

Administration de la sécurité sous Solaris



La formation "Administration de la sécurité sous Solaris" apporte aux participants les compétences nécessaires pour mettre en place, administrer et gérer un système d'exploitation Solaris sûr

Objectifs

- Expliquer la terminologie associée à la sécurité ainsi que les principaux types d'attaques
- Utiliser les outils de journalisation et d'audit de Solaris pour identifier les attaques réelles et potentielles
- Sécuriser un hôte Solaris contre les attaques utilisateur et réseau
- Utiliser des outils, comme SST (Solaris Security Toolkit), pour renforcer la sécurité du système

Public concerné

- Ce cours s'adresse aux administrateurs systèmes ou aux administrateurs de sécurité Solaris chargés de l'administration d'un ou de plusieurs systèmes Solaris homogènes ou responsables de la sécurité d'un ou de plusieurs systèmes Solaris.

Pré requis

- Maîtriser les fonctions d'administration réseau et système de base du système d'exploitation Solaris
- Installer le SE Solaris
- Savoir administrer les utilisateurs, les imprimantes, les systèmes de fichiers, les réseaux et les périphériques sous Solaris

Une formation de 5 jours

Caractéristiques	Paris
Tarif : 2850 € HT par personne	17/01/2011
Numéro de formateur : 11921795692	14/03/2011
Nombre d'heures : 35	23/05/2011
Référence : S300	27/06/2011
Contact : Loic LE FUR	05/09/2011
Telephone : 01.41.16.83.70	14/11/2011
Email : formation@alterway.fr	

Description des modules

num	Module
1	Exploration de la sécurité
Détails	<ul style="list-style-type: none">- Décrire le rôle de la sécurité système- Expliquer ce qu'est la sensibilisation à la sécurité- Décrire des exemples historiques de break-ins- Expliquer la terminologie associée à la sécurité- Classifier les types d'attaques- Examiner les motivations d'un attaquant- Identifier des méthodes de regroupement de données- Exécuter un système de détection des intrusions- Définir une politique de sécurité- Utiliser les outils de sécurité open source
2	Utilisation des fichiers journaux Solaris
Détails	<ul style="list-style-type: none">- Explorer les fichiers journaux standard de Solaris- Configurer et utiliser l'utilitaire de journalisation du système- Surveiller les fichiers journaux à l'aide de l'outil swatch- Décrire les outils de surveillance des processus- Collecter des informations en utilisant le package de comptabilité de Solaris
3	Examen du module de sécurité BSM Solaris
Détails	<ul style="list-style-type: none">- Configurer l'audit BSM- Démarrer et arrêter BSM- Créer une piste de vérification à l'aide de BSM- Générer une piste de vérification- Interpréter et filtrer des données d'audit- Implémenter un mécanisme de gestion de périphériques BSM
4	Prévention des attaques
Détails	<ul style="list-style-type: none">- Reconnaître les chevaux de Troie- Identifier les attaques par une porte dérobée- Détecter et prévenir les attaques par des chevaux de Troie ou des portes dérobées- Utiliser des rootkits pour cacher les attaquants- Identifier les attaques DoS
5	Administration de comptes utilisateurs sécurisés
Détails	<ul style="list-style-type: none">- Administrer des utilisateurs réguliers- Administrer d'autres comptes utilisateurs- Configurer la sécurité pour des utilisateurs spéciaux- Limiter les options utilisateurs avec des shells restreints
6	Administration de la sécurité par mot de passe
Détails	<ul style="list-style-type: none">- Décrire les mécanismes des mots de passe- Exécuter un programme de craquage de mot de passe
7	Sécurisation de l'accès root
Détails	<ul style="list-style-type: none">- Contrôler l'accès root en utilisant le contrôle d'accès basé sur les rôles (RBAC)- Contrôler l'accès root en utilisant l'utilitaire sudo
8	Prévention des attaques du système de fichiers
Détails	<ul style="list-style-type: none">- Définir la partition root- Définir les droits d'accès au système de fichiers à des fins de sécurité- Explorer les permissions set-user-ID et set-group-ID- Utiliser les listes de contrôle d'accès (ACL)- Examiner d'autres mécanismes de défense- Protéger les systèmes à l'aide de sauvegardes et restaurations

9 **Audit de systèmes de fichiers**

- Détails**
- Examiner l'audit de systèmes de fichiers
 - Explorer les outils d'audit de systèmes de fichiers

10 **Attaque de données réseau**

- Détails**
- Examiner les analyseurs de réseaux
 - Explorer les outils d'analyse des réseaux
 - Se défendre contre les attaques des services réseau

11 **Sécurisation des données réseau**

- Détails**
- Décrire une communication sécurisée en utilisant SSL (Secure Socket Layer)
 - Configurer SSL pour le cryptage et le décryptage de fichiers

12 **Analyse de services réseau**

- Détails**
- Appliquer les outils de vérification pour la sécurité des réseaux
 - Décrire l'utilisation de l'interface graphique pour configurer l'outil d'analyse SAINT
 - Configurer l'outil d'analyse réseau SAINT
 - Interpréter les rapports SAINT
 - Détecter les attaques de l'analyseur de réseaux

13 **Sécurisation des services réseau**

- Détails**
- Restreindre les services réseau
 - Défendre les services réseau
 - Utiliser les commandes r de Berkeley pour les connexions à distance
 - Sécuriser des services avec la commande chroot
 - Intégrer des services à l'aide du PAM
 - Décrire le SEAM (Sun Enterprise Authentication Mechanism)

14 **Automatisation du renforcement de la sécurité de serveur**

- Détails**
- Décrire le renforcement de la sécurité d'un système
 - Décrire le renforcement de la sécurité d'un système à l'aide de SST (Solaris Security Toolkit)
 - Configuration de SST

15 **Authentification des services réseau**

- Détails**
- Décrire l'authentification réseau en utilisant les wrappers TCP
 - Configurer le contrôle d'accès des hôtes
 - Utiliser des bannières avec les TCP wrappers

16 **Sécurisation de l'accès à distance**

- Détails**
- Décrire les avantages du SSH (Secure Shell)
 - Configurer SSH

17 **Sécurisation de l'accès physique**

- Détails**
- Évaluer le risque d'une intrusion physique
 - Appliquer des mesures de sécurité physiques

18 **Connexion du réseau d'entreprise avec le monde extérieur**

- Détails**
- Concevoir un réseau pour augmenter la sécurité
 - Exécuter des audits de sécurité d'entreprise
 - Expliquer le rôle des audits de sécurité
 - Identifier les sources communes d'informations de sécurité