KIAN TECHNOLOGIES

The Cyebrsecurity & Ethical Hacking Institute

HACK THE SYSTEM. SECURE THE FUTURE

IT SECURITY & ETHICAL HACKING

BEGINNER TO PRO

Master the fundamentals of cybersecurity with in-depth, hands-on training

KIAN Technologies

GET 25% OFF ON OUR EXCLUSIVE CYBERSECURITY COURSES!

We see ethical hacking as the key to mastering cybersecurity—learning how systems work, identifying vulnerabilities, and strengthening defenses to create a safer digital world.

IT Security & Ethical Hacking Beginner to Pro

Duration: 4 Months (96 Sessions | 6 Sessions per Week)

Course Description: The IT Security & Ethical Hacking: Beginner to Pro course is an extensive, hands-on program designed to take learners from the fundamentals of cybersecurity to advanced penetration testing techniques. Covering network security, reconnaissance, exploitation, malware analysis, red teaming, and digital forensics, this course provides real-world experience with industry-standard tools like Kali Linux, Metasploit, Nmap, Wireshark, and Burp Suite. Participants will develop practical skills in ethical hacking while learning security best practices to defend against cyber threats.

This course is structured to align with industry certifications and cybersecurity trends, ensuring up-to-date knowledge and skills. Course content may be updated periodically to maintain accuracy and relevance. Whether you are a beginner or an aspiring cybersecurity professional, this course is your gateway to a career in ethical hacking.

Month 1: Foundations of Ethical Hacking

Week 1: Introduction to Ethical Hacking and Networking Basics

Session 1: Ethical Hacking Overview and Career Path

- What is Ethical Hacking?
- Types of Hackers (White, Black, Grey Hat)
- Importance of Ethical Hacking in Cybersecurity
- Career Path in Ethical Hacking

Session 2: Types of Hackers and Cyber Attacks

- Different Categories of Hackers
- Common Cyber Attacks (MITM, Phishing, DoS/DDoS)
- Real-World Examples of Cyber Attacks

Session 3: Networking Basics

- Understanding IP, DNS, MAC Addresses
- Basics of Subnetting
- Role of Networking in Ethical Hacking

Session 4: Protocols and Communication

- Overview of TCP/IP, HTTP, HTTPS, FTP, SSH
- How Protocols are Exploited in Cyber Attacks

Session 5: Lab Setup for Ethical Hacking

- Installing Kali Linux and Virtual Machines
- Setting Up Networking Tools
- Introduction to the Terminal and Basic Commands

Session 6: Quiz and Practical Lab
- Recap of Key Concepts
- Hands-on Lab Practice
- Q&A Session

Week 2: OSI Model and Network Security

Session 7: OSI Model and its Layers
- Understanding OSI Model and Network Layers
- Importance of Each Layer in Security

Session 8: Packet Analysis with Wireshark
- Introduction to Packet Capturing
- Hands-on Wireshark Analysis

Session 9: Firewalls, VPNs, IDS/IPS Basics
- Role of Firewalls in Cybersecurity
- VPNs and Their Importance
- IDS vs. IPS: Understanding Differences

Session 10: Basics of Cryptography
- Hashing and Encryption Basics
- Symmetric vs. Asymmetric Encryption

Session 11: Introduction to Cybersecurity Frameworks
- Overview of NIST, ISO 27001, OWASP
- How Frameworks Improve Security

Session 12: Quiz and Lab Practice
- Recap of Network Security Concepts
- Hands-on Practical Labs
- Q&A and Discussion

Week 3: Information Gathering and Reconnaissance

Session 13: OSINT (Open-Source Intelligence) Tools
- Introduction to OSINT
- Using Shodan, Maltego for Recon

Session 14: Google Dorking and Social Media Recon
- Using Google Dorking for Advanced Search
- Social Media Footprinting Techniques

Session 15: DNS Reconnaissance and Whois Lookup
- Understanding DNS Records
- Whois Lookup for Domain Information

Session 16: Lab: Information Gathering Practice
- Hands-on Practice with OSINT Tools
- Analyzing Real-World Scenarios

Session 17: Scanning Networks with Nmap and Zenmap
- Introduction to Network Scanning
- Understanding Nmap and Zenmap Features

Session 18: Quiz and Practical Exercises
- Recap and Hands-on Practice
- Case Study Discussion
- Q&A and Discussion

Week 4: Vulnerability Scanning and Enumeration

Session 19: Introduction to Vulnerability Scanning
- Tools: OpenVAS, Nessus
- Identifying Security Weaknesses

Session 20: Common Vulnerabilities (CVE, CVSS)
- Understanding CVE and CVSS
- Exploiting Known Vulnerabilities

