Administration de la Sécurité de Serveurs Linux

LINUXADM

Objectifs

Maîtriser l'Administration de la Sécurité sous Linux.

Public Visé

Techniciens et Administrateurs Linux.

Pré Requis

Avoir suivi la formation Linux : Technician ou posséder les compétences équivalentes.

Méthodes et moyens pédagogiques

PREREQUIS :Matériel
• Un poste 64 bits (MacOS, Linux, Windows™ ou Solaris™),
• Dans le cas de Windows™, **seulement** la version 7 ou 10 avec Hyper-V **désinstallé**,
• Le mot de passe du compte administrateur du système,
• Clavier AZERTY FR ou QWERTY US,
• 8 Go de RAM minimum,
• Processeur 4 cœurs minimum,
• 8 Go d'espace disque disponible,
• Un casque ou des écouteurs (si **MOOC** ou **FAD**),
• Un micro (optionnel).
Logiciels
• Oracle VirtualBox v 6.0 ou plus (MacOS, Linux, Windows™ ou Solaris™),
• Si Windows™ - Putty et WinSCP.
Internet
• Un accès à Internet rapide **sans** passer par un proxy,
•

Qualification Intervenant(e)(s)

Expert

Parcours pédagogique

- **Droits Unix** - 3 heures.
  - Présentation
  - Préparation
  - Les Droits Unix Simples
    - La Modification des Droits
      - La Commande chmod
        - Mode Symbolique
        - Mode Octal
      - La Commande umask
  - Modifier le propriétaire ou le groupe
    - La Commande chown
    - La Commande chgrp
  - Les Droits Unix Etendus
    - SUID/SGID bit
    - Inheritance Flag
    - Sticky bit
  - Les Droits Unix Avancés
    - Les ACL
    - Les Attributs Etendus
- **Netfilter et Firewalld** - 4 heures
  - Les Problématiques
    - L'IP Spoofing
    - Déni de Service (DoS)
    - SYN Flooding
    - Flood
  - Le Contre-Mesure
    - Le Pare-feu Netfilter/iptables
    - LAB #1 - Configuration par Scripts sous RHEL/CentOS 6 et versions Antérieures
    - LAB #2 - La Configuration par firewalld sous RHEL/CentOS 7
      - La Configuration de Base de firewalld
      - La Commande firewall-cmd
      - La Configuration Avancée de firewalld
      - Le mode Panic de firewalld
- **Authentification** - 3 heures.
  - Le Problématique
    - LAB #1 - Installer John the Ripper
  - Surveillance Sécuritaire
    - La commande last
    - La commande lastlog
    - La Commande lastb
    - /var/log/secure
  - Les Contre-Mesures
    - LAB #2 - Renforcer la sécurité des comptes

STRATEGIE Formation - Numéro de déclaration d'activité (ne vaut pas agrément de l'état) : 95970120697

- LAB #3 - PAM sous RHEL/CentOS 6
  - Utiliser des Mots de Passe Complexe
  - Bloquer un Compte après N Echecs de Connexion
  - Configuration
- LAB #4 - PAM sous RHEL/CentOS 7
  - Utiliser des Mots de Passe Complexe
  - Bloquer un Compte après N Echecs de Connexion
  - Configuration
- LAB #5 - Mise en place du Système de Prévention d'Intrusion Fail2Ban
  - Installation
  - Configuration
    - Le répertoire /etc/fail2ban
      - Le fichier fail2ban.conf
      - Le répertoire /etc/fail2ban/filter.d/
      - Le répertoire /etc/fail2ban/action.d/
  - Commandes
    - Activer et Démarrer le Serveur
    - Utiliser la Commande Fail2Ban-server
    - Ajouter un Prison

