EC-COUNCIL CERTIFIED SECURITY ANALYST

CURSUS:
EC-COUNCIL

CODE DE LA FORMATION:
EC-SC-ECSA

VERSION:
9.0

DURÉE:
5 JOURS

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

PRÉREQUIS:
Pour suivre ce cours dans de bonnes conditions, les stagiaires doivent posséder une expérience des systèmes d’exploitation Windows et/ ou UNIX/LINUX, ainsi que des connaissances en réseau et TCP/ IP.
La certification CEH, CISSP ou CISA est obligatoire.

PUBLIC:
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.

OBJECTIFS:
- La pratique d'un test de pénétration avancé
- Au management d'un projet sécurité
- Après avoir suivi ce cours, le stagiaire sera capable d'identifier et de réduire les risques liés aux infrastructures
- Vous faire certifier comme Expert en sécurité
- Préparer l'examen 412-79

CONTENU:
- Les besoins pour une analyse de la sécurité
- Analyse de paquets TCP/ IP
- Méthodologies de tests de pénétration
- Les clients et les accords juridiquesLes règles d'engagement
- Planification et ordonnancement des tests de pénétrations
- Les étapes de pré-pénétration
- Collecte d'information

- Analyse de la vulnérabilité
- Test de pénétration Externe
- Internal Network Penetration Testing
- Test de penetration des Firewall
- Test de pénétration IDS
- Password Cracking Penetration Testing
- Test de pénétration des réseaux sociaux
- Test de pénétration des applications Web Application
- Test de Pénétration SQL
- Pénétration rapports d'essais et mesures des tests post Pénétration
- Test de pénétration des routeurs et switch
- Test de pénétration des réseaux sans fil
- Déni de service, tests de Pénétration
- Portables volés, téléphones mobile et tablettes, les tests de pénétration
- Test Code source Pénétration
- Pénétration physiques tests de sécurité
- Test de pénétration des cameras de surveillance
- Test de Pénétration des bases de données
- Test de Pénétration de la VoIP
- Test de Pénétration des VPN
- Test de Pénétration du Cloud
- Test de Pénétration des machines Virtuelles
- War Dialing
- Détection des Virus et Cheval de Troie
- Log Management Penetration Testing
- File Integrity Checking
- Mobile Devices Penetration Testing
- Test de Pénétration des télécommunications et de la communication haut débit
- Sécurité des emails
- Patches de sécurité des fuites de données
- SAP Penetration Testing
- Normes et conformité
- Information System Security Principles
- Information System Incident Handling and Response
- Information System Auditing and Certification

CERTIFICATION:

Ce cours prépare à l'examen *412-79* ECSA (EC Council Certified Security Analyst), puis à l'obtention de la licence LPT basé sur l'apprentissage d'une véritable méthodologie.

Seule certification reconnue à l'échelle mondiale pour faire valoir vos compétences d'auditeur technique en sécurité informatique.

Après la formation, vous passerez un QCM de 150 questions en 4h.