HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

PROFESSIONAL COURSE

Ethical Hacking Mastery

(H|EHM)

Detailed Course Curriculum

From Beginner to Professional in Ethical Hacking.
Levels, modules and learning outcomes at a glance.



DURATION
4 Months

CURRICULUM
8 Levels

MODULES
46 Modules

OUTCOMES
310 Learning Outcomes

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

COURSE OVERVIEW

Course Overview

Hackinetix's Ethical Hacking Mastery is an advanced course designed to provide comprehensive training in the art and science of ethical hacking and penetration testing. Participants will gain expertise in identifying, exploiting, and mitigating vulnerabilities in various systems, including networks, web applications, and wireless networks. The course covers key areas such as network scanning, vulnerability assessment, system exploitation, and advanced techniques for penetration testing. Through hands-on labs, real-world case studies, and practical exercises, learners will develop the skills to conduct thorough security assessments and improve organizational security postures while adhering to ethical and legal standards.

4 Months
Duration

8
Levels

46
Modules

310
Learning Outcomes

Who Should Enroll in this Program?

The Ethical Hacking Mastery program is designed for individuals interested in advanced cybersecurity skills and careers in ethical hacking and penetration testing. Here's a detailed breakdown of who should consider enrolling:

IT and Security Professionals

Cybersecurity Specialists

Students and Recent Graduates

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

PROGRAM ELIGIBILITY CRITERIA

Eligibility & Prerequisites

01 Basic Understanding

Familiarity with basic networking concepts and operating systems (Windows and Linux) is important.

02 Networking Concepts

Understanding of fundamental networking concepts, including IP addressing, network topologies, and common protocols (e.g., TCP/IP, HTTP, DNS).

03 Windows and Linux

Basic knowledge of navigating and using Windows and Linux operating systems.

04 Security Basics

Basic knowledge of cybersecurity principles, including common threats, vulnerabilities, and protective measures.

Course Roadmap

8 levels · 46 modules · 310 learning outcomes

01 **Introduction to Cybersecurity** — 6 Modules · 40 Learning Outcomes — p. 06

02 **Web Application Security** — 7 Modules · 47 Learning Outcomes — p. 08

03 **Threat Intelligence and VAPT** — 9 Modules · 54 Learning Outcomes — p. 10

04 **Scripting for Security** — 4 Modules · 30 Learning Outcomes — p. 13

05 **Security Operations Architecture and Detection** — 7 Modules · 53 Learning Outcomes — p. 15

06 **API Pentesting** — 6 Modules · 43 Learning Outcomes — p. 17

07 **Network Penetration Testing** — 4 Modules · 25 Learning Outcomes — p. 19

08 **Android Penetration Testing** — 3 Modules · 18 Learning Outcomes — p. 21

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

PROGRAM OUTCOMES

Program Outcomes

01 Mastery of Ethical Hacking Techniques

- **Advanced Knowledge**
  Gain deep understanding and expertise in ethical hacking methodologies, tools, and techniques.
- **Practical Skills**
  Develop hands-on experience in conducting penetration tests, exploiting vulnerabilities, and assessing system security.

02 Proficiency in Security Assessments

- **Network Security**
  Ability to perform comprehensive network scans, identify security weaknesses, and apply remediation strategies.
- **Web Application Security**
  Skill in evaluating and exploiting web applications to uncover vulnerabilities such as SQL Injection and Cross-Site Scripting (XSS).
- **Wireless Security**
  Expertise in assessing and securing wireless networks against common threats and attacks.

03 Competency in Using Ethical Hacking Tools

- **Tool Utilization**
  Proficiency in using popular ethical hacking tools and frameworks, including Nmap, Metasploit, Burp Suite, and Wireshark.
- **Tool Customization**
  Ability to configure and customize tools for specific testing scenarios and security assessments.

04 Advanced Exploitation Techniques

- **Exploitation Skills**
  Develop the capability to exploit complex vulnerabilities and perform advanced attacks.
- **Privilege Escalation**
  Expertise in techniques for gaining elevated privileges and maintaining access in compromised systems.

