**TASK-3**

**Nessus Vulnerability Report**

**Summary**

| **Scan Tool** | **Nessus Essentials** |
| --- | --- |
| Target | Local PC (192.168.1.3) |
| Scan Date | 07/08/2025 |
| Total Findings | 7 (Informational Level) |

**Vulnerabilities Identified**

| **Plugin ID** | **Title** | **Severity** | **Description** |
| --- | --- | --- | --- |
| 45590 | Common Platform Enumeration (CPE) | Info | Detected CPE values useful for system fingerprinting. |
| 10736 | DCE Services Enumeration | Info | Lists DCE RPC services, can help attackers identify vulnerable services. |
| 54615 | Device Type | Info | Reveals the type of device scanned. |
| 10107 | HTTP Server Type and Version | Info | Leaks server software and version (can be used in targeted exploits). |
| 12053 | Host Fully Qualified Domain Name (FQDN) Resolution | Info | Identifies FQDN from IP, useful for mapping internal networks. |
| 24260 | HyperText Transfer Protocol (HTTP) Information | Info | Leaks HTTP headers and banners (discloses configuration info). |
| 42410 | Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure | Info / Low | May reveal internal network names via NTLM auth requests. Could helpattackers with lateral movement or domain targeting. |

**🔧 Mitigation Strategies**

**1. Limit Information Disclosure**

* Disable unnecessary HTTP headers (e.g., Server, X-Powered-By).
* Use a reverse proxy or web application firewall (WAF) to mask internal details.
* Configure servers to avoid banner/version exposure.

**2. Restrict Network Service Enumeration**

* Disable unused DCE/RPC and SMB services.
* Apply firewall rules to block unnecessary ports (e.g., RPC, SMB, HTTP) from untrusted networks.

**3. NTLMSSP Disclosure (Plugin ID: 42410)**

* **Mitigation:**
  + Disable NTLM authentication if not needed.
  + Use Kerberos where possible.
  + Ensure SMB signing is enforced.
  + Apply latest Windows patches to secure authentication mechanisms.
* **Reference:**
  + [Microsoft: Restrict NTLM](https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-ntlm-authentication-in-this-domain)

**4. DNS and FQDN Exposure**

* Avoid unnecessary internal DNS name exposure.
* Use split-horizon DNS to separate internal/external name resolution.
* Configure PTR records properly if public DNS is not required.

Screenshots:





