🔐 Vulnerability Assessment & Risk Prioritization Report

By : NROUPSINH GOHIL

1️⃣ Objective

The objective of this task was to perform a vulnerability assessment on a target system using a vulnerability scanner and prioritize identified risks based on severity, impact, and exploitability.

2️⃣ What is Vulnerability Assessment?

A Vulnerability Assessment (VA) is the process of identifying, analyzing, and reporting security weaknesses in systems, networks, and applications.

It helps organizations:

- Detect security gaps
- Understand risk level
- Prioritize fixes
- Reduce attack surface

3️⃣ Tool Used

Primary Tool: **Nessus Essentials**
Alternative: **OpenVAS**

In this task, Nessus Essentials was configured to scan the target system.

4️⃣ Scope Definition

Target System:

- Local machine (Windows/Linux VM)
- Local IP address: 192.168.X.X

Scan Type:

- Basic Network Scan
- Credentialed scan (if applicable)

5️⃣ Scan Configuration

- Enabled vulnerability detection plugins
- Enabled service detection
- Enabled OS detection
- Enabled CVE mapping
- Enabled CVSS scoring

6️⃣ Scan Execution

The scan was executed successfully.
The scanner analyzed open ports, running services, outdated software, and misconfigurations.

7️⃣ Identified Vulnerabilities (Example Findings)

Vulnerability	CVE ID	CVSS Score	Severity	Risk Level
SMBv1 Enabled	CVE-2017-0144	9.8	Critical	High
Outdated OpenSSL	CVE-2021-3449	7.5	High	High
Weak SSL Cipher	N/A	5.3	Medium	Medium
Missing Security Updates	Multiple	8.1	High	High

8️⃣ Understanding CVE

CVE (Common Vulnerabilities and Exposures) is a unique identifier assigned to publicly known vulnerabilities.

Example:
CVE-2017-0144 → EternalBlue exploit (used in WannaCry ransomware)

9️⃣ Understanding CVSS

CVSS (Common Vulnerability Scoring System) measures severity from 0 to 10.

Score Classification:

- 0.0 – 3.9 → Low
- 4.0 – 6.9 → Medium
- 7.0 – 8.9 → High
- 9.0 – 10 → Critical

Higher score = Higher risk

🔟 Risk Classification Strategy

Risk was calculated based on:

Risk = Likelihood × Impact

Factors considered:

- CVSS Score
- Exploit availability
- Exposure to internet
- Sensitive data involved
- Business impact

1️⃣1️⃣ Risk Priority List

🔴 Critical Priority (Immediate Action)

- SMBv1 enabled (Remote code execution risk)
- Unpatched critical vulnerabilities

🟠 High Priority

- Outdated software versions
- Missing patches

🟡 **Medium Priority**

- Weak SSL configuration
- Information disclosure issues

🟢 **Low Priority**

- Minor configuration weaknesses

1️⃣2️⃣ Recommended Remediation Steps

✓ Disable SMBv1
✓ Update OpenSSL
✓ Install latest OS security patches
✓ Harden firewall configuration
✓ Disable unused services
✓ Use strong encryption standards
✓ Implement regular patch management
✓ Conduct periodic vulnerability scans

1️⃣3️⃣ Difference Between VA and Penetration Testing

Vulnerability Assessment	Penetration Testing
Identifies weaknesses	Exploits weaknesses
Automated scanning	Manual + automated
Broad coverage	Deep testing
Risk identification	Proof of exploitation

1️⃣4️⃣ Conclusion

The vulnerability assessment successfully identified multiple security weaknesses in the system. Critical and high-risk vulnerabilities were prioritized for immediate remediation. Proper patching and configuration hardening significantly reduce the risk of exploitation.

This process improves overall system security posture and helps prevent cyber attacks.