

Linux - Sécurisation avancée



Informatique

Référence formation : 4-UX-SEC - Durée : 3 jours

Objectifs

Connaître les failles du système, savoir s'en protéger et surveiller les accès.

Pré-requis

Administrateurs système ou réseau, responsables informatiques, autres professionnels de l'informatique
Pratique courante de Linux en tant qu'administrateur

Contenu pédagogique

1. Linux / Unix et la sécurité

- Parvenir à la sécurité de Linux / 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»

2. Renforcer l'authentification

- Connexion au réseau
- Risque 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

3. Limiter les privilèges utilisateur

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



XXL Formation

34 rue Raymond Aron
76130 Mont Saint Aignan

Tél : 02 35 12 25 55 – Fax : 02 35 12 25 56

N° siret : 485 050 611 00014 – N° d'agrément : 23.76.03752.76



- 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» de Linux / Unix
- RBAC avec Solaris
- Ajout de RBAC avec sudo

4. 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
- Renforcement des systèmes Linux / 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

5. 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

6. 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



XXL Formation

34 rue Raymond Aron
76130 Mont Saint Aignan

Tél : 02 35 12 25 55 – Fax : 02 35 12 25 56

N° siret : 485 050 611 00014 – N° d'agrément : 23.76.03752.76

Membre du réseau
aginius
formation

- Réduction des problèmes de «buffer overflow»
- Réduction des fuites d'information
- Sécurisation des accès de type messagerie, FTP et Web (sécurisation des ports)

Méthodes pédagogiques	Présentation des concepts, démonstration, exécution, synthèse et exercices pratiques d'assimilation
Modalités pédagogiques	Présentiel - Distanciel - AFEST
Moyens pédagogiques	Formateur expert du domaine - 1 ordinateur, 1 support de cours version papier ou numérique, un bloc-note et un stylo par personne - vidéo projecteur - tableau blanc
Modalités d'évaluation	Positionnement préalable oral ou écrit - Evaluation formative tout au long de la formation - Evaluation sommative faite par le formateur ou à l'aide de la certification RS2722 - Certification IT - Administration d'un système Linux - France Compétences (francecompetences.fr) : https://www.francecompetences.fr/recherche/rs/2722
Durée journée de formation	7h00
Public concerné	Salariés - Demandeur d'emploi - Reconversion professionnelle - Public en situation de handicap



XXL Formation

34 rue Raymond Aron
76130 Mont Saint Aignan

Tél : 02 35 12 25 55 – Fax : 02 35 12 25 56

N° siret : 485 050 611 00014 – N° d'agrément : 23.76.03752.76

