VAPT Lab Report – Post-Exploitation & Capstone Project

---

1. Post-Exploitation Practice

1.1 Privilege Escalation

- Exploit Module: `exploit/windows/local/bypassuac`
- Session ID: 1
- Payload: `windows/meterpreter/reverse_tcp`
- Elevated Privileges: SYSTEM

1.2 Evidence Collection

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

---

2. Capstone Project – Full VAPT Cycle

2.1 Simulation – SQL Injection on DVWA

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

2.2 Detection – OpenVAS Findings

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

2.3 Remediation

- Suggested fixes:

    1. Input sanitization on all user inputs
    2. Use parameterized queries for SQL
    3. Rescan after remediation to verify

2.4 Reporting

- **PTES Report (200 words)**:
  The VAPT exercise was conducted on the target machine at IP 192.168.56.107, using Kali Linux as the attacker. 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 in the application, 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 for identifying, exploiting, and documenting security weaknesses in both system and application layers.

- **Non-technical briefing (100 words)**:
  During the security assessment of the target system (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 and resilience against cyber threats.