POEI - Neurones

LF01 - Linux – Les Fondamentaux

Programme

- **Systèmes de Fichiers**.
  - Linux File Hierarchy System
  - L'organisation
  - La commande mount
  - La commande umount
  - Systèmes de fichiers Unix
  - Validation des acquis
  - **Commandes** : mount, umount.
- **L'Editeur VI**.
  - Présentation
  - Lancer et Quitter VI
  - Set
  - Commandes du Curseur
  - Insertion de Texte
  - Recherche de Texte
  - Suppression de Texte
  - Copier - Coller
  - Couper - Coller
  - En cas de problème
  - Validation des acquis
  - **Commandes** : view, vi.
- **Aide et Documentation**.
  - L'aide des commandes

    - L'aide du shell
    - La commande man
    - La commande whatis
    - La commande apropos
    - La commande info
    - Sites Internet
    - Validation des acquis
    - **Commandes** : help, man, mandb, whatis, apropos, info.

- **Commandes de Base et Outils de Manipulation de Fichiers Textes**.
    - Etude des commandes de base
    - Options et arguments
    - Expressions Régulières
        - Expressions régulières basiques
        - Expressions régulières étendues
    - Outils et Commandes sur les Fichiers
        - La commande grep
        - La commande egrep
        - La commande fgrep
        - La commande sed
        - La commande awk
        - La commande tr
        - La commande paste
        - La commande cut
        - La commande uniq
        - La commande split
        - La commande diff
        - La commande cmp
        - La commande patch
        - La commande strings
        - La commande comm
        - La commande head
        - La commande tail
        - La commande screen

        - La commande wall
    - Validation des acquis
    - **Commandes** : stty, date, who, df, free, whoami, pwd, cd, ls, touch, echo, cp, file, cat, mv, mkdir, rmdir, rm, sort, more, find, su, locate, updatedb, whereis, which, uptime, w, uname, du, lsmod, modprobe, rmmod, modinfo, clear, exit, logout, shutdown, reboot, halt, poweroff, sleep, grep, egrep, fgrep, sed, awk, tr, paste, cut, split, diff, cmp, uniq, patch, strings, comm, od, head, tail, screen, wall.

- **La Ligne de Commande**.
    - Le Shell
        - Les Commandes Internes et Externes au shell
        - Les alias
        - Le Prompt
        - Rappeler des Commandes
        - Générer les fins de noms de fichiers
        - Le shell interactif
        - Affichage des variables du shell
            - Les variables principales
            - Régionalisation et Internationalisation
        - Options du shell bash
    - Les Scripts Shell
        - Exécution
        - Les variables spéciales
        - La commande read
        - Code de retour
        - La variable IFS
        - La commande test
        - La commande [[expression]]
        - Opérateurs du shell
        - L'arithmétique
            - La commande expr
            - La commande let
        - Structures de contrôle
        - Boucles
        - Scripts de Démarrage
    - Validation des acquis

- **Commandes** : type, alias, unalias, chsh, history, wc, tee, set, vi, script, read, test, expr, let, if, case, for, while.

LF02 - Linux Administration N1 – Système

Programme

- **Gestion des Utilisateurs**.
  - Groupes
  - Utilisateurs
  - Commandes
  - LAB #1 - Gestion des Utilisateurs
  - su et su -
  - sudo
  - Validation des acquis
  - **Commandes** : getent, grpck, grpconv, grpunconv, pwck, pwconv, pwunconv, groupadd, groupdel, groupmod, newgrp, gpasswd, useradd, userdel, usermod, passwd, chage, id, groups, su, sudo.
- **Gestion des Paquets**.
  - Installer à partir des sources
  - La commande rpm sous RHEL et SLES
  - La commande yum sous RHEL
  - La commande yumdownloader sous RHEL
  - La commande dpkg sous Debian et Ubuntu
  - La commande apt-get/apt-cache sous Debian et Ubuntu
  - La commande zypper sous SLES
  - LAB #1 - Gestion des Paquets
  - Les Bibliothèques Partagées
    - La Commande ldd
    - Le fichier /etc/ld.so.conf
    - La Commande ldconfig
  - Validation des acquis
  - **Commandes** : rpm, dpkg, yum, yumdownloader, apt-get, apt-cache, zypper, mc, wget, make, ldd, ldconfig.

