Ethical Hacking Training

Duration: 06 weeks – (05 days a week class)

EMPOWERIC
Empowering Youth and Businesses

Week 1: Introduction to Ethical Hacking

Day 1: Understanding Ethical Hacking

- Definition of ethical hacking
- Differences between ethical hacking, penetration testing, and malicious hacking
- The role of an ethical hacker in cybersecurity
- Overview of legal and ethical considerations in hacking

Day 2: Information Security Fundamentals

- Core concepts of information security (confidentiality, integrity, availability)
- Common security principles and policies
- Types of threats and vulnerabilities
- Understanding cybersecurity frameworks and standards (ISO 27001, NIST, etc.)

Day 3: Cybersecurity Laws and Regulations

- Overview of cybersecurity laws (CFAA, GDPR, etc.)
- Ethical guidelines and compliance frameworks
- Legal implications of ethical hacking
- Discussion on responsible disclosure

Day 4: Methodologies and Tactics

- Overview of ethical hacking methodologies (PTES, OWASP, NIST)
- Understanding the phases of ethical hacking: Reconnaissance, Scanning, Gaining Access, Maintained Access, and Coverage
- Tools and technologies used in each phase

Day 5: Setting Up the Lab Environment

- Introduction to virtual lab environment using tools such as VirtualBox or VMware
- Installation of necessary software: Kali Linux, Metasploit Framework, Wireshark, Burp Suite
- Configuration of a vulnerable environment for experimentation

Week 2: Reconnaissance and Footprinting

Day 6: Techniques for Information Gathering

- Passive vs. active reconnaissance
- Tools for information gathering (Nmap, Recon-ng, theHarvester)
- Social engineering basics

Day 7: Open-Source Intelligence (OSINT)

- Understanding OSINT and its role in ethical hacking
- OSINT tools and techniques (Maltego, Shodan)

Day 8: Network Footprinting

- Techniques for network footprinting
- Identifying network ranges and IP addresses
- Using toolsets for network discovery

Day 9: Website Footprinting

- Techniques for gathering information from websites
- Analyzing website structure and technologies (BuiltWith, Netcraft)

Day 10: Practical Lab Session

- Hands-on lab to conduct footprinting on pre-defined targets
- Documentation and reporting of findings

Week 3: Scanning and Enumeration

Day 11: Introduction to Scanning

- Understanding the scanning process
- Types of scanning techniques (ping scans, port scans, service scans)

Day 12: Network Scanning Tools

- In-depth exploration of Nmap and its advanced features
- Using Netcat for network exploration

Day 13: Vulnerability Scanning

- Understanding vulnerability scanning vs. penetration testing
- Tools for vulnerability scanning (Nessus, OpenVAS)
- Analyzing scan results

Day 14: Enumeration Techniques

- Understanding the significance of enumeration
- Techniques for gathering detailed information
- Tools for enumeration (Enum.exe, SNMP, LDAP)

Day 15: Practical Lab Session

- Conducting scanning and enumeration on designated targets
- Compiling a report detailing vulnerabilities discovered

Week 4: Gaining Access

Day 16: Exploitation Fundamentals

- Overview of exploitation techniques
- Understanding system vulnerabilities and exploits

Day 17: Web Application Attacks

- Introduction to OWASP Top Ten vulnerabilities
- SQL injection, Cross-Site Scripting (XSS), and Server-Side Request Forgery (SSRF)

Day 18: Social Engineering Tactics

- Techniques and methodologies used in social engineering
- Case studies of social engineering attacks

Day 19: Wireless Network Attacks

- Understanding wireless security protocols (WEP, WPA, WPA2)
- Tools for cracking wireless passwords (Aircrack-ng, Wireshark)

Day 20: Practical Lab Session

- Hands-on exploitation exercises based on learned techniques
- Special focus on web applications and social engineering scenarios

Week 5: Maintaining Access and Covering Tracks

Day 21: Post-Exploitation Techniques

- Understanding the post-exploitation phase
- Tools for maintaining access (Netcat, reverse shells)

Day 22: Data Exfiltration Techniques

- Methods for exfiltration of sensitive data from compromised systems
- Importance of stealth and data concealment

Day 23: Clearing Footprints

- Techniques to erase traces of intrusion
- Understanding logs and log management

Day 24: Incident Response

- Overview of incident response strategies
- Understanding the roles of ethical hackers during an incident

Day 25: Practical Lab Session

- Engaging in a capture-the-flag (CTF) exercise focusing on maintaining access and track-covering techniques

Week 26: Reporting and Best Practices

Day 1: Reporting Vulnerabilities

- Importance of clear and actionable reporting
- Structure of an ethical hacking report
- Tools for reporting vulnerabilities (Dradis, Serpico)

Day 27: Remediation and Recommendations

- Understanding risk management techniques
- Strategies for vulnerability remediation
- Discussing common pitfalls in security practices

Day 28: Ethical Hacking Best Practices

- Best practices for ethical hackers
- Techniques to stay updated with trends in cybersecurity

Day 29: Course Review and Q&A

- Recap of key areas covered in the course
- Open forum for student questions and clarifications

Day 30: Final Assessment and Certification

- Conducting a practical and theoretical final assessment
- Issuance of certificates to successful participants
- Discussion on further learning paths and certifications in ethical hacking (CEH, OSCP, etc.)