775 route de l'aérodrome
ZA Agroparc
84000 Avignon
Tél 04 90 85 98 12
Fax 04 90 86 26 24
info@cit.fr
www.cit.fr

Linux – Sécurité des accès

Objectif : Toute personne souhaitant sécuriser les accès à un système Linux.

À l'issue de la formation, le stagiaire sera capable de :

- Savoir configurer les mécanismes de sécurité réseau de Linux

Prérequis : une bonne connaissance du système Unix/Linux est nécessaire

- 3 jours -

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
- Travaux pratiques : mise en oeuvre de tcpdump, options usuelles, et possibilités de filtrage
- Installation de Wireshark, capture et analyse de paquets

Outils de Diagnostic

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

Audit réseau

- OpenVAS : principe de fonctionnement, installation
- Travaux pratiques : 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
- Travaux pratiques : 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

Déroulé de l'action

- **Type de stage**

  Session Inter-entreprises
  Session Intra

- **Horaires**

  9H00-12H30 /13H30-17H00

- **Méthode pédagogique**

  Alternance exposés théoriques et exercices pratiques

- **Suivi et assistance**

  Support de cours adapté au logiciel étudié et au niveau suivi
  Assistance téléphonique gratuite et illimitée

- **Validation des acquis**

  Exercice de validation en fin d'action

775 route de l'aérodrome
ZA Agroparc
84000 Avignon
Tél 04 90 85 98 12
Fax 04 90 86 26 24
info@cit.fr
www.cit.fr

Linux – Sécurité des accès

VPN , tunnels, iptables

- Définitions : DMZ, coupe-feux, proxy
- VPN et tunnels
- Principe de fonctionnement
- Présentation des tunnels chiffrés
- Travaux pratiques : mise en oeuvre de stunnel pour sécuriser une messagerie smtp
- Présentation d'openVPN
- Travaux pratiques : installation, configuration, tests de connexion,création d'u ntunnel sécurisé par clé statique
- Certificats : SERV et CLT
- Pare-feux : les iptables, le filtrage de paquets,définition d'une politique de sécurité
- Travaux pratiques : 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

Déroulé de l'action

- **Type de stage**

  Session Inter-entreprises
  Session Intra

- **Horaires**

  9H00-12H30 /13H30-17H00

- **Méthode pédagogique**

  Alternance exposés théoriques
  et exercices pratiques

- **Suivi et assistance**

  Support de cours adapté au logiciel étudié et au niveau suivi
  Assistance téléphonique gratuite et illimitée

- **Validation des acquis**

  Exercice de validation en fin d'action