- **Gestion de Droits**.
  - Les Droits Unix Simples
  - La Modification des Droits
  - Modifier le propriétaire ou le groupe
  - Les Droits Unix Etendus
  - Les ACL
  - Les Attributs Ext2/Ext3/Ext4 et XFS
  - Validation des acquis
  - **Commandes** : chmod, umask, chown, chgrp, setfacl, getfacl, chattr, lsattr.
- **Gestion des Disques, des Systèmes de Fichiers et du Swap**.
  - Périphériques de stockage
  - Partitionnement
  - Systèmes de Fichiers Journalisés
    - Présentation
      - Ext3
      - Ext4
      - ReiserFS
      - XFS
      - JFS
      - Btrfs
  - Pagination
    - Taille du swap
    - Partitions de swap
    - Fichiers de swap
    - La commande swapon
    - La commande swapoff
    - Le fichier /etc/fstab
  - Logical Volume Manager (LVM)
    - Physical Volume (PV)
    - Volume Group (VG) et Physical Extent (PE)
    - Logical Volumes (LV)
    - Administration
    - Snapshots

        - Suppression des Volumes
        - Logical Volumes en Miroir
        - Les Attributs
        - Logical Volumes en Bandes
        - Métadonnées
    - Validation des acquis
    - **Commandes** : fdisk, gdisk, parted, swapon, swapoff, mkswap, dumpe2fs, tune2fs, mke2fs, mkfs.ext3, e2fsck, resize2fs, debugfs, e2label, mkfs.ext4, mkfs.xfs, xfs_check, xfs_repair, xfs_admin, xfs_growfs, xfs_info, xfs_metadump, xfs_db, xfs_admin, mkfs.reiserfs, mkreiserfs, reiserfsck, reiserfstune, resize_reiserfs, debugreiserfs, mkfs.jfs, jfs_tune, jfs_fsck, jfs_febugfs, btrfs-balance, btrfs-check, btrfs-device, btrfs-filesystem, btrfs-inspect-internal, btrfs-property, btrfs-qgroup, btrfs-quota, btrfs-qgroup, btrfs-receive, btrfs-replace, btrfs-rescue, btrfs-restore, btrfs-scrub, btrfs-send, btrfs-subvolume, pvcreate, vgcreate, lvcreate, pvdisplay, vgdisplay, lvdisplay, lvextend, lvreduce, resize2fs, lvs, lvremove, vgremove, pvremove, lvconvert, vgs, pvs, lvchange, vgcfgbackup, vgcfgrestore.

- **Gestion des Tâches**.
    - cron
    - anacron
    - at
    - Validation des acquis
    - **Commandes** : crond, crontab, anacrond, at.

- **Gestion de l'Archivage et de la Compression**.
    - Archivage
    - Compression
    - LAB #1 - Archivage et Compression
    - Validation des acquis
    - **Commandes** : tar, cpio, dd, dump, restore, gzip, gunzip, bzip2, bunzip2, xz.

- **Gestion des Processus**.
    - Les Types de Processus
    - Les Commandes relatives aux Processus
    - Synchrone vs Asynchrone
    - Priorités de processus
    - Validation des acquis
    - **Commandes** : ps, pstree, pgrep, top, fg, bg, wait, nice, renice, nohup, kill, pkill, fuser.

- **Gestion de la Journalisation**.

- Le fichier /var/log/messages
- Surveillance Sécuritaire
  - La commande last
  - La commande lastlog
  - La Commande faillog
  - /var/log/secure
- La commande /bin/dmesg
- Le fichier /var/log/audit/audit.log
  - Gestion des évènements audit
    - auditd
    - auditctl
    - audispd
  - La consultation des évènements audit
    - La commande aureport
    - La commande ausearch
- Applications
- rsyslog
  - Priorités
  - Sous-systèmes applicatifs
    - /etc/rsyslog.conf
    - Modules
    - Directives Globales
    - Règles
      - Sous-système applicatif.Priorité
      - Sous-système applicatif!Priorité
      - Sous-système applicatif=Priorité
      - L'utilisation du caractère spécial *
      - n Sous-systèmes avec la même priorité
      - n Sélecteurs avec la même Action
  - /usr/bin/logger
    - Options de la commande
  - /usr/sbin/logrotate
    - Options de la commande
- La Journalisation avec journald

        - Consultation des Journaux
        - Consultation des Journaux d'une Application Spécifique
        - Consultation des Journaux depuis le Dernier Démarrage
        - Consultation des Journaux d'une Priorité Spécifique
        - Consultation des Journaux d'une Plage de Dates
        - Consultation des Journaux en Live
        - Consultation des Journaux avec des Mots Clefs
    - Validation des acquis
    - **Commandes** : dmesg, auditd, auditctl, audoispd, aureport, ausearch, rsyslog, logger, logrotate, journalctl.