PROGRAM OUTCOMES

Program Outcomes

Continued

05 Effective Vulnerability Management

- **Risk Assessment**
  Ability to conduct thorough vulnerability assessments and identify potential security risks.
- **Remediation Strategies**
  Skill in developing and implementing remediation strategies to address identified vulnerabilities.

06 Knowledge of Legal and Ethical Standards

- **Legal Compliance**
  Understanding of relevant laws and regulations governing ethical hacking and penetration testing.
- **Ethical Conduct**
  Commitment to ethical standards and professional conduct in security assessments.

07 Preparation for Industry Certifications

- **Certification Readiness**
  Preparation for advanced industry certifications, such as Certified Ethical Hacker (CEH) or CompTIA Security +.
- **Career Advancement**
  Enhanced qualifications for careers in cybersecurity and ethical hacking.

08 Continuous Learning and Adaptation

- **Emerging Trends**
  Awareness of emerging trends, technologies, and advancements in the field of ethical hacking.
- **Ongoing Development**
  Commitment to continuous learning and professional development in cybersecurity.

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 01

Introduction to Cybersecurity

01

This Section serves as a foundational overview of Cybersecurity, introducing students to essential concepts, terminology, and practices that are critical in protecting information systems. Participants will learn about the various types of cyber threats, including malware, phishing, and denial-of-service attacks, along with risk management principles, security policies, and compliance frameworks. The course emphasizes the importance of network security, data protection, and incident response strategies. Through case studies and real-world examples, students will gain insights into the evolving cybersecurity landscape and the roles and responsibilities of cybersecurity professionals. By the end of the module, learners will have a solid understanding of cybersecurity fundamentals and the significance of safeguarding digital assets.

Key Learning Outcomes

- Understanding Cybersecurity Fundamentals
- Cybersecurity Policies and Compliance
- Basic Cybersecurity Skills and Practices
- Professional and Ethical Considerations
- Knowledge of Cybersecurity Domains
- Risk Management and Assessment
- Awareness of Emerging Threats and Trends

Curriculum

6 modules · 40 learning outcomes

01 Key Elements of CyberSecurity

- LO 1 Understand Core Cybersecurity Principles
- LO 2 Analyze Risk in Cyber Systems
- LO 3 Define and Map the Attack Surface
- LO 4 Classify and Prioritize Threats
- LO 5 Develop Mitigation and Response Strategies
- LO 6 Integrate Cybersecurity into System Design

02 Defense-In-Depth, Authentication, and Authorization

- LO 1 Understand the Concept of Layered Security
- LO 2 Evaluate Multi-Layered Defense Strategies
- LO 3 Design and Implement Layered Security
- LO 4 Explore Authentication Mechanisms
- LO 5 Implement Robust Authentication Solutions
- LO 6 Distinguish Between Authentication and Authorization
- LO 7 Implement Access Control Models
- LO 8 Integrate Authorization into System Design

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 01

Introduction to Cybersecurity

Curriculum (continued)

03 AAA Services

- LO 1 Understand the Core Components of AAA
- LO 2 Explore the Importance of AAA in Security
- LO 3 Implement AAA Protocols
- LO 4 Analyze Use Cases for AAA in Modern Networks
- LO 5 Mitigate Risks in AAA Implementations

04 Cybersecurity Governance and Strategy

- LO 1 Explore the Importance of a Cybersecurity Strategy
- LO 2 Develop Security Policies and Standards
- LO 3 Assess Regulatory and Compliance Requirements
- LO 4 Define Roles and Responsibilities
- LO 5 Integrate Risk Management into Governance
- LO 6 Plan Incident Response and Recovery

05 Risk Management

- LO 1 Understand the Fundamentals of Risk Management
- LO 2 Identify Cybersecurity Risks
- LO 3 Conduct Risk Assessments
- LO 4 Develop Risk Mitigation Strategies
- LO 5 Apply Risk Management Frameworks
- LO 6 Incorporate Risk Management into Decision-Making
- LO 7 Evaluate the Impact of Emerging Technologies on Risk

