Forebrain — Penetration Testing & Ethical Hacking (3 Months / 12 Weeks)

Duration: 3 Months (12 Weeks)

Format: Daily Practical-Based Learning (1 hr class + 1 hr lab, Monday–Friday)

Focus: Hands-on pentesting skills, ethical frameworks, and real-world reporting

Outcome: Portfolio with minimum 3 projects + Capstone practical engagement

Daily Routine (Standard)

- 1 hr: Concept lecture & tool demo

- 1 hr: Guided hands-on lab practice

- Saturday: Activity Day – practical session based on weekly topics

- Learning Model: 85% Labs, 15% Theory — practical immersion with team tasks and individual missions

Phase-wise Curriculum Overview

Phase 1 — Foundations & Recon (Weeks 1–3)

- Linux essentials for pentesters (Kali/Ubuntu): shell, file system, package management

- Networking essentials: TCP/IP, ports, routing, packet capture basics

- OSINT & passive reconnaissance: Amass, Subfinder, crt.sh, theHarvester, Shodan

- Active reconnaissance & scanning: Nmap (SYN/UDP/Version), Netcat, hping3

- Scripting basics for automation: Python and Bash snippets for recon

- Safe lab operations, Rules of Engagement (RoE), snapshot & rollback procedures

Practical Assignment I: OSINT + Recon Pack — asset inventory, subdomain list, initial Nmap scan outputs

Phase 2 — Web Application Pentesting (Weeks 4–6)

- Web fundamentals: HTTP/HTTPS, sessions, cookies, headers, API basics

- OWASP Top 10 deep-dive: SQLi, XSS, CSRF, IDOR, RCE basics

- Tool mastery: Burp Suite (proxy, repeater, intruder), OWASP ZAP, sqlmap

- Manual testing techniques: parameter tampering, logic flaws, auth bypass

- API testing: JWT handling, rate-limit bypass, parameter pollution

- Exploit chaining & safe use of Metasploit for web-related modules

Practical Assignment II: Web App Pentest Report — DVWA/Juice Shop engagement, PoC, remediation suggestions

Phase 3 — Network & Host Exploitation (Weeks 7–9)

- Advanced scanning & service enumeration (NSE, versioning, banner analysis)

- Vulnerability validation: OpenVAS/Nessus basics and tuning for false positives

- Service/host exploitation: SMB, FTP, RCE, and common service weaknesses

- Post-exploitation: credential harvesting, data exfiltration, lateral movement basics

- Privilege escalation: Linux (SUID, kernel vectors) and Windows (service misconfig, token abuse)

- Active Directory basics for pentesters: enumeration, BloodHound mapping (collector safe), Kerberoast concepts

Practical Assignment III: Network Pentest — exploit lab host, document steps, privilege escalation proof (lab-safe)

Phase 4 — Advanced Techniques, Reporting & Capstone (Weeks 10–12)

- Advanced exploitation concepts: exploit chaining, safe payload crafting, and module customization

- Operational security (OpSec) and detection awareness — what defenders see

- C2 basics and beaconing patterns (conceptual & simulated) and detection heuristics

- Social engineering awareness (phishing analysis, templates) — no live phishing

- Automation & scripting for pentesters (fast recon, PoC generation)

- Final capstone: team-based red/blue engagement with full reporting and demo

Capstone Deliverables: Red Team logbook, Blue Team detection metrics & dashboards, final technical report, demo video

Tools & Technologies Covered

Recon & Scanning:

- Nmap
- Amass
- Subfinder
- theHarvester
- crt.sh
- Shodan
- Netcat
- hping3

Web:

- Burp Suite (Community/Pro)
- OWASP ZAP
- sqlmap
- Nikto
- DVWA
- OWASP Juice Shop
- Postman

Exploitation & Post-Exploitation:

- Metasploit
- searchsploit
- msfvenom
- Meterpreter

- Mimikatz (demo)
- BloodHound (collector safe)
- CrackMapExec

Network Analysis & IDS:

- Wireshark
- tcpdump
- Suricata
- Zeek
- Snort

Scripting & Automation:

- Python 3
- Bash
- PowerShell (conceptual)

Reporting & Management:

- Markdown
- Git
- CVSS
- LaTeX/Markdown templates

Cloud & APIs:

- AWS basics (sandbox)
- ScoutSuite (audit)
- Postman
- jwt.io

Lab Manual Summary (Selected Labs)

- Kali Linux setup & hardening

Forebrain — Penetration Testing & Ethical Hacking (3-Month Syllabus)

- OSINT collection sprint (Amass/Subfinder/CRT.sh)
- Nmap NSE and scanning workshop
- Burp Suite manual testing labs (XSS, SQLi, auth bypass)
- DVWA & Juice Shop exploit chaining
- OpenVAS scan & triage lab
- Privilege escalation workshops (LinPEAS/WinPEAS)
- Active Directory enumeration (BloodHound collector)
- Wireshark & tcpdump PCAP analysis
- Suricata/Zeek basic detection and alerting
- Capstone red/blue engagement environment

Assessment & Certification Mapping

- Weekly lab submissions and evidence (screenshots, PCAPs, scripts)
- Three practical assignments (web, network, recon packs)
- Mid-course practical assessment (structured lab)
- Final capstone assessment and presentation
- Certification guidance: eJPT pathway, OSCP prep recommendations (post-course)