ECSA – EC-Council Certified Secure Analyst

Hackers Are Here. Where Are You?...

DESCRIPTION DU COURS

Le programme ECSAv10 est la continuité logique après avoir étudié le CEHv10.

Le nouveau ECSAv10 présente un plan de cours mis à jour et une méthodologie de pen test étape par étape, largement et globalement reconnue par le marché. Cela va permettre aux étudiants d'augmenter leurs compétences en apprenant de nouvelles techniques à travers d'intenses challenges et labs.

A l'inverse d'autres programmes de formation pen test, le cours ECSA présente un ensemble de méthodologies complètes et diverses pouvant répondre aux prérequis des différents marchés. C'est un cours interactif, exhaustif, basé sur des normes, se dispensant en 5 jours et qui permettra aux stagiaires d'apprendre à mener des vrais pen test professionnels.

Ce cours fait partie de la « VAPT Track » d'EC-Council (Vulnerability Assessment Penetration Testing).
C'est un cours de niveau "Professionnel", avec le CEH étant le cours principal et le LPT étant la certification « Master ».
Dans ce nouveau programme ECSAv10, les étudiants passant l'examen de certification ECSAv10 auront la possibilité de poursuivre un examen entièrement pratique, leur proposant donc de tester leurs compétences en obtenant la certification ECSA Practical. (cf. page suivante.)

PLAN DE COURS

1. Introduction to Penetration Testing and Methodologies
2. Penetration Testing Scoping and Engagement Methodology
3. Open Source Intelligence (OSINT) Methodology
4. Social Engineering Penetration Testing Methodology
5. Network Penetration Testing Methodology- External
6. Network Penetration Testing Methodology- Internal
7. Network Penetration Testing Methodology- Perimeter Devices
8. Web Application Penetration Testing Methodology
9. Database Penetration Testing Methodology
10. Wireless Penetration Testing Methodology
11. Cloud Penetration Testing Methodology
12. Report Writing and Post Testing Actions

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...

CERTIFICATION

Titre de l'examen: EC-Council Certified Security Analyst v10
Examen : 150 QCM
Score requis : 70%
Durée : 4 heures
Disponibilité : ECC exam

MODULES EN AUTO APPRENTISSAGE

1. Penetration Testing Essential Concepts
2. Password Cracking 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

DUREE

5 jours (9h00 – 17h00)