- **Gestion des Impressions**.
    - Cups
        - Protocoles
        - Paquets
        - Daemon
        - cupsd.conf
        - Filtres
        - Backends
        - Journaux
        - Imprimantes
        - Administration
        - LAB #1 - Gestion des Impressions
    - Validation des acquis
    - **Commandes** : lpadmin, accept, reject, cupsenable, cupsdisable, lpstat, cancel, lpmove, lpinfo, lppasswd, lp.

LF03 - BASH – Programmation de scripts shell

Programme

- **LAB #1**.
    - Automatiser la Gestion des Utilisateurs et Groupes,
        - Fonction **cree_user**,

        - Fonction **modif_user**,
        - Fonction **affiche_user**,
        - Fonction **cree_liste_user**,
        - Fonction **cree_group**,
        - Fonction **modif_group**,
        - Fonction **delete_group**,
        - Fonction **affiche_group**,
        - Menu des choix.

- **LAB #2**.
    - Automatiser la Gestion des Sauvegardes,
        - Fonction **archive_rep**,
        - Fonction **restaure_rep**,
        - Fonction **affiche_archive**,
        - Fonction **compress_archive**,
        - Fonction **decompress_archive**,
        - Gestion des erreurs.

LF04 - Linux Administration N2 – Avancée

Programme

- **Gestion du Démarrage et de l'Arrêt du Système**.
    - Détail du démarrage
        - Systèmes à base du BIOS
        - Systèmes EFI
        - Autres Systèmes
        - Gestionnaire d'amorçage
            - LILO
            - Grub Legacy sous RHEL 6
                - Le fichier menu.lst
                - Configurer l'Authentification

        - Modifier la Configuration de GRUB Legacy en Ligne de Commande
    - Grub2 sous RHEL 7, Debian 8, Ubuntu 16.04 et SLES 12
        - Le fichier /boot/grub/device.map
        - Le fichier /etc/default/grub
        - Les fichiers du répertoire /etc/grub.d
        - Le fichier /etc/grub.d/10_Linux
        - Le fichier /etc/grub.d/30_os-prober
        - Les fichiers /etc/grub.d/40_custom et /etc/grub.d/41_custom
        - Configurer l'Authentification
        - Modifier la Configuration de GRUB 2 en Ligne de Commande
- Initramfs
    - Examiner l'image existante
    - Le script init
    - Créer un Initial Ram Disk
        - La commande dracut sous RHEL et SLES
        - La commande mkinitramfs sous Debian et Ubuntu
        - La commande mkinitrd sous SLES
- Le Démarrage du Noyau
- Le Processus Init
- Le Système de Démarrage SysVinit sous RHEL 5 et Debian 6
    - Niveaux d'exécution sous RHEL 5
    - Niveaux d'exécution sous Debian 6
    - Scripts de Démarrage
        - rc.sysinit sous RHEL
        - rcS sous Debian
    - Scripts Unix Système V sous RHEL 5 et Debian 6
        - inittab
        - Répertoire init.d
        - Répertoires rcX.d
        - Linux Standard Base
        - La commande chkconfig sous RHEL 5 et Debian 6
        - La commande update-rc.d sous Debian 6
    - La Gestion des Services sous SysVinit
- Le Système de Démarrage Upstart sous RHEL 6 et Debian 7

        - Scripts Upstart
            - Initialisation du Système
            - Runlevels
            - [CTL]-[ALT]-[DEL]
            - mingetty
        - La Gestion des Services sous Upstart
    - Le Système de Démarrage Systemd sous RHEL 7, Debian 8, Ubuntu 16.04 et SLES 12
        - La Commande systemctl
        - Fichiers de Configuration
        - La Commande systemd-analyze
        - La Gestion des Services sous Systemd
    - Arrêt Système du Système
        - La commande shutdown
        - La commande reboot
        - La commande halt
        - La commande poweroff
    - Validation des acquis
    - **Commandes** : grub_install, grub-mkconfig, grub2-mkconfig, runlevel, init, telinit, chkconfig, dracut, mkinitramfs, mkinitrd, initctl, start, stop, restart, systemctl, systemd-analyze, lightdm, shutdown, halt, reboot, poweroff.

