CompTIA Security+

Objectifs

- Créer et configurer une liste de contrôle d'accès (ACL) ;
- Établir des services de pare-feu avec des règles personnalisées en appliquant des filtres dynamiques de paquets et un filtrage de périphériques ;
- Identifier les ports réseau et les différents outils de piratage les plus utilisés par les hackers ;
- Réaliser un balayage de port et s'en servir judicieusement pour protéger un système d'information ;
- Surveiller et identifier des attaques et des vulnérabilités pour les affaiblir avant leurs déploiements dans un système d'information ;
- Assimiler la virtualisation sécurisée, le déploiement d'applications sécurisées et les concepts d'automatisation ;
- Caractériser, conseiller et appliquer les meilleures solutions de sécurité au sein d'une entreprise ;

Prérequis

- Disposer de compétences et de connaissances de base en cybersécurité ;
- Une expérience professionnelle de 2 ans en administration de système informatique ;
- Savoir lire et comprendre l'anglais, le japonais, le portugais ou l'espagnol pour le passage de l'examen SY0-701.

Programme

Cours 1 : à propos de la cybersécurité

- Les notions de base de la sécurité informatique.
- La gestion des risques d'un projet informatique.
- L'évaluation de la vulnérabilité et du risque.

Cours 2 : comprendre les cyberattaques

- Le hacking et les hackers.
- La pratique de l'ingénierie sociale.
- Les programmes malveillants.
- Les attaques réseau.
- Les attaques de malwares.

Lab informatique :

- Détecter des logiciels malveillants ;
- Effectuer une analyse de vulnérabilité d'un site web ;
- simuler une attaque DDoS ;
- casser un mot de passe ;
- réaliser un test d'intrusion ;
- effectuer une analyse de vulnérabilité d'application ;

- observer des attaques par injection de commandes SQL ;
- observer des attaques côté client.

Cours 3 : comprendre la cryptographie

- Les différentes techniques de cryptographie.
- Les infrastructures à clés publiques (ICP).

Lab informatique :

- mettre en œuvre une cryptographie symétrique et asymétrique ;
- utiliser des fonctions de hachage pour des fichiers ;
- mettre en place une autorité de certification.

Cours 4 : connaitre les fondamentaux des réseaux

- Les composants de base d'un réseau.
- Le système d'adressage IP.
- Les ports réseaux et les ports logiciels.

Lab informatique :

- Utiliser des outils de dépannage TCP/IP en ligne de commande.

Cours 5 : sécurisé un réseau d'entreprise

- Les composants de la protection réseau.
- Le chiffrement de la couche transport.
- L'amélioration des performances du réseau.
- L'analyse et la détection des anomalies.

Lab informatique :

- configurer une stratégie de pare-feu avec des règles personnalisées ;
- vérifier et tester des certificats SSL ;
- sécuriser un WAP (Wireless Application Protocol) ;
- analyser un journal d'événement système ;
- mettre en œuvre des procédures de numérisation réseau.

Cours 6 : sécuriser des hôtes et assurer la confidentialité

- La sécurité des ordinateurs hôtes.
- La sécurité des données.
- La sécurité des appareils mobiles.

Lab informatique :

- chiffrer et sécuriser avec BitLocker.

Cours 7 : sécuriser les services réseaux

- La sécurité d'une application.
- La sécurité des machines virtuelles.
- La sécurité des services dans le cloud.

Lab informatique :

- identifier des codes vulnérables.

Cours 8 : comprendre les processus d'authentification

- Les différents types de facteurs d'authentification.
- Les différents types de protocoles d'authentification.

Lab informatique :

- installer et configurer un serveur RADIUS ;
- effectuer une analyse avec Active Directory.

Cours 9 : comprendre le contrôle d'accès des SI

- Les différentes techniques de contrôle d'accès.
- La gestion des comptes utilisateurs.

Lab informatique :

- effectuer un audit et rédiger un rapport sur les autorisations NTFS ;
- utiliser des outils de ligne de commande pour gérer les objets Active Directory ;
- appliquer des objets de stratégie de groupe ;
- créer un modèle de sécurité informatique.

Cours 10 : gérer les risques

- Les lois, les normes et les politiques de sécurité informatique.
- La formation des utilisateurs.
- La sécurité physique et la sûreté des systèmes d'information.

Cours 11 : planifier la récupération après sinistre

- La reprise après sinistre.
- La haute disponibilité.
- La tolérance de pannes et la récupération.
- La réponse aux incidents.

Lab informatique :

- paramétrer et utiliser des sauvegardes sur Windows Server.