3-31– Unix/Linux Sécurité

Référence : 3-31
Durée : 4 jour(s) (28h)
Théorie : 30 %
Pratique : 70 %
Certification : Aucune
Appréciation : Evaluation qualitative de fin de stage
Modalités et moyens pédagogiques : Démonstrations – Cas pratiques – Synthèse et évaluation des acquis

A l'issue de ce stage vous serez capable de : Acquérir des connaissances et compétences pour sécuriser un système UNIX ou LINUX et les applications réseaux grâce à Unix/Linux – firewall, filtrage, proxy

Prérequis : Etre familiarisé avec le système d'exploitation Linux et une expérience d'administration de Unix/Linux est recommandée. Avoir des connaissances de base en sécurité des systèmes d'information

Public concerné : Administrateurs – Techniciens

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.

PROGRAMME

JOUR 1

▪ INTRODUCTION

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

EXEMPLES DE TRAVAUX PRATIQUES (A TITRE INDICATIF)

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

▪ LES POLITIQUES DE SECURITES

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 (A TITRE INDICATIF)

Mise en place d'une PSSI...

▪ GUIDE DES BONNES PRATIQUES DE DEPLOIEMENT DU SYSTEME 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 (A TITRE INDICATIF)

Déploiement sécurisé de système Linux...

▪ IDENTIFICATION ET AUTHENTIFICATION

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

EXEMPLES DE TRAVAUX PRATIQUES (A 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 (A TITRE INDICATIF)

Chiffrement de partitions
Mcrypt
VeraCrypt
Chiffrement hardware
Déploiement d'un système de contrôle

JOUR 2

▪ LA SECURITE DU NOYAU

SELinux
GrSecurity
Sysctl

EXEMPLES DE TRAVAUX PRATIQUES (A 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 (A TITRE INDICATIF)

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

JOUR 3

▪ LA SECURITE DU RESEAU

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 (A TITRE INDICATIF)

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

▪ LA SECURITE PAR LA SURVEILLANCE DU SYSTEME

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 (A TITRE INDICATIF)

LogCheck
Osquery
Splunk...

▪ LE PATCH MANAGEMENT

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

EXEMPLES DE TRAVAUX PRATIQUES (A TITRE INDICATIF)

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

JOUR 4

▪ LES SONDES DE DETECTION 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 (A TITRE INDICATIF)

Mise en place d'OSSIM, de Tripwire, d'un EDR…

▪ DURCISSEMENT COMPLEMENTAIRE

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 (A TITRE INDICATIF)

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

FICHE RESSOURCES

- **CONFIGURATION MATERIELLE ET LOGICIELLE – FORMATEUR**

Un poste Windows 10 avec du VMware Workstation 15 ou plus.
16go ram ou plus
500 go de disqur dur (SSD)
VMWARE Workstation 15 ou plus
Images OVA fournies au début de la formation

- **CONFIGURATION MATERIELLE ET LOGICIELLE – STAGIAIRE**

Un poste Windows 10 avec du VMware Workstation 15 ou plus.
16go ram ou plus
500 go de disqur dur (SSD)
VMWARE Workstation 15 ou plus
Images OVA fournies au début de la formation

- **MATERIEL PEDAGOGIQUE**

1 tableau blanc
1 vidéoprojecteur connecté sur le poste du formateur