Version 2020.01

Dernière mise-à-jour : 1970/01/01 00:00

LRF400 - Administration de la Sécurité de Serveurs Linux

Présentation

Type d'Action (Article L. 6313-1) : Action d'acquisition, d'entretien ou de perfectionnement des connaissances.
Objectif : Maîtriser l'Administration de la Sécurité sous Linux.
Public : Techniciens et Administrateurs Linux.
Pré requis : Avoir suivi la formation **LCF500 - CentOS 8 Linux (RHEL 8) : Technician** ou posséder les compétences équivalentes.
Méthode d'apprentissage : Alternance entre un scénario pédagogique clair et précis et des travaux pratiques basés sur des cas et exemples concrets.
Validation des acquis : Évaluations à l'aide de tests auto-correctifs.
Durée : 4 jours (28h).
Formateur : Certifié **LPI**.

Support de Cours

L'accès au supports de cours ainsi que les LABS et les validations des acquis se fait grâce à un abonnement annuel par stagiaire à une plateforme de cours sur Internet. Cette abonnement est facturé 35 € HT par stagiaire et par session.

L'utilisation de cette plateforme permet :

- de mesurer le niveau du stagiaire avant la formation et celui atteint en fin de formation grâce aux tests de validations des acquis,
- de suivre du travail de chaque participant en termes de temps passé dans chaque module grâce à un reporting détaillé.

L'abonnement permet aux stagiaires :

- de télécharger des supports de cours et des LABS au format PDF le dernier jour de la formation,
- de refaire les LABS en mode autonome en cas de missions décalées en relation avec le contenu de la formation initiale,
- de rester en contact avec le formateur en cas de problèmes en production liés au contenu du cours,
- de consulter les mises à jour du contenu des supports de cours pendant la période de l'abonnement,
- d'échanger avec les autres participants de votre session ainsi qu'avec les anciens stagiaires.

Prérequis

Matériel

- Un poste (MacOS, Linux, Windows™ ou Solaris™),
- Clavier AZERTY FR ou QWERTY US,
- 4 Go de RAM minimum,
- Processeur 2 cœurs minimum,
- Un casque ou des écouteurs,
- Un micro (optionnel).

Logiciels

- Si Windows™ - Putty et WinSCP,
- Navigateur Web Chrome, Edge ou Firefox.

Internet

- Un accès à Internet **rapide** (4G minimum) **sans** passer par un proxy,
- Accès **débloqué** aux domaines suivants : https://ittraining.network, https://ittraining.io ainsi que leurs sous-domaines et https://online.ittraining.team/.
- Ports accessibles : 80,443.

Programme

Jour #1

- **LRF401 - 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

- **LRF402 - 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

Jour #2

- **LRF403 - 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
  - 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

- **LRF404 - 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

Jour #3

- **LRF405 - 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
                - 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

- **LRF406 - 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

Jour #4

- **LRF407 - System Hardening** - 3 heures.
  - System Hardening Manuel
    - Les compilateurs
    - Les paquets
    - Les démons et services
    - Les fichiers .rhosts
    - Les fichiers et les repertoires sans propriétaire
    - Interdire les connexions de root via le réseau
    - Limiter le délai d'inactivité d'une session shell
    - Renforcer la sécurité d'init
      - Les Distributions SysVInit
      - Les Distributions Upstart
    - Renforcer la sécurité du Noyau
      - La commande sysctl
  - LAB #1 - System Hardening à l'aide de l'outil Bastille
    - Présentation
    - Installation
    - Utilisation
  - LAB #2 - Mise en place de SELinux pour sécuriser le serveur
    - Introduction
    - Définitions
      - Security Context
      - Domains et Types
      - Roles
      - Politiques de Sécurité
      - Langage de Politiques
        - allow
        - type
      - type_transition
    - Décisions de SELinux
      - Décisions d'Accès
      - Décisions de Transition
    - Commandes SELinux
    - Les Etats de SELinux
    - Booléens
  - LAB #3 - Travailler avec SELinux
    - Copier et Déplacer des Fichiers
    - Vérifier les SC des Processus
    - Visualiser la SC d'un Utilisateur
    - Vérifier la SC d'un fichier
    - Troubleshooting SELinux
      - La commande chcon
    - La commande restorecon
    - Le fichier /.autorelabel
    - La commande semanage
    - La commande audit2allow

- **LRF409 - Sécurité Applicative** - 3 heures.
  - Le Problématique
  - Préparation
  - Les Outils
    - LAB #1 - Netwox
      - Installation
      - Utilisation
      - Avertissement important
    - LAB #2 - OpenVAS
      - Présentation
      - Préparation
      - Installation
      - Configuration
      - Utilisation
      - Analyse des Résultats
  - Les Contres-Mesures
    - LAB #3 - La commande chroot
    - LAB #4 - Sécuriser Apache
      - Installation
      - Testez le serveur apache
        - Avec un navigateur
        - Avec Telnet
      - Préparation
      - Gestion de serveurs virtuels
        - Hôte virtuel par nom
        - Hôte virtuel par adresse IP
      - mod_auth_basic
        - Configuration de la sécurité avec .htaccess
        - Mise en place d'un fichier de mots de passe
      - mod_auth_mysql
        - Installation
        - Configuration de MariaDB
        - Configuration d'Apache
      - mod_authnz_ldap
      - mod_ssl
        - Présentation de SSL
        - Fonctionnement de SSL
        - Installation de ssl
        - Configuration de SSL
        - Mise en place des paramètres de sécurité SSL
        - Tester la Configuration

<html> <DIV ALIGN="CENTER"> Copyright © 2020 Hugh Norris

 Document non-contractuel. Les prix, les conditions et le programme peuvent être modifiés sans préavis. </html>