Version : **2026.01**

Dernière mise-à-jour : 2025/12/03 16:51

LDF400 - Administration de la Sécurité

Contenu du Module

- **LDF400 - Administration de la Sécurité**
  - Contenu du Module
  - Pré-requis
    - Matériel
    - Logiciels
    - Internet
  - Programme de la Formation

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

- Navigateur Web Chrome ou Firefox.

Internet

- Un accès à Internet **rapide** (4G minimum) **sans** passer par un proxy,
- Accès **débloqué** aux domaines suivants : *.ittraining.team.

Programme de la Formation

- **LDF400 - Administration de la Sécurité**.
    - Contenu du Module
    - Pré-requis
        - Matériel
        - Logiciels
        - Internet
    - Programme de la Formation
- **LDF401 - Gestion des Droits**
    - Présentation
    - Préparation
    - LAB #1 - Les Droits Unix Simples
        - 1.1 - La Modification des Droits
            - La Commande chmod
                - Mode Symbolique
                - Mode Octal
            - La Commande umask
        - 1.2 - Modifier le propriétaire ou le groupe
            - La Commande chown
            - La Commande chgrp
    - LAB #2 - Les Droits Unix Étendus
        - 2.1 - SUID/SGID bit
        - 2.2 - Inheritance Flag
        - 2.3 - Sticky bit
    - LAB #3 - Les Droits Unix Avancés

        - 3.1 - Les ACL
        - 3.2 - Les Attributs Étendus

- **LDF402 - Netfilter et Firewalld**
    - Les Problématiques
        - L'IP Spoofing
        - Déni de Service (DoS)
        - SYN Flooding
        - Flood
    - La Contre-Mesure
        - LAB #1 - La Configuration de firewalld
            - 1.1 - La Configuration de Base de firewalld
            - 1.2 - La Commande firewall-cmd
            - 1.3 - La Configuration Avancée de firewalld
            - 1.4 - Le mode Panic de firewalld

- **LDF403 - Authentification**
    - Le Problématique
    - Surveillance Sécuritaire
        - La commande last
        - La commande lastlog
        - La Commande lastb
        - /var/log/secure
    - Les Contre-Mesures
        - LAB #1 - Renforcer la sécurité des comptes
    - LAB #2 - PAM
        - 2.1 - Configuration des modules
        - 2.2 - Utiliser des Mots de Passe Complexes
    - LAB #3 - Mise en place du Système de Prévention d'Intrusion Fail2Ban
        - 3.1 - Installation
        - 3.2 - Configuration
            - Le répertoire /etc/fail2ban
            - Le fichier fail2ban.conf
            - Le répertoire /etc/fail2ban/filter.d/
            - Le répertoire /etc/fail2ban/action.d/

        - 3.3 - Commandes
            - Activer et Démarrer le Serveur
            - Utiliser la Commande Fail2Ban-server
            - Ajouter un Prison

- **LDF404 - Système de Fichiers**
    - La sécurisation des systèmes de fichiers
        - Le Fichier /etc/fstab
            - Comprendre le fichier /etc/fstab
            - Options de Montage
    - Systèmes de Fichiers Chiffrés
        - LAB #1 - Créer un Système de Fichiers Chiffré avec encryptfs
        - LAB #2 - Créer un Système de Fichiers Chiffré avec LUKS
            - 2.1 - Présentation
            - 2.2 - Mise en Place
            - 2.3 - Le fichier /etc/crypttab
            - 2.4 - Ajouter une deuxième Passphrase
            - 2.5 - Supprimer une Passphrase
            - 2.6 - Supprimer LUKS
    - LAB #3 - Mise en place du File Integrity Checker Afick
        - 3.1 - Présentation
        - 3.2 - Installation
        - 3.3 - Configuration
            - La Section Directives
            - La Section Alias
            - La Section File
        - 3.4 - Utilisation
        - 3.5 - Automatiser Afick
    - Root Kits
        - Le Problématique
        - Contre-Mesures
        - LAB #4 - Mise en place de rkhunter
            - 4.1 - Installation
            - 4.2 - Utilisation

        - 4.3 - Configuration
    - LAB #5 - Mise en place de chkrootkit
        - 5.1 - Installation
        - 5.2 - Utilisation
        - 5.3 - Configuration

