HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

PROFESSIONAL COURSE

Ethical Hacking Specialist

(H|EHS)

Detailed Course Curriculum

Skills and knowledge to identify and address computer system and network vulnerabilities.



DURATION
6 Months

CURRICULUM
4 Levels

MODULES
39 Modules

OUTCOMES
239 Learning Outcomes

MASTERING THE CYBER FLOW

www.hackinetix.com | info@hackinetix.com

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

COURSE OVERVIEW

Course Overview

Hackinetix's Introduction to the Ethical Hacking Specialist course will equip aspiring cybersecurity professionals with the skills and knowledge to identify and address computer systems and network vulnerabilities. This comprehensive program covers the fundamental and advanced concepts of ethical hacking, offering a blend of theoretical insights and hands-on experience.

6 Months
Duration

4
Levels

39
Modules

239
Learning Outcomes

Who Should Enroll in this Program?

For a wide spectrum of people who want to learn more about ethical hacking or advance their careers in cybersecurity, the Ethical Hacking Specialist program is perfect. The following outlines who ought to think about signing up for this program:

- **IT Professionals**
- **All levels of IT auditor**
- **Technical support engineers**

PROGRAM ELIGIBILITY CRITERIA

Eligibility & Prerequisites

01 Proficiency in using computers, including installing software, managing files, and navigating graphical user interfaces, is necessary. Participants should be comfortable with using a variety of software tools and applications.

02 Prior knowledge of any programming language is recommended but not mandatory.

Course Roadmap

4 levels · 39 modules · 239 learning outcomes

01 **Fundamentals of Networking** — 4 Modules · 17 Learning Outcomes — p. 05

02 **Kali Linux Essentials** — 8 Modules · 46 Learning Outcomes — p. 07

03 **Ethical Hacking** — 17 Modules · 109 Learning Outcomes — p. 09

04 **Penetration Testing** — 10 Modules · 67 Learning Outcomes — p. 13

PROGRAM OUTCOMES

Program Outcomes

01	Understand the core principles of ethical hacking and the role of ethical hackers in protecting information systems.
02	Articulate the differences between ethical hacking, penetration testing, and malicious hacking.
03	Utilize open-source intelligence (OSINT) tools and methods to identify potential security weaknesses.
04	Utilize vulnerability scanners to identify and prioritize potential security issues in networked systems.
05	Execute advanced techniques to exploit vulnerabilities in operating systems and network services.
06	Conduct attacks on wireless networks (e.g., cracking WEP/WPA encryption) to assess security measures.
07	Collect and preserve evidence, document incidents, and communicate findings to stakeholders.
08	Proficiently use industry-standard ethical hacking and penetration testing tools, including Nmap, Metasploit, Burp Suite, and Wireshark.
09	Create detailed and actionable security reports that communicate findings, risk assessments, and recommendations.
10	Use practical simulations and real-world case studies to apply ethical hacking skills in varied scenarios.
11	Demonstrate the ability to adapt and apply learned techniques to new and evolving security challenges.

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 01

Fundamentals of Networking

01

This is a comprehensive introduction to modern computer networks' essential concepts and technologies. It is designed to equip learners with a solid foundation in networking principles, protocols, and practices, enabling them to effectively understand, design, and troubleshoot network systems.

Key Learning Outcomes

- Define key networking concepts such as networks, nodes, and network topologies.
- Explain the OSI (Open Systems Interconnection) and TCP/IP (Transmission Control Protocol/Internet Protocol) models.
- Understand services such as DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), and NAT (Network Address Translation).
- Identify and describe fundamental networking protocols including TCP, IP, UDP, and HTTP.
- Describe the functions and roles of network devices such as routers, switches, hubs, and access points.
- Tools and utilities such as ping, traceroute, and netstat are used to analyze network performance.

