

IDENTIFICATION	
Intitulé de l'Unité d'Enseignement : ADMINISTRATION, GESTION ET SECURISATION DES RESEAUX	Niveau d'études : A – B – C - D
Intitulé du cours : Laboratoire : Administration et gestion des réseaux Laboratoire : Sécurisation des réseaux	Nombre de crédits ECTS : 8
Nombre de périodes : 100	Code : N°UE 753247U32D2

DESCRIPTION
Prérequis : UE 933 – BASE DES RESEAUX
Documents de référence pour une préparation préalable au cours : Syllabus BASE DES RESEAUX (publication sur le portail CLAROLINE)
<p>Objectifs : L'unité de formation vise à permettre à l'étudiant:</p> <ul style="list-style-type: none"> ◆ de mettre en œuvre, d'une manière appropriée, un ensemble de compétences, de techniques, de procédures et de méthodes spécifiques pour administrer, gérer et sécuriser un réseau local, câblé ou sans fil, pour : <ul style="list-style-type: none"> o administrer le serveur ; o administrer les périphériques des réseaux tels que routeurs, switches, etc. ; o administrer un poste de travail ; ◆ d'autoriser, de gérer et de sécuriser les accès réseaux aux différents périphériques des réseaux tels que routeurs, serveurs, postes de travail, etc. ; ◆ de développer des compétences de travail en équipe pour des applications plus larges ; ◆ d'acquérir des compétences pour répondre d'une manière appropriée à l'évolution des techniques et des besoins de la clientèle.
<p>Contenu du cours :</p> <p style="text-align: center;">TABLE DES MATIERES</p> <p>Introduction</p> <hr/> <p>CHAPITRE 1 : Domaine ou groupe de travail ? Qu'est-ce qu'un domaine ? Administration et gestion des comptes utilisateurs locaux</p>

CHAPITRE 2 : Systèmes d'exploitation : Installation et paramétrage

Installation, gestion et paramétrage Windows Serveur 2008 & Windows Serveur 2008 R2

- Introduction
- Types d'installation
- Installation complète
- Installation du serveur DHCP
- Installation et configuration d'un serveur DNS
- Active Directory (AD)
 - Organisation de l'AD
 - Unité d'organisation (OU)
 - Principaux objets de l'AD
 - Maître d'opérations FSMO
 - Le maître de schéma
 - Le maître d'attribution des noms de domaine
 - Le maître RID
 - Identification des objets
 - Le maître d'infrastructure
 - Le maître émulateur PDC
 - Le serveur catalogue global
 - Configuration des FSMO
- Mise en œuvre de l'Active Directory
 - Prérequis
 - Installation du contrôleur de domaine

Gestion des comptes utilisateurs Active Directory

- Introduction
- Compte utilisateur
- Création d'un compte utilisateur de domaine
- Propriétés liées aux comptes utilisateurs

Connexion du poste client au domaine

- côté serveur
- côté client

Notion de groupe

- Introduction
- Types de groupe
- Stratégies d'utilisation des groupes
- Tableau récapitulatif
- Création et gestion des groupes

Sécurité et permissions NTFS

- Introduction
- Affectation des permissions NTFS

Partage de fichiers et/ou de répertoires

- Introduction
- Fichiers et dossiers partagés

Stratégies de groupe

- Introduction
- Stratégies de groupe (domaine)
- Outil des gestion des stratégies de groupe (GPMC)

CHAPITRE 3 : Virtualisation

Virtualisation : Le cloisonnement par isolement (« LXC » : Conteneur Linux)

- Introduction
- Installation de LXC sur une machine hôte (Ubuntu 16.04 LTS)
- Création de conteneurs Linux (unités virtuelles)
- Démarrage d'un conteneur
- Visualisation de conteneurs nouvellement créés
- Visualisation des détails complets liés à un conteneur
- Visualisation de l'adresse IP et du statut lié à un conteneur particulier

Arrêt d'un conteneur particulier
Duplication d'un conteneur
Prendre une image d'un conteneur
Restaurer l'image d'un conteneur
Destruction d'un conteneur
Gérer des conteneurs en utilisant la console Web LXC

CHAPITRE 4 : Rôles des machines : Installation, paramétrage et sécurisation

Installation d'un serveur Web (Apache 2.4.3)

Première partie : Serveur Web Apache - Protocole HTTP

- Introduction
- Vérification de paramètres liés au réseau
 - Adressage IP
- Configuration du serveur Web Apache
 - Introduction
 - Configuration du serveur Web
- Redémarrage des services
- Accès au site Web

Deuxième partie : Serveur Web Apache - Protocole HTTPS

- Initialisation du module SSL
 - Introduction
 - SSL - Secure Socket Layer
 - Modifications du fichier de configuration httpd.conf et httpd_ssl.conf
- Génération des certificats
- Script
- Redémarrage du service

Mise en place d'un serveur Proxy Web (Installation d'un serveur mandataire) - SQUID

Première partie : Schéma de principe

- Topologie
 - Contrôle des flux de données et des accès internet
- Plan d'adressage