Session 21: Enumeration Basics
- SMB, SNMP, LDAP Enumeration Techniques
- Extracting Data from Network Services

Session 22: Network Mapping and Service Discovery
- Identifying Open Ports and Services
- Practical Enumeration Exercises

Session 23: Lab: Recon and Scanning on Simulated Targets
- Practical Hands-on Lab
- Ethical Use of Reconnaissance Techniques

Session 24: Recap, Quiz, and Practice
- Summary of Key Learnings
- Hands-on Evaluation
- Final Q&A

Month 2: System Hacking and Web Application Attacks

Week 5: Exploiting Systems

Session 25: Introduction to Exploits and Payloads
- Understanding Vulnerabilities and Exploits
- Types of Exploits and Payloads
- Ethical Considerations of Exploitation

Session 26: Basics of Metasploit Framework
- Introduction to Metasploit
- Running Basic Exploits
- Hands-on Lab with Metasploit

Session 27: Exploiting Windows Systems
- Gaining Initial Access
- Privilege Escalation Techniques
- Post-Exploitation and Maintaining Access

Session 28: Exploiting Linux Systems
- Common Linux Vulnerabilities
- SSH Exploits and Privilege Escalation
- Practical Exploitation Lab

Session 29: Bypassing Firewalls and Antivirus
- Techniques for Evasion
- Creating Undetectable Payloads
- Hands-on Evasion Techniques

Session 30: Quiz and Lab Practice
- Recap of System Hacking Techniques
- Hands-on Exploitation Challenges
- Q&A and Discussion

Week 6: Password Cracking and Wireless Hacking

Session 31: Password Cracking with Hashcat and John the Ripper
- Understanding Password Hashes
- Cracking Passwords using Hashcat & John
- Hands-on Password Cracking Lab

Session 32: Brute-Force Attacks and Dictionary Attacks
- Understanding Brute-Force Attacks
- Using Wordlists for Dictionary Attacks
- Best Practices for Strong Passwords

Session 33: Wireless Networks: WEP/WPA/WPA2 Basics
- Understanding Wireless Security Protocols
- Identifying Weaknesses in Wireless Networks
- Ethical Hacking Practices for Wi-Fi

Session 34: Cracking Wi-Fi Passwords with Aircrack-ng
- Capturing and Cracking Handshakes
- Hands-on Wireless Hacking Lab

Session 35: Rogue Access Points and MITM on Wireless Networks
- Understanding Rogue APs and Evil Twins
- MITM Attacks on Wi-Fi
- Defending Against Wireless Attacks

Session 36: Quiz and Practical Lab
- Recap and Hands-on Challenges
- Ethical Considerations in Wireless Attacks
- Q&A and Discussion

Week 7: Web Application Hacking - Part 1

Session 37: Introduction to Web Application Security
- Understanding Web Application Architecture
- Common Web Security Vulnerabilities
- Ethical Hacking in Web Security

Session 38: OWASP Top 10 Overview
- Understanding OWASP Top 10 Security Risks
- Examples and Real-World Case Studies
- Best Practices for Web Security

Session 39: SQL Injection (SQLi) Attacks
- Understanding SQL Injection Techniques
- Exploiting SQLi Vulnerabilities
- Hands-on SQLi Lab

Session 40: Cross-Site Scripting (XSS) Attacks
- Types of XSS Attacks (Reflected, Stored, DOM-Based)
- Exploiting XSS Vulnerabilities
- Hands-on XSS Lab

Session 41: Hands-on Web Hacking Challenges
- Simulated Web Hacking Scenarios
- Practicing Exploitation Techniques
- Ethical Considerations in Web Hacking

Session 42: Quiz and Lab Practice
- Recap of Web Security Topics
- Hands-on Web Security Challenges
- Q&A and Discussion

Week 8: Web Application Hacking - Part 2

Session 43: Cross-Site Request Forgery (CSRF) Attacks
- Understanding CSRF Attacks
- Exploiting CSRF Vulnerabilities
- Hands-on CSRF Lab

Session 44: Security Misconfigurations and Broken Authentication
- Identifying and Exploiting Security Misconfigurations
- Understanding Authentication and Session Management Issues
- Hands-on Security Misconfiguration Lab

Session 45: Web Application Enumeration and Burp Suite Basics
- Introduction to Burp Suite for Web Testing
- Enumerating Web Applications for Vulnerabilities
- Practical Burp Suite Lab

Session 46: Server-Side Request Forgery (SSRF) and File Inclusion Attacks
- Understanding SSRF and LFI/RFI Attacks
- Exploiting Server-Side Vulnerabilities
- Hands-on SSRF and File Inclusion Lab