Curriculum

4 modules · 17 learning outcomes

01 Concepts of Networking

- LO 1 What is a Computer Network
- LO 2 Types of Computer Networks
- LO 3 Networking Devices
- LO 4 Client Server Model
- LO 5 Server-Client-based Networks

02 OSI Model and TCP/IP Model

- LO 1 OSI Model Introduction
- LO 2 TCP/IP Model Introduction
- LO 3 Three-Way Handshake and SSL/TLS Handshake

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 01

Fundamentals of Networking

Curriculum (continued)

03 Internet Protocols

- LO 1 Types of Internet Protocols
- LO 2 Internet Security Protocols
- LO 3 Types of Internetworks
- LO 4 Network Layer Protocols
- LO 5 IPSec Protocol
- LO 6 Network Control Protocol (NCP)

04 Remote Services (Telnet and SSH)

- LO 1 Introduction to Remote Services
- LO 2 Remote Desktop Protocol
- LO 3 What is Telnet and SSH

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 02

Kali Linux Essentials

02

This section introduces participants to Kali Linux, a powerful and versatile operating system designed for penetration testing and cybersecurity tasks. This section covers the fundamental aspects of Kali Linux, including its installation, configuration, and core tools. Participants will gain hands-on experience with the operating system's features and capabilities, preparing them to use Kali Linux effectively in various ethical hacking scenarios.

Key Learning Outcomes

- Successfully installed Kali Linux on different platforms, including virtual machines and physical hardware.
- Understand the purpose and application of these tools in penetration testing and security assessments.
- Execute common administrative tasks such as updating the system, managing users, and configuring network settings.
- Install additional tools and packages to extend the functionality of Kali Linux.
- Understand the file system structure and manage files and directories in Kali Linux.
- Identify and use key security tools pre-installed in Kali Linux, such as Nmap, Metasploit, and Wireshark.
- Learn how to leverage Kali Linux tools for various stages of a penetration test, including reconnaissance, scanning, and exploitation.

Curriculum

8 modules · 46 learning outcomes

01 Getting Started with Kali Linux

- LO 1 Introduction to Kali Linux
- LO 2 Installation of Kali Linux
- LO 3 Navigating Kali Linux and Exploring Kali Linux Tools

02 Accessing the Command Line (CLI)

- LO 1 Understand the Command Line Interface's (CLI) Role
- LO 2 Navigate the Command Line Environment and Execute Basic Commands
- LO 3 Utilize Command Line Utilities and Tools
- LO 4 Text Manipulation
- LO 5 Understand and Utilize the File System
- LO 6 Practice Command Line Skills

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 02

Kali Linux Essentials

Curriculum (continued)

03 Managing Local Users and Groups

- LO 1 Understand User and Group Concepts
- LO 2 Create and Manage User Accounts and Groups
- LO 3 Manage User and Group Memberships
- LO 4 Implement User Account Policies
- LO 5 Understand System Files Related to User and Group Management

04 Controlling Access to Files and Directory

- LO 1 Understand File Permissions Basics
- LO 2 Interpret File Permissions
- LO 3 Modify File Permissions
- LO 4 Manage File Ownership
- LO 5 Configure Access Control Lists (ACLs)
- LO 6 Understand and Use Advanced Permissions Tools

05 Monitoring and Managing Linux Processes

- LO 1 Understand Linux Process Concepts
- LO 2 View and Analyse Running Processes
- LO 3 Manage Process Lifecycle
- LO 4 Control Process Priority
- LO 5 Automating Tasks and Job Scheduling
- LO 6 Practice Process Management Tasks
- LO 7 Understand and Use Advanced Process Management Tools

06 Debian Package Management

- LO 1 Introduction to APT
- LO 2 Basic Package Interaction
- LO 3 Advanced APT Configuration and Usage
- LO 4 Package Reference: Digging Deeper into the Debian Package
- LO 5 Configuration Scripts

08 Bash Scripting

- LO 1 Introduction to Bash Shell Scripting
- LO 2 Variables
- LO 3 If, Else, Elif Statement
- LO 4 Boolean Logical Operations
- LO 5 Loops
- LO 6 Functions
- LO 7 Tasks

07 Configuring Kali Linux and Securing SSH

- LO 1 Configuring the Network
- LO 2 Configuring and Managing Services
- LO 3 Start and Manage SSH Service
- LO 4 Set Up SSH Key-Based Authentication
- LO 5 Configure and Use SSH Agent and Forwarding
- LO 6 Troubleshoot SSH Connectivity and Configuration Issues
- LO 7 Understand Advanced SSH Features

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 03

Ethical Hacking

03

Ethical hacking and penetration testing aims to give participants the cutting-edge abilities and expertise needed to carry out exhaustive and successful penetration tests in a range of IT settings. Using industry-standard tools and methodology, this part focuses on the practical implementation of ethical hacking techniques, such as vulnerability assessment, exploitation, and post-exploitation strategies.

