**Network Scanning and Nessus Vulnerability Assessment Report**

**Objective**

This document provides a detailed account of the network scanning and Nessus Vulnerability Assessment process performed on a target system within a local network. The goal was to identify active hosts, open ports, running services, and gather additional system information for further analysis.

**Step 1: Host Discovery using Netdiscover**

**Command Executed:**

sudo netdiscover -r [IP\_RANGE] -P > MRVA.txt

**Description:**

* netdiscover was used to scan the local network for active hosts.
* The -r [IP\_RANGE] flag specifies the IP range to scan.
* The -P flag ensures passive scanning.
* The results were saved into MRVA.txt for further analysis.

**Findings:**

* One active host was detected:
  + **IP Address:** 192.168.1.47
  + **MAC Address:** 08:00:27:AB:4D:CC
  + **Vendor:** PCS Systemtechnik GmbH (indicating a virtual machine)

**Step 2: Network and Service Enumeration using Nmap**

**Command Executed:**

nmap -sT -sV -sC -oN - 192.168.1.47 -p- -Pn -vv -A >> MRVA.txt

**Description:**

* -sT → Conducts a full TCP connect scan.
* -sV → Detects service versions running on open ports.
* -sC → Runs default Nmap scripts for additional enumeration.
* -oN - → Outputs scan results in normal format.
* -p- → Scans all 65,535 TCP ports.
* -Pn → Skips host discovery and treats the target as online.
* -vv → Enables verbose output.
* -A → Enables OS detection, version detection, script scanning, and traceroute.

**Findings:**

* **Host is Up:** Confirmed by ARP response.
* **Operating System Detected:**
  + OS: Linux Kernel 2.6
* **Open Ports:**
  + **22/tcp (SSH):** Closed (Connection refused)
  + **80/tcp (HTTP):** Open (Apache HTTP server detected)
  + **443/tcp (HTTPS):** Open (Apache HTTP server with SSL detected)
* **SSL Certificate Details:**
  + Issued: 2015-09-16
  + Expiry: 2025-09-13
  + Weak security (1024-bit RSA key, SHA-1 signature)
* **Traceroute Result:**
  + Single hop detected (local network system)

**Step 3: Nessus Vulnerability Assessment**

**Command Executed:**

systemctl start nessusd

**visit** [**http://localhost:8834/**](http://localhost:8834/) **in the browser**

**Findings:**

**High Severity Vulnerabilities:**

1. **SSL Certificate Signed Using Weak Hashing Algorithm (7.5 CVSS Score)**
   * A weak cryptographic hash algorithm (SHA-1) is used.
   * Risk: Allows attackers to create fake certificates.
   * Solution: Replace the SSL certificate with one signed using SHA-256 or higher.

**Medium Severity Vulnerabilities:**

1. **SSL Certificate Cannot Be Trusted (6.5 CVSS Score)**
   * The SSL certificate is self-signed or untrusted.
   * Risk: Users cannot verify the identity of the server, allowing MITM attacks.
   * Solution: Obtain a certificate from a trusted Certificate Authority.
2. **TLS Version 1.0 and 1.1 Detection (6.5 CVSS Score)**
   * These outdated protocols lack modern security measures.
   * Risk: Susceptible to cryptographic attacks.
   * Solution: Disable TLS 1.0/1.1 and enforce TLS 1.2 or higher.
3. **OpenSSL AES-NI Padding Oracle MitM Information Disclosure (5.9 CVSS Score)**
   * OpenSSL vulnerability allowing potential data decryption in MITM attacks.
   * Risk: Attackers can decrypt HTTPS traffic.
   * Solution: Upgrade OpenSSL to version 1.0.1t / 1.0.2h or later.

**Conclusion and Next Steps**

* The scan confirmed the presence of a virtual machine running Apache on ports 80 and 443.
* The SSL certificate is outdated and insecure.
* The host uses **Linux Kernel 2.6**, an old version with potential vulnerabilities.
* Nessus detected several security risks, particularly related to **SSL/TLS security**.
* Immediate remediation steps involve updating OpenSSL, replacing the SSL certificate, and disabling weak TLS versions.

**Recommendations:**

1. Verify the purpose of the virtual machine and update its OS if possible.
2. Upgrade OpenSSL to the latest version.
3. Replace the SSL certificate with one signed using a strong algorithm (SHA-256 or higher).
4. Disable TLS 1.0/1.1 and enforce TLS 1.2 or higher.
5. Ensure that Apache and any web applications are up to date and secured.