06 Compliance in Cybersecurity

- LO 1 Understand the Role of Compliance in Cybersecurity
- LO 2 Identify Key Cybersecurity Regulations and Standards
- LO 3 Align Cybersecurity Policies with Compliance Requirements
- LO 4 Implement Compliance Monitoring Processes
- LO 5 Mitigate Risks of Non-Compliance
- LO 6 Understand the Role of Data Protection in Compliance
- LO 7 Adapt to Evolving Compliance Requirements
- LO 8 Communicate Compliance Goals to Stakeholders

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 02

Web Application Security

02

This Section provides a comprehensive overview of Web Application Security, focusing on identifying, analyzing, and mitigating security vulnerabilities in web applications. Students will learn about common vulnerabilities as outlined in the OWASP Top Ten, including SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). The course emphasizes both static and dynamic testing techniques, utilizing tools such as Burp Suite and OWASP ZAP for vulnerability scanning and exploitation. Participants will engage in hands-on labs to practice secure coding practices and remediation strategies, ensuring they can effectively protect web applications against evolving threats. By the end of the module, students will have a solid understanding of web security principles and the skills to conduct security assessments of web applications.

Key Learning Outcomes

- Understanding Application Security Fundamentals
- Web Application Security Mechanisms
- Compliance and Best Practices
- Identifying and Mitigating Vulnerabilities
- Web Application Security Testing

Curriculum

7 modules · 47 learning outcomes

01 Information Gathering

- LO 1 Introduction to Information Gathering
- LO 2 Passive Information Gathering
- LO 3 Active Information Gathering
- LO 4 Social Engineering Techniques
- LO 5 Analysing and Interpreting Collected Data
- LO 6 OSINT Tools

02 Burp Suite for Web Security

- LO 1 Intercepting and Modifying Traffic
- LO 2 Automated Crawling and Mapping
- LO 3 Automated Attacks and Brute Force
- LO 4 Manual Testing and Exploitation
- LO 5 Burp Suite Decoder & Comparer
- LO 6 Burp Suite for API Security Testing
- LO 7 Manual Web Application Penetration Testing with Burp Suite
- LO 8 Burp Suite Reporting and Collaboration
- LO 9 Advanced Burp Suite Techniques

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 02

Web Application Security

Curriculum (continued)

03 Top 10 Web Application Security Risks

- LO 1 Injection Attacks
- LO 2 Broken Authentication
- LO 3 Sensitive Data Exposure
- LO 4 XML External Entities (XXE)
- LO 5 Broken Access Control
- LO 6 Security Misconfiguration
- LO 7 Cross-Site Scripting (XSS)
- LO 8 Insecure Deserialization
- LO 9 Using Components with Known Vulnerabilities
- LO 10 Insufficient Logging & Monitoring

04 Identifying Unknown Vulnerabilities

- LO 1 Understanding Unknown Vulnerabilities
- LO 2 Techniques for Identifying Unknown Vulnerabilities
- LO 3 Key Indicators of Unknown Vulnerabilities
- LO 4 Vulnerability Discovery Process
- LO 5 Reporting and Patching
- LO 6 Tools for Identifying Unknown Vulnerabilities
- LO 7 Preventing Unknown Vulnerabilities

05 Cryptography and Authentication

- LO 1 Introduction to Cryptography
- LO 2 Cryptographic Concepts
- LO 3 Types of Cryptography
- LO 4 Hashing
- LO 5 Digital Signatures and Certificates
- LO 6 Authentication
- LO 7 Authentication Protocols

06 Security Misconfigurations

- LO 1 Introduction to Security Misconfigurations
- LO 2 Types of Security Misconfigurations
- LO 3 Common Causes of Security Misconfigurations
- LO 4 Best Practices for Preventing Security Misconfigurations
- LO 5 Tools for Identifying and Fixing Security Misconfigurations

07 Incident Response for Web Application Security

- LO 1 Incident Response Lifecycle
- LO 2 Common Web Application Security Incidents
- LO 3 Tools and Techniques for Incident Response

