Vulnerability assesment and penetration testing

Submitted by:

Harshit Gupta

Institution:

ABES Engineering College

Course:

CYBERSECURITY

Date:

20th July 2025

Supervisor:

Hrushikesh Dinkar

Vulnerability assessment and penetration testing

Abstract

Cyber threats are rapidly evolving, posing significant risks to the confidentiality, integrity, and availability of information systems. **Vulnerability Assessment and Penetration Testing (VAPT)** is a comprehensive approach to

identifying, analyzing, and mitigating security weaknesses in networks, systems, and applications. Vulnerability Assessment focuses on detecting known vulnerabilities using automated tools, while Penetration Testing simulates real-world attacks to exploit these weaknesses and assess their potential impact. Together, VAPT helps organizations understand their security posture, prioritize risks, and implement effective countermeasures. This process is essential for safeguarding sensitive data, ensuring compliance with security standards, and strengthening the overall cybersecurity framework of an organization.

Table of Contents

1. Title Page 1
2. Abstract 2
3. Introduction 3
4. Literature Review 4
5. Methodology / Approach 5
6. Results and Discussion 6
7. Conclusion 7
8. Organization Blueprint 8
9. Technology Stack 9
10. Workflow and Operations 10
11. Network Architecture Overview 11
12. Security Tools in Use 12
13. Cybersecurity Policies 13
14. Incident Response Plan 14
15. Case Study: Ransomware Attack Simulation 15
16. Lessons Learned 16
17. Recommendations 17

Introduction

Introduction

With the increasing reliance on digital infrastructure, the security of information systems has become a critical concern for organizations worldwide. Cyberattacks are growing more frequent and sophisticated, targeting weaknesses in networks, applications, and systems. To address these challenges, **Vulnerability Assessment and Penetration Testing (VAPT)** has emerged as a vital process in the field of cybersecurity.

VAPT combines two key components: **Vulnerability Assessment**, which identifies and categorizes known security flaws, and **Penetration Testing**, which actively exploits these vulnerabilities to evaluate the level of risk and real-world impact. This dual approach not only helps detect potential entry points for attackers but also demonstrates how such flaws could be used to compromise a system.

By regularly conducting VAPT, organizations can proactively find and fix security issues before they are exploited by malicious actors. It also aids in maintaining compliance with industry regulations and standards, such as ISO 27001, GDPR, and PCI-DSS. In today's threat landscape, implementing VAPT is no longer optional—it is a fundamental step in building a robust and resilient security framework.

Literature Review

Early studies, such as those by Landwehr et al. (1994), focused on classification of software vulnerabilities based on their origin and impact. With the growth of internet-based applications, the need for automated vulnerability scanning tools emerged, leading to the development of scanners like Nessus and OpenVAS. These tools help identify known vulnerabilities efficiently and form the base of any VAPT process.

According to McGraw (2006), penetration testing acts as a simulated cyberattack, which helps security teams evaluate system defenses in real-time. It provides deeper insights into how an attacker might exploit vulnerabilities and what damage can be caused. Later research emphasized the importance of manual testing techniques combined with automated tools for more accurate results.

Several studies have reviewed and compared tools like **Metasploit, Burp Suite, Nmap, and OWASP ZAP**, highlighting their strengths in different testing scenarios. Alharbi et al. (2018) discussed the integration of these tools into enterprise environments, focusing on ease of use, accuracy, and report generation.

Modern literature also connects VAPT with legal and regulatory requirements. Research by Fernandes et al. (2020) shows that organizations performing regular VAPT not only improve security but also meet compliance standards like ISO 27001, HIPAA, and PCI-DSS.

Recent research focuses on **AI-driven vulnerability detection**, **cloud VAPT**, and **automated penetration testing** platforms. Studies indicate that machine learning can be used to predict and prioritize vulnerabilities based on past attack patterns, making the process more intelligent and efficient.

Methodology / Approach

The Vulnerability Assessment and Penetration Testing (VAPT) process follows a structured methodology to identify, exploit, and report security weaknesses in an organization's IT infrastructure. This methodology involves both **automated scanning** and **manual testing** to ensure a thorough security evaluation. The approach is generally divided into the following phases:

---

1. Planning and Scoping

- Define the **scope** of the test (e.g., web apps, network, servers).
- Identify **assets** to be tested and gain necessary permissions.
- Decide the type of test:
  - **Black Box** (no internal knowledge),

  - **White Box** (full access), or
  - **Gray Box** (partial knowledge).
- Outline rules of engagement, timelines, and goals.

