HACKANICS™

H|EHS
Ethical Hacking Specialist

Unlock Your Cybersecurity Potential
with Our Ethical Hacking Specialist Course

ethical hacking <
penetration testing<
potential security weaknesses<
Utilize vulnerability scanners<
exploit vulnerabilities<
open-source intelligence<

www.hackanics.com

HACKANICS™

H|EHS
Ethical Hacking Specialist

ABOUT COURSE

Hackanics 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.

HACKANICS™

H|EHS
Ethical Hacking Specialist

PROGRAM OUTCOMES

- Articulate the differences between ethical hacking, penetration testing, and malicious hacking.
- Utilize open-source intelligence (OSINT) tools and methods to identify potential security weaknesses.
- Utilize vulnerability scanners to identify and prioritize potential security issues in networked systems.
- Execute advanced techniques to exploit vulnerabilities in operating systems and network services.
- Use practical simulations and real-world case studies to apply ethical hacking skills in varied scenarios.

H|EHS
Ethical Hacking Specialist

ELIGIBILITY CRITERIA AND PREREQUISITES

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.

Enroll Now

WHO SHOULD ENROLL IN THIS PROGRAM?

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 & applications.

- IT Professionals
- All levels of IT auditor
- Technical support engineers
- Students and Graduates in IT/Computer Science

HACKANICS™

H|EHS
Ethical Hacking Specialist

Level - 1

FUNDAMENTALS OF NETWORKING

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

HACKANICS™

H|EHS
Ethical Hacking Specialist

Level - 1

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 various network devices such as routers, switches, hubs, and access points.
- To analyze network performance, use network tools and utilities such as ping, traceroute, and netstat.

H|EHS
Ethical Hacking Specialist

Level - 1

CURRICULUM

MODULE 1 : 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

MODULE 2: 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

H|EHS
Ethical Hacking Specialist

Level - 1

CURRICULUM

MODULE 3: INTERNET PROTOCOLS

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

MODULE 4: REMOTE SERVICES (TELNET AND SSH)

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

HACKANICS™

H|EHS

Ethical Hacking Specialist

Level - 2

KALI LINUX ESSENTIALS

This section introduces participants to Kali Linux, a powerful and versatile operating system specifically 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 in various ethical hacking scenarios effectively.

HACKANICS™

H|EHS
Ethical Hacking Specialist

Level - 2

KEY LEARNING OUTCOMES

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

H|EHS
Ethical Hacking Specialist

Level - 2

CURRICULUM

MODULE 1: 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.

MODULE 2: 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.

HACKANICS™

H|EHS
Ethical Hacking Specialist

Level - 2

CURRICULUM

MODULE 3: 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

MODULE 4: MANAGE FILE AND DIRECTORY ACCESS

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

H|EHS
Ethical Hacking Specialist

Level - 2

CURRICULUM

MODULE 5: 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

MODULE 6: DEBIAN PACKAGE MANAGEMENT

- LO1: 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

H|EHS
Ethical Hacking Specialist

Level - 2

CURRICULUM

MODULE 7: CONFIGURING KALI LINUX & SECURING SSH

- LO 1: Configuring the Network
- LO 2: Configuring and Managing Services
- LO 3: Start and Manage SSH Service
- LO 5: Configure and Use SSH Agent and Forwarding:
- LO 6: Troubleshoot SSH Connectivity & Configuration Issues
- LO 7: Understand Advanced SSH Features

MODULE 8: 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: Scenario Based Programs.

HACKANICS™

H|EHS
Ethical Hacking Specialist

Level - 3

ETHICAL HACKING

This module provides a comprehensive introduction to **ETHICAL HACKING**, focusing on the principles, practices, and techniques used to identify and address **security vulnerabilities** in systems and networks. Students will learn about the mindset of **ethical hackers** and the importance of ethical considerations in **cybersecurity**.

