Formation Mettre en oeuvre la sécurité réseaux

Code : SEC-NETWORK-100 Durée : 4 jours (28 heures)

Public visé

Responsables de la sécurité des systèmes d'information (RSSI), directeurs des systèmes d'information (DSI), administrateurs système et réseau, techniciens de maintenance système et réseau, consultants en sécurité informatique.

{{< formation-prerequis >}}

Objectifs pédagogiques

À l'issue de cette formation, vous serez capable de :

- Identifier les enjeux de la sécurité des systèmes d'information, ainsi que ses acteurs et ses limites
- Proposer des solutions pour pouvoir faire transiter et stocker des données sur un réseau d'entreprise de façon sécurisée
- Installer et paramétrer un pare-feu approprié au réseau d'une entreprise
- Installer et configurer un proxy
- Mettre en place un filtrage
- Utiliser différents outils permettant de prévenir et détecter une intrusion sur un réseau

Programme

Jour 1 - Matin : Les fondamentaux de la sécurité système et réseau

- Définition de la cybersécurité et terminologie de base
- Aperçu des menaces, vulnérabilités et attaques courantes
- L'importance de la sécurité pour les entreprises et les organisations gouvernementales
- Le pilotage et la maîtrise des risques
- Les normes et règlements de la sécurité
- Les méthodologies appliquées
- Les documentations essentielles
- Les architectures réseaux et leurs évolutions
- Les systèmes d'exploitation modernes et leur sécurité
- La conception d'application et ses évolutions en cybersécurité

Jour 1 - Après-midi : Principes de sécurité des réseaux

- Rappels sur le modèle OSI
- Les composants d'un réseau (routeurs, switches, hubs, firewalls...)
- La sécurité des protocoles réseau (TCP/IP, DNS, DHCP, HTTP...)
- Les forces et faiblesses d'un commutateur
- Les faiblesses de l'accès réseau
- Les faiblesses de la couche d'interconnexions des réseaux
- Les faiblesses de la couche transport
- Les principales faiblesses de la pile TCP/IP
- Les faiblesses de la couche application
- La démarche de sécurisation des réseaux
- Les techniques de sécurisation des réseaux (pare-feu, VPN, IDS/IPS...)
- Maîtriser l'interprétation des flux réseaux
- Panorama des solutions du marché

Travaux pratiques indicatifs

- Réaliser une attaque d'ARP Cache Poisoning et proposer des mesures de prévention
- Déterminer l'ensemble des ports TCP/IP ouverts sur la machine jouant le rôle de routeur
- Réaliser une attaque MITM entre deux machines du réseau
- Evader la sécurité IPS d'une machine du réseau

Jour 2 - Matin : Intégrer et gérer un firewall

- Le rôle et le positionnement d'un firewall
- Les différents types de firewalls et leurs avantages
- Les composantes d'une règle de filtrage
- ACL (Access Control List)
- Eviter les faux positifs
- Les bonnes pratiques
- La gestion de la journalisation
- L'utilisation des agents SNMP (Simple Network Management Protocol)

Travaux pratiques indicatifs

- Déployer un firewall stateful
- Créer des règles pour n'autoriser que la station à communiquer avec la machine de formation, sauf pour le DNS et l'HTTP / HTTPS
- Réaliser une attaque de SYN Flood et proposer des mesures de prévention

Jour 2 - Après-midi : Mise en place d'un proxy

- Le rôle et le positionnement d'un proxy
- Les différents types de proxies et leurs avantages
- Les étapes de déploiement d'un proxy
- La création de règles et de listes
- Les bonnes pratiques

Travaux pratiques indicatifs

- Déploiement d'un proxy et paramétrage d'un filtrage utilisateur par Blacklist

Jour 2 - Après-midi (suite) : Les IDS et IPS

- Le rôle et le positionnement des IPS et des IDS
- Les différents types d'IPS et d'IDS (HIDS, NHIDS, HIPS...)
- Les composantes d'une règle de détection et de filtrage
- Les bonnes pratiques
- La gestion de la journalisation
- La remontée des alertes

Travaux pratiques indicatifs

- Déploiement d'un NIDS et paramétrage des remontées de logs
- Déploiement d'un HIPS et paramétrage des remontées de logs