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 03

Threat Intelligence and VAPT

03

This Section explores the integration of Threat Intelligence with Vulnerability Assessment and Penetration Testing (VAPT) to enhance an organization's cybersecurity posture. Students will learn how to gather, analyze, and apply threat intelligence to identify and prioritize vulnerabilities effectively. The course covers key concepts in vulnerability assessment methodologies, including scanning, risk assessment, and reporting, alongside hands-on penetration testing techniques. Participants will gain insights into the lifecycle of threat intelligence, the use of threat feeds, and the correlation between threat intelligence and vulnerability management. By the end of the module, students will be equipped to leverage threat intelligence to inform VAPT efforts and improve overall security strategies.

Key Learning Outcomes

- Understanding Threat Intelligence
- Integrating Threat Intelligence into Security Operations
- Penetration Testing (PT)
- Threat Intelligence Collection and Analysis
- Vulnerability Assessment (VA)
- Reporting and Documentation

Curriculum

9 modules · 54 learning outcomes

01 Introduction to Penetration Testing & Types

- LO 1 What is Penetration Testing?
- LO 2 Types of Penetration Testing
- LO 3 Penetration Testing Methodology

02 Manual and Automated Scanning

- LO 1 Automated Scanning Tools & Techniques
- LO 2 Manual Scanning Tools & Techniques
- LO 3 Combining Manual and Automated Scanning

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 03

Threat Intelligence and VAPT

Curriculum (continued)

03 Types of Security Vulnerability

- LO 1 Software Vulnerabilities
- LO 2 Network Vulnerabilities
- LO 3 Authentication and Access Control Vulnerabilities
- LO 4 Configuration Vulnerabilities
- LO 5 Social Engineering Vulnerabilities
- LO 6 Zero-Day Vulnerabilities

04 Malware and Its Type

- LO 1 Introduction & Types of Malwares
- LO 2 Malware Analysis Techniques
- LO 3 Tools for Malware Analysis and Detection
- LO 4 Malware Mitigation and Prevention

05 Vulnerability Assessment & Management Tools

- LO 1 What Is a Vulnerability Assessment?
- LO 2 Seeking Out Vulnerabilities
- LO 3 Detecting Vulnerabilities via Security Technologies
- LO 4 The Importance of Seeking Out Vulnerabilities
- LO 5 Using a Vulnerability Assessment Tools
- LO 6 Open Source and Free Vulnerability Management Tools
- LO 7 Managed Vulnerability Services
- LO 8 Common Vulnerabilities and Exposures (CVE)

06 Using the Metasploit Framework

- LO 1 Introduction to Metasploit Framework
- LO 2 Information Gathering Using Metasploit
- LO 3 Exploiting Vulnerabilities
- LO 4 Payloads and Post-Exploitation
- LO 5 Custom Exploits and Scripting
- LO 6 Evading Detection
- LO 7 Web Application Exploitation with Metasploit
- LO 8 Social Engineering with Metasploit

07 Privileges Escalation on Windows and Linux

- LO 1 Introduction to Privilege Escalation
- LO 2 Privilege Escalation on Windows Systems
- LO 3 Privilege Escalation on Linux Systems
- LO 4 Automated Privilege Escalation Tools
- LO 5 Privilege Escalation in Cloud Environments
- LO 6 Privilege Escalation in Containers

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 03

Threat Intelligence and VAPT

Curriculum (continued)

08 Cloud Penetration Testing

- LO 1 Enumeration & Reconnaissance in Cloud Environments
- LO 2 Identity and Access Management (IAM) Testing
- LO 3 Exploiting Cloud Misconfigurations
- LO 4 Testing Serverless and Containers in the Cloud
- LO 5 Exploiting Cloud-Specific Vulnerabilities
- LO 6 Network Penetration Testing in Cloud
- LO 7 Cloud Security Tools and Automation
- LO 8 Post-Exploitation and Data Extraction

