Week2_Task

Theoretical Knowledge

1. Vulnerability Scanning Techniques
What to Learn:

- **Core Concepts:**
  - Scan Types: Network (e.g., Nmap port scans), application (e.g., Nikto for web flaws), authenticated vs. unauthenticated.
  - Vulnerability Scoring: Use CVSS v4.0 (e.g., CVSS 8.8 for RCE = High). Example: Apache Struts (CVE-2017-5638) = Critical.
  - False Positives: Validate findings (e.g., manual checks for open ports).
- **Key Objectives:** Configure and validate scans for accurate risk assessment.
- **How to Learn:**
  - Study OWASP Testing Guide for web scanning.
  - Review NIST SP 800-115 for scanning methods.
  - Analyze WannaCry case for CVSS mapping.

2. Penetration Testing Techniques
What to Learn:

- **Core Concepts:**
  - Phases: Recon (e.g., OSINT with Shodan), Scanning (e.g., Nessus), Exploitation (e.g., Metasploit), Post-Exploitation (e.g., privilege escalation), Reporting.
  - Methodologies: PTES, OWASP WSTG. Example: PTES for scoping web tests.
  - Ethics: Ensure client authorization and defined scope.
- **Key Objectives:** Execute structured, ethical pentests.
- **How to Learn:**
  - Explore PTES for phase details.
  - Study OWASP WSTG for web pentesting.

    - Review SANS pentest case studies.

3. Exploit Development Basics
What to Learn:

- **Core Concepts:**
    - Exploit Types: Buffer overflows, SQL injection, XSS. Example: XSS via unescaped input.
    - Exploit Writing: Craft basic exploits (e.g., Python for buffer overflows) using Exploit-DB PoCs.
    - Mitigations: Understand ASLR, WAFs, and patching.
- **Key Objectives:** Develop and test exploits safely.
- **How to Learn:**
    - Study Exploit-DB for PoC examples.
    - Use TCM Security's exploit guides.
    - Try TryHackMe's buffer overflow room.

Practical Application

1. Vulnerability Scanning Lab
Activities:

- **Tools:** Nmap, OpenVAS, Nikto.
- **Tasks:** Run scans, prioritize vulnerabilities, document results.
- **Enhanced Tasks:**
    - **Scan Setup:** Track results in a table (copy-paste into Slack):

Scan ID	Vulnerability	CVSS Score	Priority	Host
001	SQL Injection	9.1	Critical	192.168.1.20
002	Open Port 445	6.5	Medium	192.168.1.30

- **Test Case:** Scan a Metasploitable2 VM with Nmap (nmap -sV 192.168.1.100) and OpenVAS.

- **Prioritization:** Score using CVSS in Google Sheets.
- **Report:** Draft in Google Docs:

Title: Critical Web Vulnerabilities

Findings: [CVE-2021-41773], [Host: 192.168.1.20]

Remediation: Patch Apache, disable unused ports

- **Escalation:** Write a 100-word email to developers with PoC.

2. Reconnaissance Practice

Activities:

- **Tools:** Maltego, Shodan, Google Docs.
- **Tasks:** Perform OSINT, map assets, document steps.
- **Enhanced Tasks:**
  - **Recon Template:** Document in Google Docs:
    i. Domain Info
    ii. Subdomains
    iii. Exposed Services
  - **Asset Mapping:** Log steps (Slack-friendly):

```
Timestamp           | Tool    | Finding
--------------------|---------|----------------------------
2025-08-18 10:00:00 | Shodan  | Exposed SSH on 192.168.1.50
2025-08-18 10:30:00 | Maltego | Subdomain: dev.example.com
```

- **Checklist:** In Google Docs:
- Check WHOIS
- Enumerate subdomains (Sublist3r)
- Identify tech stack (Wappalyzer)
- **Summary:** Write a 50-word recon summary.

3. Exploitation Lab

Activities:

- **Tools:** Metasploit, Burp Suite, sqlmap.
- **Tasks:** Simulate exploits, validate results.
- **Enhanced Tasks:**
  - **Exploit Simulation:** Exploit Metasploitable2 with Metasploit (use exploit/multi/http/tomcat_mgr_login). Log:

Exploit ID	Description	Target IP	Status	Payload
003	Tomcat RCE	192.168.1.100	Success	Java Shell

- **Validation:** Check Exploit-DB for PoC. Summarize in 50 words.

4. Post-Exploitation Practice

Activities:

- **Tools:** Meterpreter, Volatility, sha256sum.
- **Tasks:** Escalate privileges, collect evidence.
- **Enhanced Tasks:**
  - **Escalation:** Use Metasploit (exploit/windows/local/bypassuac). Save logs.
  - **Evidence Collection:** Hash a file:

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

5. Capstone Project: Full VAPT Cycle

Activities:

- **Tools:** Kali Linux, Metasploit, OpenVAS, Google Docs.
- **Tasks:** Simulate pentest, exploit, report.
- **Enhanced Tasks:**
  - **Simulation:** Exploit DVWA with sqlmap for SQL injection. Follow TryHackMe.
  - **Detection:** Log OpenVAS findings:

Timestamp	Target IP	Vulnerability	PTES Phase

2025-08-18 12:00:00	192.168.1.200	XSS	Exploitation

- **Remediation:** Suggest input sanitization, rescan.
- **Reporting:** Write a 200-word PTES report in Google Docs.
- **Briefing:** Draft a 100-word non-technical summary.