Programme

Information Technology Specialist

Network Security

SkillsUp

CERTIFIER

IT SPECIALIST : NETWORK SECURITY CERTIFICATION

Les objectifs de la certification

La certification Information Technology Specialist : Network Security prouve la maîtrise des principes fondamentaux de :

- la défense en profondeur ;
- la sécurité des systèmes d'exploitation ;
- la sécurité des appareils réseau ;
- la gestion de l'informatique sécurisée.

Une personne obtenant cette certification peut démontrer qu'elle possède les connaissances et compétences fondamentales en matière de sécurité.

Durée : 50 minutes d'examen

Langues : français, anglais

IT SPECIALIST : NETWORK SECURITY CERTIFICATION

Les objectifs de la certification

1. DÉFENDRE EN PROFONDEUR

- **Identifier les principes fondamentaux de la sécurité**
  - Confidentialité, intégrité, disponibilité, non-répudiation, menace, risque, vulnérabilité, principe du moindre privilège, surfaces d'attaque, y compris *IoT*

- **Définir et appliquer la sécurité physique**
  - Sécurité des sites, sécurité des ordinateurs, dispositifs et lecteurs amovibles, sas de sécurité

- **Identifier les types de politiques de sécurité**
  - Contrôles administratifs, contrôles techniques

- **Identifier les types d'attaques**
  - Dépassement de tampon, virus, virus polymorphes, vers, chevaux de Troie, logiciels espions, *ransomwares*, publiciels, *rootkits*, portes dérobées, attaques/vulnérabilités *zero day*, attaques par déni de service (*DoS*), méthodes d'attaque courantes, types de vulnérabilités, scripts intersites (*XSS*), injection *SQL*, attaque par force brute, attaque de l'Homme du milieu (*MITM*) et de l'Homme dans le navigateur (*MITB*), ingénierie sociale, *keyloggers* (logiciels et matériels), bombes logiques

- **Identifier les types de sauvegarde et de restauration**
  - Complète, incrémentielle, différentielle

IT SPECIALIST : NETWORK SECURITY CERTIFICATION

Les objectifs de la certification

2. SÉCURISER LES SYSTÈMES D'EXPLOITATION

- **Identifier la protection des clients et des serveurs**
  - Séparation des services, renforcement de la sécurité, gestion des correctifs, réduction de la surface d'attaque, stratégie de groupe (*gpupdate* et *gpresult*), mises à jour sécurisées du *DNS* dynamique, contrôle de compte utilisateur (*UAC*), maintien à jour des systèmes d'exploitation et des logiciels des clients, chiffrement des dossiers hors ligne, politiques de restriction logicielle

- **Configurer l'authentification des utilisateurs**
  - Authentification multifactorielle, application des politiques de mots de passe, accès à distance, utilisation de la connexion secondaire pour effectuer des tâches administratives (Exécuter en tant que, *sudo*), création d'utilisateurs et de groupes locaux et de domaine, *Kerberos*

- **Gérer les permissions sous *Windows* et *Linux***
  Permissions des fichiers et des dossiers, permissions de partage, héritage, déplacement ou copie de fichiers sur le même disque ou sur un autre disque, groupes multiples avec différentes permissions, prise de propriété, délégation

- **Faciliter la non-répudiation en utilisant les politiques d'audit et les fichiers journaux**
  - Types d'audit, ce qui peut être audité, activation de l'audit, ce qu'il faut auditer pour des objectifs spécifiques, où enregistrer les informations d'audit, révision des fichiers journaux

IT SPECIALIST : NETWORK SECURITY CERTIFICATION

Les objectifs de la certification

2. SÉCURISER LES SYSTÈMES D'EXPLOITATION

- **Démontrer des connaissances en chiffrement**
  - Chiffrement de fichiers et de dossiers, impact du chiffrement sur le déplacement/la copie de fichiers et de dossiers, chiffrement de disques, *TPM*, processus de communication sécurisée (email, SMS, chat, réseaux sociaux), *VPN*, méthodes de chiffrement, clé publique/clé privée, propriétés et services de certificat, *Bitlocker*

