APITUX
AUDIT ▪ CONSEIL ▪ FORMATION ▪ RÉSEAU

SÉCURITÉ RÉSEAU ET FIREWALL SOUS LINUX

Public et objectifs de la formation

Type de public

- Responsables de systèmes informatiques, administrateurs réseaux.

Prérequis

- Bonne culture informatique et réseaux ;
- Connaissance des commandes Unix de base ;
- Une première expérience sous Linux quelle que soit la distribution pratiquée.

Objectifs

- Etre capable d'administrer un firewall GNU-Linux avec Iptables ;
- Apprendre à suivre l'activité de son firewall ;
- Savoir tester son firewall avec nmap ;
- Découvrir la distribution Debian.

Programme

Administration d'un firewall GNU-Linux avec Iptables

- Politique de sécurité par défaut ;
- Sélection de paquets selon protocole et le port ;
- Sélection de paquets selon l'adresse IP ;
- Sélection de paquets selon l'interface réseau ;
- Ecriture de scripts pour Iptables ;
- Configuration du masquerading ;
- Redirection de ports.

Suivre l'activité de son firewall

- Détecter les attaques : l'exemple du fichier auth.log ;
- Suivre l'activité de son firewall avec Ulog.

Tester son firewall

- Scan de ports avec Nmap ;
- Analyse réseau avec Ethereal.

Modalités pédagogiques

Durée

- 2 jours (14 heures).

Supports

- Scripts commentés écrits pendant la formation ;
- Mémento : Les iptables Linux (100 pages).

Méthodes pédagogiques

- Apports théoriques : fonctionnement de Netfilter, écriture de scripts Iptables ;
- Mise en pratique : réalisation de différentes configurations de firewall GNU-Linux.

SIRET 452 887 441 00023 - APE 7212

Jean-Christophe BECQUET
3 rue Beethoven 04000 DIGNE LES BAINS 06 25 86 07 92 - www.apitux.com - jcb@apitux.com