📘 Ethical Hacking — 5-Week Syllabus

WEEK 1 — Foundations & ReconnaissanceClass 1 — Course Intro, Legal & Ethics, Lab Setup

Theory

- What is *ethical hacking* vs malicious hacking
- Rules of Engagement (RoE): scope, authorization, reporting
- Responsible disclosure basics
- Attack lifecycle overview (recon → scanning → exploitation → post-exploit → remediation)

Practical scenario

- Boot Kali + Metasploitable 2 VM; confirm host-only network isolation
- Create a written RoE for a mock client engagement (define scope, timelines, allowed tools)
- VirtualBox / VMware, Kali, Metasploitable 2, DVWA

Class 2 — Footprinting & Passive Recon

Theory

- Passive vs active recon; intelligence sources (DNS, WHOIS, social footprints)
- OSINT basics and privacy concerns
- How attackers gather business info (subdomains, email formats, external services)

Practical scenario

- OSINT lab (lab domains only):
  - Map domain → subdomains (using lab tools/simulated data)
  - Collect intentionally published service banners
- Produce an intelligence brief summarizing discovered assets & risks

Tools

- Browser, responsibly configured OSINT tools, `dig`, `nslookup`, simulated WHOIS

WEEK 2 — Scanning, Enumeration & Vulnerability Analysis

Class 3 — Active Scanning & Service Discovery

Theory

- Discovery vs enumeration
- TCP vs UDP scanning; timing, stealth vs speed
- How to interpret scan results and prioritize follow-ups

Practical scenario

- Controlled network discovery in lab: identify live hosts & open services; create an asset inventory
- Prioritize hosts by exposed services (HTTP, SSH, DB, etc.)
- Nmap (lab only), `netstat` on targets, simple port inventory scripts

Deliverable

- Scanning report with host/service inventory and recommended next steps

Defensive follow-up

- Hardening exposed services and reducing attack surface

Class 4 — Vulnerability Analysis & Prioritization

Theory

- Types of vulnerabilities: misconfigurations, unpatched software, weak auth
- CVE & CVSS basics (scoring & prioritization)
- False positives and validation best practices

Practical scenario

- Run a vulnerability scanner (OpenVAS / Nessus trial) against Metasploitable 2 (lab only)
- Validate 2 findings manually (e.g., outdated web app or misconfig) and propose remediation steps
- OpenVAS / Nessus, NVD / vulnerability databases

WEEK 3 — System Hacking & Web Application Security

Class 5 — System Hacking Fundamentals & Privilege Escalation

Theory

- Local vs remote exploitation concepts (defensive focus)
- Privilege escalation weaknesses: misconfigs, SUID, weak file perms
- Logging and detection controls

Practical scenario

- In Metasploitable 2, identify a weak service or misconfiguration that could allow lateral movement. Document the weakness and propose mitigation (no exploit code).
- Simulated detection: configure logging and show how suspicious activity appears in logs
- Metasploitable 2, log viewers, file permission audit scripts

---

Class 6 — Web App Security: OWASP Top 10 & Hands-on Labs

Theory

- Overview of OWASP Top 10 (Injection, Auth flaws, CSRF, XSS, etc.)
- Secure coding practices: input validation, parameterized queries

Practical scenario

- Using **Metasploitable 2** / DVWA:
    - Identify and document an injection-type vulnerability conceptually using Burp Suite
    - Demonstrate a safe proof-of-concept in lab (screenshots only) and propose mitigations
- Metasploitable 2 / DVWA, Burp Suite, browser dev tools

WEEK 4 — Network Attacks, Sniffing & Wireless

Class 7 — Network Sniffing & Traffic Analysis

Theory

- Packet structure basics; what traffic reveals (cleartext creds, tokens)
- Detecting sniffing + defenses (switch hardening, encryption)

Practical scenario

- Capture lab traffic with Wireshark:
    - Identify benign protocols and find unencrypted credentials (lab data only)
    - Compare HTTP vs HTTPS payloads
- Wireshark, lab HTTP server configured for HTTP/HTTPS

Class 8 — Wireless Security & Attacks

Theory

- Wi-Fi standards: WEP, WPA, WPA2, WPA3
- Rogue APs, Evil Twin attacks, enterprise Wi-Fi controls

Practical scenario

- Audit a lab SSID for weak encryption/config problems
- Create a remediation plan: strong encryption, 802.1X, SSID policies
- Wi-Fi tools in Kali (scan/assessment mode), lab AP or simulated SSID

WEEK 5 — Advanced Topics & Capstone

Class 9 — Social Engineering, Phishing & Human Factors

Theory

- Phishing anatomy, common social engineering techniques
- Safe phishing awareness testing & metrics
- Building effective awareness programs

Practical scenario

- Mock phishing awareness campaign (simulation only):
    - Draft a benign test email template (no spoofing)
    - Simulate metrics collection (click rates)
    - Plan educational follow-up for users who clicked
- Simulated phishing platform, spreadsheets, awareness materials

---

Class 10 — DoS/Resilience, Incident Response & Capstone

Theory

- DoS basics: flooding vs resource exhaustion; detection & mitigation (rate limiting, load balancing)
- Incident response lifecycle (detect → contain → eradicate → recover → lessons learned)
- Reporting & stakeholder communication

Capstone Practical (choose one)

1. **Vulnerability Assessment & Remediation Plan** — scan multi-host lab network; create prioritized remediation roadmap.
2. **Web App Assessment + WAF Rules** — test Metasploitable 2 / DVWA; document findings + WAF tuning recommendations.
3. **Monitoring & Detection Playbook** — set up log collection for Metasploitable 2; implement detection rules (e.g., failed logins); write incident response playbook.

- Nmap, OpenVAS, Burp Suite, Wireshark, SIEM (ELK lite or Splunk trial), Python scripts
- Career pathways & certifications: OSCP, CEH, eJPT
- Continuous learning resources
