

Sécurisation des services internet

Durée: 4 jours

2085 €

6 au 9 mars

6 au 9 juin

16 au 19 octobre

11 au 14 décembre

Public:

Les administrateurs réseaux, et toute personne souhaitant sécuriser les services internet et/ou intranet.

Objectifs:

Connaître les moyens de sécuriser les réseaux IP et d'apporter des solutions aux risques liés à internet.

Connaissances préalables nécessaires:

Connaissances de bases sur les réseaux IP et les systèmes d'exploitation.

Programme:

- Introduction** : La sécurité : Définitions
Le DIC : Disponibilité, Intégrité, Confidentialité
Evaluation des risques.
Elaboration d'une politique de sécurité.
Définitions : DMZ, proxy, pare-feux, routeurs filtrants
Fonctionnement, mise en oeuvre
- Les ports de niveau 5** : Rappels sur la notion de ports.
Principe d'empilement des trames.
Les ports UDP.
Exemples de trames.
- Outils réseaux** : Le principe des traces, les informations disponibles dans les captures de trames.
Travaux pratiques :
Traçage des flux réseaux: wireshark, tcpdump.
- DMZ et pare-feux** : Définition, et architecture
Fonctionnement des pare-feux.
- Firewall iptables** : Description du filtrage avec iptables.
Syntaxe.
Traduction d'adresses. Traduction de ports.
Notion de politique de sécurité par défaut.
Sécurisation de l'ouverture d'un port.
Travaux pratiques :
Mise en oeuvre d'une fonction d'activation d'ouverture avec les iptables.

Sécurisation des services internet

- SSH et GPG** : SSH : Secure SHell
Présentation du protocole de connexion SSH
Utilisation de la cryptographie. Authentification par clé.
Travaux pratiques :
configuration,
sécurisation de l'ouverture du port.
GPG : GNU Privacy Guard
Transmission de messages chiffrés et signés.
- VPN et tunnels** : Objectifs.
Fonctionnement. Mise en oeuvre : tunnels ssh, stunnel.
Travaux pratiques avec openVPN.
Principe d'IPsec.
Implémentation avec FreeS/WAN.
- Proxy** : Introduction : la fonction d'un serveur proxy.
Les multi-serveurs proxys.
Mise en oeuvre avec squid.
Architecture Squid.
Exemples d'utilisation.
Travaux pratiques :
configuration réseau d'un serveur Squid.
Les Access Control List.
Optimisation de la bande passante.
Programmes d'authentification.
Exemple d'authentification NCSA, LDAP.
- Services reseaux** : Sécurisation DNS :
architecture redondante, DNS fermé, Hidden master, Stealth DNS.
Mise en oeuvre de la sécurisation d'un DNS.
Authentification.
Les signatures TSIG. Les ACL.
- Messagerie** : Sécurisation.
Notion de relais ouvert.
Outils de test du serveur.
Travaux pratiques :
mise en oeuvre avec postfix.
Apport de Cyrus.
- Serveur http** : Restriction d'accès.
Authentification http.
Sécurité avec SSL et HTTPS : principe, configuration par défaut.
Génération de clés SSL
- Acces reseaux** : Authentification par un serveur radius.
Techniques de filtrage à base d'iptables.
Mise en oeuvre d'un système d'authentification par utilisateur et non par adresse : NuFW.

Sécurisation des services internet

Détection de failles

: Outils : snort, openvas.

Travaux pratiques :

mise en oeuvre et réalisation d'un audit de sécurité de l'environnement de test.