Key Learning Outcomes

- Techniques for footprinting and scanning, including DNS enumeration, network mapping, and social engineering tactics.
- Testing for SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and other common web vulnerabilities.
- Assessing wireless network security configurations and identifying potential weaknesses.
- Performing comprehensive vulnerability scans using tools like Nessus, OpenVAS, and Qualys.
- Capturing and cracking WPA/WPA2 encryption using tools like Aircrack-ng and Reaver.

Curriculum

17 modules · 109 learning outcomes

01 Introduction to Ethical Hacking and Cybersecurity

- LO 1 Understand Cybersecurity Fundamentals
- LO 2 Recognize the Legal and Ethical Implications
- LO 3 Introduction to Penetration Testing
- LO 4 Understand the Ethical Hacking Process
- LO 5 Learn About Common Tools and Techniques
- LO 6 Recognize the Importance of Security Policies and Procedures
- LO 7 Explore Career Paths in Cybersecurity
- LO 8 Understand Emerging Trends and Challenges

02 Reconnaissance and Foot-Printing

- LO 1 Understand Reconnaissance and Foot-Printing
- LO 2 Distinguish Between Active and Passive Reconnaissance
- LO 3 Perform Passive Reconnaissance
- LO 4 Conduct Active Reconnaissance
- LO 5 Use Foot-Printing Techniques
- LO 6 Analyze and Interpret Reconnaissance Data
- LO 7 Understand Legal and Ethical Considerations
- LO 8 Utilize Reconnaissance Tools and Resources
- LO 9 Apply Reconnaissance Skills in Practical Scenarios

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 03

Ethical Hacking

Curriculum (continued)

03 In-depth Network Scanning

- LO 1 Understand Network Scanning Fundamentals
- LO 2 Explore Different Types of Network Scanning
- LO 3 Use Network Scanning Tools
- LO 4 Conduct Comprehensive Port Scanning
- LO 5 Implement Advanced Scanning Techniques
- LO 6 Perform OS and Service Fingerprinting
- LO 7 Understand Network Scanning Best Practices

04 Enumeration User Identification

- LO 1 Understand Enumeration and User Identification
- LO 2 Learn Enumeration Techniques
- LO 3 Perform User Enumeration on Windows and Linux Systems
- LO 4 Understand Directory and Network Resource Enumeration
- LO 5 Use Enumeration Tools and Scripts
- LO 6 Implement Security Measures Based on Enumeration Findings
- LO 7 Apply Enumeration Skills in Practical Scenarios

05 System Hacking Password Cracking & Bypassing

- LO 1 Understand System Hacking Basics
- LO 2 Learn Password Cracking Fundamentals
- LO 3 Explore Password Cracking Techniques
- LO 4 Utilize Password Cracking Tools
- LO 5 Understand Password Hashing Algorithms
- LO 6 Implement Password Cracking Strategies
- LO 7 Apply Password Cracking and Bypassing Skills in Practical Scenarios

06 Malware Threats

- LO 1 Understand the Fundamentals of Malware
- LO 2 Understand Computer Viruses and Worms
- LO 3 Explore Trojans and Backdoor
- LO 4 Analyze the Impact of Viruses and Worms
- LO 5 Examine Malware Detection Techniques
- LO 6 Understand Malware Prevention Strategies
- LO 7 Explore Case Studies of Notable Viruses and Worms
- LO 8 Understand Legal and Ethical Considerations

07 Spoofing and Sniffing

- LO 1 Understand Spoofing and Sniffing Basics
- LO 2 Explore Spoofing Techniques
- LO 3 Learn Sniffing Techniques
- LO 4 Implement Spoofing Detection and Prevention
- LO 5 Implement Sniffing Detection and Prevention
- LO 6 Apply Spoofing and Sniffing Skills in Practical Scenarios

08 Social Engineering

- LO 1 Understand Social Engineering Fundamentals
- LO 2 Learn About Social Engineering Tactics
- LO 3 Develop Incident Response Plans
- LO 4 Apply Social Engineering Skills in Practical Scenarios

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 03

Ethical Hacking

Curriculum (continued)

09 Denial of Service DOS & DDOS Attacks

- LO 1 Understand DoS and DDoS Fundamentals
- LO 2 Explore DDoS Attacks
- LO 3 Detect and Monitor DoS and DDoS Attacks
- LO 4 Implement Prevention and Mitigation Strategies