09 Threat Intelligence (Cyber Kill Chain / Diamond Model)

- LO 1 Introduction to Threat Intelligence
- LO 2 Sources of Threat Intelligence
- LO 3 Threat Intelligence Collection and Analysis
- LO 4 Threat Intelligence Tools and Platforms
- LO 5 Threat Intelligence Frameworks
- LO 6 Threat Intelligence in Incident Response
- LO 7 Measuring the Effectiveness of Threat Intelligence
- LO 8 Cyber Kill Chain / Diamond Model

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 04

Scripting for Security

04

This Section introduces students to the fundamentals of scripting in the context of cybersecurity, emphasizing how automation can enhance security operations and incident response. Participants will learn popular scripting languages such as Python and Bash, focusing on writing scripts to automate routine security tasks, analyze log files, and develop security tools. The module covers key concepts like data manipulation, API interaction, and vulnerability scanning through scripting. Students will engage in hands-on projects that reinforce their skills in building custom scripts for tasks such as network scanning, malware analysis, and threat detection, ultimately equipping them with the ability to enhance their security posture through automation.

Key Learning Outcomes

- Fundamentals of Scripting Languages
- Writing and Debugging Security Scripts
- Security Testing and Exploitation
- Automation in Security Operations
- Scripting for Automation
- Data Manipulation and Analysis
- Scripting for Penetration Testing

Curriculum

4 modules · 30 learning outcomes

01 Scripting for Security with Bash

- LO 1 Command-Line Basics for Security
- LO 2 Automating Security Tasks with Bash
- LO 3 Scripting for Network Security
- LO 4 System Hardening with Bash
- LO 5 Network Monitoring and Analysis with Bash
- LO 6 System and File Analysis with Bash
- LO 7 Scan Web Applications with Bash
- LO 8 Best Practices for Secure Bash Scripting

02 Scripting for Security with Python

- LO 1 Introduction to Python for Security
- LO 2 Automating Security Tasks with Python
- LO 3 Network Security Scripting
- LO 4 File and Log Analysis
- LO 5 Web Application Security Automation
- LO 6 Network Monitoring and Intrusion Detection
- LO 7 Cryptography with Python
- LO 8 Best Practices for Secure Python Scripting

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 04

Scripting for Security

Curriculum (continued)

03 Scripting for Security with PowerShell Scripting

- LO 1 Introduction to PowerShell for Security
- LO 2 Automating System Tasks with PowerShell
- LO 3 Network Security with PowerShell
- LO 4 Incident Response with PowerShell
- LO 5 Defensive Security with PowerShell
- LO 6 Best Practices for Secure PowerShell Scripting

04 Penetration Testing with Scripts

- LO 1 Introduction to Scripting in Penetration Testing
- LO 2 Automating Reconnaissance and Information Gathering
- LO 3 Network Scanning and Enumeration
- LO 4 Web Application Penetration Testing with Scripts
- LO 5 Advanced Payload Development
- LO 6 Scripted Social Engineering Attacks
- LO 7 Reporting and Documentation with Scripts
- LO 8 Best Practices and Secure Scripting

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 05

Security Operations Architecture and Detection

This Section covers the design and implementation of Security Operations Centers (SOC), focusing on the architecture, processes, and technologies used for real-time detection and response to cybersecurity threats. Students will learn about the components of an effective SOC, including SIEM (Security Information and Event Management) systems, log management, threat intelligence, and incident response workflows. The module emphasizes threat detection techniques, network monitoring, and the use of detection tools like IDS/IPS and endpoint detection solutions. Learners will also gain insights into threat hunting, incident analysis, and reporting, with a focus on continuous monitoring and improving detection capabilities.

