



# ECSA – EC-Council Certified Secure Analyst

## DESCRIPTION DU COURS

La formation ECSAv9 vous apporte une réelle expérience pratique de tests d'intrusion. Ce cours va notamment couvrir les tests sur des infrastructures actuelles, sur des systèmes d'exploitation et sur des environnements d'application tout en enseignant aux stagiaires comment documenter et écrire un rapport de test d'intrusion.

Le contenu du cours ECSAv9 utilise les outils et les techniques que vous avez appris lors de la formation Certified Ethical Hacker (CEH).

Le cours ECSAv9 va vous permettre d'utiliser la totalité de vos compétences, en vous enseignant comment les appliquer tout en utilisant la méthodologie publiée d'EC-Council sur les tests d'intrusion.

C'est une formation sécurité intensive programmée sur 5 jours avec un contenu complet très interactif, basé sur des normes et concentré sur la méthodologie. Ce cours enseigne aux professionnels de la sécurité de l'information comment mener de réels tests d'intrusion.

Ce cours fait partie du cursus « Information Security » d'EC-Council. C'est un cours de niveau « Professional » avec la formation Certified Ethical Hacker comme étant le corps du cours et la Licensed Penetration Tester comme étant la certification « Master » de ce cursus.

## PLAN DE COURS

1. Security Analysis & 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

## CERTIFICATION

A la fin de la semaine, l'étudiant aura 60 jours pour soumettre un rapport de pen-testing. Après validation d'EC-Council, il disposera de 30 jours pour passer l'examen de certification.

Titre de l'examen : ECSAv9
Examen : 150 QCM
Score requis : 70%
Durée : 4 heures
Disponibilité : ECC exam / VUE

## DUREE

5 jours (9h00 – 17h00)

## MODULES EN AUTO APPRENTISSAGE

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
16. Penetration Testing
17. Email Security Penetration Testing
18. Security Patches Penetration Testing
19. Data Leakage Penetration Testing
20. SAP Penetration Testing
21. Standards and Compliance
22. Information System Security Principles
23. Information System Incident Handling and Response
24. Information System Auditing and Certification

## PROFIL DES STAGIAIRES

Ce cours s'adresse particulièrement aux administrateurs de serveur réseau, administrateurs pare-feu, analystes sécurité de l'information, administrateurs système, professionnels d'évaluation des risques...