30 Days - Foundation and Core Ethical Hacking Techniques

Module 1: Introduction to Ethical Hacking (Week 1-2)

- Overview of information security and the ethical hacking process
- Types of hacking: Black hat, white hat, grey hat
- Information security frameworks, laws, and regulations
- The role of ethical hackers in the cybersecurity landscape
- **Practical Lab:** Set up hacking lab environment (VMs, penetration testing tools)

Module 2: Footprinting and Reconnaissance (Week 3-4)

- Footprinting techniques: Active vs Passive Footprinting
- Tools: WHOIS, DNS Interrogation, Google Hacking
- Reconnaissance through social media and public sources
- **Practical Lab:** Conduct footprinting on a simulated target

Module 3: Scanning Networks (Week 5-6)

- Types of network scanning: Port scanning, Ping sweeps
- Tools: Nmap, Hping, Netcat
- Network mapping and service discovery
- **Practical Lab:** Network scanning and enumeration using Nmap and Hping

Module 4: Enumeration (Week 7-8)

- Techniques for enumerating target systems: NetBIOS, SNMP, DNS
- Extracting information from network services
- **Practical Lab:** Enumeration exercises using SNMP, NetBIOS, and other protocols

Module 5: Vulnerability Analysis and System Hacking (Week 9-12)

- Identifying vulnerabilities using Nessus, OpenVAS, Nikto
- Techniques for system exploitation, password cracking, privilege escalation
- **Practical Lab:** Perform vulnerability scanning using Nessus or OpenVAS
- Exploiting system vulnerabilities on Windows/Linux using John the Ripper for password cracking

45 Days - Intermediate Ethical Hacking Techniques

Includes All 30-Day Modules

Module 6: Malware Threats (Week 13-14)

- Types of malware: Trojans, viruses, worms, APTs
- Malware analysis: Static and dynamic techniques
- **Practical Lab:** Analyzing malware using sandboxes like Cuckoo Sandbox

Module 7: Social Engineering (Week 15-16)

- Social engineering tactics: Phishing, baiting, pretexting, tailgating
- Recognizing and defending against social engineering attacks
- **Practical Lab:** Simulating social engineering attacks (phishing emails, pretexting)

Module 8: Hacking Web Servers and Applications (Week 17-20)

- Web server vulnerabilities: HTTP response splitting, DoS attacks
- Tools: Nikto, Burp Suite for web server testing
- **Practical Lab:** Hacking a vulnerable web server and implementing hardening techniques

Module 9: Web Application Vulnerabilities (Week 19-20)

- OWASP Top 10 vulnerabilities (XSS, SQL Injection, CSRF)
- Tools for web application hacking: Burp Suite, Acunetix, OWASP ZAP
- **Practical Lab:** Web application penetration testing (SQL Injection, XSS)

60 Days - Advanced Ethical Hacking Techniques

Includes All 45-Day Modules

Module 10: Wireless Network Hacking (Week 21-22)

- Wireless protocols: WEP, WPA, WPA2, WPA3
- Cracking wireless networks with Aircrack-ng
- **Practical Lab:** Hacking wireless networks using Aircrack-ng and implementing security protocols

Module 11: IoT and Cloud Security (Week 23-24)

- IoT vulnerabilities and attacks, Operational Technology security issues
- Cloud security risks and tools for platforms like AWS, Azure
- **Practical Lab:** Securing IoT devices and auditing cloud environments

90 Days - Professional Ethical Hacking

Includes All 60-Day Modules

Module 12: Advanced Malware and Evasion Techniques (Week 25-28)

- Advanced malware techniques: Fileless malware, APTs
- Evasion of Antivirus and IDS
- **Practical Lab:** Evasion techniques and malware persistence

Module 13: Advanced System Hacking Techniques (Week 29-32)

- Privilege escalation: Windows/Linux
- Maintaining access: Backdoors, Web Shells
- **Practical Lab:** Post-exploitation techniques on Windows and Linux

Module 14: Penetration Testing Methodology and Reporting (Week 33-36)

- Structured penetration testing methodologies (PTES, OWASP)
- Writing and presenting penetration testing reports
- **Practical Lab:** Create detailed penetration test reports for web apps and systems

Module 15: Final Project and Exam Preparation (Week 37-40)

- Full penetration testing engagement from start to finish
- Mock exams and practice with real-world scenarios
- **Practical Lab:** Full mock exam simulation

180 Days - Master Ethical Hacking

Includes All 90-Day Modules

Module 16: Red Teaming and Adversary Simulation (Week 41-44)

- Simulating Advanced Persistent Threats (APT)
- Red teaming tactics and attack simulation

- **Practical Lab:** Conduct red team exercises and simulate APTs

Module 17: Ethical Hacking Automation and Scripting (Week 45-48)

- Automating tasks using Python and Bash for penetration testing
- Writing custom scripts for vulnerability scanning and exploitation
- **Practical Lab:** Write automation scripts for common penetration testing tasks

Module 18: Career Development and Certification (Week 49-52)

- Preparing for certifications (CEH, OSCP, CISSP)
- Building a portfolio and penetration testing resume
- **Practical Lab:** Mock exams, resume building, and interview preparation

Final Week: Exam Preparation and Review

- Full mock exam simulation
- Review of all modules and techniques
- **Practical Lab:** Resolve doubts and clarify questions