🔎 Vulnerability Assessment Using Nessus Essentials – Practical Guide

Primary Tool: Nessus Essentials
Alternative Tool: OpenVAS

✅ Step 1: Define Scope & Target Systems

Before scanning, clearly define:

🎯 Target Examples:

- Localhost (127.0.0.1)
- Internal IP (192.168.1.10)
- Entire subnet (192.168.1.0/24)

⚠️ Important:

- Always get **written permission**
- Scan only authorized systems

📌 Example Scope (for practical record):

"The vulnerability assessment was performed on the internal lab machine with IP 192.168.1.10."

✅ Step 2: Install & Configure Nessus Essentials

🔹 Installation (Ubuntu/Kali)

1. Download from Tenable website.
2. Install:

```
sudo dpkg -i Nessus-*.deb
```

3. Start service:

```
sudo systemctl start nessusd
```

4. Open browser:

```
https://localhost:8834
```

5. Register for free activation code (Nessus Essentials allows 16 IPs).

✅ Step 3: Create & Configure a Scan

1️⃣ Click: New Scan

Choose:
✓ Basic Network Scan

2️⃣ **Configure:**

- Name: Lab Scan
- Target: 192.168.1.10
- Schedule: On demand

3️⃣ **Scan Settings:**

- Port scan: Default
- Credentials (optional but recommended)
- Severity level: All

Click **Save**

✅ Step 4: Run Vulnerability Scan

Click ▶ **Launch**

During scanning:

- Monitor progress
- Check number of hosts scanned
- Observe plugin execution

Scan may take 10–30 minutes depending on target.

✅ Step 5: Review Identified Vulnerabilities

After completion:

Nessus categorizes findings by severity:

Severity	Meaning
🔴 Critical	Immediate risk
🟠 High	Serious vulnerability
🟡 Medium	Moderate risk
🔵 Low	Minor risk
ℹ Info	Informational

Click each vulnerability to view:

- Description
- Affected service

- Risk factor
- Solution

✅ Step 6: Map Findings to CVE & CVSS

Each vulnerability includes:

🔹 CVE (Common Vulnerabilities and Exposures)

Example:

CVE-2023-12345

🔹 CVSS Score (0–10 scale)

Score Range	Risk Level
9.0–10	Critical
7.0–8.9	High
4.0–6.9	Medium
0.1–3.9	Low

📌 Example:

- CVSS: 9.8
- Severity: Critical
- Impact: Remote Code Execution

✅ Step 7: Classify & Prioritize Vulnerabilities

🔥 Prioritization Strategy:

1. Critical vulnerabilities
2. Internet-facing services
3. Exploitable remotely
4. Sensitive system exposure

Example classification:

Vulnerability	CVSS	Risk	Priority
Open SSH outdated	9.8	Critical	Immediate
TLS 1.0 enabled	6.5	Medium	Moderate

Vulnerability	CVSS	Risk	Priority
Missing security headers	3.1	Low	Low

✅ Step 8: Recommend Remediation

For each critical finding:

Example 1: Outdated Software

✓ Update packages:

```
sudo apt update && sudo apt upgrade
```

Example 2: Open Ports

✓ Close unnecessary ports using UFW:

```
sudo ufw deny 23
```

Example 3: Weak SSL/TLS

✓ Disable TLS 1.0 in server config
✓ Enable TLS 1.2/1.3