

## A5 - Sécurité Réseau

### Securing Linux server, Internet ou Intranet

#### Objectifs

- Savoir déployer et utiliser des outils de sécurisation et de test sur plate-forme Linux

#### Matériel

- Un PC par stagiaire
- Support de cours

#### Pré-requis

- Connaissance de Linux et de l'administration réseau (niveau cours A2)
- Maîtrise de la gestion de l'arborescence du système
- Maîtrise d'un éditeur de fichier texte

#### Course Environment

- Theoretical course
  - PDF course material (in English) supplemented by a printed version for face-to-face courses.
  - Online courses are dispensed using the Teams video-conferencing system.
  - The trainer answers trainees' questions during the training and provide technical and pedagogical assistance.
- At the start of each session the trainer will interact with the trainees to ensure the course fits their expectations and correct if needed

#### Target Audience

- Any embedded systems engineer or technician with the above prerequisites.

#### Evaluation modalities

- The prerequisites indicated above are assessed before the training by the technical supervision of the trainee in his company, or by the trainee himself in the exceptional case of an individual trainee.
- Trainee progress is assessed by quizzes offered at the end of various sections to verify that the trainees have assimilated the points presented
- At the end of the training, each trainee receives a certificate attesting that they have successfully completed the course.
  - In the event of a problem, discovered during the course, due to a lack of prerequisites by the trainee a different or additional training is offered to them, generally to reinforce their prerequisites, in agreement with their company manager if applicable.

## Plan

### Sécurisation des accès

- Notions de base sur TCP/IP
- Parefeu Netfilter/iptables, zone démilitarisée (DMZ), gestion avec fwbuilder
  - Installation de iptables et fwbuilder
  - Les directives définissant les règles
  - Configuration de base pour faire du routage
  - Configuration de base pour faire du filtrage
  - La translation d'adresse NAT
  - La gestion des règles avec fwbuilder

### Communications sécurisées

- OpenSSL
  - Installation
  - Création des certificats pour un client ou un serveur
- Accès distant avec OpenSSH
  - Installation/configuration du serveur OpenSSH
  - Installation/configuration du client SSH Linux ou Windows
- Mise en place de réseaux privés virtuels (VPN) avec FreeSWAN et IPsec
  - Installation/Configuration
  - Liaison entre sites
  - Liaison entre un site et des portables (Road Warrior)

### Administration de la sécurité

- Détection d'intrusion (IDS) avec SNORT sur Linux
  - Installation de SNORT
  - Configuration
  - Suivi des logs
  - Ecriture des règles
- Supervision du réseau avec NAGIOS
  - Installation/configuration de NAGIOS
  - Les plugins
  - Analyse du réseau
  - Suivi des éléments actifs du réseau
- Outils de surveillance réseau : hping, ethereal, tcpdump, nmap, netcat
  - Installation
  - Utilisation de ces outils pour analyser le fonctionnement du réseau

## Renseignements pratiques

**Duration : 2 days**  
**Cost : 1400 € HT**