Développez vos talents
Certifiez vos compétences

Sécurité défensive

Durcissement sécurité Linux

4 jours (28 heures) | ★★★★½ 4,4/5 | SEC-LEC | 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 principales menaces de l'environnement Linux et les différentes solutions qui s'y rapportent
- Pouvoir optimiser la sécurisation du système.

Niveau requis

Etre familiarisé avec le système d'exploitation Linux. Avoir des connaissances de base en sécurité des systèmes d'information.

Public concerné

Responsables sécurité du SI, chefs de projets informatiques, ingénieurs et administrateurs systèmes.

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

- Généralités sur Linux
- Menaces et attaques sur l'environnement Linux
- La sécurité de l'environnement Linux
- Les test d'exposition (Shodan)

Exemples de travaux pratiques (à titre indicatif)

- *Simulation d'attaque sous Linux*
- *Test d'exposition avec Shodan*
- *Recherches des CVE...*

Les politiques de sécurités

- Les politiques de sécurité
- Caractéristiques d'une PSSI (Politique de Sécurité du Système d'Information)
- Types de politiques de sécurité
- Normes et standards de sécurité

Exemple de travaux pratiques (à titre indicatif)

- *Mise en place d'une PSSI...*

Guide des bonnes pratiques de déploiement du système Linux

- Matériel
- Démarrage
- Configuration du noyau
- Paquetages logiciels
- Partitionnement des disques durs
- Les scripts de démarrage
- Réseau
- Ecrire des procédures Shell sécurisées (script)

Exemple de travaux pratiques (à titre indicatif)

- *Déploiement sécurisé de système Linux...*

Identification et authentification

- Définitions
- Gestion des mots de passe
- Gestion des comptes utilisateurs
- Présentation de PAM (Pluggable Authentication Modules)
- Les niveaux de sécurité PAM
- Les OTP (Sécurité Hardware et Software)

Exemples de travaux pratiques (à titre indicatif)

- *Cracking de mots de passe*
- *Durcissement des configurations des mots de passe*
- *Durcissement de l'authentification via les modules PAM...*

Protection des fichiers

- Droits standards des systèmes de fichiers Unix
- Les listes de contrôle d'accès
- Les attributs étendus
- Vérification de l'intégrité d'un système de fichiers
- Le chiffrement des fichiers
- Le ACL (Access Control List)

Exemples de travaux pratiques (à titre indicatif)

- *Chiffrement de partitions*
- *Mcrypt*
- *VeraCrypt*
- *Chiffrement hardware*
- *Déploiement d'un système de contrôle d'intégrité...*

Jour 2

La sécurité du noyau

- SELinux
- GrSecurity
- Sysctl

Exemples de travaux pratiques (à titre indicatif)

- *Configuration du grsecurity*
- *Configuration SELinux*
- *Création d'une politique SELinux...*

Les malwares sous Linux

- Les types de malwares sous Linux
- Simulation d'attaque
- Les rootkits
- Solutions anti-malwares

Exemples de travaux pratiques (à titre indicatif)

- *Simulation d'attaque via malware*
- *Simulation de rootkits*
- *Mise en place d'une solution anti-malware...*

Jour 3

La sécurité du réseau

- Panorama des attaques
- Sécurité au niveau de la couche physique
- Sécurité au niveau de la couche liaison
- Sécurité au niveau de la couche réseau
- Daemons et serveurs
- VPN

Exemples de travaux pratiques (à titre indicatif)

- *Mise en place d'attaque MiTM*
- *Mise en place d'une connexion VPN "Point-to-Site"...*

La sécurité par la surveillance du système

- L'utilitaire de consignation
- Outils d'analyse des logs
- Le dispositif d'accounting system
- Application de patchs
- Mise à jour du système

Exemples de travaux pratiques (à titre indicatif)

- *LogCheck*
- *Osquery*
- *Splunk...*

Le patch management

- Mise en place d'une politique et solution de patch management

Exemples de travaux pratiques (à titre indicatif)

- *Déploiement d'une politique de patch management*
- *Déploiement d'une solution de patch management (ManagemEngine...)*

Jour 4

Les sondes de détection d'intrusions

- Les IDS (Intrusion Detection System)
- Les IPS (Intrusion Prevention System)
- Les HIDS (Host-based Intrusion Detection System)
- Les HIPS (Host-based Intrusion Prevention System)
- Modèle de déploiement
- OSSEC et Tripwire
- OSSIM
- Les EDR (Endpoint Detection and Response)

Exemple de travaux pratiques (à titre indicatif)

- *Mise en place d'OSSIM, de Tripwire, d'un EDR...*

Durcissement complémentaire

- Durcissement
  - Des serveurs Web
  - Des serveurs mail
  - Des serveurs FTP
  - Applicatif
  - Des hyperviseurs
  - Des VM
  - IPv6
- Sécurité des données (RGPD)
- Les plans DLP (Data Loss Prevention)

Exemples de travaux pratiques (à titre indicatif)

- *Lynis*
- *Durcissement d'un serveur Web / mail / FTP*
- *Durcissement d'hyperviseurs*
- *Mise en place d'une solution DLP : MyDLP...*