- **Balayage des Ports** - 4 heures.
  - Le Problématique
  - LAB #1 - Utilisation de nmap et de netcat
    - nmap
      - Installation
      - Utilisation
      - Fichiers de Configuration
      - Scripts
    - netcat
      - Utilisation
  - Les Contre-Mesures
    - LAB #2 - Mise en place du Système de Détection d'Intrusion Snort
      - Installation
      - Configuration de Snort
        - Editer le fichier /etc/snort/snort.conf
      - Utilisation de snort en mode “packet sniffer”
      - Utilisation de snort en mode “packet logger”
      - Journalisation
    - LAB #3 - Mise en place du Système de Détection et de Prévention d'Intrusion
      - Portsentry
        - Installation
        - Configuration
        - Utilisation
- **Cryptologie** - 4 heures.
  - Le Problématique
  - LAB #1 - Utilisation de tcpdump
    - Utilisation
      - L'option -i
      - L'option -x
      - L'option -X
      - L'option -w
      - L'option -v
    - Filtrage à l'écoute
  - Les Contre-Mesures
    - Introduction à la cryptologie
      - Définitions
      - Algorithmes à clé secrète
        - Le Chiffrement Symétrique
      - Algorithmes à clef publique
        - Le Chiffrement Asymétrique

Stratégie Informatique
Guadeloupe : Immeuble la Coupole, Grand-Camp 97142 ABYMES Tél : 05 90 83 06 18 Fax : 05 90 83 46 71
Martinique : Immeuble Sera n°6, Zone de Manhity 97232 LAMENTIN Tél : 05 96 57 40 20 Fax : 05 96 51 60 53
SARL AU CAPITAL DE 7775€ - SIRET 352 717 193 00044-APE 6202 A

- La Clef de Session
- Fonctions de Hachage
- Signature Numérique
- PKI
- Certificats X509

- LAB #2 - Utilisation de GnuPG
  - Présentation
  - Installation
  - Utilisation
    - Signer un message
    - Chiffrer un message
- LAB #3 - Mise en place de SSH et SCP
  - Introduction
    - SSH-1
    - SSH-2
  - L'authentification par mot de passe
  - L'authentification par clef asymétrique
    - Installation
    - Configuration
    - Serveur
  - Utilisation
  - Tunnels SSH
  - SCP
    - Introduction
    - Utilisation
    - Mise en place des clefs
- LAB #4 - Mise en place d'un VPN avec OpenVPN
  - Présentation
  - Configuration commune au client et au serveur
  - Configuration du client
  - Configuration du serveur
  - Tests
    - Du client vers le serveur
    - Du serveur vers le client

- **Système de Fichiers** - 3 heures.
  - La sécurisation des systèmes de fichiers
    - Le Fichier /etc/fstab
      - Comprendre le fichier /etc/fstab
      - Options de Montage
  - LAB #1 - Créer un Système de Fichiers Chiffré avec LUKS
    - Présentation
    - Préparation
    - Ajouter une deuxième Passphrase
    - Supprimer une Passphrase
  - LAB #2 - Mise en place du File Integrity Checker Afick
    - Présentation
    - Installation
    - Configuration
      - La Section Directives
      - La Section Alias
      - La Section File
    - Utilisation
    - Automatiser Afick
  - Root Kits
    - Le Problématique
    - Contre-Mesures
    - LAB #3 - Mise en place de rkhunter
      - Installation
      - Les options de la commande
      - Utilisation
      - Configuration

Stratégie Informatique
Guadeloupe : Immeuble la Coupole, Grand-Camp 97142 ABYMES Tél : 05 90 83 06 18 Fax : 05 90 83 46 71
Martinique : Immeuble Sera n°6, Zone de Manhity 97232 LAMENTIN Tél : 05 96 57 40 20 Fax : 05 96 51 60 53
SARL AU CAPITAL DE 7775€ - SIRET 352 717 193 00044-APE 6202 A

- **System Hardening** - 3 heures.
  - System Hardening Manuel
    - Les compilateurs
    - Les paquets
    -
-

Méthodes et modalités d'évaluation

Alternance entre un scénario pédagogique clair et précis et des travaux pratiques basés sur des cas et exemples concrets.

Modalités d'Accessibilité

Nous consulter

Durée

35.00 Heures

5 Jours

Effectif

8

Stratégie Informatique
Guadeloupe : Immeuble la Coupole, Grand-Camp 97142 ABYMES Tél : 05 90 83 06 18 Fax : 05 90 83 46 71
Martinique : Immeuble Sera n°6, Zone de Manhity 97232 LAMENTIN Tél : 05 96 57 40 20 Fax : 05 96 51 60 53
SARL AU CAPITAL DE 7775€ - SIRET 352 717 193 00044-APE 6202 A