



Profil stagiaires :

La formation s'adresse à des responsables informatiques d'un système réseau Unix souhaitant intégrer la gestion de la sécurité sous Linux.

Pré requis :

Pour suivre ce cours, les stagiaires doivent disposer des connaissances sur les systèmes informatiques Unix et Linux

Durée :

3 jours

Moyens Pédagogiques

Alternance de cours théoriques et d'exercices pratiques.

Une personne par poste micro.
Support de cours.

Modalités de suivi :

- Validation des compétences acquises par des exercices pratiques à la fin de chaque module.
- Test pratique reprenant l'intégralité des modules étudiés en fin de formation.
- A l'issue de la formation est remis un bilan stagiaire et une évaluation du formateur.
- Feuilles d'émargement.

Animateur :

Consultant informaticien spécialiste Certifié MCT.

Contact commercial :

David DEHAIS

Tél : 02.35.590.591

Fax : 02.35.80.82.99

Email : d.dehais@aemy.fr

Cours:

Sécurité UNIX ET LINUX

Objectif de la formation

A l'issue de ce cours, les stagiaires seront capables de :
établir la sécurité des plates-formes Unix et Linux .

Module 1 : UNIX ET LA SÉCURITÉ

Les buts de la sécurité

- Authenticité
- Confidentialité
- Disponibilité
- Intégrité
- Protection contre les "exploits"

Parvenir à la sécurité d'UNIX

- Détecter les intrusions avec audits/journaux
- Eviter des défauts de sécurité en remplaçant les composants faibles

Protection des données et systèmes avec la cryptographie

- PGP (Pretty Good Privacy)
- GnuPG (Gnu Privacy Guard)
- Authenticité et intégrité grâce aux signatures numériques et aux "hash codes"

Module 2 : PROTÉGER LES COMPTES UTILISATEURS ET RENFORCER L'AUTHENTIFICATION

Utilisation sécurisée des comptes

- Le processus de connexion à UNIX
- Contrôle de l'accès aux comptes avec les "PAM" (Pluggable Authentication Modules)
- Assurer des mots de passe de "bonne qualité"

Suivi et désactivation des comptes

- Suivi de l'utilisation des comptes
- Comment et quand désactiver des comptes
- Gestion des numéros d'identification des utilisateurs et des groupes

Connexions à travers le réseau

- Le danger de la confiance entre machines et réseaux
- Authentification plus forte lors de la connexion avec S/Key, jetons et OPIE
- Remplacement des clients et serveurs TELNET et **rlogin** avec SSH
- passwd et group

Module 3 : RÉDUIRE LES MENACES EN LIMITANT LES PRIVILÈGES SUPER UTILISATEUR

Contrôle de l'accès aux racines

- Configuration de terminaux sûrs
- Empêcher l'accès aux réseaux non sécurisés

- Acquérir des privilèges **root** avec **su**
- Utilisation de groupes au lieu de l'identité **root**

Contrôle de l'accès basé sur le rôle (RBAC)

- Risques de l'accès "tout ou rien" d'UNIX
- RBAC avec Solaris
- RBAC avec la sécurité NSA de Linux
- Ajout de RBAC avec **sudo**

Module 4 : Protéger les données essentielles en sécurisant les systèmes de fichiers locaux et en réseau

Structure et partitionnement des répertoires pour la sécurité

- Fichiers, répertoires, périphériques et liens
- Utilisation de partitions en lecture seule
- Permissions d'accès et propriété
- Utilisation de listes de contrôle d'accès (ACL)
- Fichiers immuables et en ajout seul

Sauvegarde et test de l'intégrité

- Sauvegarde des données
- Détection d'intrusions avec Tripwire

NFS : le système de fichiers réseau

- Identifier les faiblesses de NFS
- Options de sécurité pour clients et serveurs
- Sécurité de NFS via Secure RPC

Renforcement des systèmes UNIX

Amélioration de la sécurité avec **TITAN**

- Défense contre les attaques distribuées de type refus de service



Cours :

Sécurité UNIX ET LINUX (fin)

Module 5 : Eviter l'exécution de Programmes

Les risques provenant d'exécutions de programme non souhaitées

- Démarrage subreptice des programmes
- Exécution de programmes en tant qu'autre utilisateur
- Contrôle des files d'attente **cron** et **at**

Scripts

- Réduction des faiblesses dans les scripts de démarrage
- Empêcher les attaques

Module 6 : Minimiser les risques des services réseau

TCP/IP et les points faibles de la sécurité

- Le rôle critique de DNS
- Renforcer la sécurité de la suite TCP/IP

La sécurité des services réseau internes

- Amélioration des enregistrements
- Configuration de OpenSSH et OpenSSL
- Chiffrement DES pour des RPC sûrs
- Authentification du réseau avec Kerberos
- Système X Window : faiblesses/solutions

Connexion sûre aux réseaux externes

- Contrôle et enregistrement de l'accès aux serveurs avec des **tcp wrappers** et **xinetd**
- Réduction des problèmes de "buffer overflow"
- Réduction des fuites d'information
- Sécurisation des accès de type messagerie, FTP et Web