10 Session Hijacking

- LO 1 Understand Session Hijacking Fundamentals
- LO 2 Learn About Session Hijacking Techniques
- LO 3 Explore Common Session Hijacking Attack Vectors
- LO 4 Analyze the Impact of Session Hijacking
- LO 5 Implement Detection and Prevention Strategies

11 SQL Injection

- LO 1 Understand SQL Injection Fundamentals
- LO 2 Learn About SQL Injection Types
- LO 3 Explore Common SQL Injection Vulnerabilities
- LO 4 Identify SQL Injection Attack Vectors

12 Hacking Web Servers Server Rooting

- LO 1 Understand Web Server Fundamentals
- LO 2 Identify Common Web Server Vulnerabilities
- LO 3 Perform Information Gathering and Enumeration
- LO 4 Exploit Web Server Vulnerabilities
- LO 5 Gain Unauthorized Access and Privileges
- LO 6 Root a Web Server
- LO 7 Use Tools and Techniques for Server Rooting

13 Hacking Wireless Network

- LO 1 Understand Wireless Network Fundamentals
- LO 2 Explore Wireless Network Protocols and Standards
- LO 3 Perform Wireless Network Scanning and Enumeration
- LO 4 Exploit Wireless Network Vulnerabilities
- LO 5 Conduct Wireless Network Attacks
- LO 6 Implement Wireless Network Security Measures
- LO 7 Use Tools and Techniques for Wireless Network Testing

14 Evading IDS, Firewall

- LO 1 Understand IDS and Firewall Fundamentals
- LO 2 Explore IDS and Firewall Mechanisms
- LO 3 Identify Common Evasion Techniques
- LO 4 Implement Evasion Techniques
- LO 5 Analyze IDS and Firewall Logs
- LO 6 Perform Evasion Testing
- LO 7 Develop Defensive Strategies
- LO 8 Implement Monitoring and Response Mechanisms

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 03

Ethical Hacking

Curriculum (continued)

15 Cryptography

- LO 1 Understand Cryptography Fundamentals
- LO 2 Explore Types of Cryptographic Algorithms
- LO 3 Study Key Management Practices
- LO 4 Implement Encryption and Decryption Techniques
- LO 5 Explore Cryptographic Protocols and Applications
- LO 6 Analyze Cryptographic Security
- LO 7 Apply Cryptographic Techniques in Real-World Scenarios

16 Internet of Things (IoT) Hacking

- LO 1 IoT Concepts
- LO 2 Identify IoT Security Risks and Vulnerabilities
- LO 3 Perform IoT Device Discovery and Reconnaissance
- LO 4 Conduct Vulnerability Assessment and Exploitation
- LO 5 Test IoT Communication and Data Security
- LO 6 Develop and Implement IoT Security Strategies

17 Cyber Forensics

- LO 1 Understand Cyber Forensics Fundamentals
- LO 2 Understand Legal and Ethical Considerations
- LO 3 Utilize Forensic Tools and Techniques
- LO 4 Identify and Preserve Digital Evidence
- LO 5 Conduct Incident Response

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 04

Penetration Testing

04

This module serves as an introduction to the fundamental concepts and practices of penetration testing. Students will explore the ethical hacking landscape, learning how to assess the security of systems, networks, and applications through systematic testing. The module covers key methodologies, tools, and techniques penetration testers use to identify vulnerabilities and evaluate security controls.

Key Learning Outcomes

- Techniques for privilege escalation on various operating systems, including Linux and Windows.
- Gain experience in performing comprehensive web application and wireless network security tests.
- Master advanced techniques in ethical hacking and penetration testing.
- Understanding the ethical responsibilities and legal implications of penetration testing.
- Produce effective reports and documentation to communicate findings and recommendations.
- Develop proficiency in using industry-standard tools for vulnerability assessment and exploitation.