- **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

                - Options de la commande
        - 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
            - Les options de la commande
    - Système de fichiers /sys
    - Limiter les Ressources
    - Prévoir des Besoins en Ressources
        - La commande collectd

- Validation des acquis
- **Commandes** : netstat, pstree, w, lsof, free, top, uptime, lspci, lsusb, dmidecode, free, uptime, w, iostat, vmstat, hdparm, mpstat, sar, udevadm, collectd, sysctl.

- **Gestion des Données avec MySQL**
  - Le Client MySQL
  - SQL, Champs, Moteurs et Jointures
    - SQL
      - Chaînes de caractères
      - Nombres
        - Nombres Entiers
        - Nombres Décimaux
        - Nombres Négatifs
      - Valeurs NULL
      - Noms de Fichiers
      - Variables Utilisateurs
      - Commentaires
      - Commandes
        - SELECT
        - UPDATE
        - DELETE FROM
        - DROP TABLE
        - INSERT
        - ALTER
        - MATCH
      - Opérateurs
        - Mathémathiques
        - Logiques
        - Comparaison
      - Fonctions
        - Mathémathiques
        - Chaînes
        - Dates
        - Contrôle

        - Agrégation
        - Autres
    - Jointures
        - FULL JOIN
        - LEFT JOIN
        - RIGHT JOIN
    - LAB #1 - Le Langage SQL
  - Validation des acquis
  - **Commandes**: mysql, mysqld.

- **Gestion du Système X et de l'Accès Universel**
  - X Window System
  - Gestionnaire de Fenêtres
  - Toolkits
  - Freedesktop
  - Display Manager
  - Xorg
    - Présentation
    - Utilisation
    - Configuration
    - La Section ServerFlags
    - La Section ServerLayout
    - La Section Files
    - La Section Modules
    - La Section InputDevice
    - La Section Monitor
    - La Section Device
    - La Section Screen
  - L'Accès Universel
    - Le Clavier et la Souris
    - Claviers Visuels
    - L'Ecran
    - Autres Technologies
  - Validation des acquis

    - **Commandes** : xorg, xwininfo, AccessX.

- **Gestion des Modules du Noyau Linux et l'Implémentation des Quotas Disque**
    - Rôle du noyau
    - Les modules
    - L'implémentation des Quotas Disque
        - La commande quotacheck
        - La commande quotaon
        - La commande repquota
        - La commande quota
        - La commande warnquota
    - Validation des acquis
    - **Commandes**: modprobe, modinfo, insmod, rmmod, quotacheck, edquota, quotaon, repquota, quota, warnquota.

LF05 - Linux – TCP/IP et Réseaux

Programme

- **Gestion du Réseau**.
    - Introduction
        - Modèles de Communication
        - Message/Datagramme/Segment
        - Etablissement de la connexion TCP
        - En-tête TCP
        - En-tête UDP
        - Fragmentation et Ré-encapsulation
        - Adressage
        - Masques de sous-réseaux
        - VLSM
        - Ports et sockets
    - Configuration du Réseau sous RHEL 5, RHEL 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
- Configuration du Réseau sous Debian 6
    - Configuration de TCP/IP
        - /etc/network/interfaces
        - DHCP
        - IP Fixe
- Configuration du Réseau sous RHEL/CentOS 7, Debian 8, Ubuntu 16.04 et SLES 12
    - 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
- Services réseaux
    - xinetd
    - TCP Wrapper
- Diagnostique du Réseau
    - La commande ping
    - La commande ping6
    - La commande netstat -i
    - La commande traceroute

        - La commande traceroute6
        - La commande tracepath6
    - Routage Statique
        - RHEL 6
            - La Commande route
            - Activer/désactiver le routage sur le serveur
        - RHEL 7, Debian 8, Ubuntu 16.04 et SLES 12
            - La commande ip
            - Activer/désactiver le routage sur le serveur
    - Connexions à Distance
        - telnet
        - ftp
        - ssh
        - scp
    - La Gestion du Serveur NFS
        - Présentation
        - Les Services et Processus du Serveur NFSv3
        - Options d'un Partage NFS
        - Commandes de Base
        - Mise en Place
            - Configuration du Serveur sous RHEL 6 et Debian 6
            - Configuration du Serveur sous RHEL 7 et Debian 8
            - Configuration du Client sous RHEL 6 et Debian 6
            - Configuration du Client sous RHEL 7 et Debian 8
        - Surveillance du Serveur
            - La Commande rpcinfo
            - La Commande nfsstat
    - Packet Sniffers
        - TCPdump
            - Installation
            - Utilisation
        - Wireshark
            - Installation
            - Utilisation