Key Learning Outcomes

- Understanding Security Operations Architecture
- Implementing Security Monitoring Solutions
- Threat Intelligence Integration
- Designing Security Operations Frameworks
- Effective Detection and Response Strategies
- Automating Security Operations

Curriculum

7 modules · 53 learning outcomes

01 Network Architecture Design

- LO 1 Introduction to Network Architecture Design
- LO 2 Layered Network Design and the OSI Model
- LO 3 Designing for High Availability and Redundancy
- LO 4 Secure Network Design Principles
- LO 5 Wide Area Network (WAN) Design
- LO 6 Wireless Network Architecture
- LO 7 Network Design for Cloud and Hybrid Environments
- LO 8 Advanced Network Security Features
- LO 9 Case Studies and Real-World Applications

02 Virtual Private Cloud (VPC)

- LO 1 Introduction to Virtual Private Cloud (VPC)
- LO 2 VPC Design Principles
- LO 3 Networking in VPCs
- LO 4 Security in VPCs
- LO 5 VPC Integration with On-Premises Networks
- LO 6 Advanced VPC Configurations
- LO 7 Monitoring and Troubleshooting in VPCs
- LO 8 Compliance and Governance for VPCs
- LO 9 VPC Use Cases and Real-World Scenarios

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 05

Security Operations Architecture and Detection

Curriculum (continued)

03 Firewall Configuration

- LO 1 Firewall Rules and Policies
- LO 2 Stateful and Stateless Firewall Configurations
- LO 3 Intrusion Detection System (IDS), Intrusion Prevention System (IPS)
- LO 4 Network Address Translation (NAT) and Firewalls
- LO 5 Firewall Logging and Monitoring
- LO 6 Zone-Based Firewall Configurations
- LO 7 Firewall Configuration for Virtual Environments
- LO 8 Testing and Auditing Firewall Configurations

04 Proxies, Remote Access, VPN

- LO 1 Understanding and Configuring Proxies
- LO 2 Virtual Private Networks (VPNs): Fundamentals
- LO 3 Configuring VPNs for Secure Access
- LO 4 Remote Access Security Best Practices
- LO 5 Proxy and VPN Troubleshooting
- LO 6 Proxies, Remote Access, and VPN in Enterprise Environments

05 Cloud Infrastructure Auditing

- LO 1 Cloud Security Frameworks and Standards
- LO 2 Tools for Cloud Auditing
- LO 3 Identity and Access Management (IAM) Auditing
- LO 4 Network Security Auditing in the Cloud
- LO 5 Storage and Data Protection Auditing
- LO 6 Automation in Cloud Auditing
- LO 7 Incident Response and Reporting in Cloud Audits

06 Security Information Event Management (SIEM)

- LO 1 Introduction to SIEM
- LO 2 Setting Up a SIEM Environment
- LO 3 Log Collection and Management
- LO 4 Event Correlation and Threat Detection
- LO 5 Alerting and Incident Response
- LO 6 SIEM Dashboard Customization
- LO 7 Use Cases for SIEM in Cybersecurity

07 Cryptography

- LO 1 Introduction to Cryptography
- LO 2 Symmetric Key Cryptography
- LO 3 Asymmetric Key Cryptography
- LO 4 Hashing Algorithms
- LO 5 Digital Signatures and Certificates
- LO 6 Cryptographic Protocols
- LO 7 Advanced Cryptographic Techniques

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 06

API Pentesting

06

This Section focuses on the principles and techniques of API Penetration Testing, with an emphasis on identifying vulnerabilities in web and mobile APIs. Students will learn how to assess API security, including authentication, authorization, rate limiting, and data validation. Topics include exploiting common API vulnerabilities such as injection attacks, broken authentication, and sensitive data exposure using tools like Burp Suite, Postman, and OWASP Zap. Learners will gain hands-on experience testing RESTful and SOAP APIs, analyzing API traffic, and reporting findings with mitigation strategies for securing APIs against real-world threats.

