LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

Adv Certificate in Network Security & Ethical Hacking

Practitioner Level

LAPT — London Academy of Professional Training

Address 85 Great Portland Street, W1W 7LT, London, United Kingdom

Email info@lapt.org

Telephone +44 7513 283044

Web lapt.org

Reference IT-CSI-P • IT Centres

UKPRN 10067351 • Registered in England and Wales, company 4984798

6	30	180	440	60%	Lifetime
SUBJECTS	CHAPTERS	CLASSES	TOTAL MARKS	PASS MARK	VALIDITY

AT A GLANCE

REFERENCE	**IT-CSI-P**
AWARD	**Certificate**
ASSESSMENT	**440 marks — 264 to pass (60%)**
PREREQUISITES	**None**
VALIDITY	**Lifetime**
AWARDING BODY	**LAPT — London Academy of Professional Training**

CURRICULUM

1 Advanced Security Protocols

5 chapters · 30 classes · **65 marks**

- **1 Cryptography Essentials in Network Security** — 6 classes
  - 1.1 Understanding the Fundamentals of Cryptography
  - 1.2 Exploring Symmetric Encryption Algorithms
  - 1.3 Analyzing Asymmetric Encryption Processes
  - 1.4 Implementing Hash Functions for Data Integrity
  - 1.5 Applying Cryptographic Protocols in Network Security
  - 1.6 Evaluating the Role of Cryptography in Ethical Hacking
- **2 Advanced Authentication Protocols** — 6 classes
  - 2.1 Understanding Advanced Authentication Protocols
  - 2.2 Exploring Multi-Factor Authentication Techniques
  - 2.3 Analyzing Biometric Authentication Methods
  - 2.4 Implementing Secure Kerberos Protocol
  - 2.5 Comparing Token-Based Authentication Systems
  - 2.6 Evaluating Real-World Authentication Protocol Scenarios
- **3 Secure Transport Layer Protocols** — 6 classes
  - 3.1 Understand the Basics of Secure Transport Layer Protocols
  - 3.2 Explore the Functionality of SSL/TLS Protocols
  - 3.3 Analyze the Handshake Process in TLS
  - 3.4 Evaluate the Role of Certificates in Secure Connections
  - 3.5 Implement Secure Channel Establishment Practices
  - 3.6 Troubleshoot Common Issues in Transport Layer Security
- **4 Next-Generation Firewall and Intrusion Detection Systems** — 6 classes
  - 4.1 Introduction to Next-Generation Firewalls
  - 4.2 Analyzing Firewall Capabilities and Features
  - 4.3 Understanding Intrusion Detection Systems
  - 4.4 Comparing Intrusion Detection and Prevention Systems
  - 4.5 Configuring Next-Generation Firewall Policies
  - 4.6 Implementing Intrusion Detection Strategies
- **5 Incident Response and Secure Cyber Operations** — 6 classes
  - 5.1 Understanding Incident Response Frameworks
  - 5.2 Identifying and Classifying Security Incidents
  - 5.3 Implementing Incident Detection Techniques
  - 5.4 Coordinating Incident Response Teams Effectively
  - 5.5 Applying Secure Cyber Operations in Real-Time Scenarios
  - 5.6 Evaluating Post-Incident Recovery and Reporting

2 Ethical Hacking Techniques

5 chapters · 30 classes **65 marks**

- **1 Understanding Ethical Hacking Frameworks and Legal Considerations** — 6 classes
  - 1.1 Defining Ethical Hacking and Its Purpose
  - 1.2 Exploring Key Ethical Hacking Frameworks
  - 1.3 Comparing Ethical Hacking and Malicious Hacking
  - 1.4 Examining Legal Considerations in Hacking
  - 1.5 Understanding Privacy Laws and Regulations
  - 1.6 Applying Ethical Principles in Hacking Scenarios
- **2 Reconnaissance Techniques and Information Gathering** — 6 classes
  - 2.1 Understanding Reconnaissance in Ethical Hacking
  - 2.2 Exploring Passive Information Gathering Techniques
  - 2.3 Leveraging Active Reconnaissance Tactics
  - 2.4 Utilizing Open Source Intelligence (OSINT) Tools
  - 2.5 Applying Network Scanning and Enumeration
  - 2.6 Analyzing and Documenting Gathered Information
- **3 Network Scanning and Vulnerability Identification** — 6 classes
  - 3.1 Understanding Network Scanning Fundamentals
  - 3.2 Exploring Common Network Scanning Tools
  - 3.3 Identifying Open Ports and Services
  - 3.4 Detecting Vulnerabilities Using Automated Scanners
  - 3.5 Analyzing Vulnerability Assessment Reports
  - 3.6 Implementing Network Security Improvements
- **4 Exploitation Techniques and Gaining Access** — 6 classes
  - 4.1 Understanding Vulnerabilities and Exploits
  - 4.2 Analyzing Common Exploitation Techniques
  - 4.3 Crafting and Deploying Exploit Code
  - 4.4 Gaining Access Through Password Cracking
  - 4.5 Performing Privilege Escalation Tactics
  - 4.6 Securing Systems Against Exploitation
- **5 Post-Exploitation, Maintaining Access, and Covering Tracks** — 6 classes
  - 5.1 Understanding Post-Exploitation Activities
  - 5.2 Utilizing Persistence Mechanisms for Maintaining Access
  - 5.3 Implementing Backdoor Techniques for Ongoing Access
  - 5.4 Strategies for Covering Tracks and Avoiding Detection
  - 5.5 Analyzing Log Files for Trace Removal
  - 5.6 Applying Best Practices for Ethical Hacking Operations