- Port Scanners
  - nmap
    - Installation
    - Utilisation
    - Fichiers de configuration
    - Scripts
  - netcat
    - Installation
    - Utilisation
- Le Pare-feu Netfilter/iptables
  - Introduction
  - La Configuration par Scripts sous RHEL 6 et Debian 6
    - LAB #1
    - LAB #2
  - La Configuration par firewalld sous RHEL 7, Debian 8, Ubuntu 16.04 et SLES 12
    - La Configuration de Base de firewalld
    - La Commande firewall-cmd
    - La Configuration Avancée de firewalld
    - Le mode Panic de firewalld
- Encryption
  - GnuPG
    - Presentation
    - Installation
    - Utilisation
  - Public Key Infrastructures - PKI
    - Certificats X509
  - SSH et SCP
    - SSH
      - Introduction
        - SSH-1
        - SSH-2
      - Authentification par mot de passe
      - Authentification par clefs asymétriques
        - Serveur SSH

            - Client SSH
            - Utilisation
        - SCP
            - Introduction
            - Utilisation
        - Tunnels SSH
    - Validation des acquis
    - **Commandes** : netstat, arp, nslookup, dig, ifconfig, ifup, ifdown, ifstatus, NetworkManager, hostname, uname, nmcli, ip, network-manager, ping, ping6, Traceroute, Traceroute6, Tracepath6, tcpd, xinetd, route, ntpd, telnet, wget, ftp, tcpdump, wireshark, nmap, netcat, iptables, gpg, firewall-cmd, ssh, scp.

LF06 - Linux Administration N3 – Sécurité

Programme

- **Risque : Chevaux de Troie et Scans**
    - Définitions
        - Chevaux de Troie
        - Scans
    - LAB #1 - Utilisation de nmap et de netcat
        - nmap
            - Installation
            - Options de la commande
            - Utilisation
            - Fichiers de Configuration
            - Scripts
        - netcat
            - Installation
            - Options de la commande
            - Utilisation
    - LAB #2 - Mise en place du Système de Détection d'Intrusion Snort
        - Installation

        - Options de la commande
        - Utilisation de snort en mode “packet sniffer”
        - Utilisation de snort en mode “packet logger”
        - Journalisation
        - Utilisation de snort en mode “NIDS”
    - LAB #3 - Mise en place du Système de Détection et de Prévention d'Intrusion Portsentry
        - Installation
        - Configuration
        - Utilisation

- **Risque - Sniffing**
    - Définition
    - LAB #4 - Utilisation de tcpdump et de Wireshark
        - TCPdump
            - Installation
            - Options de la commande
            - Utilisation
        - Wireshark
            - Installation
            - Options de la commande
            - Utilisation
    - LAB #5 - Utilisation du Chiffrement
        - 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
            - Utilisation de GnuPG
                - Présentation
                - Installation

        - Utilisation
    - PKI
        - Certificats X509
- LAB #6 - Mise en place de SSH et SCP
    - SSH
        - Introduction
        - SSH-1
        - SSH-2
        - L'authentification par mot de passe
        - L'authentification par clef asymétrique
        - Installation
        - Options de la commande
        - Configuration
        - Serveur
        - Client
        - Utilisation
    - Tunnels SSH
    - SCP
        - Introduction
        - Utilisation
        - Mise en place des clefs
- LAB #7 - Mise en place d'un VPN avec OpenVPN
    - Présentation
    - Architecture de test
    - Configuration commune au client et au serveur
    - Configuration du client
    - Configuration du serveur
    - Tests
        - Du client vers le serveur
        - Du serveur vers le client

- **Risque : IP Spoofing, Déni de Service (DoS), Syn Flooding et Flood**
    - Définitions
        - L'IP Spoofing

        - Déni de Service (DoS)
        - SYN Flooding
        - Flood
    - LAB #8 - Configuration du Pare-feu Netfilter/iptables
        - Introduction
        - Configuration par Scripts sous RHEL/CentOS 6
    - LAB #9 - La Configuration par firewalld sous RHEL/CentOS 7
        - La Configuration de Base de firewalld
        - La Configuration Avancée de firewalld
        - Le mode Panic de firewalld

- **Risque : Crackage**
    - Définition
    - LAB #10 - Installer et utiliser John the Ripper
    - LAB #11 - Renforcer la sécurité des comptes
    - LAB #12 - Forcer l'utilisation des mots de passe complexe avec PAM
        - Utiliser des Mots de Passe Complexe
        - Bloquer un Compte après N Echecs de Connexion
        - Configuration
    - LAB #13 - 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

