

Version : **2026.01**

Dernière mise-à-jour : 2025/12/29 13:31

Administration de la Sécurité

Contenu du Module

- Prérequis
 - Matériel
 - Logiciels
 - Internet
- Programme de la Formation

Prérequis

Matériel

- Un poste (MacOS, Linux, Windows™ ou Solaris™),
- Clavier AZERTY FR,
- Un casque ou des écouteurs,
- Un micro.

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

- **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**
 - 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 Lynis
 - 1.1 - Présentation
 - 1.2 - Installation
 - 1.3 - Utilisation
 - LAB #2 - Mise en Place d'un Chroot pour isoler un utilisateur/une application
 - LAB #3 - Mise en place d'AppArmor pour sécuriser le serveur
 - 3.1 - Présentation
 - 3.2 - Définitions
 - Les Profils d'AppArmor
 - Les Etats ou Modes d'AppArmor
 - 3.3 - Installation
 - Installation des Paquets
 - Modification de GRUB
 - Vérification de l'Activation d'AppArmor
 - LAB #4 - Travailler avec AppArmor
 - 4.1 - Consulter la Liste des Profils Chargés
 - La Commande aa-status
 - 4.2 - Passer le Mode d'un Profil de Complain à Enforce
 - La Commande aa-complain
 - 4.3 - Passer le Mode d'un Profil d'Enforce à Complain
 - La Commande aa-enforce
 - 4.4 - Désactiver et Réactiver tous les Profils
 - 4.5 - Créer un Profil
-

- La Commande aa-genprof
 - La Commande aa-logprof
 - 4.6 - Supprimer un Profil
 - La Commande apparmor_parser
 - La Commande aa-remove-unknown
 - LAB #5 - Mise en place de SELinux pour sécuriser le serveur
 - 5.1 - Présentation
 - 5.2 - 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
 - 5.3 - Commandes SELinux
 - 5.4 - Les Etats de SELinux
 - 5.5 - Booléens
 - LAB #6 - Travailler avec SELinux
 - 6.1 - Copier et Déplacer des Fichiers
 - 6.2 - Vérifier les SC des Processus
 - 6.3 - Visualiser la SC d'un Utilisateur
 - 6.4 - Vérifier la SC d'un fichier
 - 6.5 - Troubleshooting SELinux
 - La commande chcon
 - La commande restorecon
 - 6.6 - Le fichier /.autorelabel
 - 6.7 - La commande semanage
 - 6.8 - La commande audit2allow
-

- **LDF406 - 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
 - LAB #3 - Sécuriser le Serveur DNS
 - 3.1 - Le Serveur DNS
 - 3.2 - Préparation à l'Installation
 - 3.3 - Installation
 - 3.4 - Les fichiers de configuration
 - 3.5 - Utilisation
 - 3.6 - Créer les Pairs de Clefs
 - 3.7 - Modifier la Configuration de Bind
 - 3.8 - Signer la Zone
 - 3.9 - La chaîne de confiance DNS
 - LAB #4 - Sécuriser Apache
 - 4.1 - Installation
 - 4.2 - Testez le serveur apache
 - Avec un navigateur
 - Avec Telnet
 - 4.3 - Préparation
 - 4.4 - Gestion de serveurs virtuels
 - Hôte virtuel par nom
 - Hôte virtuel par adresse IP

- 4.5 - mod_auth_basic
 - Configuration de la sécurité avec .htaccess
 - Mise en place d'un fichier de mots de passe
- 4.6 - mod_auth_mysql
 - Installation
 - Configuration de MariaDB
 - Configuration d'Apache
- 4.7 - mod_authnz_ldap
- 4.8 - mod_ssl
 - Présentation de SSL
 - Fonctionnement de SSL
 - Installation de ssl
 - Configuration de SSL
 - Mise en place des paramètres de sécurité SSL
 - Tester Votre Configuration

- **LDF407 - 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
 - 2.3 - Utilisation
 - LAB #3 - Mise en place du Système de Détection et de Prévention d'Intrusion Portsentry
 - 3.1 - Installation
 - 3.2 - Configuration

- 3.3 - Utilisation

- **LDF408 - 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 serveur OpenVPN
 - 4.1 - Installation
 - 4.2 - Configuration du Serveur
 - 4.3 - Configuration du client
 - 4.4 - Les Clefs du Client
 - 4.5 - Tester la Configuration
- LAB #5 - Mise en place d'un serveur Wireguard
 - 5.1 - Installation et Configuration du Serveur
 - 5.2 - Installation et Configuration du Client
 - 5.3 - Tester la Configuration