Session 47: Hands-on Web Penetration Testing
- Applying Web Security Concepts in Real-World Scenarios
- Simulated Web Penetration Testing Challenges
- Ethical Considerations and Defensive Measures

Session 48: Quiz and Final Web Security Lab
- Recap of Web Application Hacking Topics
- Hands-on Web Security Challenges
- Q&A and Discussion

Month 3: Advanced Exploitation and Malware Analysis

Week 9: Advanced System Exploitation

Session 49: Privilege Escalation Techniques on Windows/Linux
- Identifying Privilege Escalation Opportunities
- Exploiting Weak Permissions and Misconfigurations
- Hands-on Privilege Escalation Labs

Session 50: Post-Exploitation: Persistence and Backdoors
- Maintaining Access on Compromised Systems
- Creating Persistent Backdoors
- Advanced Post-Exploitation Techniques

Session 51: Data Exfiltration Techniques
- Methods of Extracting Sensitive Information
- Evading Detection during Data Theft
- Hands-on Exfiltration Lab

Session 52: Exploiting Misconfigured Services (SMB, FTP, etc.)
- Identifying Misconfigurations
- Exploiting Unsecured Network Services
- Hands-on Exploitation Scenarios

Session 53: Advanced Lab on Exploitation
- Simulated Red Teaming Exercise
- Applying Exploitation Techniques in a Realistic Environment
- Report Writing and Documentation

Session 54: Quiz and Lab Practice
- Recap of Exploitation Techniques
- Hands-on Challenges and Q&A

Week 10: Malware and Payload Development

Session 55: Creating Custom Payloads with Metasploit
- Writing and Modifying Payloads
- Generating Undetectable Malware
- Hands-on Custom Payload Lab

Session 56: Understanding Malware Types (Trojans, Ransomware, Rootkits)
- Classification of Malware
- Real-World Malware Case Studies
- Techniques for Identifying Malware

Session 57: Malware Analysis Basics
- Static vs. Dynamic Malware Analysis
- Tools and Techniques for Malware Research
- Hands-on Malware Analysis Lab

Session 58: Reverse Engineering Malware
- Introduction to Reverse Engineering
- Disassembling and Debugging Malware
- Hands-on Reverse Engineering Exercises

Session 59: Tools: Strings, Ghidra, and IDA Basics
- Using Open-Source Tools for Reverse Engineering
- Extracting Hidden Information from Binaries
- Practical Lab on Malware Deconstruction

Session 60: Quiz and Lab Practice
- Recap and Hands-on Malware Analysis Challenges
- Ethical Considerations and Case Studies
- Q&A and Discussion

Week 11: Advanced Web Exploitation

Session 61: Server-Side Template Injection (SSTI) Attacks
- Understanding SSTI Vulnerabilities
- Exploiting SSTI in Various Frameworks
- Hands-on SSTI Lab

Session 62: NoSQL Injection and Deserialization Attacks
- Exploiting NoSQL Injection in MongoDB
- Understanding and Exploiting Deserialization Vulnerabilities
- Practical Lab on NoSQL and Deserialization Attacks

Session 63: Web Cache Poisoning and Business Logic Flaws
- Understanding Web Cache Poisoning
- Identifying and Exploiting Business Logic Flaws
- Hands-on Web Security Lab

Session 64: Advanced Lab on Web Exploitation
- Simulated Real-World Web Attacks
- Applying Advanced Web Exploitation Techniques
- Ethical Considerations and Remediation

Session 65: Capture the Flag (CTF) Challenge - Web Security
- Engaging in Web Security CTF Challenges
- Applying Skills from Previous Sessions

- Hands-on CTF Practice

Session 66: Quiz and Recap
- Reviewing Key Web Exploitation Concepts
- Hands-on Practical Challenges
- Q&A and Discussion

Week 12: Advanced System and Network Attacks

Session 67: Advanced Network Attacks and BGP Hijacking
- Understanding Advanced Network Exploitation
- BGP Hijacking and Route Manipulation
- Practical Network Attacks Lab

Session 68: Zero-Day Vulnerabilities and Exploit Development
- Introduction to Zero-Day Exploits
- Exploit Development Basics
- Hands-on Exploit Writing Lab

Session 69: Advanced Wireless Attacks (Wi-Fi & Bluetooth)
- Exploiting Modern Wireless Technologies
- Attacking Bluetooth and IoT Devices
- Hands-on Wireless Exploitation Lab

Session 70: Cloud Security Attacks and Misconfigurations
- Identifying Cloud-Based Security Risks
- Exploiting Cloud Misconfigurations
- Hands-on Cloud Security Lab

