VULNERABILITY ASSESSMENT & RISK PRIORITIZATION REPORT

1. INTRODUCTION

Vulnerability Assessment (VA) is a systematic process used to identify, classify, and prioritize security weaknesses in systems, networks, and applications. This report demonstrates a structured vulnerability assessment using Nessus Essentials or OpenVAS, followed by risk-based prioritization and remediation planning.

2. SCOPE DEFINITION

- Target System: Ubuntu/Kali Linux test machine
- IP Range: 192.168.1.0/24 (example lab network)
- Scan Type: Basic Network Scan
- Exclusions: Production systems excluded
- Objective: Identify security misconfigurations and known vulnerabilities

3. SCANNER CONFIGURATION

- Configured Nessus/OpenVAS with updated vulnerability database
- Enabled service detection and OS fingerprinting
- Enabled credentialed scan (if available)
- Selected appropriate scan template (Basic/Advanced Scan)
- Configured scan policies for safe testing

4. IDENTIFIED VULNERABILITIES

- Outdated OpenSSH version detected
- Apache server with outdated modules
- Weak SSL/TLS configuration
- Missing security patches
- Open unnecessary ports (e.g., FTP, Telnet)

5. CVE & CVSS MAPPING

Each identified vulnerability was mapped to a CVE (Common Vulnerabilities and Exposures) identifier and assigned a CVSS (Common Vulnerability Scoring System) score to determine severity.

Vulnerability	CVE ID	CVSS Score	Severity
Outdated OpenSSH	CVE-2023-XXXX	9.8	Critical
Weak TLS Config	CVE-2022-XXXX	7.5	High
Outdated Apache	CVE-2021-XXXX	6.8	Medium

6. RISK CLASSIFICATION & PRIORITIZATION

- Critical (CVSS 9.0 – 10.0): Immediate remediation required
- High (CVSS 7.0 – 8.9): Fix as soon as possible
- Medium (CVSS 4.0 – 6.9): Schedule patching
- Low (CVSS 0.1 – 3.9): Monitor and document

7. REMEDIATION RECOMMENDATIONS

- Update vulnerable software packages immediately
- Disable unnecessary services and close unused ports
- Apply latest security patches
- Enforce strong encryption configurations
- Implement regular vulnerability scanning schedule

8. RISK PRIORITY LIST

- 1. Patch Critical vulnerabilities (CVSS > 9.0)
- 2. Fix High severity issues affecting exposed services
- 3. Harden SSL/TLS configurations
- 4. Remove unnecessary open ports
- 5. Address Medium and Low findings in maintenance cycle

9. INTERVIEW QUESTIONS & ANSWERS

1. What is Vulnerability Assessment?
A process of identifying, analyzing, and prioritizing security weaknesses in systems.

2. What is CVE?
Common Vulnerabilities and Exposures (CVE) is a standardized identifier for publicly known security v

3. What is CVSS?
Common Vulnerability Scoring System (CVSS) is a framework used to calculate the severity score of vul

4. VA vs Penetration Testing?
VA identifies vulnerabilities; Penetration Testing actively exploits vulnerabilities to assess real-w

5. Why is Prioritization Important?
Organizations have limited resources; prioritization ensures critical risks are addressed first.

10. FINAL OUTCOME

Through this task, the ability to conduct vulnerability scanning, interpret CVSS scores, map findings to CVE identifiers, and prioritize remediation efforts was demonstrated. This skill is essential for SOC analysts, security engineers, and risk management teams.