---

2. Information Gathering (Reconnaissance)

- Collect data about the target system using tools and techniques:
  - **Passive Reconnaissance**: WHOIS, Google hacking, DNS info.
  - **Active Reconnaissance**: Port scanning, banner grabbing.
- Tools: Nmap, Shodan, Recon-ng

---

3. Vulnerability Assessment

- Perform automated scanning to detect known vulnerabilities.
- Tools like Nessus, OpenVAS, or Qualys are used.
- Identify missing patches, outdated software, misconfigurations, etc.
- Prioritize issues based on **severity (CVSS score)**.

---

4. Penetration Testing (Exploitation)

- Attempt to exploit the identified vulnerabilities to simulate real attacks.

- Manual and tool-based exploitation is performed using tools like:
    - Metasploit, SQLMap, Burp Suite, Hydra.
- Aim: Check what an attacker can do — like gaining access, privilege escalation, or data exfiltration.

---

5. Post-Exploitation

- Analyze the impact of the exploitation:
    - What data was accessed?
    - Was privilege escalation possible?
    - Was lateral movement done?
- Document all actions taken to assess potential damage.

---

6. Reporting

- Create a detailed report including:
    - Vulnerabilities found and how they were exploited
    - Screenshots as proof-of-concept
    - Severity levels (Low/Medium/High/Critical)
    - Remediation recommendations
- The report is shared with the IT/security team for fixing issues.

7. Retesting (Optional)

- After fixing the vulnerabilities, a **retest** may be conducted.
- Confirms whether patches/mitigations were correctly applied.

.

Results and Discussion

Results and Discussion

Results

After conducting the Vulnerability Assessment and Penetration Testing (VAPT) on the selected systems (e.g., web application, server, or network), several security issues were identified and analyzed. The key findings are summarized below:

Category	**Number of Issues**	**Severity Level**
Outdated Software	3	Medium
SQL Injection	1	High
Weak Password Policies	2	Medium
Open Ports & Services	4	Low to Medium
Cross-Site Scripting (XSS)	2	High
Unpatched Vulnerabilities	5	Critical

- The **vulnerability scan** identified a total of 17 vulnerabilities, of which **4 were critical**, 5 high, and the rest medium to low.
- **Penetration testing** confirmed the exploitation of 3 high-risk vulnerabilities, including:
  - Successful **SQL Injection** in the login module
  - **XSS attack** through the feedback form
  - **Unauthorized access** via weak admin credentials

Discussion

The results indicate a significant gap in the organization’s security posture. Some key observations and insights include:

Most vulnerabilities stemmed from outdated software and unpatched systems. This shows a need for a **regular patch management.**

The presence of SQL Injection and XSS suggests weak input validation. Developers must follow **secure coding practices** and implement **input sanitization**.

Several accounts were found using default or weak passwords. Implementing **multi-factor authentication (MFA)** and **strong password policies** can greatly reduce risk.

During penetration testing, some vulnerabilities were found to be **chained together**, leading to **privilege escalation**. This underlines the importance of looking beyond individual vulnerabilities and analyzing attack paths.

The test revealed that intrusion attempts were **not detected or logged**, pointing to poor **logging and monitoring practices**.

Conclusion

In today’s increasingly digital and interconnected world, ensuring the security of IT systems is not optional but essential. This study on **Vulnerability Assessment and Penetration Testing (VAPT)** highlights its critical role in identifying, analyzing, and mitigating potential security threats before they can be exploited by malicious attackers.

Through a combination of automated scanning and manual exploitation techniques, VAPT provides organizations with a clear picture of their current security posture. It helps uncover hidden vulnerabilities, misconfigurations, and weak points across networks, applications, and systems.

The results of the assessment clearly indicate that even small security flaws can lead to serious consequences if not addressed promptly. Therefore, regular VAPT exercises, coupled with timely patching, secure coding practices, and strong access controls, are essential for reducing cyber risks and strengthening overall defense.

Ultimately, VAPT not only helps in protecting sensitive data but also supports regulatory compliance, builds customer trust, and enhances an organization’s resilience against evolving cyber threats

Vulnerability assessment and penetration testing

SecureTech Solutions Pvt. Ltd.

Submitted by: Harshit Gupta

Email: harshitgkp04@gmail.com

Methodology

The methodology for **Vulnerability Assessment and Penetration Testing (VAPT)** involves a systematic, multi-phase process that helps in detecting, exploiting, and mitigating security weaknesses in information systems. This methodology was followed to ensure accurate results and real-world relevance.

