**ASSIGNMENT NO : 1**

**Use the NESSUS/ISO Kali Linux tool to scan the network for vulnerabilities.**

Submission Date : 08-09-2025

Note : installation of NESSUS/ISO KALI LINUX TOOL & implementation using Nmap for vulnerabilities.

Output : screenshots of vulnerabilities implemented

# What is Nessus?

**Nessus** is a **vulnerability assessment tool** developed by **Tenable, Inc.** It’s one of the most widely used tools by security professionals, system admins, and penetration testers for **finding security weaknesses in networks, systems, and applications.**

## Key Features of Nessus

1. **Vulnerability Scanning**
   * Detects OS, applications, and service vulnerabilities.
   * Maps them to **CVE IDs** (Common Vulnerabilities and Exposures).
2. **Cryptographic Weakness Detection**
   * Identifies weak SSL/TLS versions (SSLv2, SSLv3, TLS 1.0).
   * Detects weak ciphers (RC4, DES, MD5, SHA-1).
   * Flags expired, self-signed, or misconfigured certificates.
3. **Configuration Auditing**
   * Checks whether systems are securely configured (e.g., firewalls, databases).
4. **Credentialed & Non-Credentialed Scans**
   * **Non-credentialed scan**: Like an outsider (tests open ports, banners).
   * **Credentialed scan**: Logs in with admin/SSH credentials to find deeper issues.
5. **Compliance Audits**
   * Helps check against security standards like **PCI-DSS, HIPAA, CIS Benchmarks**.
6. **Extensive Plugin Library**
   * Tens of thousands of plugins for detecting vulnerabilities.
   * Updated regularly by Tenable.

## How Nessus Works (Simplified)

1. You install Nessus on Kali Linux (or any supported OS).
2. Nessus runs a **scanner** against your target IPs/hosts.
3. It probes open ports, services, SSL/TLS handshakes, configs, etc.
4. It compares results with its **vulnerability database**.
5. Nessus generates a report showing:
   * Vulnerabilities found (with CVE ID)
   * Severity (Critical, High, Medium, Low, Info)
   * Recommended fixes

**Nessus is like a doctor for your IT systems — it diagnoses security weaknesses and tells you how to fix them before hackers exploit them.**

**1. Installing Nessus on Kali Linux (ISO or VM)**

Nessus is not pre-installed on Kali, but installation is straightforward:

**Step 1: Update Kali Linux**

sudo apt update && sudo apt upgrade -y

**Step 2: Download Nessus**

* Go to [Tenable Nessus Downloads](https://www.tenable.com/downloads/nessus)
* Choose **Debian/Kali Linux (amd64 .deb package)**.
* Example filename: Nessus-10.x.x-debian6\_amd64.deb

**Step 3: Install the package**

sudo dpkg -i Nessus-10.x.x-debian6\_amd64.deb

If dependencies are missing, run:

sudo apt --fix-broken install

**Step 4: Start Nessus service**

sudo systemctl start nessusd

sudo systemctl enable nessusd

**Step 5: Access Web Interface**

Open browser → https://localhost:8834

* Create an admin account.
* Enter **Activation Code** (Nessus Essentials is free, limited to 16 IPs).
* Nessus will download plugin feeds (takes ~15–20 mins).

**2. Using Nessus for Vulnerability Scanning**

1. **Login** at https://127.0.0.1:8834
2. **Create a new scan** → choose template:
   * **Basic Network Scan** → for IPs, servers
   * **Advanced Scan** → customized ports & services
   * **Credentialed Scan** → deeper analysis with SSH/Windows credentials
3. **Enter target IP / subnet**  
   Example: 192.168.1.0/24
4. **Launch Scan** → Nessus probes services, OS, and checks for vulnerabilities.
5. **View Reports**: Results show:
   * CVEs (Common Vulnerabilities & Exposures)
   * Risk Levels (Critical, High, Medium, Low, Info)
   * Suggested remediation steps

**3. Features of Kali Linux (relevant to vulnerability assessment)**

* **Preloaded Security Tools** → Metasploit, Nmap, Hydra, Wireshark, BurpSuite
* **Penetration Testing Categories**:
  + **Information Gathering** → nmap, whois, dnsenum
  + **Vulnerability Analysis** → Nessus, OpenVAS, Nikto
  + **Exploitation Tools** → Metasploit, Armitage
  + **Forensics & Reverse Engineering**
* **Live Boot / ISO Support** → can run without installation
* **Cryptographic Tools** → gpg, openssl, hashcat, john for password/crypto testing

**4. Cryptographic Vulnerabilities (and how they are tested in Kali/Nessus)**

Nessus and Kali tools can detect **weak or misconfigured cryptography** such as:

**Common Crypto Vulnerabilities**

1. **Weak SSL/TLS Versions** (SSLv2, SSLv3, TLS 1.0)
2. **Weak Ciphers** (DES, 3DES, RC4, MD5, SHA-1)
3. **Expired/Invalid Certificates**
4. **Self-signed Certificates** → not trusted
5. **Improper Key Lengths** (RSA < 2048 bits, ECC < 256 bits)
6. **Unencrypted Services** (FTP, Telnet, HTTP)

**Tools to Implement/Check**

* **Nessus** → automatically checks SSL/TLS misconfigs.
* **Nmap with NSE Scripts** →
* nmap --script ssl-enum-ciphers -p 443 target.com
* **OpenSSL** → test handshake:
* openssl s\_client -connect target.com:443
* **Test Password Hash Strength** → john the ripper, hashcat

**5. Example Workflow**

1. Boot Kali Linux ISO in VM or bare-metal.
2. Install and start Nessus.
3. Run a **network vulnerability scan** (e.g., on 192.168.1.0/24).
4. Check reports for **outdated crypto protocols** like TLS 1.0.
5. Validate findings with **Nmap SSL scripts**.
6. Attempt exploitation (e.g., downgrade attacks, weak cert brute-force) using Kali tools.