- **Risque : Système de Fichiers et Données**
    - Gestion de Droits
        - Les Droits Unix Simples
        - La Modification des Droits
        - Modifier le propriétaire ou le groupe
        - Les Droits Unix Etendus
        - Les ACL

        - Les Attributs Ext2/Ext3/Ext4 et XFS
        - LAB #14 - Mise en place du File Integrity Checker Afick
            - Présentation
            - Installation
            - Configuration
                - La Section Directives
                - La Section Alias
                - La Section Files
                - Utilisation
                - Automatiser Afick
    - La sécurisation des systèmes de fichiers
        - Le Fichier /etc/fstab
            - Comprendre le fichier /etc/fstab
            - Options de Montage
            - LAB #15 - Créer un Système de Fichiers Chiffré avec encryptfs
            - LAB #16 - Créer un Système de Fichiers Chiffré avec LUKS
                - Présentation
                - Mise en Place
                - Ajouter une deuxième Passphrase
                - Supprimer une Passphrase
        - Root Kits
            - Présentation
            - LAB #17 - Mise en place de Chkrootkit
                - Installation
                - Options de la commande
                - Utilisation
                - Automatiser chkrootkit
            - LAB #18 - Mise en place de rkhunter
                - Installation
                - Les options de la commande
                - Utilisation
                - Configuration
        - Gestion des Disques - RAID
            - Concepts RAID

        - Préparation du disque
        - Mise en Place du RAID Logiciel
        - Quotas

- **Risque : OS Linux**
    - Les compilateurs
    - Les paquets
    - Les démons et services
    - Les fichiers .rhosts
    - Les fichiers et les repertoires sans proprietaire
    - Les connexions de root via le reseau
    - Limiter le delai d'inactivite d'une session shell
    - Renforcer la securite d'init
    - Renforcer la sécurité du Noyau
        - La commande sysctl
        - Options de la commande
    - LAB #19 - Utilisation de Bastille Linux pour sécuriser Linux
        - Présentation
        - Installation
        - Utilisation
    - Mise en place de SELinux pour sécuriser le serveur
        - Introducton
        - Définitions
        - Security Context
        - Domains et Types
        - Roles
        - Politiques de Sécurité
        - Commandes SELinux
        - Les Etats de SELinux
        - Booléens
        - LAB #20 - 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
    - La commande last
    - La commande lastlog
    - La Commande faillog
    - /var/log/secure

- **Risque : Spam et Virus**
    - Définitions
        - Spam
        - Virus
            - Virus de Boot
            - Vers
            - Bombes Logiques
            - Trappes
            - Macro-virus
    - Postfix et Cyrus SASL
        - Présentation
        - Configuration de Postfix
        - smtpd_recipient_restrictions
        - smtpd_client_restrictions
        - smtpd_sasl_security_options
    - TLS
    - Antispam et Antivirus
        - SpamAssassin
        - ClamAV
    - Le Mandataire MailScanner
        - Préparation à l'Installation
        - Installation

        - Configuration du couple MailScanner/Postfix

- **Risque : Sécurité Applicative**
    - LAB #21 - Mise en place d'Openvas
        - Présentation
        - Installation
        - Configuration
        - Utilisation
        - Analyse des Résultats
    - LAB #22 - Mise en place de Netwox
        - Installation
        - Utilisation
        - Avertissement important
    - LAB #23 - La commande chroot
    - LAB #24 - Sécuriser Apache
        - 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 MySQL
            - Configuration d'Apache
    - mod_ssl
        - Présentation de SSL
        - Fonctionnement de SSL
        - Configuration de SSL
        - Mise en place des paramètres de sécurité SSL
    - Tester la Configuration

- **Commandes** : chroot, sudo, who, w, last, lastlog, afick, bastille, chcon, audit2allow, restorecon, setfiles, getsebool, sestatus, setsebool, togglesebool, semodule, checkmodule, semodule_package, semanage, sesearch, seinfo, getenforce, setenforce, nmap, netcat, tcpdump, wireshark, snort, nessus, chkrootkit, rkhunter, netwox, ssh, openssl, iptables, openvpn, mdadm, quotaon, quotacheck, edquota, squid, squidGuard, dansguardian, chmod, umask, chown, chgrp, setfacl, getfacl, chattr, lsattr.

