Sécuriser un système Linux/Unix

Cours Pratique de 3 jours - 21h
Réf : SRX - Prix 2024 : 2 030CHF HT

Ce stage très pratique vous montrera comment définir une stratégie de sécurité, sécuriser des serveurs Linux et maintenir un niveau de sécurité. Le cours prévoit entre autres la sécurisation du système isolé, la sécurisation du réseau dans l'entreprise ainsi que le nécessaire pour mener à bien un audit de sécurité.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Mesurer le niveau de sécurité de votre système Linux/Unix

Connaître les solutions de sécurisation du système

Mettre en place la sécurité d'une application Linux/Unix

Établir la sécurisation au niveau réseau

TRAVAUX PRATIQUES

Les nombreux exercices seront effectués sur un réseau de serveurs Unix et Linux.

LE PROGRAMME

dernière mise à jour : 08/2018

1) Introduction

- Pourquoi sécuriser un système ?
- Définir une stratégie d'authentification sécurisée.
- Les différents algorithmes de chiffrement. Chiffrement d'un mot de passe. Vérification d'un mot de passe.
- Exemples d'attaques par dictionnaire.

2) La sécurité et l'Open Source

- Les corrections sont rapides, les bugs rendus publics.
- La technique d'approche d'un hacker : connaître les failles, savoir attaquer.
- Exemple d'une vulnérabilité et solution de sécurisation. Quelle solution ?

3) L'installation trop complète : exemple Linux

- Debian, RedHat et les autres distributions.
- Eviter le piège de l'installation facile.
- Allégement du noyau. Drivers de périphériques.

Travaux pratiques : Optimisation des installations dans une optique de gestion de la sécurité.

4) La sécurité locale du système

- Exemples de malveillance et d'inadvertance.
- Faible permissivité par défaut. Vérification des droits des fichiers, scripts et commandes efficaces pour diagnostiquer.
- FS en lecture seule : les attributs des fichiers, disponibilité et intérêt. Outils Tripwire.
- Conservation des logs, combien de temps ?
- L'outil d'analyse des logs : logwatch. Réagir en temps réel : exemple de script. Utiliser RPM comme HIDS.
- Paramétrage de PAM dans les différents contextes.

PARTICIPANTS

Techniciens et administrateurs systèmes et réseaux.

PRÉREQUIS

Bonnes connaissances en administration des systèmes et réseaux.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Confinement de l'exécution des processus. Terminologie DAC, MAC, RBAC, contexte, modèle...
Travaux pratiques : Travail sur les droits, les logs et les processus.

5) La sécurité au niveau réseau
- Utiliser un firewall ? Utiliser les wrappers ?
- Mettre en place des filtres d'accès aux services.
- Configurer un firewall de manière sécurisée.
- Les commandes de diagnostic. Mise en place d'un firewall NetFilter sous Linux.
- Philosophie et syntaxe de iptables.
- Le super-serveur xinetd. Les restrictions d'accès par le wrapper, les fichiers de trace.
- Réaliser un audit des services actifs. Le ssh.
Travaux pratiques : Configurer un firewall. Auditer les services fonctionnels.

6) Les utilitaires d'audit de sécurité
- Les produits propriétaires et les alternatives libres.
- Crack, John the Ripper, Qcrack.
- Les systèmes de détection d'intrusion HIDS et NIDS.
- Tester la vulnérabilité avec Nessus.
- La mise en œuvre d'un outil de sécurité.
Travaux pratiques : Mise en œuvre de quelques outils.

LES DATES

CLASSE À DISTANCE
2024 : 10 juin, 09 sept., 25 nov.