Deuxième partie : Distribution Slackware 14.1

- Installation
 - Prérequis matériel
 - Partitionnement
 - Packages
 - Linux Loader
 - Composants additionnels
 - Configuration du réseau
 - Activation des services
 - Configuration des polices de caractères
 - Finalisation de l'installation
 - Lancement du système d'exploitation

Troisième partie : SQUID

- Téléchargement et installation des packages
- Approche conceptuelle
- Contrôle des accès à SQUID
- Configuration des SQUID
- Les ACL ou Access Control List
- Contrôle des accès par authentification
- Installation du Proxy SQUID
- Analyses statistiques

Agrégation de liens ou "bonding" sous Linux

Agrégation de liens ou "Port Teaming"

- Introduction
- Avantages de la mise en place d'une solution de "bonding"
- Type de "bonding"

- Liste des modes disponibles
- Prérequis
 - Au niveau du système d'exploitation
 - Au niveau du matériel actif
- Scripting
 - Introduction
 - Variante Slackware
 - Variante Ubuntu

CHAPITRE 5 : Sécurité informatique

Authentification centralisée – Déploiement d'un annuaire LDAP (OpenLDAP)

- Généralités
- Installation de LDAP et des utilitaires
- Configuration de SLAPD
- Installation de l'outil de gestion phpLDAPAdmin (Interface WEB)
- Configuration de phpLDAPAdmin
- Création d'un certificat SSL
- Création d'un fichier d'authentification avec mot de passe
- Sécurisation d'Apache2
- Modification de la configuration Apache phpLDAPAdmin
- Configuration de l'hôte Virtuel http
- Configuration de l'hôte virtuel https
- Connexion à l'interface de gestion web (phpLDAPAdmin)

Les failles liées aux réseaux

- Généralités
- Rappels
- Outils pratiques
 - Informations sur les sockets
- Informations sur une adresse publique ou un nom de domaine
- "Scanner" de ports TCP
- Gestion des sockets
- Transfert de fichiers entre deux machines
- Prise de contrôle d'un ordinateur sur un réseau privé
- SSH

Protection du réseau

- Routage et filtrage
 - Configuration d'une serveur Linux en tant que routeur
 - Activation du routage sur un serveur Linux
 - Consultation de la table de routage
 - Gestion des routes statiques
- Notions d'IPTables
 - Les Tables
 - Les Chaînes
 - Les Actions
 - Le traitement des règles
- Administration d'un parefeu avec IPTables
 - Politiques - Généralités
 - Principes des politiques de parefeu
 - Définition de la politique par défaut des iptables
 - Configuration d'une politique de base
 - Configuration d'une politique restrictive
 - Filtrage de paquets
 - Création de règles
 - Autorisation des "ping" sortants et entrants
 - Gestion des règles
 - Suppression d'une règle
 - Insertion d'une règle
 - Exemple de gestion des règles

- Gestion des flux de retour
 - Autorisation implicite des flux de retour
- Gestion du NAT ("Network Address Translation")
 - Diagnostic de la configuration NAT d'un routeur
 - Affichage de la configuration NAT
 - Configuration du NAT
- Script de configuration des règles de filtrage

Cas pratique

Configuration des cartes réseaux suivant la topologie physique
 Routage du noyau - Activation de l'IP Forwarding
 Règles à mettre en place
 Règles IPTables
 Sauvegarde des règles dans un fichier
 Restauration des règles à partir d'un fichier
 Modification des droits

Bibliographie :

Livres/ouvrages :

MCSE – Réseaux informatiques et réseaux TCP/IP

Auteur : Rob Scrimger & Kelli Adam

Editeur : CampusPress

Date de publication : 25 mars 1999

La théorie des réseaux locaux et étendus

Auteur : Patrick Hautrive

Date de publication : 07/10/2006

Réseaux d'entreprise par la pratique

Auteur : Jean-Luc MONTAGNIER

Editeur : Eyrolles

Date de publication : 18 mars 2004

La sécurité informatique dans la petite entreprise

Auteur : Jean-François CARPENTIER

Editeur : ENI

Date de publication : 13 janvier 2016

Internet :

Slackware : CentOS linux container

<http://www.airaghi.net/en/2015/02/23/slackware-centos-linux-container>

Les systèmes pare-feu(firewall)

<http://tvaira.free.fr/bts-sn/reseaux/cours/cours-reseaux-firewall.pdf>

Microsoft TechNet

<http://social.technet.microsoft.com/wiki/>

PERSONNEL ENSEIGNANT

Mr / Mme **Emmanuel GODISSART**

METHODOLOGIE

Laboratoire :

- Mise en situation pratique permettant aux étudiants de concevoir, gérer, administrer et sécuriser un réseau informatique en se basant sur un cahier spécial des charges.

Utilisation de la plateforme CLAROLINE :

- Notes de cours (diffusion par chapitres)
- Fiches techniques (au besoin)
- Laboratoire

MODES D'EVALUATION

Evaluation de l'étudiant en deux étapes :

- Laboratoire parcourant l'ensemble des acquis d'apprentissage
 - Mise en situation pratique permettant aux étudiants de concevoir, gérer, administrer et sécuriser un réseau informatique en se basant sur un cahier spécial des charges.
 - Remise d'un rapport complet
- Evaluation orale (rapport)