Arrow ECS Finland Oy - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS Finland Oy, Lars Sonckin kaari 16, 02600 Espoo, Finland

Email: education.ecs.fi@arrow.com
Phone: 0870 251 1000

Certified Penetration Testing Professional AI (v2)

CODE:	LENGTH:	PRICE:
ECC_CPENT	40 Hours (5 days)	€3,595.00

Description

Why Join the C|PENT Course?

- Gain mastery in a complete hands-on pen testing methodology.
- Master AI pen testing skills mapped to all pen testing phases.
- Validate and test your skills across five unique multi-disciplinary courses, facing challenges at every level of the attack spectrum.
- Expand technical expertise in advanced penetration testing tools, techniques,
- methodologies, and AI tools.
- Become proficient in skills beyond the essential pen testing skills.
- Prioritize often-overlooked and critical aspects—scoping engagements, understanding design, estimating effort, and presenting findings.
- Develop the mindset of well-rounded, versatile professionals and lead red teams with offensive security skills.
- Engage in a hybrid learning model that combines guided learning and self-learning.
- Practice in diverse scenarios that mimic real-world enterprise environments with IoT systems, segmented networks, and advanced defenses.
- Participate in a highly tactical program with offensive security training.
- Gain deep practice through CTF challenges, the largest library of 100+ labs, and live cyber ranges.
- Follow and learn a rigorous, systematic approach that emulates a hacker’s movement through configured target domains.
- Learn how to infiltrate organizations, evaluate risks, and write an actionable report.
- Show your prowess in a 100% practical exam, validating both your technical and nontechnical skills.
- Validate your elite offensive security skills on a global scale.
- Become VAPT-ready to handle real-world challenges and compliance requirements

AI Skills, you learn from C|PENT Program:
AI empowers penetration testers by automating repetitive tasks, enhancing accuracy, and uncovering complex security flaws that traditional methods might overlook.
• Enhanced efficiency • Improved accuracy • Real-time threat detection • Advanced vulnerability analysis
• Customization and scalability

Programme

Module 01: Introduction to Penetration Testing and Methodologies • Learning Objectives

