

Version : **2022.01**

Dernière mise-à-jour : 2023/02/15 16:13

LCF300 - Présentation de la Formation

Contenu du Module

- **LCF300 - Présentation de la Formation**
 - Contenu du Module
 - Prérequis
 - Matériel
 - Logiciels
 - Internet
 - Programme de la Formation
 - Évaluation des Compétences

Prérequis

Matériel

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

Logiciels

- Web Chrome version 72+ ou
- Microsoft Edge version 79+ ou
- Firefox version 65+.

Internet

- Un accès à Internet **rapide** (4G minimum) **SANS** passer par un proxy.

Programme de la Formation

- **LCF300 - Présentation de la Formation**
 - Prérequis
 - Matériel
 - Logiciels
 - Internet
 - Programme de la Formation
 - Évaluation des Compétences
- **LCF301 - Gestion des Paramètres et les Ressources du Matériel**
 - Fichiers Spéciaux
 - Commandes
 - La Commande lspci
 - La Commande lsusb
 - La Commande dmidecode
 - Répertoire /proc
 - Répertoires
 - ide/scsi
 - acpi
 - bus
 - net
 - sys
 - La Commande sysctl

- Fichiers
 - Processeur
 - Interruptions système
 - Canaux DMA
 - Plages d'entrée/sortie
 - Périphériques
 - Modules
 - Statistiques de l'utilisation des disques
 - Partitions
 - Espaces de pagination
 - Statistiques d'utilisation du processeur
 - Statistiques d'utilisation de la mémoire
 - Version du noyau
- Interprétation des informations dans /proc
 - Commandes
 - free
 - uptime ou w
 - iostat
 - vmstat
 - mpstat
 - sar
 - Utilisation des commandes en production
 - Identifier un système limité par le processeur
 - Identifier un système ayant un problème de mémoire
 - Identifier un système ayant un problème d'E/S
 - Modules usb
 - udev
 - La Commande udevadm
 - Système de fichiers /sys
 - Limiter les Ressources
 - ulimit
 - Groupes de Contrôle
 - LAB #1 - Travailler avec les cgroups sous RHEL/CentOS 7

- **LCF302 - Comprendre le Réseau TCPv4**

- Comprendre les Réseaux
 - Présentation des Réseaux
 - Classification des Réseaux
 - Classification par Mode de Transmission
 - Classification par Topologie
 - La Topologie Physique
 - La Topologie en Ligne
 - La Topologie en Bus
 - La Topologie en Étoile
 - La Topologie en Anneau
 - La Topologie en Arbre
 - La Topologie Maillée
 - Classification par Étendue
 - Les Types de LAN
 - Réseau à Serveur Dédié
 - Réseau Poste-à-Poste
 - Le Modèle Client/Serveur
 - Modèles de Communication
 - Le modèle OSI
 - Les Couches
 - Les Protocoles
 - Les Interfaces
 - Protocol Data Units
 - Encapsulation et Désencapsulation
 - Spécification NDIS et le Modèle ODI
 - Le modèle TCP/IP
 - Les Raccordements
 - Les Modes de Transmission
 - Les Câbles
 - Le Câble Coaxial
 - Le Câble Paire Torsadée
 - Catégories de Blindage
 - La Prise RJ45

- Channel Link et Basic Link
- La Fibre Optique
- Les Réseaux sans Fils
- Le Courant Porteur en Ligne
- Technologies
 - Ethernet
 - Token-Ring
- Périphériques Réseaux Spéciaux
 - Les Concentrateurs
 - Les Répéteurs
 - Les Ponts
 - Le Pont de Base
 - Le Pont en Cascade
 - Le Pont en Dorsale
 - Les Commutateurs
 - Les Routeurs
 - Les Passerelles
- Comprendre TCP Version 4
 - En-tête TCP
 - En-tête UDP
 - Fragmentation et Ré-encapsulation
 - Adressage
 - Masques de sous-réseaux
 - VLSM
 - Ports et sockets
 - /etc/services
 - Résolution d'adresses Ethernet
- Comprendre le Chiffrement
 - Introduction à la cryptologie
 - Définitions
 - La Cryptographie
 - Le Chiffrement par Substitution
 - Algorithmes à clé secrète
 - Le Chiffrement Symétrique

