Développez vos talents
Certifiez vos compétences

Sécurité défensive

Sécurité des systèmes et services réseaux

4 jours (28h00) | ★★★★☆ 4/5 | SEC-ESS | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Cybersécurité › Sécurité défensive

À l'issue de ce stage vous serez capable de :

- Connaître les enjeux de la sécurité des systèmes d'information, ainsi que ses acteurs et ses limites
- Proposer des solutions pour pouvoir faire transiter 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 détecter une intrusion sur un réseau.

Niveau requis

Avoir des connaissances en réseau et système.

Public concerné

Administrateurs système et réseau, consultants en sécurité informatique.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

(1) Modalité et moyens pédagogique :

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel). Environnements de formation installés sur les postes de travail ou en ligne. Supports de cours et exercices.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

Programme

Jour 1

Les fondamentaux de la sécurité système et réseau

- Quelques fondamentaux
- Les fondamentaux de la SSI
- Panorama des risques actuels
- Piloter et maîtriser les risques
- Méthodologies appliquées
- Les documentations essentielles
- Les architectures réseaux
- Evolution des architectures
- La sécurisation d'un système
- Réussir et mettre en oeuvre une bonne sécurisation
- Panorama des solutions du marché

Les forces et faiblesses des protocoles TCP/IP

- Principales faiblesses de la pile TCP/IP
- Contourner un environnement Linux
- Les faiblesses de l'accès réseau
- La couche d'interconnexion des réseaux
- La couche transport
- La couche application
- Maîtriser l'interprétation des flux réseaux
- La sécurisation des réseaux
- Forces et faiblesses d'un commutateur

Exemple de travaux pratiques (à titre indicatif)

- *Démonstration d'attaques et défense sur TCP/IP*

Jour 2

Intégrer et gérer un firewall

- Utiliser un firewall
- Utiliser des ACL (Access Control List)
- Utiliser les agents SNMP (Simple Network Management Protocol)
- Gérer la journalisation
- Eviter les faux positifs

Exemple de travaux pratiques (à titre indicatif)

- *Déploiement d'un firewall*

Proxy, IDS (Intrusion Detection System) et IPS (Intrusion Prevention System)

- Les proxies
- Installation
- Création de règles et listes
- Bonnes pratiques
- Les IDS et IPS
- Différents IDS (HIDS, NHIDS...)
- Installation d'un NIDS (Network Based Intrusion Detection System)
- Mise en pratiques des règles
- Remonter les alertes

Exemple de travaux pratiques (à titre indicatif)

- *Déploiement d'un IDS*

Jour 3

Sécurité du routage

- Les "appliances" de sécurité
- Les 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)

Exemple de travaux pratiques (à titre indicatif)

- Mise en place d'un routage sécurisé

Virtualisation et durcissement

- Contre-mesures
- Virtualisation
- Risques et faiblesses
- Les éléments de sécurisation
- Nouveaux concepts

Jour 4

Durcissement Windows

- Sécurisation du démarrage (Secure Boot - UEFI)
- Chiffrement des disques durs (Bitlocker, TPM, agent de récupération)
- Pare-feu Windows (configuration et règles)
- Contrôler l'élévation de privilèges (UAC)
- Sécurisation des contenus Web (Smartscreen)
- Windows Defender
- Fonctionnalités antivirales (Device Guard, Credential Guard, AMSI)

Exemple de travaux pratiques (à titre indicatif)

- *Elévation de privilèges avec et sans UAC*
- *Durcissement d'une machine Windows*

Durcissement Linux

- Services exposés à des flux non maîtrisés
- Configuration système - sysctl
- Gestion de comptes d'accès
- Désactivation des comptes utilisateurs inutilisés
- Délai d'expiration de sessions utilisateurs
- PAM et NSS
- PAM (Pluggable Authentication Modules)
- NSS (Name Service Switch)
- Vérification systèmes de fichiers et droits
- Umask
- Fichiers à contenu sensible
- Les fichiers exécutables setuid ou setgid
- Fichiers sans utilisateur ou groupe propriétaire
- Les fichiers et répertoires accessibles à tous en écriture
- Les fichiers IPC nommés, sockets ou pipes
- Services réseau résidents
- Configuration d'outils et services de monitoring
- Syslog
- Mails et mails root
- Surveillance du système par auditd

Exemple de travaux pratiques (à titre indicatif)

- *Durcissement d'une machine Linux*

Modalités d'évaluation des acquis

L'évaluation des acquis se fait :

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)