Cybersecurity Vulnerability Assessment Report

Name : Shlok Jadhav

Theoretical Knowledge

1. Understanding Security Assessment

Objective:
Understand how to evaluate system security using open-source tools and standardized frameworks.

Explanation:
A **Security Assessment** involves identifying weaknesses in systems, applications, and networks to reduce risk. It relies on recognized frameworks such as **NIST SP 800-115**, **OWASP**, and **CIS Benchmarks**.

Types of Security Testing:

1. **Vulnerability Assessment**
   - Purpose: Detect known vulnerabilities.
   - Tools:
     - **OpenVAS/Greenbone** (open-source vulnerability scanner)
     - **Nmap NSE scripts**
   - Output: Severity-based vulnerability listing.
2. **Penetration Testing**
   - Purpose: Simulate real-world attacks to validate security gaps.
   - Tools:
     - **Kali Linux**
     - **Metasploit Framework**

        - **Nmap**
        - **Burp Suite Community Edition**
    - Output: Verified exploitable vulnerabilities.
3. **Compliance Testing**
    - Purpose: Evaluate adherence to security standards.
    - Examples:
        - **CIS Benchmarks**
        - **NIST 800-53 controls**
        - **GDPR/HIPAA checks**
    - Uses checklists and best-practice guides.

---

2. VAPT Methodology

Objective:
Follow industry-aligned methodologies for conducting VAPT assessments.

Explanation:

Phases of VAPT:

1. **Planning & Pre-Engagement**
    - Define scope, rules of engagement.
    - Tools: **Dradis CE**, Notion, or manual documentation.
2. **Discovery / Information Gathering**
    - Network scanning: **Nmap**
    - Web scanning: **OWASP ZAP**, Nikto

    - Enumeration: SMB, SSH, HTTP enumeration using **enum4linux**, **WhatWeb**, etc.

3. **Attack / Exploitation**
    - Use validated vulnerabilities to attempt exploitation.
    - Tools:
        - **Metasploit** (exploiting known CVEs)
        - **Hydra** (password attacks)
        - Manual exploitation techniques.
4. **Post-Exploitation**
    - Privilege escalation
    - Persistence testing
    - Extraction of key insights
5. **Reporting**
    - Include vulnerabilities, CVSS scores, screenshots, and fixes.
    - Tools:
        - Dradis CE
        - Pentest-Tools templates
        - Custom reporting formats

---

3. Security Standards & Compliance

Objective:
Understand regulatory and industry-level security standards.

Key Standards:

- **GDPR** – Data privacy regulations for EU citizens.
- **HIPAA** – Protects patient health information (US healthcare).
- **ISO 27001** – International standard for information security management systems.
- **PCI-DSS** – Payment card data security.

---

4. Risk Assessment Basics

Objective:
Learn to prioritize security issues based on impact and likelihood.

Tools & Concepts:

1. **CVSS Scoring (v3.1/v4.0)**
   - Use the **NVD CVSS Calculator** to derive Base, Temporal, and Environmental scores.
   - Helps classify vulnerabilities as Low, Medium, High, or Critical.
2. **Risk Matrix (3x3 or 5x5)**
   Risk = Likelihood × Impact
   - High Impact + High Likelihood = **Critical**
   - Low Impact + Low Likelihood = **Low**

Tools:

- Google Sheets
- Excel
- SecurityScorecards

---

5. Common Vulnerabilities

Objective:
Recognize typical weaknesses found in assessments.

Network Vulnerabilities:

- Misconfigured services
- Weak SSH/FTP passwords
- Open unnecessary ports
- Outdated software versions
  Tools: Nmap, OpenVAS, Hydra

Web Vulnerabilities:

- SQL Injection (SQLi)
- Cross-Site Scripting (XSS)
- Broken Authentication
- Insecure Direct Object Reference (IDOR)

Practice Targets:

- **Metasploitable 2/3** (virtual machines for exploitation practice)
- **OWASP Juice Shop** (modern web app vulnerabilities)
- **VulnHub Machines** (boot-to-root challenges)

6. Documentation Fundamentals

Objective:
Create polished, professional reports that reflect your assessment accurately.

