CompTIA Security +

CompTIA Security +

durée : 5 jour(s) code formation : SEC

Description :

La certification CompTIA Security + est une validation indépendante des constructeurs et éditeurs de solutions de sécurité. L`obtention de l`examen valide les connaissances et compétences requises pour identifier les risques, proposer des solutions et maintenir un niveau de sécurité adéquat.

Pré-requis :

Avoir un connaissance de base de la pile TCP/IP
Savoir configurer les paramètres IP d'une machine
Avoir une première expérience idéalement dans le domaine IT

Programme :

Sécurité réseau

- Les Firewalls
- Les routeurs
- Les switch
- Les load balancer
- Les proxies
- Les passerelles sécurité Web
- Les concentrateurs VPN
- Les analyseurs de flux
- Les anti spam
- URL Filering
- Les VLAN
- Le 802.1x
- Les logs
- Les DMZ
- Le NAT
- Les accès distants
- La virtualisation
- Le cloud computing
- IPSec
- SNMP
- Les principaux ports TCP et UDP
- Le sécurité des réseaux sans-fil

La sécurité opérationnelle

- Identification des risques
- Les false positives
- Les règles de confidentialité
- Les politiques de sécurité
- Le calcul du risque
- Acceptation du risque
- Gestion du changement
- Gestion des incidents
- Les audits de routine
- Création de procédure suite à un incident
- Sensibilisation des utilisateurs
- Les meilleures pratiques
- Les standards
- Continuité de l'activité
- Impacts sur l'activité
- Création d'un plan de récupération sur incident
- CIA (Confidentiality, Integrity, Availability)

Les menaces et les vulnérabilités

- Les différents types de malware
- Les virus
- Les vers
- Les spyware
- Les Trojan
- Les botnets
- Les backdoors
- Les types d'attaques
- DoS
- Spoofing
- DDoS
- Spam
- Phishing
- Privilege Escalation
- Poisoning
- Replay
- Smurf
- Le social engineering
- Les attaques sur les réseaux Wi-Fi
- Les attaques sur les applications
- Les moyens de sécurisation
- Sécurité physique
- Port Security

- Validation de posture
- Gestion des rapports
- Détection d'intrusion
- Les outils
- Tester la sécurité

Sécurité des postes utilisateurs et des applications

- Fuzzing
- Concepts clés de sécurisation d'une application
- Le Cross-site scripting
- Gestion des patchs
- Les dispositifs mobiles
- La virtualisation
- Data Loss Prevention (DLP)
- Les dispositifs de cryptages
- Les dongles
- Les clés USB de cryptage
- Le cloud computing
- Sécurité des navigateurs Web
- Sécurité des protocoles d'échanges de données
- Les firewalls basés sur les postes clients
- La sécurité physique
- GPS Tracking

Gestion de l'identité et des contrôles d'accès

- Les dispositifs d'authentification
- RADIUS
- TACACS
- XTACACS
- Kerberos
- LDAP
- La biométrie
- Les ACLs
- Les Tokens
- Les cartes d'accès
- Les Smart Card
- SSO
- Les OS de confiance
- Gestion des comptes
- Gestion des rôles
- Gestion des droits
- Politiques d'identification

- Les privilèges
- La rotation des travaux
- Le deny implicite

La cryptographie

- Cryptographie symétrique
- Cryptographie asymétrique
- Le hashage
- La non répudiation
- Les algorithmes
- WEP/WPA/WPA2
- DES/3DES/AES
- SHA/MD5
- Diffie/Hellman
- Les certificats
- PKI
- Clé privée
- Clé publique
- Les serveurs de certificats
- Durée de validité
- Recovery Agent
- Les modèles de confiances
- Les listes de révocation
- Renforcement des politiques de contrôles
- NTLM
- PAP
- CHAP
- BlowFish
- SSL
- TLS
- IPSEC
- HTTPS
- RC4