- **Validation des Acquis**

LF07 - Linux Services Réseaux

Programme

- **Gestion des Serveurs DNS, NTP, FTP et DHCP**
    - Le serveur DNS
        - Préparation à l'Installation
        - Installation
            - Options de la commande named
        - Les fichiers de configuration
            - named.ca
            - named.conf
            - Les Sections de Zone
                - La Valeur Type
                - La Valeur File
                - Exemples de Sections de Zone
                - Sections de Zones de votre Machine
                - Les fichiers de zone
                    - db.fenestros.loc.hosts
                    - db.2.0.10.hosts
        - rndc
            - La clef rndc
            - Fichiers de Configuration
            - Options de la commande
        - LAB #1
    - Le Serveur d'Horloge
        - Introduction
        - Installation
        - Le fichier ntp.conf
        - Options de la commande

        - LAB #2
    - Le Serveur FTP
        - Installation
        - Configuration de base
        - /etc/ftpusers
        - Serveur vsftpd Anonyme
            - Configuration
        - Serveur vsftpd et Utilisateurs Virtuels
            - Introduction
            - Configuration
            - LAB #3
    - Le Serveur DHCP
        - Introduction
        - Installation
        - Configuration de base
            - Le fichier dhcpd.conf

LF08 - Virtualisation Légère -Docker

Programme

- **Gestion de la Virtualisation Légère avec Docker**
    - Présentation de Docker
    - Installer docker
    - LAB #1 - Démarrer avec Docker
        - Démarrer un Conteneur
        - Consulter la Liste des Conteneurs et Images
        - Rechercher une Image dans un Dépôt
        - Supprimer un Conteneur d'une Image
        - Créer une Image à partir d'un Conteneur Modifié
        - Supprimer une Image
        - Créer un Conteneur avec un Nom Spécific

        - Exécuter une Commande dans un Conteneur
        - Injecter des Variables d'Environnement dans un Conteneur
        - Modifier le Nom d'Hôte d'un Conteneur
        - Mapper des Ports d'un Conteneur
        - Démarrer un Conteneur en mode Détaché
        - Accèder aux Services d'un Conteneur de l'Extérieur
        - Arrêter et Démarrer un Conteneur
        - Utiliser des Signaux avec un Conteneur
        - Forcer la Suppression d'un Conteneur en cours d'Exécution
        - Utilisation Simple d'un Volume
        - Télécharger une image sans créer un conteneur
        - S'attacher à un conteneur en cours d'exécution
        - Installer un logiciel dans le conteneur
        - Utilisation de la commande docker commit
        - Se connecter au serveur du conteneur de l'extérieur
    - LAB #2 - Re-créer une image officielle docker
        - Utilisation d'un Dockerfile
        - FROM
        - RUN
        - ENV
        - VOLUME
        - COPY
        - ENTRYPOINT
        - EXPOSE
        - CMD
        - Autres Commandes
    - LAB #3 - Créer un Dockerfile
        - Création et test du script
        - Bonnes Pratiques liées au Cache
            - Opérations Non-Idempotentes
    - LAB #4 - Installer un Registre Privé
        - Créer un Serveur de Registre Dédié
            - Configurer le clone comme Registre Dédié
            - Configurer le Client

- LAB #5 - Gestion des Volumes
  - Gestion Automatique par Docker
  - Gestion Manuelle d'un Volume
- LAB #6 - Gestion du Réseau
  - Bridge
  - None
  - Liens
- LAB #7 - Superviser les Conteneurs
  - Les Journaux
  - Les Processus
  - L'Activité en Continu
- LAB #8 - Gestion des Ressources
  - Docker Compose
  - Installation
  - LAB #9 - Utiliser docker-compose
- Docker Machine
  - Présentation
  - Préparation
    - Docker-CE
      - Mac
      - Linux
      - Windows
    - VirtualBox
  - Installation
    - Mac
    - Linux
    - Windows
  - LAB #10 - Création de Machines Virtuelles Docker
    - Lister les VM Docker
    - Obtenir l'adresse IP des VM
    - Se connecter à une VM Docker
- Docker Swarm
  - Présentation
  - Initialiser Docker Swarm

        - LAB #11 - Utiliser Docker Swarm
            - Le Statut Leader
            - Rejoindre le Swarm
            - Consulter les Informations de Swarm
            - Démarrer un Service
            - Augmentation et Réduction du Service
            - Consulter le Statut d'un Noeud
            - Haute Disponibilité
            - Supprimer un Service

