

## 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)