Key Learning Outcomes

- Understanding API Security Fundamentals
- Proficiency in API Reconnaissance and Enumeration
- Mastery of API Authentication and Authorization Testing
- Ability to Test for Data Exposure and Input Validation Issues
- Ability to Bypass Security Controls and Exploit API Misconfigurations
- Skills in Reporting and Documenting API Security Findings
- Defensive Awareness and API Security Best Practices

Curriculum

6 modules · 43 learning outcomes

01 Fundamentals of API

- LO 1 Introduction to APIs
- LO 2 RESTful API Design Principles
- LO 3 Authentication and Authorization in APIs
- LO 4 API Rate Limiting and Throttling
- LO 5 API Testing and Debugging
- LO 6 GraphQL APIs
- LO 7 API Monitoring and Analytics
- LO 8 Assessment Approach Testing Viewpoints
- LO 9 OWASP Top 10 API Security Risks

02 Monolithic Architecture & Microservices Architecture

- LO 1 Introduction to Software Architecture
- LO 2 Monolithic vs. Microservices: A Comparison
- LO 3 Building a Monolithic Application
- LO 4 Service Discovery and API Gateway
- LO 5 Data Management in Microservices
- LO 6 Scalability and Performance in Monolithic and Microservices

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 06

API Pentesting

Curriculum (continued)

03 Tools in API Security

- LO 1 OWASP ZAP (Zed Attack Proxy)
- LO 2 Postman for API Security Testing
- LO 3 Burp Suite for API Security
- LO 4 API Gateway Security Features
- LO 5 API Security Scanners (e.g., 42Crunch, APIsec)
- LO 6 API Security Monitoring Tools (e.g., Datadog, Sumo Logic)
- LO 7 API Protection Tools (e.g., ShieldX, Salt Security)
- LO 8 Integrating API Security Tools into CI/CD Pipelines

04 Testing on Live API

- LO 1 Understanding the API Lifecycle and Production Testing
- LO 2 Types of Tests for Live APIs
- LO 3 Tools for Testing Live APIs
- LO 4 Non-Intrusive Testing Techniques for Live APIs
- LO 5 Authentication & Authorization Testing in Live APIs
- LO 6 Performance Testing on Live APIs
- LO 7 Monitoring and Logging During Live API Testing
- LO 8 Finding and Exploiting an Unused API Endpoint

05 Difference Between REST and SOAP

- LO 1 SOAP (Simple Object Access Protocol) Overview
- LO 2 REST (Representational State Transfer) Overview
- LO 3 Key Differences Between REST and SOAP
- LO 4 SOAP and REST Use Cases
- LO 5 Security Features in SOAP and REST
- LO 6 Interoperability Between SOAP and REST

06 Exploiting an API Endpoint Using Documentation

- LO 1 Common API Vulnerabilities Exposed Through Documentation
- LO 2 Exploiting Insecure Endpoints via Documentation
- LO 3 Exploiting API Rate Limiting and DoS Vulnerabilities
- LO 4 Exploiting Injection Vulnerabilities via API Documentation
- LO 5 Exploiting Cross-Site Scripting (XSS) in API Responses
- LO 6 Real-World Examples of API Exploitation

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 07

Network Penetration Testing

07

This Section introduces students to the core concepts and techniques of Network Penetration Testing, emphasizing the discovery and exploitation of network vulnerabilities. Topics covered include reconnaissance, network scanning, vulnerability identification, and exploitation of common network services using industry-standard tools like Nmap and Metasploit. Students will also learn advanced techniques like privilege escalation, firewall/IDS evasion, and wireless network attacks. The module emphasizes real-world scenarios, allowing students to practice ethical hacking skills and produce comprehensive penetration testing reports with actionable security recommendations.

Key Learning Outcomes

- Understanding of Network Penetration Testing Concepts
- Competency in Network Scanning and Vulnerability Identification
- Proficiency in Bypassing Network Security Mechanisms
- Mastery of Network Exploitation Techniques
- Understanding of Wireless Network Penetration Testing
- Ability to Analyze and Exploit Web Applications via the Network
- Skills in Conducting Post-Exploitation Activities

Curriculum

4 modules · 25 learning outcomes

01 Introduction to Network Penetration Testing

- LO 1 Penetration Testing Methodologies
- LO 2 Information Gathering and Reconnaissance
- LO 3 Network Scanning and Vulnerability Identification
- LO 4 Network Exploitation Techniques
- LO 5 Network Penetration Assessments
- LO 6 Network Defense Mechanisms
- LO 7 Social Engineering in Network Penetration Testing