H|EHS
Ethical Hacking Specialist

Level - 3

KEY LEARNING OUTCOMES

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

HACKANICS™

H|EHS
Ethical Hacking Specialist

Level - 3

CURRICULUM

MODULE 1: INTRODUCTION TO ETHICAL HACKING

- 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

MODULE 2: RECONNAISSANCE AND FOOT-PRINTING

- LO 1: Understand Reconnaissance and Foot-Printing
- LO 2: Distinguish Between Active and Passive Reconnaissance
- LO 3: Perform Active & Passive Reconnaissance
- LO 4: Use Foot-Printing Techniques

- LO 5: Analyze and Interpret Reconnaissance Data
- Lo 6: Understand Legal and Ethical Considerations
- LO 8: Utilize Reconnaissance Tools and Resources
- LO 9: Apply Reconnaissance Skills in Practical Scenarios

MODULE 3: 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

HACKANICS™

H|EHS
Ethical Hacking Specialist

Level - 3

CURRICULUM

MODULE 4: 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

MODULE 5: SYSTEM HACKING

- 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 & Bypassing Skills in Practical Scenarios

MODULE 6: MALWARE THREATS

- LO 1: Understand the Fundamentals of Malware
- LO 2: Understand Computer Viruses & 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

MODULE 7: 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 & Prevention
- LO 5: Implement Sniffing Detection & Prevention
- LO 6: Apply Spoofing and Sniffing Skills in Practical Scenarios

MODULE 8: 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

HACKANICS™

H|EHS

Ethical Hacking Specialist

Level - 3

CURRICULUM

MODULE 9: DOS & DDOS ATTACKS

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

MODULE 10: SESSION HIJACKING

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

CURRICULUM

MODULE 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

MODULE 12: HACKING WEB SERVERS

- LO 1: Understand Web Server Fundamentals
- LO 2: Identify Common Web Server Vulnerabilities
- LO 3: Perform Information Gathering & 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

H|EHS
Ethical Hacking Specialist

Level - 3

CURRICULUM

MODULE 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 TestingTesting

MODULE 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

MODULE 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

CURRICULUM

MODULE 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

MODULE 17: CYBER FORENSICS

- LO 1: Understand Cyber Forensics Fundamentals
- LO 2: Conduct Network Forensics
- LO 3: Utilize Forensic Tools and Techniques:

HACKANICS™

H|EHS

Ethical Hacking Specialist

Level - 4

PENETRATION TESTING

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.

HACKANICS™

H|EHS

Ethical Hacking Specialist

Level - 4

KEY LEARNING OUTCOMES

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

H|EHS
Ethical Hacking Specialist

Level - 4

CURRICULUM

MODULE 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

MODULE 02: SCRIPTING BASICS FOR PENTESTING

- LO 1: Understand the Role of Scripting
- 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 & Information Gathering
- LO 7: Apply Scripting Skills in Practical Scenarios
- LO 8: Explore Advanced Scripting Techniques:

MODULE 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

H|EHS
Ethical Hacking Specialist

Level - 4

CURRICULUM

- LO 9: Follow Legal and Ethical Guidelines
- LO 10: Apply Network Penetration Testing Skills in Real-World Scenarios

MODULE 04: MOBILE APP 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

MODULE 05: AD 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

MODULE 06: WEB 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

H|EHS
Ethical Hacking Specialist

Level - 4

CURRICULUM

MODULE 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

MODULE 08:PRIVILEGE ESCALATION

- 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

MODULE 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

H|EHS
Ethical Hacking Specialist

Level - 4

CURRICULUM

MODULE 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

H|EHS
Ethical Hacking Specialist

ABOUT US

One of the most reputable and trustworthy companies for information and **cybersecurity** training is **Hackanics**, which offers businesses and individuals all around the world unparalleled, hands-on training. Our mission is to assist, guide, and train you in your cybersecurity profession.

Hackanics supports industry growth through education, training, certifications, philanthropy, and market research. It also works to develop a highly skilled workforce and is dedicated to fostering an environment that fosters innovation and ensures that everyone can take advantage of the opportunities and benefits that come with technology.

HACKANICS™

Elevate your security skills

LEARN. PROTECT. CONQUER

contact@hackanics.com

www.hackanics.com