X Project 4: Vulnerability Assessment & Reporting



© Goal

Perform a vulnerability scan against a test machine, analyze results, validate at least one finding, and produce a professional risk assessment report.

You'll show you can:

- Set up a vulnerability scanner (Nessus Essentials or OpenVAS)
- Run scans and interpret results
- Validate vulnerabilities
- Write a structured risk-based remediation report

Setup

- Vulnerability Scanner VM →
 - o Nessus Essentials (Free, up to 16 hosts) OR OpenVAS (open-source)
- Target $VM \rightarrow$
 - Ubuntu Server OR Windows 10 VM

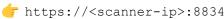


Step 1: Install Nessus Essentials

On your scanner VM (Ubuntu):

```
curl --request GET \
  --url
'https://www.tenable.com/downloads/api/v1/public/pages/nessus/downloads/18545
/download?i agree to tenable license agreement=true' \
  --output Nessus.deb
sudo dpkg -i Nessus.deb
sudo systemctl start nessusd
```

Then access Nessus at:



- Register for Nessus Essentials (free license key).
- Activate scanner.

星 Step 2: Run Vulnerability Scan

- 1. Add a New Scan \rightarrow Basic Network Scan.
- 2. Enter your target VM's IP.
- 3. Start scan and wait for results.
- 4. Take screenshots of:
 - Scan progress
 - Scan results summary

Step 3: Analyze & Validate Findings

- Look at Critical/High vulnerabilities first.
- Example findings:
 - o OpenSSH outdated → CVE listed
 - Weak SSL/TLS cipher suites
 - Outdated Apache version
- Validate at least one finding manually:
 - If Nessus says "Weak SSH password," try brute-forcing with Hydra (from Project 3).
 - If it says "Apache outdated," run apache2 -v on target to confirm.
- im Screenshot validation proof.

Step 4: Create a Vulnerability Report

Format it professionally:

Vulnerability Assessment Report

Executive Summary

- Scope: One Ubuntu target scanned.
- Objective: Identify vulnerabilities, assess risks, recommend fixes.
- Result: 10 findings (2 critical, 3 high, 5 medium).

Findings (Sample)

1. Vulnerability: OpenSSH 7.2 outdated (CVE-2016-6515)

o Evidence: Detected via Nessus scan

o Impact: Allows potential remote code execution

o CVSS Score: 9.8 (Critical)

o **Remediation:** Upgrade to OpenSSH 8.x

2. Vulnerability: Apache 2.4.29 outdated (CVE-2017-15710)

o **Evidence:** Version found via service fingerprinting

o **Impact:** May allow DoS attack

o CVSS Score: 7.5 (High)

o Remediation: Patch to latest Apache release

Conclusion

- System is vulnerable to multiple high-risk CVEs.
- Immediate patching + hardening recommended.

Deliverables for Portfolio

- Vulnerability Assessment Report (PDF)
- Screenshots (Nessus dashboard, vulnerability details, validation proof)
- GitHub Repo Folder:
- project4-vulnerability-scan/
- \to vuln-assessment-report.pdf
- screenshots/
 - scan-methodology.md