Jour 3 - Matin : La sécurité du routage

- Le rôle et le fonctionnement des routeurs
- Les attaques sur les routeurs
- Les attaques sur les protocoles de routage :
- RIP (Routing Information Protocol)
- OSPF (Open Shortest Path First)
- EIGRP (Enhanced Interior Gateway Routing Protocol)
- HSRP (Hot Standby Router Protocol)
- IS-IS
- BGP (Border Gateway Protocol)
- Les "Appliances" de sécurité

Travaux pratiques indicatifs

- Mise en place d'un routeur et sécurisation de la couche de routage

Jour 3 - Après-midi : La virtualisation et son durcissement

- Rappel sur la virtualisation
- Les composantes principales d'un système de virtualisation
- Les risques et faiblesses inhérents à la virtualisation
- Les éléments de sécurisation
- Les nouveaux concepts de virtualisation (NFV...)
- Les autres solutions d'abstraction (conteneurisation, isolation...)

Jour 3 - Après-midi (suite) : Durcissement Windows

- La politique de mises à jour et de patchs
- La sécurité des comptes utilisateurs :
- Politique de gestion des mots de passe
- Désactivation des comptes utilisateurs inutilisés

- La politique de gestion du contrôle d'accès aux fichiers et au registre
- La sécurité des données et de l'exécution :
- Les antivirus et antimalwares (Microsoft Defender, Device Guard, Credential Guard, AMSI)
- Le chiffrement des disques durs (Bitlocker, TPM, agent de récupération)
- La prévention de l'exécution (Applocker, DEP, ASLR, CFG, SEHOP…)
- La sécurité des contenus Web (Smartscreen)
- La sécurité du démarrage (Secure Boot - UEFI)
- Le pare-feu Windows (configuration et règles)
- Le contrôle de l'élévation de privilèges (UAC)
- La politique d'audit et de logs
- Les Group Policies

Jour 4 - Matin : Durcissement Windows - Suite

Travaux pratiques indicatifs

- Déploiement d'Applocker et paramétrage d'une interdiction d'exécution d'application en dehors de "Program Files" et "Windows"
- Création d'une exception dans Applocker pour Teams
- Modification de l'élévation de privilèges pour mettre l'accès aux privilèges avec ou sans UAC
- Création de règles de firewall pour durcir l'accès aux protocoles d'infrastructure
- Mise en place d'IPSec pour l'administration du poste Windows

Jour 4 - Matin (suite) : Durcissement Linux

- La politique de mises à jour et de patchs
- La sécurité des comptes utilisateurs :
- Gestion de comptes d'accès
- Politique de gestion des mots de passe
- Désactivation des comptes utilisateurs inutilisés
- Délai d'expiration de sessions utilisateurs
- PAM et NSS
- La minimisation des services :
- Services exposés à des flux non maîtrisés
- Services réseau résidents
- Configuration des services avec sysctl

Jour 4 - Après-midi : Durcissement Linux - Suite

- La gestion des privilèges :
- Vérification du système de fichiers et des droits
- Gestion des droits d'accès
- L'Umask
- Les fichiers sans utilisateur ou groupe propriétaire
- Les fichiers et répertoires accessibles à tous en écriture
- Les fichiers IPC nommés, sockets ou pipes

- Les fichiers à contenu sensible
- Le pare-feu et sa configuration de base
- La prévention et la sécurisation de l'exécution :
- Le chiffrement des partitions
- Les fichiers exécutables setuid ou setgid
- Les systèmes de contrôle d'accès mandataire (SELinux, AppArmor, Smack...)
- Les systèmes de jails et de conteneurs (chroot, schroot, docker, LXC, firejail...)
- Protection contre les buffer-overflows (PaX, Grsecurity, GCC avec SSP, ASan, Valgrind...)
- La configuration d'outils et services de monitoring :
- Surveillance du système par auditd
- Utilisation et gestion de Syslogd
- La sécurisation des mails système et root
- Le Kernel Hardening

Travaux pratiques indicatifs

- Création d'un script système de surveillance des configurations dans /etc et sécurisation de son exécution
- Création d'un script de surveillance de l'activité du système de fichiers et sécurisation de son exécution
- Configuration du firewall pour limiter l'accès à SSH à votre poste

Modalités d'évaluation des acquis

En cours de formation, par des études de cas ou des travaux pratiques. En fin de formation, par un questionnaire d'auto-évaluation.

{{< formation-require >}}

{{< formation-seealso >}}