



Linux Sécurité des accès (UX118)

À qui s'adresse cette formation ?

Toute personne souhaitant sécuriser les accès à un système Linux

Quels sont les objectifs ?

- Savoir configurer les mécanismes de sécurité réseau de Linux.

Pré-requis

Une bonne connaissance de l'administration des systèmes Unix/Linux et des réseaux TCP/IP est nécessaire.

Programme

Introduction

- Le besoin, définition du D.I.C. Les attaques possibles. Evaluation des risques. Méthodes de protection.

Les ports de niveaux 5

- Rappels sur la notion de port. Les ports UDP et les ports liés au réseau. Exemples de trames.

Outils de captures réseau

- Les analyseurs de trames : tcpdump, wireshark.
- Atelier : mise en oeuvre de tcpdump, options usuelles, et possibilités de filtrage.
- Installation de Wireshark, capture et analyse de paquets.

Durée

3j ours (soit 21 heures)

Tarif

En intra seulement

Modalités

100 % à distance (D)
ou en présentiel (P)

Dates

En intra seulement

Pédagogie

Alternance théorie /pratique

Modalités d'évaluation

QCM d'évaluation des acquis

Mise à jour Mars 2023

Programme (suite)

Outils de Diagnostic

- Scanners de ports, outils d'audit externe et d'audit interne. Exemples de nmap, hping, sniffit...

Audit réseau

- OpenVAS (Open source Vulnerability Assessment Scanner) : principe de fonctionnement, installation.
- Atelier : réalisation d'un audit réseau avec openVAS.

Sécurisation des accès réseau

- Protection de services réseaux au travers de xinetd. Les tcp-wrappers: telnet, tftp, snmp, ftp, pop3s, imap4s
- Les contrôles d'accès : Etude des fichiers /etc/hosts.allow et /etc/hosts.deny
- Les accès réseaux : sftp, les r-commandes (rlogin, rsh). Sécurisation des transferts de fichiers avec vsftp
- Présentation d'openSSH.
- Atelier : configuration du serveur et du client pour la mise en place d'un tunnel X11 et ssh.

- Sécurisation http (apache) : lors de l'exécution des processus (directives user et group),
- portée des balises, restriction d'accès par méthode : balise Limit, LimitExcept, le fichier .htaccess : autorisation ou restriction d'accès.
- Authentification HTTP. Création d'utilisateurs avec htpasswd.

VPN , tunnels, iptables

- Définitions : DMZ, coupe-feux, proxy. VPN et tunnels. Principe de fonctionnement.
- Présentation des tunnels chiffrés.
- Atelier : mise en oeuvre de stunnel pour sécuriser une messagerie smtp.
- Présentation d'openVPN.
- Atelier : installation, configuration, tests de connexion, création d'un tunnel sécurisé par clé statique. Certificats : SERV et CLT. Pare-feux : les iptables, le filtrage de paquets, définition d'une politique de sécurité.
- Atelier : mise en place des iptables. Traduction d'adresse, traduction de ports. Architecture avec pare-feux et tunneling.

Proxy Squid

- Présentation, principe de fonctionnement. Architecture, hiérarchie de serveurs cache. Exemple d'utilisation, systèmes d'exploitation concernés, logiciels complémentaires.
- Mécanismes de configuration manuelle, automatique. Scripts d'auto-configuration, filtrage suivant DNS, par protocole.
- Clients en mode texte, robots. Installation dans le navigateur. Principe et syntaxe des ACL. Optimisation de l'utilisation du serveur. Restriction d'accès par hôte, par réseau, par plage horaire, par jour, par site.
- Mise en cache des données. Méthodes d'authentification.

Contactez-nous

Cergy-Pontoise

8, rue Pierre de Coubertin
95 300 PONTOISE
01 30 75 36 36

Montigny-le-Bretonneux

7, avenue des Trois Peuples
78 180 MONTIGNY-LE-BRETONNEUX
01 30 48 80 00

formationcontinue@esiee-it.fr
www.esiee-it.fr