Session 71: Capture the Flag (CTF) Challenge - Advanced Attacks
- Engaging in Advanced Exploitation CTF Challenges
- Applying Skills from Previous Modules
- Hands-on CTF Practice

Session 72: Quiz and Recap
- Reviewing Advanced System and Network Attacks
- Hands-on Practical Challenges
- Q&A and Discussion

Month 4: Red Teaming, Defense, and Career Development

Week 13: Red Team vs Blue Team

Session 73: Red Teaming Basics and Simulated Attacks
- Understanding Red Teaming Methodologies
- Running Simulated Attacks on Secure Environments
- Ethical Boundaries in Red Teaming

Session 74: Blue Team Strategies: Defense-in-Depth
- Defensive Security Techniques
- Log Analysis and Threat Hunting
- Hands-on Blue Team Defense Lab

Session 75: Using SIEM Tools for Threat Detection
- Introduction to SIEM and Threat Intelligence
- Analyzing Attack Logs for Incident Detection
- Hands-on SIEM Lab

Session 76: Practical Red Team vs Blue Team Exercise
- Simulated Attack-Defense Exercise
- Strategies for Offensive and Defensive Teams

- Debrief and Analysis of Results

Session 77: Incident Response Simulation
- Real-Time Incident Handling Scenarios
- Steps to Contain and Mitigate Attacks
- Hands-on Response Exercise

Session 78: Quiz and Case Study
- Recap of Red Team vs. Blue Team Strategies
- Hands-on Cybersecurity Defense Scenarios
- Ethical and Legal Implications Discussion

Week 14: Full Penetration Testing

Session 79: Planning a Penetration Test (Scoping and Rules of Engagement)
- Understanding the Penetration Testing Process
- Legal and Ethical Boundaries
- Writing a Scope and Engagement Plan

Session 80: Conducting Reconnaissance and Exploitation
- Using OSINT and Scanning Techniques
- Executing Exploits and Gaining Access
- Hands-on Penetration Testing Lab

Session 81: Post-Exploitation and Reporting
- Extracting and Analyzing Data
- Writing Reports for Clients and Organizations
- Best Practices for Documenting Findings

Session 82: Writing Professional Penetration Test Reports
- Structuring Reports for Technical and Non-Technical Audiences
- Providing Recommendations and Risk Assessments
- Hands-on Report Writing Exercise

Session 83: Lab: Conducting a Penetration Test on a Simulated Network
- Real-World Penetration Testing Scenario
- Applying Skills from the Course in a Practical Environment
- Hands-on Evaluation

Session 84: Recap and Feedback
- Review of Key Takeaways
- Q&A and Course Adjustments Based on Feedback

Week 15: Career Guidance and Project Completion

Session 85: Certifications Overview: CEH, OSCP, etc.
- Understanding Cybersecurity Certifications
- Preparing for Certification Exams
- Choosing the Right Certification for Your Career Path

Session 86: Building a Cybersecurity Resume and Portfolio
- Creating an Effective Resume for Cybersecurity Roles
- Showcasing Skills and Projects Online
- Portfolio Development Strategies

Session 87: Mock Interviews for Cybersecurity Roles
- Common Interview Questions and Best Practices
- Technical and Behavioral Interview Preparation
- Hands-on Mock Interview Sessions

Session 88: Final Hands-On Project: Full Cybersecurity Assessment
- Conducting an End-to-End Cybersecurity Assessment

- Identifying and Mitigating Vulnerabilities
- Writing a Professional Security Report

Session 89: Project Presentations and Feedback

- Presenting Findings to a Panel
- Receiving Constructive Feedback
- Refining Cybersecurity Analysis Skills

Session 90: Certification Test

- Final Course Assessment
- Evaluating Knowledge Across All Modules
- Certification Awarded Upon Completion

Week 16: Closing and Beyond

Session 91: Final Recap of Key Concepts

- Summarizing Course Content
- Addressing Final Questions and Concerns
- Industry Insights and Trends

Session 92: Q&A Session with Industry Experts

- Engaging with Experienced Cybersecurity Professionals
- Gaining Career Advice and Guidance

Session 93: Certificate Ceremony

- Awarding Completion Certificates
- Celebrating Achievements

Session 94: Career and Networking Tips

- Strategies for Job Hunting and Career Growth
- Leveraging Online Platforms for Networking

Session 95: Introduction to Advanced Topics (OSCP/Red Teaming Overview)

- Exploring Advanced Cybersecurity Certifications
- Next Steps for Continuous Learning

Session 96: Course Conclusion and Feedback

- Final Discussion and Takeaways
- Gathering Feedback for Future Improvements