LF09 - Virtualisation – KVM

Programme

- **Virtualiser**
    - Définition
    - Intérêts
    - Historique
    - Méthodes
    - Paravirtualisation
    - Assistance matérielle
    - QEMU
    - KVM
- **Utiliser QEMU et KVM**
- Créer une image disque
- Paramètres
- Paramètres initiaux
- Architecture et processeurs
- Carte son
- Carte graphique
- Date RTC

- Réseau
- USB
- Disques
- VNC

- **Monitoring**
  - Depuis un console
  - Depuis la machine virtuelle
  - Commande du mode monitor
  - Snapshots
  - Gérer l'exécution

- **Migration à chaud**
  - Pré-requis
  - Migration

- **Monitoring QMP**
  - Lancer QMP
  - Accès par telnet
  - QMP Shell
  - Libvirt

- **Fichier de configuration**

- **KVM**
  - Installation
  - Chargement des modules
  - Installation de Linux

- **Libvirt**
  - Service de virtualisation
  - Administration graphique
    - Virt-manager
    - Créer une machine virtuelle
    - Installer un système invité
    - Modifier les paramètres de la VM

        - Gestion des disques
        - Branchement USB à chaud
        - Configuration réseau
        - Interface réseau ponté
    - Administration en ligne de commande
        - Virsh
        - Connexion à l'hyperviseur
        - Lister les VM
        - Contrôler une VM
        - Informations
        - Configuration XML
        - Création et destruction
        - Suspendre et reprendre
        - Sauver et restaurer

LF10 - Gestion du Serveur OpenLDAP

Programme

- **Gestion du Serveur OpenLDAP**
    - Présentation
        - Qu’est-ce que LDAP ?
            - Le Protocole X.500
            - LDAP v3
        - Comment fonctionne LDAP ?
            - Le Modèle d'Information de LDAP
            - Les DN et les RDN
        - La Structure d’un annuaire LDAP
            - Les Attributs
                - Les Attributs Utilisateur
                - Les Attributs Opérationnels
                - Les Classes d'Objets

        - Les Types de Classe d'Objets
      - Les OID
      - Les Schémas de l'Annuaire
  - Installation du serveur LDAP
  - Configuration de Démarrage du serveur LDAP
  - Configuration du serveur LDAP
    - L'annuaire Local
    - L''annuaire Local avec des Referrals
    - L'annuaire local avec réplication
  - Fichier(s) de Configuration
    - Le Fichier slapd.conf
      - Les Directives du Fichier slapd.conf
        - include
        - allow
        - referral
        - pidfile
        - argsfile
        - modulepath
        - moduleload
        - TLSCACertificateFile, TLSCertificateFile & TLSCertificateKeyFile
        - security
        - access to
        - database config
        - backend
        - suffix DN
        - checkpoint
        - rootdn <DN>
        - rootpw <mot de passe>
        - directory
        - index
        - replogfile <filename>
        - replica host <hostname>[:<port>] [bindmethod={ simple | kerberos | sasl }]
      - Autres Directives Utiles
        - loglevel

        - password-hash
        - schemacheck
        - idletimeout
        - sizelimit
        - timelimit
        - readonly <on | off>
        - lastmod <on | off>
    - Le Fichier /etc/openldap/ldap.conf
    - cn=config
    - Sécuriser l'Annuaire
        - Créer le Mot de Passe de l'Administrateur
        - Sécuriser avec SSL
    - Options de la ligne de commande de slapd
- Création et maintenance de la base de données
    - Le format LDIF
    - Création d’une base de données en ligne
        - La commande ldapadd
        - Utilisation du client graphique luma
        - Le Directory Information Tree
        - Les alias
        - Les attributs
        - Les classes
        - Les schémas
        - Les referrals
        - La commande ldapsearch
        - La commande ldapmodify
        - La commande ldapdelete
    - Création d’une base de données hors ligne
        - La commande slapadd
    - Maintenance d’une base de données LDAP
        - La commande slapcat
        - La commande slapindex
        - La commande slapdn
        - La commande slaptest

            - La commande slapauth
    - LAB #1 - Replication de Serveurs OpenLDAP
        - Préparation
        - Replication
            - Configuration du serveur fournisseur
            - Configuration du serveur consommateur
            - Mise en place
    - LAB #2 - Authentification Apache en utilisant OpenLDAP
    - Validation des acquis
    - **Commandes** : ldapadd, ldapsearch, ldapmodify, ldapdelete, slapcat, slapindex, slapdn, slaptest, slapauth.