Capstone Project: Full VAPT Engagement Workflow

Observables

- **Tools Used:** Kali Linux, OpenVAS, Burp Suite, Google Docs
- **Attacker IP:** 192.168.56.108
- **Target IP:** 192.168.56.109
- **Exploits / Methods:** Manual FTP testing, OpenVAS vulnerability scan, Burp Suite API testing
- **Detection Source:** OpenVAS scan / Burp Suite logs
- **Protocol:** FTP (port 21), HTTP/HTTPS for API testing

Step-by-Step Workflow

1. Recon & Scanning

1. Conduct network and service enumeration:

```
nmap -sV -p 21,80,443 192.168.56.109
```

2. Identify open services, versions, and potential vulnerabilities (e.g., VSFTPD 2.3.4, outdated HTTP services).

2. Exploitation / Vulnerability Verification

1. Perform manual exploitation using tested methods (FTP commands, injection tests, etc.).
2. Use Burp Suite to test API endpoints for vulnerabilities (SQLi, broken auth, input validation).
3. Record evidence of potential exploitation in logs.

3. Vulnerability Scanning with OpenVAS

1. Start OpenVAS and scan the target VM:

```
openvas-start
```

2. Identify vulnerabilities including VSFTPD RCE and other system weaknesses.

4. Remediation

- Patch vulnerable services (e.g., VSFTPD, outdated HTTP components).
- Enforce least privilege for FTP and web accounts.
- Validate input on all services to prevent injection attacks.
- Rescan using OpenVAS to confirm vulnerabilities are mitigated.

5. Metrics and Logging

Timestamp	Target IP	Vulnerability	PTES Phase
2025-08-30 15:00:00	192.168.56.109	VSFTPD RCE	Exploitation

6. Root Cause Analysis (RCA)

- Legacy services exposed on target VM (VSFTPD 2.3.4, outdated web components).
- Lack of patch management initially.
- No automated detection or monitoring in place.

7. Recommendations

1. Patch all vulnerable services immediately.
2. Restrict service access using least privilege.
3. Implement regular automated vulnerability scans.
4. Monitor network and API activity for abnormal patterns.

8. Reporting

Executive Summary :
A full VAPT engagement was conducted on the VirtualBox lab VM (192.168.56.109) from the attacker VM (192.168.56.108). Reconnaissance and scanning identified FTP and web services running outdated versions, including VSFTPD 2.3.4. Manual exploitation techniques and API testing using Burp Suite verified the vulnerabilities without using Metasploit. OpenVAS scans confirmed the VSFTPD RCE vulnerability and revealed additional weaknesses.

The engagement consisted of recon, vulnerability verification, API testing, and comprehensive scanning. Remediation steps included patching the vulnerable services, enforcing least privilege on accounts, validating input to prevent injections, and rescanning to ensure mitigation. Root cause analysis highlighted exposed legacy services and the absence of automated monitoring, which were addressed in the remediation plan.

Remediation Plan:

- Patch VSFTPD 2.3.4 and any outdated web services.
- Enforce least privilege on all accounts.
- Validate inputs to prevent command injection or API abuse.
- Rescan using OpenVAS to confirm mitigation.
- Implement continuous monitoring and regular vulnerability assessments to reduce future risks.