CompTIA Security+ (SY0-601)

Durée: 5 jours

Aperçu:

L'examen CompTIA Security+ certifiera que le candidat retenu possède les connaissances et les compétences requises pour installer et configurer des systèmes pour sécuriser les applications, les réseaux et les appareils ; effectuer une analyse des menaces et réagir avec des techniques d'atténuation appropriées ; participer aux activités d'atténuation des risques ; et opérer en étant conscient des politiques, lois et réglementations applicables.

.

Objectifs:

Ce cours vous enseignera les principes fondamentaux de l'installation et de la configuration des contrôles de cybersécurité et de la participation à la réponse aux incidents et à l'atténuation des risques. Il vous préparera à passer l'examen CompTIA Security + SY0-601 en fournissant une couverture à 100% des objectifs et des exemples de contenu énumérés dans le programme. L'étude du cours peut également aider à établir les conditions préalables pour étudier des qualifications de sécurité informatique plus avancées, telles que CompTIA Cybersecurity Analyst (CSA) +, CompTIA Advanced Security Practitioner (CASP) et CISSP (Certified Information Systems Security Professional) de l'ISC.

À la fin du cours, vous serez capable de :

Identifier les stratégies développées par les cyber-adversaires pour attaquer les réseaux et les hôtes et les contre-mesures déployées pour les défendre.

Comprendre les principes de la sécurité organisationnelle et les éléments de politiques de sécurité efficaces.

Connaître les technologies et les usages des normes et produits cryptographiques.

Installer et configurer les technologies de sécurité basées sur le réseau et l'hôte.

Décrire comment la sécurité de l'accès sans fil et à distance est appliquée.

Décrire les normes et les produits utilisés pour renforcer la sécurité sur le Web et les technologies de communication.

Identifier des stratégies pour assurer la continuité des activités, la tolérance aux pannes et la reprise après sinistre.

Explorer la sécurité du cloud et les techniques utilisées dans les tests d'intrusion

Sécuriser les appareils et les applications utilisés par votre entreprise

Identifier et protéger contre divers types de logiciels malveillants et de virus

Protéger votre environnement contre l'ingénierie sociale et les attaques avancées

Comprendre et mettre en œuvre les concepts PKI

Certifications

• Examen CompTIA Security+ SY0-601.

Public visé:

CompTIA Security+ s'adresse aux professionnels de l'informatique occupant des postes tels qu'ingénieur en sécurité, consultant/spécialiste en sécurité, technicien en assurance de l'information, auditeur junior/testeur de pénétration, administrateur de sécurité, administrateur système et administrateur réseau.

Conditions préalables:

Compétences en mise en réseau et en administration dans les réseaux TCP/IP basés sur Windows et familiarité avec d'autres systèmes d'exploitation, tels que OS X, Unix ou Linux.

Présenter:

1 Introduction au cours

• Présentations et logistique du cours

• Objectifs du cours

Table des matières

Comprendre les concepts de gestion des identités et des accès

Types d'identité

Types de compte

Types d'authentification

Implémentation de solutions d'authentification et d'autorisation

Résumer les concepts de conception d'authentification et d'autorisation

Authentification sur le cloud et sur site

Politiques communes de gestion des comptes

Exercice pratique – Politique de mot de passe

Questions de révision

5 Chapitre 4 : Exploration des concepts de virtualisation et de cloud

Présentation du Cloud Computing

Implémentation de différents modèles de déploiement cloud

Comprendre les modèles de service cloud

Comprendre les concepts du cloud computing

Comprendre les concepts de stockage cloud

Sélection des contrôles de sécurité du cloud

Explorer les environnements de réseau virtuel

Questions de révision

6 Section 2 : Surveillance de l'infrastructure de sécurité

7 Chapitre 5 : Surveillance, analyse et test d'intrusion

Concepts de test de pénétration

Reconnaissance passive et active

Types d'exercices

Concepts d'analyse des vulnérabilités

Syslog / Informations de sécurité et gestion des événements

Orchestration, automatisation et réponse de la sécurité

Exercice pratique - Exécution d'un scanner de vulnérabilités avec authentification

Questions de révision

8 Chapitre 6: Comprendre les protocoles sécurisés et non sécurisés

Introduction aux protocoles

Protocoles non sécurisés et leurs cas d'utilisation

Protocoles sécurisés et leurs cas d'utilisation

Cas d'utilisation supplémentaires et leurs protocoles

Questions de révision

9 Chapitre 7 : Approfondir les concepts de réseau et de sécurité

Installation et configuration des composants réseau

Capacités d'accès à distance

Concepts d'architecture de réseau sécurisé

Reconnaissance et découverte de réseau

Outils médico-légaux

Adressage IP

Questions de révision

10 Chapitre 8: Sécurisation des solutions sans fil et mobiles

Mise en œuvre de la sécurité sans fil

Contrôleurs de point d'accès sans fil

Déployer des appareils mobiles en toute sécurité

Méthodes de connexion des appareils mobiles

Questions de révision

11 Section 3: Protéger l'environnement de sécurité

12 Chapitre 9 : Identification des menaces, des attaques et des vulnérabilités

Attaques de virus et de logiciels malveillants

Attaques d'ingénierie sociale

Acteurs menaçants

Attaques avancées

Questions de révision

13 Chapitre 10 : Gouvernance, risques et conformité

Processus et concepts de gestion des risques

Acteurs de menace, vecteurs et concepts de renseignement

L'importance des politiques pour la sécurité organisationnelle

Règlements, normes et législation

Concepts de confidentialité et de données sensibles

Questions de révision

14 Chapitre 11 : Gestion de la sécurité des applications

Implémentation de la sécurité de l'hôte ou de l'application

Comprendre les implications de sécurité des systèmes embarqués et spécialisés

Comprendre le développement, le déploiement et l'automatisation d'applications sécurisées

Questions de révision

15 Chapitre 12 : Gestion des procédures de réponse aux incidents

Procédures de réponse aux incidents

Utiliser des sources de données pour soutenir les enquêtes

Savoir comment appliquer des techniques d'atténuation ou des contrôles pour sécuriser un environnement