- Algorithmes à clef publique
 - Le Chiffrement Asymétrique
 - La Clef de Session
 - Fonctions de Hachage
 - Signature Numérique
 - LAB #1 - Utilisation de GnuPG
 - Présentation
 - Installation
 - Configuration
 - Signer un message
 - Chiffrer un message
 - PKI
 - Certificats X509
-
- **LCF303 - Gestion du Réseau TCPv4**
 - Configuration du Réseau sous RHEL/CentOS 5 et 6
 - Configuration de TCP/IP
 - DHCP
 - /etc/sysconfig/network
 - /etc/sysconfig/network-scripts/ifcfg-ethX (où X=0,1 ...)
 - IP Fixe
 - /etc/sysconfig/network
 - /etc/sysconfig/network-scripts/ifcfg-ethX (où X=0,1 ...)
 - La Commande hostname
 - La Commande ifconfig
 - Activer/Désactiver une Interface Manuellement
 - /etc/networks
 - Résolution d'adresses IP
 - /etc/resolv.conf
 - /etc/nsswitch.conf
 - /etc/hosts
 - Services réseaux
 - xinetd
 - TCP Wrapper

- Routage Statique
 - La Commande route
 - Activer/désactiver le routage sur le serveur
- Configuration du Réseau sous RHEL/CentOS 7
 - La Commande nmcli
 - Connections et Profils
 - Ajouter une Deuxième Adresse IP à un Profil
 - La Commande hostname
 - La Commande ip
 - Activer/Désactiver une Interface Manuellement
 - Routage Statique
 - La commande ip
 - Activer/désactiver le routage sur le serveur
- Diagnostique du Réseau
 - ping
 - netstat -i
 - traceroute
- Connexions à Distance
 - Telnet
 - wget
 - ftp
 - SSH
 - 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

- **LCF304 - Gestion du Partage des Fichiers**

- Contenu du Module
- Gestion du Serveur NFS
 - Présentation
 - Les Services et Processus du Serveur NFSv3
 - Les Services RPC
 - Options d'un Partage NFS
 - Commandes de Base
 - Installation
 - LAB #1 Mise en Place du Serveur NFS
 - Configuration du Serveur
 - Configuration du Client
 - Surveillance du Serveur
 - La Commande rpcinfo
 - La Commande nfsstat
- Gestion du Serveur CIFS Samba
 - Les Réseaux Microsoft
 - Types de Réseaux Microsoft
 - Types de Clients Windows
 - Présentation de Samba
 - Daemons Samba
 - Commandes Samba
 - Installation de Samba
 - Configuration de base
 - Démarrage manuel de Samba
 - Configuration de Samba
 - Gestion des comptes et des groupes
 - Création du fichier smbpasswd
 - Comprendre la structure du fichier de configuration smb.conf
 - LAB #2 - Tester Samba en tant que Serveur de Fichiers

- **LCF305 - Gestion du Pare-feu**

- 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

- **LCF306 - Gestion de l'Authentification**

- Le Problématique
 - LAB #1 - 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 7
 - Bloquer un Compte après N Echecs de Connexion
 - Configuration
- LAB #4 - 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

- **LCF307 - Gestion du Balayage des Ports**

- 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

- **LRF308 - Gestion du System Hardening**

- System Hardening Manuel
 - Les compilateurs
 - Les paquets
 - Les démons et services
 - Les fichiers .rhosts
 - Les fichiers et les répertoires 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

- **LCF309 - Gestion Avancée des Disques - Raid Logiciel**

- Concepts RAID
 - Disques en miroir
 - Bandes de données
- Types de RAID
 - RAID 0 - Concaténation
 - RAID 0 - Striping
 - RAID 1 - Miroir
 - RAID 1+0 - Striping en Miroir
 - RAID 2 - Miroir avec Contrôle d'Erreurs
 - RAID 3 et 4 - Striping avec Parité
 - RAID 5 - Striping avec Parité Distribuée
 - Au-delà de RAID 5
- RAID Logiciel sous RHEL/CentOS
 - Préparation du disque
 - Partitionnement
 - Mise en Place du RAID 5 Logiciel

- **LCF310 - Gestion du Noyau et des Quotas**

- Rôle du noyau
- Compilation et installation du noyau et des modules
 - Déplacer /home
 - Créer un Nouveau Noyau
 - Préparer l'Arborescence Source du Noyau
 - Paramétrage du noyau
 - Compiler le Noyau
 - Installer le Nouveau Noyau
- Gestion des Quotas
 - La Commande quotacheck

- La Commande edquota
- La Commande quotaon
- La Commande repquota
- La Commande quota
- La Commande warnquota

- **LCF311 - Validation de la Formation**

- Support de Cours
- Rappel du Programme de la Formation
- Validation des acquis Globale
- Évaluation de la Formation

—
Copyright © 2023 Hugh Norris - Document non-contractuel. Le programme peut être modifié sans préavis.

From:

<https://ittraining.team/> - **www.ittraining.team**



Permanent link:

<https://ittraining.team/doku.php?id=elearning:workbooks:centos:6:avance:start>

Last update: **2023/02/15 16:13**