- **LDF409 - Gestion de la Sécurité de Docker**

- Présentation de la Virtualisation par Isolation
 - Historique
- Présentation des Namespaces
- Présentation des CGroups
 - LAB #1 - cgroups v1
 - 1.1 - Préparation
 - 1.2 - Présentation
 - 1.3 - Limitation de la Mémoire
 - 1.4 - La Commande cgcreate
 - 1.5 - La Commande cgexec
 - 1.6 - La Commande cgdelete
 - 1.7 - Le Fichier /etc/cgconfig.conf
 - 1.8 - La Commande cgconfigparser

- LAB #2 - cgroups v2
 - 2.1 - Préparation
 - 2.2 - Présentation
 - 2.3 - Limitation de la CPU
 - 2.4 - La Commande systemctl set-property
 - Présentation de Docker
 - Virtualisation et Containérisation
 - Le Système de Fichier AUFS
 - OverlayFS et Overlay2
 - Docker Daemon et Docker Engine
 - Docker CE et Docker EE
 - Docker CE
 - Docker EE
 - Docker et Mirantis
 - LAB #3 - Travailler avec Docker
 - 3.1 - Installer docker sous Linux
 - 3.1.1 - Debian 11
 - 3.1.2 - CentOS 8
 - 3.2 - Démarrer un Conteneur
 - 3.3 - Consulter la Liste des Conteneurs et Images
 - 3.4 - Rechercher une Image dans un Dépôt
 - 3.5 - Supprimer un Conteneur d'une Image
 - 3.6 - Créer une Image à partir d'un Conteneur Modifié
 - 3.7 - Supprimer une Image
 - 3.8 - Créer un Conteneur avec un Nom Spécifique
 - 3.9 - Exécuter une Commande dans un Conteneur
 - 3.10 - Injecter des Variables d'Environnement dans un Conteneur
 - 3.11 - Modifier le Nom d'Hôte d'un Conteneur
 - 3.12 - Mapper des Ports d'un Conteneur
 - 3.13 - Démarrer un Conteneur en mode Détaché
 - 3.14 - Accéder aux Services d'un Conteneur de l'Extérieur
 - 3.15 - Arrêter et Démarrer un Conteneur
 - 3.16 - Utiliser des Signaux avec un Conteneur
 - 3.17 - Forcer la Suppression d'un Conteneur en cours d'Exécution
-

- 3.18 - Utilisation Simple d'un Volume
- 3.19 - Télécharger une image sans créer un conteneur
- 3.20 - S'attacher à un conteneur en cours d'exécution
- 3.21 - Installer un logiciel dans le conteneur
- 3.22 - Utilisation de la commande docker commit
- 3.23 - Se connecter au serveur du conteneur de l'extérieur
- Sécurisation de Docker
 - LAB #4 - Utilisation des Docker Secrets
 - LAB #5 - Création d'un Utilisateur de Confiance pour Contrôler le Daemon Docker
 - LAB #6 - Le Script docker-bench-security.sh
 - LAB #7 - Sécurisation de la Configuration de l'Hôte Docker
 - LAB #8 - Sécurisation de la Configuration du daemon Docker
 - 8.1 - Le Fichier /etc/docker/daemon.json
 - LAB #9 - Sécurisation des Images et les Fichiers de Construction
 - LAB #10 - Sécurisation du Container Runtime
 - LAB #11 - Sécurisation des Images avec Docker Content Trust
 - 11.1 - DOCKER_CONTENT_TRUST
 - 11.2 - DCT et la commande docker pull
 - L'option disable-content-trust
 - 11.3 - DCT et la commande docker push
 - 11.4 - DCT et la commande docker build
 - Créer un deuxième Repository
 - Supprimer une Signature
 - LAB #12 - Sécurisation du Socket du Daemon Docker
 - 12.1 - Création du Certificat de l'Autorité de Certification
 - 12.2 - Création du Certificat du Serveur Hôte du Daemon Docker
 - 12.3 - Création du Certificat du Client
 - 12.4 - Démarrage du Daemon Docker avec une Invocation Directe
 - 12.5 - Configuration du Client

- **LDF410 - Validation de la Formation .**

- Rappel du Programme de la Formation
 - Évaluation de la Formation
 - Validation des acquis
-

Copyright © 2026 Hugh Norris - Document non-contractuel. Le programme peut être modifié sans préavis.