3 Network Security Fundamentals

5 chapters · 30 classes **65 marks**

- **1 Understanding Network Security Essentials** — 6 classes
  - 1.1 Identifying Network Security Threats
  - 1.2 Exploring Types of Network Attacks
  - 1.3 Understanding Firewalls and Their Functions
  - 1.4 Analyzing Network Security Protocols
  - 1.5 Implementing Network Access Controls
  - 1.6 Evaluating Security Measures in Network Design
- **2 Network Protocols and Their Vulnerabilities** — 6 classes
  - 2.1 Understanding Network Protocols and Their Functions
  - 2.2 Analyzing Common Network Protocol Vulnerabilities
  - 2.3 Exploring TCP/IP Protocol Suite and Its Security Flaws
  - 2.4 Identifying Security Challenges in Wireless Protocols
  - 2.5 Mitigating Risks Through Secure Protocol Implementation
  - 2.6 Applying Best Practices in Network Protocol Security
- **3 Implementing Network Defense Mechanisms** — 6 classes
  - 3.1 Understanding Network Threats and Vulnerabilities
  - 3.2 Identifying Common Network Defense Mechanisms
  - 3.3 Implementing Firewalls and Intrusion Detection Systems
  - 3.4 Configuring Network Access Controls
  - 3.5 Utilizing Encryption for Secure Communication
  - 3.6 Applying Best Practices for Network Defense
- **4 Securing Wireless Networks** — 6 classes
  - 4.1 Understanding Wireless Network Vulnerabilities
  - 4.2 Identifying Threats to Wireless Networks
  - 4.3 Implementing Wireless Network Security Protocols
  - 4.4 Configuring Secure Wireless Access Points
  - 4.5 Monitoring Wireless Network Traffic
  - 4.6 Conducting Wireless Network Penetration Testing
- **5 Introduction to Ethical Hacking Techniques** — 6 classes
  - 5.1 Understanding Ethical Hacking: Principles and Scope
  - 5.2 Exploring Common Ethical Hacking Methodologies
  - 5.3 Identifying Threats: Types of Network Vulnerabilities
  - 5.4 Learning Reconnaissance: Techniques and Tools
  - 5.5 Practicing Scanning: Detecting Network Weaknesses
  - 5.6 Applying Exploitation: Safe and Ethical Practices

4 Practical Security Applications

5 chapters · 30 classes **90 marks**

- **1 Understanding Security Protocols and Architectures** — 6 classes
  - 1.1 Exploring the Basics of Security Protocols
  - 1.2 Analyzing Cryptographic Principles in Network Security
  - 1.3 Understanding Authentication and Authorization Processes
  - 1.4 Examining Secure Socket Layer (SSL) and Transport Layer Security (TLS)
  - 1.5 Investigating Virtual Private Network (VPN) Architectures
  - 1.6 Applying Security Protocols in Real-world Scenarios
- **2 Implementing Firewalls and Intrusion Detection Systems** — 6 classes
  - 2.1 Exploring Firewall Fundamentals
  - 2.2 Configuring Basic Firewall Rules
  - 2.3 Analyzing Network Traffic Using Firewalls
  - 2.4 Understanding Intrusion Detection System Types
  - 2.5 Setting Up a Basic Intrusion Detection System
  - 2.6 Integrating Firewalls with Intrusion Detection Systems
- **3 Conducting Vulnerability Assessments and Penetration Testing** — 6 classes
  - 3.1 Understanding Vulnerability Assessments
  - 3.2 Identifying Network Vulnerabilities
  - 3.3 Utilizing Tools for Vulnerability Scanning
  - 3.4 Analyzing Vulnerability Scan Results
  - 3.5 Conducting Penetration Testing Techniques
  - 3.6 Reporting and Remediating Security Vulnerabilities
- **4 Cryptography and Secure Data Transmission** — 6 classes
  - 4.1 Understanding Cryptography Fundamentals
  - 4.2 Exploring Symmetric and Asymmetric Encryption Techniques
  - 4.3 Implementing Public Key Infrastructure (PKI)
  - 4.4 Securing Data Transmission with SSL/TLS Protocols
  - 4.5 Analyzing Cryptographic Algorithms and Their Applications
  - 4.6 Applying Cryptography in Practical Scenarios
- **5 Ethical Hacking Frameworks and Legal Considerations** — 6 classes
  - 5.1 Understanding Ethical Hacking Frameworks
  - 5.2 Exploring Legal Implications of Hacking
  - 5.3 Identifying Key Components of Ethical Hacking
  - 5.4 Analyzing Case Studies on Legal and Ethical Boundaries
  - 5.5 Applying Ethical Hacking Techniques within Legal Constraints
  - 5.6 Evaluating Ethical Hacking Tools and Technologies

