

Linux sécurité des accès

Durée: 3 jours

1610 €

30 janvier au 1er février

24 au 26 avril

10 au 12 juillet

2 au 4 octobre

4 au 6 décembre

Public:

Toute personne souhaitant sécuriser les accès à un système Linux

Objectifs:

Savoir configurer les mécanismes de sécurité réseau de Linux.

Connaissances préalables nécessaires:

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.
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 (OpenSource Vulnerability Assessment Scanner) :
principe de fonctionnement, installation.
Travaux pratiques :
réalisation d'un audit réseau avec openVAS.

Linux sécurité des accès

- 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.
- 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'un tunnel 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.

Linux sécurité des accès

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.