Certification IT Specialist Sécurité Internet

RS :

Les candidats à cet examen démontreront des connaissances et des compétences de base en matière de sécurité, y compris une compréhension des principes de sécurité fondamentaux de la sécurité du système d'exploitation, de la sécurité des réseaux et des appareils, des pratiques informatiques sécurisées.

Objectifs

Défense en profondeur

1.1 Identifier les principes de sécurité fondamentaux : Confidentialité, intégrité, disponibilité, non-répudiation, menace, risque, vulnérabilité, principe du moindre privilège, surfaces d'attaque

1.2 Définir et appliquer la sécurité physique : Sécurité du site, sécurité informatique, périphériques et lecteurs amovibles, pièges à main

1.3 Identifier les types de politique de sécurité : Contrôles administratifs, contrôles techniques

1.4 Identifier les types d'attaques : Débordement de la mémoire tampon, virus, virus polymorphes, vers, chevaux de Troie, logiciels espion, logiciels de rançon, logiciels publicitaires, portes dérobées, attaques/vulnérabilité zero, attaques par déni de service (DoS), méthodes d'attaques courantes, types de vulnérabilité, intersites scripting (XSS), injection SQL, attaque par force brute, man-in-the-middle (MITM) et man-in-the-browser (MITB), ingénierie sociale, enregistreurs de frappe (logiciels et matériels), bombes logiques

1.5 Identifier les types de sauvegarde et de restauration : Complète, incrémentale, différentielle

Sécurité du système d'exploitation

2.1 Identifier la protection du client et du server : Séparation des services, durcissement, gestion des correctifs, réduction de l'attaque surface, stratégie de groupe (gpupdtate et gpresult), domaine dynamique sécurisé, mise à jour du système de noms (DNS), contrôle de comptes d'utilisateurs (UAC), conservation système d'exploitation client et logiciel mis à jour, chiffrement des dossiers hors ligne, politique de restriction logicielle

2.2 Configurer l'authentification des utilisateurs : Authentification multi facteur, application des politiques de mot de passe, accès à distance, utiliser la connexion secondaire pour effectuer des tâches administratives (exécuter en tant que, sudo), création de domaines et d'utilisateurs et de groupes locaux

2.2 Gérer les autorisations sous Windows et linux : Autorisations de fichiers et de dossiers, autorisation de partage, héritage, déplacement ou copier des fichiers sur le même disque ou sur un autre disque, plusieurs groupes avec différentes autorisations, appropriation, délégation

© 2022, OPEN CERTIF - 21 Rue Jean Rostand - 91400 ORSAY- France - RCS : Evry B 797 829 199 – https://www.opencertif.fr

Sécurité du système d'exploitation

2.4 Faciliter la non-répudiation à l'aide de politiques d'audit et de fichiers journaux : Types d'audit, ce qui peut être audité, pour quoi auditer à des fins spécifiques, ou enregistrer les informations d'audit, examiner les fichiers journaux,

2.5 Démontrer la connaissance du cryptage : Cryptage de fichiers et de dossiers, impact du cryptage sur le déplacement/la copie de fichiers et dossiers, chiffrement du lecteur, TPM, processus de communication sécurisés (email, SMS, Chat, réseaux sociaux), réseau privé virtuel (VPN), méthodes de cryptage, clé publique/clé privée, propriétés du certificat et services, Bitlocker

Sécurité des périphériques réseau

3.1 Mettre en œuvre la sécurité sans fil : Types de sécurité sans fil (force de cryptage), identifiants d'ensemble de services (SSID), filtrage MAC, configuration par défaut (OOBE)

3.2 Identifier le rôle des dispositifs de protection du réseau : Objectif des pare-feu matériel contre le logiciel, pare feu réseau contre hôte, inspection de pare-feu avec état ou sans état, bases de référence de sécurité, système de détection d'intrusion (IDS), système de prévention d'intrusion (IPS), gestionnaire d'informations et d'évènements de sécurité (SIEM) , contenu filtrage, liste noire/ liste blanche

3.3 Identifier les méthodes d'isolation du réseau : Routage, honeynet, réseaux de périmètre (DMZ), NAT/PAT, VPN, IPsec, réseau air gap, DirectAccess, réseau local, virtuel (VLAN)

3.4 Identifier les concepts de sécurité des protocoles : Tunneling, DNSSEC, renfilage de réseau, ports connus (FTP, http, HTTPS, DNS, RDP, Telnet, SSH, LDAP, LAAPS, SNMP, SMTP, IMAP, SFTP)

Informatique sécurisée

4.1 Mettre en œuvre la protection des e-mails : Antispam, usurpation d'identité, phishing et pharming, protection des clients, formation des utilisateurs.

4.2 Gérer la sécurité du navigateur : Paramètres du navigateur, gestion du cache, navigation privée

4.3 Installer et configurer un logiciel anti-malware et antivirus : installation, désinstallation, réinstallation et mise à jour ; assainissement, schéma, correction, planification, enquête sur les alertes

© 2022, OPEN CERTIF - 21 Rue Jean Rostand - 91400 ORSAY- France - RCS : Evry B 797 829 199 – https://www.opencertif.fr