VAPT Lab Report - Reconnaissance, Post-Exploitation & Capstone Project

1. Reconnaissance Practice

Tools: Maltego, Shodan, Google Docs
Tasks: Perform OSINT, map assets, document steps

Recon Template
- Domain Info: example.com
- Subdomains: dev.example.com, test.example.com
- Exposed Services: SSH (22), HTTP (80), FTP (21)

Asset Mapping (Slack-friendly log)

```
Timestamp           | Tool    | Finding
2025-08-18 10:00:00 | Shodan  | Exposed SSH on 192.168.56.107
2025-08-18 10:30:00 | Maltego | Subdomain: dev.example.com
2025-08-18 11:00:00 | Shodan  | Open HTTP port 80 on 192.168.56.107
2025-08-18 11:15:00 | Maltego | Subdomain: test.example.com
```

Checklist
- Check WHOIS records
- Enumerate subdomains (using Sublist3r)
- Identify tech stack (using Wappalyzer)

Summary

Reconnaissance was performed on the target IP 192.168.56.107 using passive and active OSINT tools. Shodan revealed exposed services such as SSH and HTTP, while Maltego mapped subdomains and potential internal infrastructure. WHOIS and subdomain enumeration confirmed asset ownership, and Wappalyzer identified the technology stack used. All findings were logged systematically with timestamps for reporting and future exploitation planning.

2. Post-Exploitation Practice

Tools: Meterpreter, Volatility, sha256sum
Tasks: Escalate privileges, collect evidence

VAPT Lab Report - Reconnaissance, Post-Exploitation & Capstone Project

Privilege Escalation

- Exploit Module: exploit/windows/local/bypassuac
- Session ID: 1
- Payload: windows/meterpreter/reverse_tcp
- Elevated Privileges: SYSTEM
- Logs saved during exploitation

Evidence Collection

- File hashed: target.conf
- SHA256 hash computed using sha256sum

Item	Description	Collected By	Date	Hash Value
Config File	target.conf	VAPT Analyst	2025-08-18	<SHA256-placeholder>

3. Capstone Project - Full VAPT Cycle

Simulation - SQL Injection on DVWA

- Tool: sqlmap
- Target: 192.168.56.107
- Databases Found: <fill>

Detection - OpenVAS Findings

Timestamp	Target IP	Vulnerability	PTES Phase
2025-08-18 12:00:00	192.168.56.107	XSS	Exploitation

Remediation

- Input sanitization on all user inputs
- Use parameterized queries for SQL
- Rescan after remediation to verify

Reporting

PTES Report (200 words)

The VAPT exercise was conducted on the target IP 192.168.56.107, using Kali Linux as the attacker

(IP: 192.168.56.107). Post-exploitation tests included privilege escalation via the Windows UAC bypass module, which successfully elevated privileges to SYSTEM level. Evidence collection involved hashing sensitive configuration files to ensure integrity and maintain audit trails. For web application testing, DVWA was targeted with sqlmap, revealing potential SQL injection vulnerabilities. OpenVAS scans detected XSS vulnerabilities, highlighting insecure input handling. Recommendations include implementing strict input sanitization, parameterized queries, and regular vulnerability scanning to mitigate risks. The exercise validates the effectiveness of PTES methodologies.

Non-technical briefing (100 words)

During the security assessment of the target system (IP: 192.168.56.107) from Kali Linux (IP: 192.168.56.107), critical vulnerabilities were identified, including improper user input handling in web applications and privilege escalation potential in Windows services. Exploits were safely tested in a lab environment to simulate real-world attacks. Key findings highlight the need for stronger security controls such as input validation and access restrictions. Remediation recommendations were provided to prevent exploitation. This exercise demonstrates how proactive testing can help organizations identify and fix vulnerabilities before attackers exploit them, improving overall system security.