- **LDF405 - System Hardening**
    - Contenu du Module
    - 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 delai 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 Lynis
        - 1.1 - Présentation
        - 1.2 - Installation
        - 1.3 - Utilisation
    - LAB #2 - Mise en place d'AppArmor pour sécuriser le serveur
        - 2.1 - Présentation
        - 2.2 - Définitions
            - Les Profils d'AppArmor
            - Les Etats ou Modes d'AppArmor
        - 2.3 - Installation
            - Installation des Paquets
            - Modification de GRUB
            - Vérification de l'Activation d'AppArmor

- LAB #3 - Travailler avec AppArmor
  - 3.1 - Consulter la Liste des Profils Chargés
    - La Commande aa-status
  - 3.2 - Passer le Mode d'un Profil de Complain à Enforce
    - La Commande aa-complain
  - 3.3 - Passer le Mode d'un Profil d'Enforce à Complain
    - La Commande aa-enforce
  - 3.4 - Désactiver et Réactiver tous les Profils
  - 3.5 - Créer un Profil
    - La Commande aa-genprof
    - La Commande aa-logprof
  - 3.6 - Supprimer un Profil
    - La Commande apparmor_parser
    - La Commande aa-remove-unknown
- LAB #4 - Mise en place de SELinux pour sécuriser le serveur
  - 4.1 - Présentation
  - 4.2 - 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
  - 4.3 - Commandes SELinux
  - 4.4 - Les Etats de SELinux
  - 4.5 - Booléens
- LAB #5 - Travailler avec SELinux
  - 5.1 - Copier et Déplacer des Fichiers
  - 5.2 - Vérifier les SC des Processus

        - 5.3 - Visualiser la SC d'un Utilisateur
        - 5.4 - Vérifier la SC d'un fichier
        - 5.5 - Troubleshooting SELinux
            - La commande chcon
            - La commande restorecon
        - 5.6 - Le fichier /.autorelabel
        - 5.7 - La commande semanage
        - 5.8 - La commande audit2allow

- **LDF406 - Balayage des Ports**
    - Le Problématique
        - LAB #1 - Utilisation de nmap et de netcat
            - 1.1 - nmap
                - Installation
                - Utilisation
                - Fichiers de Configuration
                - Scripts
            - 1.2 - netcat
                - Utilisation
    - Les Contre-Mesures
        - LAB #2 - Mise en place du Système de Détection d'Intrusion Snort
            - 2.1 - Installation
            - 2.2 - Configuration de Snort
                - Editer le fichier /etc/snort/snort.conf
            - 2.3 - Utilisation de snort en mode “packet sniffer”
            - 2.4 - Utilisation de snort en mode “packet logger”
            - 2.5 - Journalisation
        - LAB #3 - Mise en place du Système de Détection et de Prévention d'Intrusion Portsentry
            - 3.1 - Installation
            - 3.2 - Configuration
            - 3.3 - Utilisation

- **LDF407 - Cryptologie**
    - Le Problématique
    - LAB #1 - Utilisation de tcpdump

        - 1.1 - Utilisation
            - L'option -i
            - L'option -x
            - L'option -X
            - L'option -w
            - L'option -v
        - 1.2 - 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
        - 2.1 - Présentation
        - 2.2 - Installation
        - 2.3 - Utilisation
            - Signer un message
            - Chiffrer un message
    - LAB #3 - Mise en place de SSH et SCP
        - 3.1 - Introduction
            - SSH-1
            - SSH-2
            - L'authentification par mot de passe
            - L'authentification par clef asymétrique
        - 3.2 - Configuration du Serveur
        - 3.3 - Utilisation
    - 3.4 - Mise en place des clefs

        - 3.5 - Tunnels SSH
        - 3.6 - SCP
            - Introduction
            - Utilisation
    - 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

- **LDF408 - Sécurité Applicative**
    - Le Problématique
    - Préparation
    - Les Outils
        - LAB #1 - Netwox
            - 1.1 - Installation
            - 1.2 - Utilisation
            - 1.3 - Avertissement important
        - LAB #2 - Greenbone Vulnerability Management (GVM)
            - 2.1 - Présentation
            - 2.2 - Préparation
            - 2.3 - Installation
            - 2.4 - Configuration
            - 2.5 - Utilisation
            - 2.6 - Analyse des Résultats
    - Les Contres-Mesures
        - LAB #3 - La commande chroot

- **LDF409 - Gestion de la Sécurité de Docker**
    - Contenu du Module
    - Présentation de Docker
    - LAB #1 - Travailler avec Docker