Tools for Reporting:

- **Dradis CE** — Collaborative reporting platform
- **CherryTree** — Technical note-taking
- **Joplin** — Secure markdown note system
- **Standard Templates** from GitHub (VAPT/PenTest/VA report formats)

What a Good Report Contains:

1. Executive Summary
2. Scope, methodology
3. Vulnerability details (with CVSS rating)
4. Screenshots/Proof of Concept
5. Remediation and best practices
6. References and tools used

Practical Application :

1. Executive Summary

The security scan against **192.168.0.103(Metaslpoitable 3)** revealed **23 actionable vulnerabilities**, including **9 high-severity issues**.
Major risks include:

- Operating system no longer supported (Ubuntu 14.04 – EOL)
- Remote Code Execution via ProFTPD mod_copy
- Default SSH & FTP credentials
- UnrealIRCd known backdoor
- Legacy PHP version with multiple CVEs
- Exposed phpMyAdmin setup interface
- Weak SSH and TLS configurations

These vulnerabilities enable **remote unauthorized access, data exposure, Privilege Escalation, and full compromise** of the host.

Overall Risk Rating: CRITICAL

---

2. Technical Details

2.1 Host Overview

- IP: 192.168.0.103
- OS: Ubuntu 14.04 (End-of-life)
- Ports: 21, 22, 80, 631, 6697
- Services: FTP, SSH, Apache/PHP, CUPS, UnrealIRCd

2.2 High Severity Findings (With CVSS & Evidence)

1. ProFTPD mod_copy RCE

- CVSS: 10.0
- Allows copying arbitrary files → Remote Code Execution
- Evidence: Vulnerable to SITE CPFR/CPTO

2. SSH Default Credentials

- CVSS: 9.8
- Successful login: **vagrant / vagrant**

3. FTP Default Credentials

- CVSS: 7.5
- Successful login: **vagrant / vagrant**

4. PHP 5.4.5 Multiple CVEs

- CVSS: 9.8
- Vulnerabilities: Heap OOB, memory corruption
- Fixed version: 5.6.30+

5. UnrealIRCd Backdoor

- CVSS: 10
- Allows full command execution

6. Apache Allowing Dangerous Methods (PUT/DELETE)

- CVSS: 7.5
- Allows arbitrary file upload and deletion

7. OS End-of-Life

- CVSS: 10
- No security patches → Extremely high exploitation risk

---

3. Risk Assessment

Likelihood vs Impact Matrix (3×3)

Legend

- **Likelihood:** Low (1), Medium (2), High (3)
- **Impact:** Low (1), Medium (2), High (3)

🔴 Critical Risks (High Impact + High Likelihood)

Vulnerability	Likelihood	Impact	Risk
ProFTPD mod_copy RCE	3	3	🔴 Critical
UnrealIRCd Backdoor	3	3	🔴 Critical
SSH default creds	3	3	🔴 Critical
FTP default creds	3	3	🔴 Critical
OS EOL	3	3	🔴 Critical

🟠 Major Risks (High Impact + Medium Likelihood)

Vulnerability	Likelihood	Impact	Risk
PHP <5.6.30 multiple CVEs	2	3	🟠 Major
phpMyAdmin exposed installer	2	3	🟠 Major

🟡 Moderate Risks (Medium Impact + Medium Likelihood)

Vulnerability	Likelihood	Impact	Risk
jQuery XSS	2	2	🟡 Moderate
Cleartext login forms	2	2	🟡 Moderate

🟢 Low Risks

Vulnerability	Likelihood	Impact	Risk
ICMP timestamp	1	1	🟢 Low

TCP timestamps	1	1	🟢 Low
Weak SSH MACs	1	1	🟢 Low

---

4. Remediation Plan

Critical Fixes (Immediate)

1. **Upgrade OS to supported Ubuntu version**
2. **Disable default credentials** (SSH, FTP)
3. **Uninstall/upgrade UnrealIRCd**
4. **Update PHP to ≥ 7.4**
5. **Fix Apache dangerous methods**
   - Disable PUT/DELETE
   - Restrict upload directories
6. **Remove ProFTPD mod_copy or update**
7. **Close or firewall unused ports**

Medium Fixes

- Update jQuery library
- Enforce HTTPS for all forms

- Remove phpMyAdmin/setup
- Disable TLS 1.0 and TLS 1.1
- Harden SSH (disable weak KEX, ciphers)

Low Fixes

- Disable ICMP timestamps
- Disable TCP timestamps
- Remove weak SSH MACs

5. Sources Consulted

(For your assignment)

- OpenVAS official documentation
- NIST NVD vulnerability database
- MITRE CVE references
- OWASP Top 10
- Ubuntu EOL documentation