Curriculum

10 modules · 67 learning outcomes

01 Vulnerability Management

- LO 1 Understand Vulnerability Management
- LO 2 Identify Vulnerability Management Components
- LO 3 Conduct Vulnerability Scanning
- LO 4 Assess and Analyze Vulnerabilities
- LO 5 Implement Remediation Strategies
- LO 6 Develop a Vulnerability Management Policy
- LO 7 Understand Compliance and Reporting Requirements
- LO 8 Apply Vulnerability Management Skills in Practical Scenarios

02 Scripting Basics for Pentesting

- LO 1 Understand the Role of Scripting in Penetration Testing
- LO 2 Learn Basic Scripting Languages
- LO 3 Develop Basic Python Scripts
- LO 4 Create and Use Bash Scripts
- LO 5 Write PowerShell Scripts
- LO 6 Utilize Scripting for Network Scanning and Information Gathering
- LO 7 Apply Scripting Skills in Practical Scenarios
- LO 8 Explore Advanced Scripting Techniques

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 04

Penetration Testing

Curriculum (continued)

03 Network Penetration Testing

- LO 1 Understand Network Penetration Testing
- LO 2 Plan and Scope a Penetration Test
- LO 3 Conduct Reconnaissance and Footprinting
- LO 4 Perform Network Scanning and Enumeration
- LO 5 Exploit Network Vulnerabilities
- LO 6 Assess Network Security Controls
- LO 7 Practice Post-Exploitation Techniques
- LO 8 Stay Updated with Emerging Threats and Tools
- LO 9 Follow Legal and Ethical Guidelines
- LO 10 Apply Network Penetration Testing Skills in Real-World Scenarios

04 Mobile Application Penetration Testing

- LO 1 Understand Mobile Application Security Fundamentals
- LO 2 Explore Mobile Platform Attacks Vectors
- LO 3 Test Mobile Application Security Controls
- LO 4 Identify and Exploit Common Mobile Vulnerabilities

05 Active Directory Penetration Testing

- LO 1 Understand Active Directory (AD) Fundamentals
- LO 2 Explore Active Directory Architecture and Components
- LO 3 Identify and Enumerate Active Directory Components
- LO 4 Exploit Common Active Directory Vulnerabilities
- LO 5 Conduct Penetration Testing on Active Directory

06 Web Application Penetration Testing

- LO 1 Understand Web Application Security Fundamentals
- LO 2 Conduct Information Gathering and Reconnaissance
- LO 3 Common Web Application Vulnerabilities OWASP Top 10 and SANS 25
- LO 4 Explore Web Application Security Threats
- LO 5 Execute Exploitation Techniques on Web
- LO 6 Implement Secure Coding Practices
- LO 7 Apply Web Security Testing and Assessment
- LO 8 Understand Compliance and Regulatory Standards
- LO 9 Implement Web Application Security Controls

07 Metasploit

- LO 1 Understand Metasploit Framework Fundamentals
- LO 2 Set Up and Configure the Metasploit Environment
- LO 3 Conduct Penetration Tests with Metasploit
- LO 4 Develop Custom Exploits and Payloads
- LO 5 Utilize Metasploit for Post-Exploitation Activities
- LO 6 Leverage Auxiliary and Meterpreter Commands

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 04

Penetration Testing

Curriculum (continued)

08 Privilege Escalation (Windows and Linux)

- LO 1 Understand the Concept of Privilege Escalation
- LO 2 Identify Vulnerabilities Leading to Privilege Escalation
- LO 3 Differentiate Between Vertical and Horizontal Privilege Escalation
- LO 4 Perform Windows Privilege Escalation Techniques
- LO 5 Perform Linux/Unix Privilege Escalation Techniques
- LO 6 Bypass User Access Controls and Security Mechanisms

09 Cloud Security

- LO 1 Understand Cloud Computing Fundamentals
- LO 2 Explore Cloud Security Concepts and Principles
- LO 3 Assess Cloud Security Risks and Threats
- LO 4 Implement Cloud Security Controls
- LO 5 Secure Cloud Infrastructure and Services

10 Cyber Security Compliance

- LO 1 Understand Cyber Security Compliance Fundamentals
- LO 2 Explore Key Cyber Security Regulations and Standards
- LO 3 Assess Compliance Requirements for Different Sectors
- LO 4 Implement Cyber Security Controls for Compliance
- LO 5 Develop and Maintain Compliance Documentation
- LO 6 Implement and Monitor Compliance Programs

HACKINETIX ACADEMY

MASTERING THE CYBER FLOW

START YOUR JOURNEY

Ready to Start Your Cybersecurity Journey?

Join Ethical Hacking Specialist (H|EHS) and build practical cybersecurity skills across all levels.

ENROLL NOW →



CONTACT US

www.hackinetix.com

info@hackinetix.com

Join Our WhatsApp Channel