

Sécurité UNIX[®] et Linux[®] : Travaux Pratiques - 4 jours

Protéger le système et le réseau contre les intrusions

formation 433

- Vous apprendrez à**
- Protéger les systèmes UNIX et Linux contre les menaces internes et externes
 - Établir un accès authentifié aux ressources locales et à distance
 - Identifier les vulnérabilités avec les scans et corriger les problèmes décelés
 - Éviter des problèmes de sécurité en limitant les privilèges de superutilisateur
 - Configurer des outils et des utilitaires pour détecter les intrusions
 - Remplacer les versions non sûres des composants logiciels

Objectif La famille UNIX des systèmes d'exploitation, y compris les versions Linux, est très appréciée pour sa souplesse et son ouverture. Cependant, les points faibles peuvent rendre les systèmes UNIX sensibles aux menaces de sécurité. Ce cours apporte les connaissances nécessaires pour sécuriser vos plates-formes UNIX et Linux. Vous apprendrez à utiliser les outils pour évaluer les vulnérabilités, détecter les menaces et fournir des contrôles d'accès efficace.

À qui s'adresse cette formation Aux administrateurs ainsi qu'à tous ceux qui sont impliqués dans le déploiement de systèmes ouverts. Des connaissances d'UNIX ou de Linux du niveau de la formation 143, "Linux : Introduction complète", ou de la formation 428, "UNIX : Introduction complète", sont nécessaires.

Travaux pratiques Vous acquerez une expérience pratique de la sécurisation de systèmes UNIX et Linux en utilisant Red Hat[®] Enterprise Linux[®], Solaris et BSD. Les exercices incluent :

- Scan de systèmes avec Nessus et réparation des vulnérabilités détectées
- Détection de paramètres de configuration faibles avec Suse
- Analyse de systèmes compromis afin d'empêcher des attaques
- Qualité des mots de passe et des règles d'utilisation de comptes utilisateur avec PAM
- Configuration des serveurs et clients OpenSSH
- Sécurisation de privilèges d'administration limités avec **sudo**

Sécurité UNIX[®] et Linux[®] : Travaux Pratiques - 4 jours

Protéger le système et le réseau contre les intrusions

formation 433

UNIX et la sécurité

Parvenir à la sécurité d'UNIX

- Détecter les intrusions avec audits/journaux
- Éviter des défauts de sécurité
- Identifier les vulnérabilités d'un logiciel et les erreurs de configuration

Protection avec la cryptographie

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

Renforcer l'authentification

Utilisation sécurisée des comptes

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

Suivi et désactivation des comptes

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

Connexion au réseau

- Risques des protocoles d'applications
- Authentification plus forte lors de la connexion grâce à la cryptographie et aux jetons
- Mise en tunnel de protocoles d'application avec SSH

Limiter les privilèges 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**

Audit de l'activité des superutilisateurs

- Limiter l'accès à des comptes privilégiés
- Détecter les utilisations abusives et attaques avec les fichiers journaux

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

- Risques de l'accès "tout ou rien" d'UNIX
- RBAC avec Solaris

- Ajout de RBAC avec **sudo**

Sécuriser les systèmes de fichiers

locaux et en réseau

Structure et partitionnement de répertoires

- Fichiers, répertoires, périphériques et liens
- Utilisation de partitions en lecture seule
- Permissions d'accès et propriété
- Fichiers immuables et en ajout seul
- Vulnérabilités de NFS

Sauvegarde et test de l'intégrité

- Sauvegarde des données
- Détection d'intrusions avec Tripwire

Renforcement des systèmes UNIX

- Amélioration de l'assurance de l'information avec yassp, TITAN et Bastille
- Scan de réseaux avec Nessus pour déceler les vulnérabilités
- Détection de mauvais choix de configuration avec Sussen

Éviter l'exécution de programmes

Risques provenant d'exécutions non souhaitées de programmes

- Démarrage subreptice des programmes
- Exécution de programmes en tant qu'autre utilisateur
- Planification de programmes avec **cron** et **at**
- Diminution des vulnérabilités dans les scripts de démarrage

Réagir aux attaques et aux intrusions

- Trouver des signes d'intrusion dans des données syslog
- Analyse d'un système compromise
- Réduire les effets des exploits de BO (buffer overflow)

Minimiser les risques des services réseau

TCP/IP et ses points faibles de sécurité

- Sniffer des mots de passe avec **Ethereal** et **dsniff**
- Tester l'exposition du réseau avec **netstat**, **isof** et **nmap**

La sécurité des services réseau internes

- Amélioration des enregistrements
- Configuration de OpenSSH et OpenSSL
- Authentification du réseau avec Kerberos

- Système X Window : vulnérabilités/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