FORMATIONS LINUX

MNIS – Tour de l'Horloge - 4, place louis Armand – 75012 Paris

TEL : 0950 070814

VPI

RESEAUX PRIVES VIRTUELS AVEC IPSEC SOUS LINUX

Durée : 4 jours

Prix : 1390€

GROUPE DE FORMATIONS

La formation fait partie du groupe de formation « Administration »

Administration		
LIN	Administration avancée	5
SRX	Sécurité sous Linux	4
VTX	Utiliser XEN sous Linux	4
VPI	IPSEC sous Linux	4

QUEL OBJECTIF

Après avoir suivi cette formation vous serez en mesure d'installer et d'administrer un réseau privé virtuel IPSEC ainsi que la PKI associée pour votre entreprise. L'accent est mis sur la pratique avec OpenSwan sous Linux suivi des explications théoriques.

PRE-REQUIS

Connaissance du système UNIX et des principales commandes.

POUR QUI

Cette formation est destinée aux ingénieurs et techniciens, architectes ou administrateurs devant mettre en œuvre un réseau privé virtuel basé sur IPSEC.

POUR QUOI

Vous travaillez dans une société pour laquelle la sécurité est un enjeu majeur, banque, assurance, défense, et vous devez mettre en œuvre ou administrer un réseau basé sur IPSEC.

DEROULE DE LA FORMATION

PRESENTATION

Historique et technique de cryptographie
TCP-IP, un protocole non sécurisé
Sécurisation du transport, SSL
Sécurisation de la couche réseau, IPSEC

STRONGSWAN

Présentation de l'architecture de Strongswan
Les fichiers de configuration
Les outils de gestion, ipsec, swanctl, charon, charon-cmd
Les outils d'analyse, tcpdump, wireshark
Travaux pratiques : mise en œuvre de openswan, analyse du traffic, utilisation de différentes configurations.

ANALYSE DES PROTOCOLES IPSEC

Architecture de IPSEC, mise en oeuvre
Les modes, transport et tunnel
Base de données des associations de sécurité et politique de sécurité
Le protocole ESP
Le protocole AH
Le protocole IPCOMP
Comprendre l'échange « Diffie Hellman »
Perfect forward secrecy
Echange dynamique de clefs, ISAKMP, phases, messages et cookies
Les échanges IKE, IKEv1 et IKEv2, les modes, le DOI
Travaux pratiques : mise en œuvre de la PFS, suivi des différents échanges IKE à l'aide de WireShark

PROBLEMES LIES AU DEPLOIEMENT

Fragmentation, PMTU et ICMP
Architecture, tunnels imbriqués ou chaînés
Scénarios de déploiement, topologies, portables itinérants, extranet
Firewalls et translation d'adresse, NAT Traversal
Traitement des paquets par le noyau, Interface avec le noyau, XFRM, algorithmes
Traitements IKE par le daemon « userland »
Travaux pratiques : Etude des sources du noyau, comment implémenter un algorithme, gestion du PMTU et du NAT. Protection par firewall.

PKI OPENSOURCE

L'infrastructure pour les Clefs Publiques
Les formats PKCS
Utiliser OpenSSL pour gérer une PKI, clefs et certificats
Travaux pratiques : Création du certificat Root CA, des certificats serveurs et clients, révocation de certificats

AUTRES ARCHITECTURES ET NOUVEAUTES

L2TP
Architecture TNC liée à OpenSwan
Secure DNS