Développez vos talents
Certifiez vos compétences

Sécurité défensive

Durcissement des systèmes et réseaux - Hardening

5 jours (35h00) | ★★★★½ 4,6/5 | SEC-DUR | 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 :

- Modifier les systèmes d'exploitation Windows et Linux pour renforcer leur sécurité.

Niveau requis

Avoir des connaissances générales sur TCP/IP et la mise en oeuvre de services réseaux et systèmes.

Public concerné

Administrateurs système et réseau, consultants en sécurité.

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

Introduction sur l'écosystème actuel

- L'évolution des systèmes d'information et leurs ouvertures sur le monde
- Les menaces courantes pesant sur les systèmes d'information
- Les menaces récentes
- Chronologie et évolutions majeures des systèmes d'exploitation Windows

Exemple de travaux pratiques (à titre indicatif)

- *Questionnaire sur les fonctionnalités Windows et les risques SI*

Une défense alignée aux attaques

- Compréhension de la défense par rapport à un scénario d'attaque
- Segmentation des phases d'un attaquant
- Etudier les outils et méthodes d'attaque par phases avec la Cyber Kill Chain (ATT&CK)
- Les attaques courantes dans un domaine Windows

Exemple de travaux pratiques (à titre indicatif)

- *Mener une étude Cyber Kill Chain*

Jour 2

Durcissement des domaines Windows

- Stratégies de contrôle d'applications (AppLocker)
- Cohérence et défauts de conception de la structure Active Directory (ACL)
- Recommandations de sécurité pour Active Directory (bonnes pratiques)

Exemples de travaux pratiques (à titre indicatif)

- *Implémentation de AppLocker via les stratégies de groupe*
- *Comment LAPS réduit les chances de réussite de mouvements latéraux ?*
- *Implémentation de LAPS pour les clients d'un domaine Windows*

Jour 3

- Utilisation d'un infrastructure de clés publiques (PKI) pour la création de stratégies de sécurité réseau (NPS, Radius)
- Sécurité des réseaux Wi-Fi
- Sécurisation de l'administration du domaine (WinRM, RPC, WMI, RDP)
- Sécurité des services et comptes de services managés (MSA)
- Classification et marquage de l'information pour les systèmes de prévention de pertes de données (DLP)
- Audit et centralisation des journaux d'évènements Windows
- Présentation d'une solution d'analyse de menaces avancées (ATA)
- Sécurité des environnements Azure (Identity Protection, RMS, bonnes pratiques)

Exemples de travaux pratiques (à titre indicatif)

- *Implémentation*
  - *D'un contrôle d'accès Radius*
  - *D'un contrôle d'accès Wi-Fi basé sur Radius*
  - *De Radius pour un contrôle d'accès VPN*

Jour 4

Durcissement de base Linux

- Mot de passe root et comptes administrateur
- Installation d'éléments supplémentaires : clés et certificats
- Pare-feu Linux
  - Configuration "iptable"
  - Règles
  - Netfilter
- Contrôler les accès et l'élévation de privilèges (SELinux)
- Configuration système (systemctl)
- Gestion de comptes d'accès et SSH
- Désactivation des comptes utilisateurs inutilisés
- Délai d'expiration de sessions utilisateurs
- Vérification systèmes de fichiers et droits (Umask)
- Les 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
- Mails et mails root

Exemple de travaux pratiques (à titre indicatif)

- *Elévation de privilèges via un CRON et sécurisation de ce dernier*

Jour 5

Durcissement des protocoles

- Les bases de l'authentification Linux (PAM, NSS)
- Analyse des protocoles actifs (Netstat, Wireshark)
- Les services réseau résidents
- Les services exposés à des flux non maîtrisés
- Etude des protocoles et services faillibles
- Maîtrise des flux (TCP Wrapper)

Exemple de travaux pratiques (à titre indicatif)

- *Renforcement d'infrastructure par la réalisation d'un script Bash*

Mécanismes de défense avancée

- Prévention contre le brute-force (Fail2ban)
- Isolation de l'exécution d'un programme (chroot)
- Sécurisation du noyau (grsecurity)
- Détection d'intrusion hôte (OSSEC)
- Configuration d'outils et services de monitoring
- Surveillance du système (auditd)

Exemple de travaux pratiques (à titre indicatif)

- *Réalisation d'un rapport d'audit*

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)