Vulnerability Assessment Report:

**General Notes:**

* This assessment is based on Nessus Essentials scans performed on August 29th and 31st, 2025.
* Only severity (CVSS) levels 5 and higher are included in our assessment
* Severity levels range from low (1) to high (10)
* Overall Assessment: The attack surface reduction tasks were highly effective. Most systems exhibit a minimal and expected footprint. The few medium-severity findings are related to service configuration rather than unpatched software.

**SYSTEM 1 (Windows Server 2022, 192.168.2.102) Vulnerable Software & Services:**

**Service** (SMB:445)

* **Finding**: SMB Signing not required (Plugin ID 57608)
* **Description**: The remote SMB server does not require message signing. This could allow an unauthenticated attacker to conduct a man-in-the-middle attack against the SMB service, potentially intercepting or modifying data.
* **Remediation Action**: Enforce SMB signing by enabling the Group Policy setting Microsoft network server: Digitally sign communications (always). Navigate to: Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options.
* **Severity**: Medium (CVSS v3.0: 5.3)

**SYSTEM 2 (Fedora 41 Workstation, 192.168.2.105) Vulnerable Software & Services:**

**Service** (DNS:53)

* **Finding**: DNS Server Cache Snooping Remote Information Disclosure (Plugin ID 12217)
* **Description**: The remote DNS server responds to queries for third-party domains even when the recursion bit is not set. This allows an attacker to determine which domains have been recently resolved by this server, revealing information about internal network browsing habits or trusted external services.
* **Remediation Action**: Configure the DNS server (systemd-resolved or BIND) to disable or restrict recursion for untrusted clients. Ensure it only provides recursive services to authorized internal networks.
* **Severity**: Medium (CVSS v3.0: 5.3)

**SYSTEM 3 (Ubuntu 24.04.2 LTS Server, 192.168.2.103) Vulnerable Software & Services:**

**Assessment**: No vulnerabilities with a CVSS score of 5.0 or higher were identified on this system. The configuration (only SSH port 22 open, key-based authentication enforced, unattended-upgrades enabled) presents a very minimal and secure attack surface. The Nessus scan primarily revealed informational findings about the SSH service configuration.

**SYSTEM 4 (Windows 10 Client, 192.168.2.108) Vulnerable Software & Services:**

**Assessment**: No vulnerabilities with a CVSS score of 5.0 or higher were identified on this system. The Nessus scan found no open ports and no network services responding, which aligns perfectly with the configured client firewall policy to block all unsolicited inbound connections. This host presents no network-based attack surface.