerability scan report with identified issues.

**My Objective:**

Due to hardware limitations preventing VMware usage, this report documents a vulnerability assessment performed directly on the host system using Nmap. The goal is to identify open ports, running services, and potential vulnerabilities, and to recommend remediation steps.

**Environment Details:**

|  |  |
| --- | --- |
| System: | Windows 10 (version from Nmap OS detection) |
| IP Address: | 127.0.0.1 (localhost) |
| Tool Used: | Nmap 7.98 |
| Scan Type: | Service Detection, Vulnerability Scripts, SMB, HTTP, RDP Enumeration |

**Explanation of Nmap Commands Used**

**1. Service and OS Detection**

**Command**

nmap -sV -O --top-ports 2000 --version-intensity 5 127.0.0.1 -oN svc\_version.txt

* **Purpose:** Identifies open ports, running services, and operating system details on the local machine.
* **Flags:**
  + -sV: Detects service versions.
  + -O: Attempts to identify the operating system.
  + --top-ports 2000: Scans the 2000 most commonly used ports.
  + --version-intensity 5: Uses aggressive version detection for more accurate results.
  + -oN svc\_version.txt: Saves output to a file named svc\_version.txt.

**2. Vulnerability Scan**

**Command**

nmap --script vuln 127.0.0.1 -oN vuln\_general.txt

* **Purpose:** Runs a collection of Nmap vulnerability detection scripts against the local host.
* **Flags:**
  + --script vuln: Executes multiple scripts that check for known vulnerabilities, misconfigurations, and CVEs.
  + -oN vuln\_general.txt: Saves output to vuln\_general.txt.

**3. SMB Enumeration**

**Command**

nmap -p 135,139,445 --script smb2-security-mode,smb-enum-shares,smb-enum-users 127.0.0.1 -oN smb\_enum.txt

* **Purpose:** Assesses the security of Windows file sharing (SMB) services.
* **Flags:**
  + -p 135,139,445: Targets ports used by Microsoft RPC and SMB.
  + --script smb2-security-mode: Checks SMBv2 security settings.
  + --script smb-enum-shares: Lists shared folders.
  + --script smb-enum-users: Enumerates user accounts.
  + -oN smb\_enum.txt: Saves output to smb\_enum.txt.

**4. Web Service Enumeration**

**Command**

nmap -p 80,8080,8085 --script http-enum,http-security-headers,ssl-enum-ciphers 127.0.0.1 -oN web\_enum.txt

* **Purpose:** Evaluates HTTP services for exposed paths, missing security headers, and weak SSL/TLS configurations.
* **Flags:**
  + -p 80,8080,8085: Targets common HTTP ports.
  + --script http-enum: Lists accessible web directories and services.
  + --script http-security-headers: Checks for missing headers like CSP and X-Frame-Options.
  + --script ssl-enum-ciphers: Identifies supported SSL/TLS ciphers and their strength.
  + -oN web\_enum.txt: Saves output to web\_enum.txt.

**5. RDP Encryption Check**

**Command**

nmap -p 3389 --script rdp-enum-encryption 127.0.0.1 -oN rdp\_enum.txt

* **Purpose:** Assesses the encryption level of Remote Desktop Protocol (RDP) to determine if it meets security standards.
* **Flags:**
  + -p 3389: Scans the RDP port.
  + --script rdp-enum-encryption: Evaluates encryption and authentication settings.
  + -oN rdp\_enum.txt: Saves output to rdp\_enum.txt.

**Research simple fixes or mitigations for found vulnerabilities:**

|  |  |  |
| --- | --- | --- |
| Vulnerability / Service | Common Issue | Simple Fix / Mitigation |
| SMB (Port 445) | SMBv1 enabled (MS17-010 / EternalBlue risk) | Disable SMBv1 via Control Panel → “Turn Windows features on or off”; restart. Restrict port 445 in firewall. |
| HTTP Services (Ports 80, 8080, 8085) | Missing security headers (X-Frame-Options, CSP) and outdated software | Add security headers in web server configs: X-Frame-Options: DENY, Content-Security-Policy: default-src 'self'. Keep software updated. Use HTTPS with strong TLS. |
| RDP (Port 3389) | Weak encryption, NLA not enforced | Enable Network Level Authentication (NLA) in System Properties → Remote Settings. Restrict access via firewall. Disable if unused. Use strong passwords. |
| Oracle TNS Listener (Port 1521) | Unauthorized access to listener | Disable Oracle DB if not needed. Restrict access in listener.ora and firewall. Apply patches and enable logging. |
| VMware Services (Ports 902, 912) | VMware Authentication Daemon exposed | Disable services if unused. Restrict to localhost or host-only network. Block ports 902/912 externally. |
| General System Hardening | Various risks from unpatched OS and weak configs | Run Windows Update regularly. Use local firewall to block unused ports. Remove unused services. Use strong passwords and limited admin accounts. |

**Document the most critical vulnerabilities.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Port | Service | Vulnerability / Issue | Severity | Impact / Risk Description | Suggested Mitigation |
| 445 | SMB | SMBv1 enabled (MS17‑010 / EternalBlue) | **High** | Allows remote code execution; exploited in major ransomware attacks | Disable SMBv1; restrict port 445 via firewall |
| 1521 | Oracle TNS | Unauthorized listener exposed | **High** | May allow unauthenticated access to Oracle DB services | Disable Oracle if unused; restrict access via listener.ora |
| 902/912 | VMware Auth | VMware Authentication Daemon exposed | **High** | Could allow unauthorized access to VM services | Restrict to localhost; disable if unused |
| 3389 | RDP | Weak encryption / NLA not enforced | **High** | Susceptible to brute-force and MITM attacks | Enable Network Level Authentication; restrict access |
| 80/8080/8085 | HTTP/Web Services | Missing security headers (CSP, X-Frame-Options) | **Medium** | Increases risk of clickjacking and content injection attacks | Add security headers in web server config |