• Principles and Objectives of Penetration Testing • Penetration Testing Methodologies and Frameworks
• Best Practices and Guidelines for Penetration Testing • Role of Artificial Intelligence in Penetration Testing
• Role of Penetration Testing in Compliance with Laws, Acts, and Standards • Module Summary
Module 02: Penetration Testing Scoping and Engagement • Learning Objectives • Penetration Testing: Pre-engagement Activities
• Key Elements Required to Respond to Penetration Testing RFPs • Drafting Effective Rules of Engagement (ROE)
• Legal and Regulatory Considerations Critical to Penetration Testing • Resources and Tools for Successful Penetration Testing
• Strategies to Effectively Manage Scope Creep • Module Summary
Module 03: Open Source Intelligence (OSINT) and Attack Surface Mapping • Learning Objectives
• Collecting Open-source Intelligence (OSINT) on Target's Domain Name • Collecting OSINT about Target Organization on the Web
• Perform OSINT on Target's Employees • Open Source Intelligence (OSINT) using Automation Tools • Attack Surface Mapping
• Module Summary Module 04: Social Engineering Penetration Testing • Learning Objectives
• Social Engineering Penetration Testing Concepts • Off-Site Social Engineering Penetration Testing
• On-Site Social Engineering Penetration Testing • Document Findings with Countermeasure Recommendations
• Module Summary Module 05: Web Application Penetration Testing • Learning Objectives
• Security Frame vs. Vulnerabilities vs. Attacks • OWASP Penetration Testing Framework
• Web Application Footprinting and Enumeration Techniques • Techniques for Web Vulnerability Scanning
• Test for Vulnerabilities in Application Deployment and Configuration
• Techniques to Assess Identity Management, Authentication, and Authorization Mechanisms
• Evaluate Session Management Security • Evaluate Input Validation Mechanisms • Detect and Exploit SQL Injection Vulnerabilities
• Techniques for Identifying and Testing Injection Vulnerabilities • Exploit Improper Error Handling Vulnerabilities
• Identify Weak Cryptography Vulnerabilities • Test for Business Logic Flaws in Web Applications
• Evaluate Applications for Client-Side Vulnerabilities • Module Summary
Module 06: API and Java Web Token Penetration Testing • Learning Objectives
• API and Java Web Tokens (JWT) Penetration Testing • Techniques and Tools to Perform API Reconnaissance
• Test APIs for Authentication and Authorization Vulnerabilities • Evaluate the security of JSON Web Tokens (JWT)
• Test APIs for Input Validation and Injection Vulnerabilities • Test APIs for Security Misconfiguration Vulnerabilities
• Test APIs for Rate Limiting and Denial of Service (DoS) Attacks • Test APIs for Security of GraphQL implementations
• Test APIs for Business Logic Flaws and Session Management • Module Summary
Module 07: Perimeter Defense Evasion Techniques
• Learning Objectives • Techniques to Evaluate Firewall Security Implementations
• Techniques to Evaluate IDS Security Implementations • Techniques to Evaluate the Security of Routers
• Techniques to Evaluate the Security of Switches • Module Summary Module 08: Windows Exploitation and Privilege Escalation
• Learning Objectives • Windows Pen Testing Methodology • Techniques to Perform Reconnaissance on a Windows Target
• Techniques to Perform Vulnerability Assessment and Exploit Verification • Methods to Gain Initial Access to Windows Systems
• Techniques to Perform Privilege Escalation • Post-Exploitation Activities • Module Summary
Module 09: Active Directory Penetration Testing • Learning Objectives • Architecture and Components of Active Directory
• Active Directory Reconnaissance • Active Directory Enumeration • Exploit Identified Active Directory Vulnerabilities
• Role of Artificial Intelligence in AD Penetration Testing Strategies • Module Summary
Module 10: Linux Exploitation and Privilege Escalation • Learning Objectives
• Linux Exploitation and Penetration Testing Methodologies • Linux Reconnaissance and Vulnerability Scanning
• Techniques to Gain Initial Access to Linux Systems • Linux Privilege Escalation Techniques • Module Summary
Module 11: Reverse Engineering, Fuzzing and Binary Exploitation • Learning Objectives
• Concepts and Methodology for Analyzing Linux Binaries • Methodologies for Examining Windows Binaries
• Buffer Overflow Attacks and Exploitation Methods • Concepts, Methodologies, and Tools for Application Fuzzing
• Module Summary Module 12: Lateral Movement and Pivoting • Learning Objectives • Advanced Lateral Movement Techniques
• Advanced Pivoting and Tunneling Techniques to Maintain Access • Module Summary Module 13: IoT Penetration Testing
• Learning Objectives • Fundamental Concepts of IoT Pen Testing • Information Gathering and Attack Surface Mapping
• Analyze IoT Device Firmware • In-depth Analysis of IoT Software • Assess the Security of IoT Networks and Protocols
• Post-Exploitation Strategies and Persistence Techniques • Comprehensive Pen Testing Reports • Learning Objectives
Module 14: Report Writing and Post-Testing Actions • Purpose and Structure of a Penetration Testing Report
• Essential Components of a Penetration Testing Report • Phases of a Pen Test Report Writing
• Skills to Deliver a Penetration Testing Report Effectively • Post-Testing Actions for Organizations • Module Summary
Self-Study Modules

- Penetration Testing Essential Concepts
- Mastering Metasploit Framework
- PowerShell Scripting
- Bash Environment and Scripting
- Python Environment and Scripting
- Perl Environment and Scripting
- Ruby Environment and Scripting

- Wireless Penetration Testing
- OT and SCADA Penetration Testing
- Cloud Penetration Testing
- Database Penetration Testing
- Mobile Device Penetration Testing

Test and Certification

Exam Code : 312-39 Duration : 24 Hours or Choose 2 Sessions of 12 Hours Each
Report Submission : Submit Pentesting Report within 7 Days of Examination Test Format : 100% Practical Exam
Dual Certification : Score more than 90% and get one more certification: Licensed Penetration Tester

Session Dates

Date	Location	Time Zone	Language	Type	Guaranteed	PRICE
10 Nov 2025	Espoo Arrow Classroom (CET +1 / UTC +2)		English	Classroom		€3,595.00
10 Nov 2025	Virtual Classroom (CET +1 / UTC +2)		English	Classroom		€3,595.00

Additional Information

This training is also available as onsite training. Please contact us to find out more.