**Ethical Hacking**

**Course Goal:** To equip students with the practical skills and knowledge necessary to perform ethical hacking and penetration testing using Kali Linux, understand attack methodologies, and implement defensive security measures.

**Target Audience:** Individuals interested in cybersecurity, aspiring penetration testers, security analysts, IT professionals, and anyone looking to understand and mitigate security vulnerabilities.

**Prerequisites:** Basic understanding of computer systems, networking concepts, and familiarity with command-line interfaces (though the course will cover essential Linux commands).

**Module 1: Introduction to Cybersecurity (Brief Overview)**

* **Defining Cybersecurity:** Threats, vulnerabilities, and assets.
* **The CIA Triad:** Confidentiality, Integrity, Availability.
* **Types of Cyberattacks:** Malware, phishing, DDoS, etc.
* **Introduction to Ethical Hacking:** Definition, scope, and importance.
* Legal and Ethical Considerations in Cybersecurity.
* **Different Roles in Cybersecurity:** Security Analyst, Penetration Tester, Security Engineer, etc.

**Module 2: Networking Fundamentals (Essential for Hacking)**

* **TCP/IP Model and OSI Model:** Layers and their functions.
* **IP Addressing:** IPv4 and IPv6, subnetting.
* **DNS:** How it works, common records.
* **DHCP:** IP address allocation process.
* **Common Network Protocols:** HTTP/HTTPS, FTP, SSH, SMTP, etc.
* **Network Devices:** Routers, switches, firewalls, and their basic functions.
* Network Topologies.
* Introduction to Network Scanning.

**Module 3: Linux for Hackers (Kali Linux Focus)**

* **Introduction to Kali Linux:** Philosophy, tools, and usage.
* **Setting up a Kali Linux Environment:** Installation (Virtual Machine, Dual Boot).
* **Basic Linux Commands:** Navigation, file manipulation, user management, permissions.
* **Package Management:** Using `apt` for installing, updating, and removing software.
* **Working with Shells:** Bash scripting basics for automation.
* **Essential Kali Linux Tools Overview:** Categorization and basic usage introduction.
* Customization and Configuration of Kali Linux.

**Module 4: Web Technologies for Hackers (Understanding Attack Surfaces)**

* **How Web Applications Work:** Client-server model, HTTP/HTTPS requests and responses.
* **Front-end Technologies:** HTML, CSS, JavaScript (basic understanding for analysis).
* **Back-end Technologies:** Introduction to common server-side languages (e.g., PHP, Python, Java) and frameworks.
* **Databases:** Basic understanding of SQL and NoSQL databases.
* **Web Servers:** Apache, Nginx (basic configuration and common vulnerabilities).
* **Introduction to Common Web Vulnerabilities:** OWASP Top 10 (SQL Injection, XSS, etc.).

**Module 5: Programming for Cybersecurity (Scripting and Tool Development)**

* **Introduction to Python:** Syntax, data types, control flow, functions.
* **Python for Networking:** Socket programming basics.
* **Python for Web Interactions:** Using libraries like `requests` and `Beautiful Soup`.
* **Scripting for Automation:** Automating repetitive tasks in penetration testing.
* **Basic Understanding of Other Relevant Languages:** Bash scripting (covered in Linux), and potentially an introduction to C for understanding low-level exploits.

**Module 6: Ethical Hacking: Attack Techniques**

* **Information Gathering (Reconnaissance):** Passive and active reconnaissance.
* **Scanning and Enumeration:** Port scanning, service enumeration, OS fingerprinting.
* **Vulnerability Analysis:** Identifying weaknesses in systems and applications.
* **Exploitation:** Understanding different types of exploits and their mechanisms.
* **Post-Exploitation:** Maintaining access, lateral movement, privilege escalation.
* **Social Engineering:** Principles and techniques.
* **Web Application Attacks:** Detailed exploration of OWASP Top 10 vulnerabilities.
* **Database Attacks:** SQL Injection and other database-related vulnerabilities.
* **Password Attacks:** Cracking techniques, password spraying.
* **Wireless Attacks:** Wi-Fi sniffing, WEP/WPA/WPA2 cracking.
* **Reverse Engineering:** Basic concepts of analyzing software for vulnerabilities.
* **Sniffing and Spoofing:** Intercepting and manipulating network traffic.