02 Wireless Network Penetration Testing

- LO 1 Wireless Network Scanning and Enumeration
- LO 2 Cracking Wireless Encryption Protocols
- LO 3 DE Authentication and Man-in-the-Middle Attacks
- LO 4 Rogue Access Points and Evil Twin Attacks
- LO 5 Wireless Network Sniffing and Eavesdropping
- LO 6 Securing Wireless Networks

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 07

Network Penetration Testing

Curriculum (continued)

03 Advanced Network Pentesting Techniques

- LO 1 Evasion Techniques for Firewalls and Intrusion Detection Systems
- LO 2 Exploiting Advanced Network Protocols
- LO 3 Lateral Movement and Pivoting Techniques
- LO 4 Exploiting Active Directory and Domain Services
- LO 5 Exploiting Cloud Infrastructure (AWS, Azure, GCP)

04 Reporting and Documentation

- LO 1 Key Components of a Penetration Testing Report
- LO 2 Writing Clear and Concise Vulnerability Descriptions
- LO 3 Risk Ratings and Severity Classification
- LO 4 Tools and Software for Documentation and Reporting
- LO 5 Writing an Executive Summary for Non-Technical Stakeholders
- LO 6 Final Report Presentation and Client Communication
- LO 7 Post-Testing Activities and Documentation Review

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 08

Android Penetration Testing

08

This Section focuses on the security assessment of Android applications, teaching students to identify and exploit vulnerabilities in the Android ecosystem. Topics include Android architecture, setting up a pen-testing environment, static and dynamic analysis, and exploiting common vulnerabilities such as insecure data storage, weak permissions, and insecure network communication. Using tools like Frida, Burp Suite, and MobSF, students will gain hands-on experience in bypassing security mechanisms and performing in-depth security testing. The module also covers reporting findings and recommending best practices for securing Android applications.

Key Learning Outcomes

- Understanding Android Architecture and Security Model
- Competency in Static Analysis of Android Applications
- Mastery of Android Application Vulnerability Exploitation
- Proficiency in Network Attacks and Exploitation of Android Apps
- Skills in Reporting Android Application Security Findings
- Proficiency in Setting Up an Android Pentesting Environment
- Proficiency in Dynamic Analysis and Runtime Exploitation
- Ability to Exploit Insecure Data Storage
- Competency in Exploiting Android Application Components

Curriculum

3 modules · 18 learning outcomes

01 Introduction to Android Penetration Testing

- LO 1 Setting Up the Android Penetration Testing Environment
- LO 2 Android Application Security Assessment
- LO 3 Identifying Insecure Data Storage and Insecure Communication
- LO 4 OWASP Mobile Application
- LO 5 Android Application Structure and Components

HACKINETIX ACADEMY
MASTERING THE CYBER FLOW

LEVEL 08

Android Penetration Testing

Curriculum (continued)

02 Android App Penetration Testing Methodology

- LO 1 Pre-engagement and Information Gathering
- LO 2 Static Analysis (Decompiling the APK)
- LO 3 Dynamic Analysis (Running the Application)
- LO 4 Assessing Insecure Communication and Authentication Flaws
- LO 5 Testing for Code Injection and Input Validation Issues
- LO 6 Exploiting and Privilege Escalation
- LO 7 Exploiting Android Components
- LO 8 Mitigation and Secure Development Practices for Android Apps

03 DEX File Analysis

- LO 1 Introduction to DEX Files
- LO 2 Tools for DEX File Analysis
- LO 3 Understanding DEX File Structure
- LO 4 Identifying Common Vulnerabilities in DEX Files
- LO 5 Analyzing Obfuscated DEX Files

HACKINETIX ACADEMY

MASTERING THE CYBER FLOW

START YOUR JOURNEY

Ready to Start Your Cybersecurity Journey?

Join Ethical Hacking Mastery (H|EHM) and build practical, job-ready cybersecurity skills across all levels.

ENROLL NOW →



CONTACT US

- www.hackinetix.com
- info@hackinetix.com
- Join Our WhatsApp Channel