IT SPECIALIST : NETWORK SECURITY CERTIFICATION

Les objectifs de la certification

3. SÉCURISER LES APPAREILS RÉSEAU

- **Mettre en œuvre la sécurité sans fil**
  - Types de sécurité sans fil (force du chiffrement), identifiants de réseau (*SSIDs*), filtrage *MAC*, configuration par défaut (*OOBE*)
- **Identifier le rôle des dispositifs de protection réseau**
  - Objectif des pare-feux, pare-feux matériels vs. logiciels, pare-feux réseau vs. hôte, inspection de pare-feu à état vs. sans état, bases de sécurité, système de détection d'intrusion (*IDS*), système de prévention d'intrusion (*IPS*), gestionnaire d'information et d'événements de sécurité (*SIEM*), filtrage de contenu, listes noires/blanches
- **Identifier les méthodes d'isolement de réseau**
  - Routage, *honeynet*, réseaux périmétriques (*DMZ*), *NAT/PAT*, *VPN*, *IPsec*, air *gap network*, *DirectAccess*, *VLAN*
- **Identifier les concepts de sécurité des protocoles**
  - *Tunneling*, *DNSSEC*, *network sniffing*, ports bien connus (*FTP*, *HTTP*, *HTTPS*, *DNS*, *RDP*, *Telnet*, *SSH*, *LDAP*, *LDAPS*, *SNMP*, *SMTP*, *IMAP*, *SFTP*)

IT SPECIALIST : NETWORK SECURITY CERTIFICATION

Les objectifs de la certification

4. GÉRER L'INFORMATIQUE SÉCURISÉE

- **Mettre en œuvre la protection des emails**
  - Antispam, usurpation d'identité, hameçonnage et *pharming*, protection des clients, formation des utilisateurs

- **Gérer la sécurité des navigateurs**
  - Paramètres du navigateur, gestion du cache, navigation privée

- **Installer et configurer les logiciels antimalware et antivirus**
  - Installation, désinstallation, réinstallation et mise à jour
  - Remédiation, planification des analyses, investigation des alertes

APPRENDRE

IT SPECIALIST : NETWORK SECURITY CERTIFICATION

E-learning

Le cours Network Security de LearnKey s'adresse à qui souhaite acquérir les fondamentaux de la sécurité des systèmes d'exploitation. Il prépare également à passer et réussir l'examen Network Security. Les quatre grands thèmes abordés sont la défense en profondeur, la sécurité des systèmes d'exploitation, la sécurité des équipements réseau et l'informatique sécurisée. Ce cours améliore aussi les perspectives d'employabilité de celles et ceux qui visent un premier poste de support informatique ou de technicien poste de travail comportant des exigences de base en sécurité. Un certificat de réussite est délivré à partir de 80 % de bonnes réponses à toutes les évaluations de fin de domaine ; un badge à partir de 90 %. Le cours couvre :

- la défense en profondeur ;
- la sécurité des systèmes d'exploitation ;
- la sécurité des appareils réseau ;
- la gestion de l'informatique sécurisée.

Les utilisateurs amélioreront leur employabilité générale tout en se préparant à l'examen Information Technology Specialist : Network Security.

Ce cours est valable pendant un an en ligne sauf indication contraire, et est limité à l'utilisation par une seule personne.
Les licences deviendront inactives si elles sont utilisées par plusieurs personnes.

Durée : 11h55 d'e-learning

Langues : français, anglais

TESTER

IT SPECIALIST : NETWORK SECURITY CERTIFICATION

S’entraîner

Les tests pratiques ITS Network Security sont alignés sur les objectifs de certification.

Les tests pratiques sont des évaluations basées sur la performance qui permettent aux candidats de se familiariser avec l'environnement de test et de gagner en confiance avant le jour de l'examen. Ils préparent les candidats à l'examen Information Technology Specialist : Network Security.

Les candidats réussissant l'examen Information Technology Specialist : Network Security auront des connaissances et des compétences fondamentales en matière de sécurité.

Inclus :

- 3 examens blancs

Langues : français, anglais