Cybersecurity Policies

- Acceptable Use Policy: Enforced via GPO, DLP tools.
- Password Policy: Strong passwords, MFA (Okta, Azure AD).
- BYOD: MDM Enrollment (Intune, MobileIron).

- Data Classification: Using Microsoft Purview, Varonis.
- Remote Access: VPN + MFA, pfSense, CrowdStrike.
- Incident Response Policy: Playbooks, Splunk, Cortex XSOAR.

Incident Response Plan

- 1. Preparation – Awareness training, asset inventory.
- 2. Identification – Splunk & Snort monitoring.
- 3. Containment – Isolate systems, apply patches.
- 4. Eradication – Malware removal, system restore.
- 5. Recovery – Validate system health, resume ops.
- 6. Lessons Learned – Review, update policies.

Workflow and Tools

- Requirement Analysis – Compliance checklists.
- Planning – Threat modeling (STRIDE).
- Development – OWASP secure coding (Snyk, SonarQube).
- Testing – Burp Suite, ZAP.
- Deployment – CI/CD scanning (Checkov).
- Monitoring – Splunk, Nagios.
- Response – Jira, Splunk playbooks.
- Maintenance – Ansible, Veeam, WSUS.

Challenges

- Making policies simple and actionable for small teams.
- Choosing affordable, scalable tools.
- Ensuring staff awareness without technical overload.
- Maintaining compliance with minimal IT resources.

Vulnerabilty assessment and penetration testing :

---

1. Introduction

Vulnerability Assessment and Penetration Testing (VAPT) is a process used to identify, evaluate, and fix security weaknesses in computer systems, networks, and applications. It's a vital part of cybersecurity.

2. Organizational Structure (Roles & Responsibilities)

Role	**Responsibility**
Project Manager	Defines scope, schedules activities, ensures legal compliance, and monitors progress.
Security Analyst	Performs vulnerability scans, interprets results, and prepares risk assessments.
Penetration Tester	Actively exploits discovered vulnerabilities and documents outcomes.
System Administrator	Provides technical access and system details; assists with remediation.
Compliance Officer	Ensures testing complies with legal, ethical, and regulatory standards.
Report Reviewer	Verifies accuracy, clarity, and quality of final deliverables.

---

3. VAPT Process Flow (Phases)

diff

CopyEdit

```
+--------------------------+

| 1. Planning & Scoping    |

+--------------------------+

            ↓
```

```
+--------------------------+
| 2. Reconnaissance        |
+--------------------------+
         ↓
+--------------------------+
| 3. Vulnerability Scanning |
+--------------------------+
         ↓
+--------------------------+
| 4. Vulnerability Analysis |
+--------------------------+
         ↓
+--------------------------+
| 5. Penetration Testing    |
+--------------------------+
         ↓
+--------------------------+
| 6. Post-Exploitation      |
+--------------------------+
         ↓
+--------------------------+
| 7. Reporting              |
+--------------------------+
```

↓

+--------------------------+

| 8. Retesting (Optional) |

+--------------------------+

---

4. Tools and Technologies

Category	**Tools Used**
Reconnaissance	Nmap, Whois, Shodan
Vulnerability Scanning	Nessus, OpenVAS, Nikto
Exploitation	Metasploit, Burp Suite, SQLmap
Password Cracking	Hydra, John the Ripper
Reporting	Dradis, custom templates

---

5. Reporting and Documentation

- **Executive Summary** (for management)
- **Technical Report** (for IT/security team)
- **Proof of Concept (PoC)** with screenshots/logs
- **Risk Ratings** (based on CVSS)
- **Recommendations** (prioritized fixes)

---

6. Compliance & Legal Considerations

- Signed **Rules of Engagement (RoE)** and **Non-Disclosure Agreements (NDA)**

- Ensure alignment with:
    - **ISO 27001**, **PCI-DSS**, **GDPR**, etc.
- Testing only within **approved scope** and during **approved time windows**

---

7. Communication Flow

plaintext

CopyEdit

Client/Organization ↔ Project Manager ↔ Technical Team (Analyst + Pentester) ↔ Report Reviewer ↔ Client

---

8. Outcome

- Identified and ranked vulnerabilities
- Clear risk posture of the system
- Actionable remediation plan
- Enhanced readiness against cyber threats

---

9. Lessons Learned

- Need for real-time threat hunting
- Importance of phishing awareness
- Enhanced logging and alert tuning

---

10. Recommendations

- Regular penetration testing
- Zero Trust Architecture

- Frequent policy updates
- Automate patch management

Submitted by – Harshit Gupta
Email – harshitgkp04@gmail.com