Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss här

Kronborgsgränd 7, 164 46 Kista

Email: edu.ecs.se@arrow.com
Phone: +46 8 555 188 00

EC-Council Certified Security Analyst (ECSA) /Licenced Pen Tester

CODE:	LENGTH:	PRICE:
ECC_ECSA	40 Hours (5 days)	kr35,900.00

Description

You are an ethical hacker. In fact, you are a Certified Ethical Hacker. Your last name is Pwned. You dream about enumeration and you can scan networks in your sleep. You have sufficient knowledge and an arsenal of hacking tools and you are also proficient in writing custom hacking code. Is that enough?
Can you become an industry accepted security professional? Will organizations hire you to help them protect their systems? Do you have any knowledge in applying a suitable methodology to conduct a penetration test for an enterprise client? Do you have any experience writing a custom penetration testing report?
More importantly, do you have a globally recognized certification that can verify your penetration testing capabilities?
If you are the person above, what you may be lacking is the knowledge and experience to execute a successful penetration test according to accepted industry standards.
The ECSA is a security credential like no other! The ECSA course provides you with a real world hands-on penetration testing experience and is a globally accepted hacking and penetration testing class available that covers the testing of modern infrastructures, operating systems and application environments while teaching the students how to document and write a penetration testing report.
The ECSA program takes the tools and techniques you learned in the Certified Ethical Hacker course (CEH) and elevates your ability into full exploitation by teaching you how to apply the skills learned in CEH by utilizing EC-Council's published penetration testing methodologies.
It is a highly interactive, comprehensive, standards-based and methodology intensive 5-day security training program 5-day which teaches information security professionals to conduct real life penetration tests.
This course is part of the Information Security Track of EC-Council. This is a "Professional" level course, with the Certified Ethical Hacker being the "Core" and the Licensed Penetration Tester being the "Master" level certification.
The design of the course is such that the instructor in the class will actually take you through the core concepts of conducting a penetration test based on EC-Council's published penetration testing methodology and guide you through the report writing process for this organization.

Objectives

The ECSAV9 penetration testing course is designed to enhance the skills based competency of a penetration tester. This course is intensively hands-on and a tremendous amount of emphasis is placed on the practical competency of the student.
Unlike the previous version of ECSA exam, in the new ECSAv9, a student will only be allowed to challenge the ECSA exam after meeting certain eligibility requirements. To become eligible, a student must conduct a detailed penetration test through the EC-Council Cyber Range iLabs environment and submit a written report via EC-Council's ASPEN system.
Only candidates that successfully complete the penetration test in the Cyber Range iLabs environment are allowed to challenge the ECSA exam. You will conduct a penetration test on a company that has various departments, subnets and servers, and multiple operating systems with defense mechanisms architecture that has both militarized and non-militarized zones.

Audience

Ethical Hackers, Penetration Testers, Network Server Administrators, Firewall Administrators, Security Testers, System Administrators and Risk Assessment Professionals.

Programme

1. Security Analysis and Penetration Testing Methodologies
2. TCP IP Packet Analysis
3. Pre-penetration Testing Steps
4. Information Gathering Methodology
5. Vulnerability Analysis
6. External Network Penetration Testing Methodology
7. Internal Network Penetration Testing Methodology
8. Firewall Penetration Testing Methodology
9. IDS Penetration Testing Methodology
10. Web Application Penetration Testing Methodology
11. SQL Penetration Testing Methodology
12. Database Penetration Testing Methodology
13. Wireless Network Penetration Testing Methodology
14. Mobile Devices Penetration Testing Methodology
15. Cloud Penetration Testing Methodology
16. Report Writing and Post Test Actions

Self-Study Modules

1. Password Cracking Penetration Testing
2. Router and Switches Penetration Testing
3. Denial-of-Service Penetration Testing
4. Stolen Laptop, PDAs and Cell Phones Penetration Testing
5. Source Code Penetration Testing
6. Physical Security Penetration Testing
7. Surveillance Camera Penetration Testing
8. VoIP Penetration Testing
9. VPN Penetration Testing
10. Virtual Machine Penetration Testing
11. War Dialing
12. Virus and Trojan Detection
13. Log Management Penetration Testing
14. File Integrity Checking
15. Telecommunication and Broadband Communication Penetration Testing
16. Email Security Penetration Testing
17. Security Patches Penetration Testing
18. Data Leakage Penetration Testing
19. SAP Penetration Testing
20. Standards and Compliance
21. Information System Security Principles
22. Information System Incident Handling and Response
23. Information System Auditing and Certification

Session Dates

På begäran, kontakta oss

Ytterligare information

Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.