Plan de cours N° : 667
Durée : 5 jours (35h)

# LINUX
## Sécuriser un serveur linux

### PARTICIPANTS / PRE-REQUIS
Administrateur de serveurs linux.
Notions réseau conseillé.

### OBJECTIFS PEDAGOGIQUES
Identifier les différents protocoles de sécurité réseau tels que SSH, SSL, Kerberos, Ipsec et OpenVPN. Expliquer les concepts de cryptologie, y compris les fonctions de hachage, les algorithmes de chiffrement à clé publique et la signature numérique. Configurer un pare-feu avec iptables et Squid pour sécuriser les connexions réseau. Analyser les journaux de bord pour détecter et répondre aux incidents de sécurité. Intégrer des techniques d'audit comme Snort, Tcpdump et Wireshark pour surveiller et analyser le trafic réseau. Evaluer l'efficacité des configurations de sécurité mises en place sur un serveur Linux. Concevoir une architecture de sécurité réseau en utilisant des VPN et des services kerbérisés. Diagnostiquer et résoudre les problèmes de sécurité liés aux services réseaux comme Apache, DNS et MySQL. Utiliser sudo et les ACL pour gérer les droits et la sécurité multi-utilisateur. Mettre en œuvre des politiques de sécurité pour SSH et configurer l'authentification à clés publiques.

### MOYENS PEDAGOGIQUES
Tour de table au début de chaque formation pour définir les objectifs de chaque participant,
Alternance entre apports théoriques (en moyenne 30%) et exercices pratiques (en moyenne 70%),
Utilisation de cas concrets issus de l'expérience professionnelle de nos formateurs,
Remise d'un support de cours,
Assistance post-formation d'une durée de 1 an sur le contenu de la formation via notre adresse mail dédiée formateurs@atp-formation.com

### MOYENS PERMETTANT LE SUIVI DE L'EXECUTION ET DES RESULTATS
Positionnement préalable oral ou écrit,
Evaluation des acquis tout au long de la formation par des exercices de synthèse,
Attestation de stage remise à chaque apprenant, avec son niveau d'acquisition pour chaque objectif pédagogique,
Feuille de présence signée par demi-journée,
Questionnaire de satisfaction pour évaluer la qualité de l'enseignement,
En option : passage certification possible selon les thématiques.

### MOYENS TECHNIQUES EN PRESENTIEL
Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs récents et performants, d'un vidéo projecteur et d'un tableau blanc.

### MOYENS TECHNIQUES DES CLASSES A DISTANCE
Grâce à un logiciel comme Teams, suivez une formation en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur.
Nous vous conseillons très fortement l'utilisation de votre webcam et de disposer d'un double écran.
Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition par téléphone au 04.76.41.14.20.

### ORGANISATION
Les cours ont lieu de 9h00-12h30 13h30-17h00 (adaptable à la demande).

### PROFIL FORMATEUR
Nous recrutons méticuleusement nos formateurs selon 3 critères: expertise, pédagogie et agilité.

### ACCESSIBILITE
Les personnes atteintes de handicap souhaitant suivre nos formations sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités d'organisation.

### MISE A JOUR
26/07/2024

Plan de cours N° : 667
Durée : 5 jours (35h)

# LINUX
## Sécuriser un serveur linux

### Introduction
- La sécurité informatique
- Attaques et logiciels malveillants
- Les politiques de sécurité
- Conduite à tenir en cas d'incident

### La cryptologie
- Les fonctions de hachage
- Les algorithmes de chiffrement à clé publique
- La signature numérique
- Le protocole OpenPGP
- Le chiffrement des systèmes de fichiers
- ATELIERS

### La sécurité locale
- La sécurité multi-utilisateur
- sudo
- La connexion
- Les mots de passe
- La sécurité pour les utilisateurs
- Les droits
- Les ACL
- ATELIERS

### SSH
- Le protocole SSH
- Les commandes SSH
- L'authentification à clés publiques
- La configuration de SSH
- Compléments
- ATELIERS

### SELinux
- L'approche SELinux
- La sécurité de type TE de SELinux
- La mise en place de SELinux
- Dépannage
- Les politiques de sécurité
- MLS/MCS
- ATELIERS

### PKI ET SSL
- Les certificats x509
- PKI
- SSL
- La commande Stunnel
- S/MIME
- ATELIERS

### KERBEROS
- Présentation de Kerberos
- Le protocole Kerberos
- L'exploitation
- L'utilisation de services « kerbérisés »
- ATELIERS

### LES PARE-FEU
- Les pare-feu
- Les pare-feu isolant deux réseaux
- Iptables
- tcp_wrappers
- Xinetd
- Squid
- ATELIERS

### VPN
- VPN
- OpenVPN .
- IPSec

### VPN
- ATELIERS

### Sécurisations des applications
- La sécurisation des services
- Chroot
- Panorama des services réseaux
- La sécurisation du Web, Apache
- La sécurisation du DNS
- La sécurisation d'une base de données MySQL
- La sécurisation de l'e-mail
- ATELIERS

Plan de cours N° : 667
Durée : 5 jours (35h)

# LINUX
## Sécuriser un serveur linux

### Audit

- Les attaques
- Les logiciels d'audit
- Tcpdump
- Wireshark
- Nmap .
- Nessus
- Tripwire
- Snort utilisé comme HIDS
- Snort utilisé comme NIDS
- Snort utilisé comme NIDS

### Sécuriser un serveur

- Sécuriser un serveur.
- Les journaux de bord
- Ateliers