**Module 7: Defensive Security (Understanding Countermeasures)**

* **Firewalls:** Principles of operation, rule sets.
* Intrusion Detection and Prevention Systems (IDS/IPS).
* **Endpoint Security:** Antivirus, EDR solutions.
* Security Information and Event Management (SIEM) systems.
* **Access Control Mechanisms:** Authentication and authorization.
* Security Policies and Procedures.
* Basic Hardening Techniques for Operating Systems and Applications.

**Module 8: Penetration Testing (Putting it All Together)**

* **Penetration Testing Methodologies:** PTES, OWASP Testing Guide, NIST.
* Scoping and Rules of Engagement.
* Planning and Preparation.
* Information Gathering and Reconnaissance (Practical exercises).
* Vulnerability Scanning and Analysis (Using tools).
* Exploitation and Post-Exploitation (Hands-on labs).
* Maintaining Persistence and Lateral Movement.
* Documenting Findings and Reporting.

**Module 9: Cryptography (Understanding Security Mechanisms)**

* **Basic Cryptographic Concepts:** Encryption, decryption, keys, algorithms.
* Symmetric vs. Asymmetric Cryptography.
* Hashing Algorithms.
* Digital Signatures and Certificates.
* **Common Cryptographic Protocols:** TLS/SSL, SSH, VPN.
* Vulnerabilities in Cryptographic Implementations.

**Module 10: Cybersecurity Tools & Platforms (Kali Linux Focus - Detailed)**

* **Information Gathering:** `nmap`, `hping3`, `dig`, `whois`, `theHarvester`, `recon-ng`, `fierce`, `dnsrecon`, `amass`.
* **Vulnerability Analysis:** `nessus` (community version), `openvas`, `nikto`, `dirb`, `w3af`, `sqlmap`, `arachni`.
* **Web Application Analysis:** Burp Suite (Community Edition), OWASP ZAP, `skipfish`.
* **Database Assessment:** `sqlmap`, `sqlninja`.
* **Password Attacks:** `hydra`, `medusa`, `john the ripper`, `hashcat`, `cewl`.
* **Wireless Attacks:** `aircrack-ng` suite ( `airodump-ng`, `aireplay-ng`, `aircrack-ng`).
* **Reverse Engineering:** `ghidra`, `binwalk`, `strings`, `ltrace`, `strace`.
* **Exploitation Tools:** Metasploit Framework (`msfconsole`, `msfvenom`), Exploit-DB, searchsploit.
* **Sniffing & Spoofing:** `wireshark`, `tcpdump`, `ettercap`, `arpspoof`.
* **Post Exploitation:** Metasploit Meterpreter, `ssh`, `scp`.
* **Forensics:** `autopsy`, `sleuthkit`, `binwalk`.
* **Reporting Tools:** Dradis Framework, MagicTree.
* **Social Engineering Tools:** `setoolkit` (Social-Engineer Toolkit).

**Module 11: Reporting (Communicating Findings)**

* Importance of Clear and Concise Reporting.
* Structure of a Penetration Testing Report: Executive summary, methodology, findings, recommendations, conclusion.
* Classifying and Prioritizing Vulnerabilities (CVSS).
* Providing Actionable Remediation Advice.
* Using Reporting Tools (brief introduction to Dradis or similar).

**Services:**

1. Vulnerability Assessment
2. Penetration Testing (Pen Testing)
3. Web Application Penetration Testing
4. Network Penetration Testing
5. Mobile Application Penetration Testing
6. API Penetration Testing
7. Cloud Security Assessments
8. Social Engineering Assessments
9. Wireless Security Audits
10. Database Security Assessments
11. Security Auditing
12. Vulnerability Management Consulting
13. Security Awareness Training
14. Incident Response Consulting (Basic Level)
15. Security Tool Implementation and Configuration (Basic Level)
16. Technical Report Writing

**Certification:**

**Entry-Level/Foundational:**

* CompTIA Security+
* EC-Council Certified Ethical Hacker (CEH)

**Intermediate/Advanced:**

* Offensive Security Certified Professional (OSCP)
* eLearnSecurity Professional Penetration Tester (eCPPT)
* GIAC Penetration Tester (GPEN)
* CREST Practitioner Security Analyst (CPSA)
* CREST Registered Penetration Tester (CRT)

**Specialized (Can be Entry to Advanced depending on focus):**

* Certified Cloud Security Professional (CCSP)
* GIAC Web Application Penetration Tester (GWAPT)
* GIAC Mobile Device Security Analyst (GMOB)
* Certified Information Systems Security Professional (CISSP)