        - 1.1 - Installer docker
        - 1.2 - Démarrer un Conteneur
        - 1.3 - Consulter la Liste des Conteneurs et Images
        - 1.4 - Rechercher une Image dans un Dépôt
        - 1.5 - Supprimer un Conteneur d'une Image
        - 1.6 - Créer une Image à partir d'un Conteneur Modifié
        - 1.7 - Supprimer une Image
        - 1.8 - Créer un Conteneur avec un Nom Spécifique
        - 1.9 - Exécuter une Commande dans un Conteneur
        - 1.10 - Injecter des Variables d'Environnement dans un Conteneur
        - 1.11 - Modifier le Nom d'Hôte d'un Conteneur
        - 1.12 - Mapper des Ports d'un Conteneur
        - 1.13 - Démarrer un Conteneur en mode Détaché
        - 1.14 - Accéder aux Services d'un Conteneur de l'Extérieur
        - 1.15 - Arrêter et Démarrer un Conteneur
        - 1.16 - Utiliser des Signaux avec un Conteneur
        - 1.17 - Forcer la Suppression d'un Conteneur en cours d'Exécution
        - 1.18 - Utilisation Simple d'un Volume
        - 1.19 - Télécharger une image sans créer un conteneur
        - 1.20 - S'attacher à un conteneur en cours d'exécution
        - 1.21 - Installer un logiciel dans le conteneur
        - 1.22 - Utilisation de la commande docker commit
        - 1.23 - Se connecter au serveur du conteneur de l'extérieur
    - LAB #2 - Création d'un Utilisateur de Confiance pour Contrôler le Daemon Docker
    - LAB #3 - Le Script docker-bench-security.sh
    - LAB #4 - Sécurisation de la Configuration de l'Hôte Docker
        - 4.1 - [WARN] 1.2.1 - Ensure a separate partition for containers has been created
        - 4.2 - [WARN] 1.2.3 - Ensure auditing is configured for the Docker daemon
    - LAB #5 - Sécurisation de la Configuration du daemon Docker
        - 5.1 - [WARN] 2.1 - Ensure network traffic is restricted between containers on the default bridge
        - 5.2 - [WARN] 2.8 - Enable user namespace support
        - 5.3 - [WARN] 2.11 - Ensure that authorization for Docker client commands is enabled
        - 5.4 - [WARN] 2.12 - Ensure centralized and remote logging is configured
        - 5.5 - [WARN] 2.14 - Ensure Userland Proxy is Disabled

        - 5.6 - [WARN] 2.17 - Ensure containers are restricted from acquiring new privileges
        - 5.7 - Le Fichier /etc/docker/daemon.json
    - LAB #6 - Sécurisation des Images et les Fichiers de Construction
        - 6.1 - [WARN] 4.1 - Ensure a user for the container has been created
        - 6.2 - [WARN] 4.5 - Ensure Content trust for Docker is Enabled
        - 6.3 - [WARN] 4.6 - Ensure that HEALTHCHECK instructions have been added to container images
    - LAB #7 - Sécurisation du Container Runtime
        - 7.1 - [WARN] 5.1 - Ensure AppArmor Profile is Enabled
        - 7.2 - [WARN] 5.2 - Ensure SELinux security options are set, if applicable
        - 7.3 - [WARN] 5.10 - Ensure memory usage for container is limited
        - 7.4 - [WARN] 5.11 - Ensure CPU priority is set appropriately on the container
        - 7.5 - [WARN] 5.12 - Ensure the container's root filesystem is mounted as read only
        - 7.6 - [WARN] 5.14 - Ensure 'on-failure' container restart policy is set to '5'
        - 7.7 - [WARN] 5.25 - Ensure the container is restricted from acquiring additional privileges
        - 7.8 - [WARN] 5.26 - Ensure container health is checked at runtime
        - 7.9 - [WARN] 5.28 - Ensure PIDs cgroup limit is used
    - LAB #8 - Sécurisation des Images avec Docker Content Trust
        - 8.1 - DOCKER_CONTENT_TRUST
        - 8.2 - DCT et la commande docker pull
            - L'option disable-content-trust
        - 8.3 - DCT et la commande docker push
        - 8.4 - DCT et la commande docker build
            - Créer un deuxième Repositry
            - Supprimer une Signature

- **LDF410 - Validation de la Formation** .
    - Rappel du Programme de la Formation
    - Évaluation de la Formation
    - Validation des acquis