5 Risk Management

5 chapters · 30 classes **65 marks**

- **1 Understanding Risk in Cyber Security Contexts** — 6 classes
  - 1.1 Defining Risk in Cyber Security
  - 1.2 Identifying Cyber Threats and Vulnerabilities
  - 1.3 Analyzing Impact and Likelihood of Cyber Risks
  - 1.4 Exploring Risk Assessment Frameworks
  - 1.5 Developing Cyber Risk Mitigation Strategies
  - 1.6 Evaluating and Monitoring Risk Management Effectiveness
- **2 Risk Assessment Methodologies and Tools** — 6 classes
  - 2.1 Understanding Risk Assessment Fundamentals
  - 2.2 Identifying and Categorizing Network Risks
  - 2.3 Analyzing Risk Impact and Likelihood
  - 2.4 Exploring Qualitative and Quantitative Assessment Tools
  - 2.5 Applying Risk Assessment Frameworks
  - 2.6 Implementing Risk Assessment in Network Security
- **3 Developing Risk Mitigation Strategies** — 6 classes
  - 3.1 Understanding Risk Mitigation Core Concepts
  - 3.2 Identifying and Prioritizing Network Risks
  - 3.3 Exploring Different Risk Mitigation Strategies
  - 3.4 Designing an Effective Mitigation Plan
  - 3.5 Implementing Risk Mitigation Techniques
  - 3.6 Evaluating and Refining Mitigation Strategies
- **4 Compliance and Regulatory Frameworks in Risk Management** — 6 classes
  - 4.1 Understanding Compliance and Regulatory Frameworks
  - 4.2 Identifying Key Regulatory Bodies and Their Roles
  - 4.3 Analyzing the Impact of GDPR on Risk Management
  - 4.4 Exploring Cybersecurity Standards and Best Practices
  - 4.5 Assessing the Importance of Continuous Compliance Monitoring
  - 4.6 Applying Compliance Frameworks in Risk Management Strategies
- **5 Implementing and Monitoring Risk Management Plans** — 6 classes
  - 5.1 Understanding Risk Management Plans
  - 5.2 Identifying Key Risk Indicators
  - 5.3 Developing Mitigation Strategies
  - 5.4 Implementing Risk Management Measures
  - 5.5 Monitoring Risk Levels Effectively
  - 5.6 Evaluating and Adjusting Risk Management Plans

6 Security Strategy Design

5 chapters · 30 classes **90 marks**

- **1 Understanding Security Principles and Standards** — 6 classes
  - 1.1 Exploring Fundamental Security Principles
  - 1.2 Distinguishing Between Security Policies and Standards
  - 1.3 Comparing Industry Security Standards
  - 1.4 Evaluating the Role of Risk Management in Security
  - 1.5 Integrating Security Controls and Best Practices
  - 1.6 Applying Security Principles to Real-World Scenarios
- **2 Risk Assessment and Management** — 6 classes
  - 2.1 Understanding the Fundamentals of Risk in Network Security
  - 2.2 Identifying and Analyzing Security Threats and Vulnerabilities
  - 2.3 Evaluating Risk Impact and Probability in IT Environments
  - 2.4 Developing Risk Mitigation Strategies for Network Security
  - 2.5 Implementing Risk Management Policies and Protocols
  - 2.6 Reviewing and Updating Risk Assessments Regularly
- **3 Designing a Comprehensive Security Strategy** — 6 classes
  - 3.1 Understanding Security Strategy Fundamentals
  - 3.2 Identifying Key Components of a Security Strategy
  - 3.3 Analyzing Internal and External Threat Landscapes
  - 3.4 Developing Risk Assessment Methodologies
  - 3.5 Integrating Compliance and Governance in Strategies
  - 3.6 Implementing and Reviewing Security Strategies
- **4 Implementing Security Controls and Technologies** — 6 classes
  - 4.1 Understanding Security Controls: Types and Purposes
  - 4.2 Identifying Key Security Technologies for Protection
  - 4.3 Integrating Access Control Mechanisms
  - 4.4 Implementing Network Security Devices
  - 4.5 Configuring Endpoint Security Solutions
  - 4.6 Evaluating the Effectiveness of Security Measures
- **5 Evaluation and Continuous Improvement of Security Strategies** — 6 classes
  - 5.1 Understanding the Importance of Security Evaluations
  - 5.2 Identifying Key Metrics for Security Performance
  - 5.3 Conducting Effective Security Audits and Assessments
  - 5.4 Implementing Feedback Loops for Continuous Improvement
  - 5.5 Adapting Security Strategies to Emerging Threats
  - 5.6 Leveraging Technology for Automated Security Improvement