Ministère de la Communauté française

Administration générale de
l'Enseignement et de la Recherche
scientifique.

Direction générale de l'Enseignement
non obligatoire et de la Recherche
scientifique.

Service de l'enseignement
de promotion sociale.

1080 Bruxelles , le 20 Avr 2005
Rue de Lavallée, 1
02 / 690.87.31

Monsieur Jacques LEFERE
Administrateur délégué
CPEONS

rue des Minimes 87-89
1000 BRUXELLES

Ref.: CC / Document de référence définitif

Objet : Document de référence définitif - Régime 1
----- Unité de formation : SECURITE DES RESEAUX PAR SYSTEME D'EXPLOITATION SECURISE
Classement : ENSEIGNEMENT SUPERIEUR TECHNIQUE DE PROMOTION SOCIALE DE TYPE COURT
Code Référence : 298303U31D1
Domaine : 206 Industrie-SU:électricité,ferronnerie,électronique...

Monsieur l'Administrateur délégué,

J'ai l'honneur de vous faire parvenir le document de référence relatif à l'unité de formation mentionnée sous rubrique, approuvé par le Gouvernement de la Communauté française le 11 Avril 2005 .

Veuillez agréer, Monsieur l'Administrateur délégué, l'assurance de ma considération distinguée.

p.O. La Directrice générale a.i.,

Chantal Kaufmann

Denis VAN LERBERGHE
Directeur

Toute demande de renseignements relative à l'objet de la présente peut être obtenue auprès de
Stéphane Abrassart ou Carine Cacheux (02/690.87.11 ou 02/690.87.10)

MINISTERE DE LA COMMUNAUTE FRANCAISE

ADMINISTRATION GENERALE DE L'ENSEIGNEMENT ET DE LA RECHERCHE SCIENTIFIQUE

ENSEIGNEMENT DE PROMOTION SOCIALE DE REGIME 1

DOSSIER PEDAGOGIQUE

UNITE DE FORMATION

SECURITE DES RESEAUX PAR SYSTEME D'EXPLOITATION SECURISE

ENSEIGNEMENT SUPERIEUR TECHNIQUE DE TYPE COURT

CODE : 29 83 03 U31 D1
CODE DU DOMAINE DE FORMATION : 206
DOCUMENT DE REFERENCE INTER-RESEAUX

Approbation du Gouvernement de la Communauté française du 11/04/2005 ,
sur avis conforme de la Commission de concertation

SECURITE DES RESEAUX
PAR SYSTEME D'EXPLOITATION SECURISE

ENSEIGNEMENT SUPERIEUR TECHNIQUE DE TYPE COURT

1. FINALITES DE L'UNITE DE FORMATION

1.1. Finalités générales

Dans le respect de l'article 7 du décret de la Communauté française du 16 avril 1991 organisant l'enseignement de promotion sociale, cette unité doit :

- concourir à l'épanouissement individuel en promouvant une meilleure insertion professionnelle, sociale, culturelle et scolaire ;
- répondre aux besoins et demandes en formation émanant des entreprises, des administrations, de l'enseignement et, d'une manière générale, des milieux socio-économiques et culturels.

1.2. Finalités particulières

L'unité de formation vise à permettre à l'étudiant :

- d'utiliser et de maîtriser les concepts de base de sécurité des réseaux en vue de collaborer efficacement à la maintenance des réseaux informatiques ;
- de maîtriser les concepts d'authentification, d'autorisation et de comptabilisation des accès (AAA) ;
- de découvrir les grands principes des réseaux virtuels privés ;
- de recourir à la théorie des tunnels IPsec et des techniques de cryptage des données pour créer un réseau informatique ;
- de procéder au dépannage d'un réseau virtuel privé de manière analytique ;
- de développer des compétences personnelles d'autoformation dans le domaine de l'informatique et des réseaux privés virtuels ;
- de préparer à une certification en sécurité.

2. CAPACITES PREALABLES REQUISES

2.1. Capacités

En disposant du matériel informatique nécessaire (routeurs, switches, câbles informatiques, ...), de la documentation requise et d'une station informatique opérationnelle connectée à Internet,

- décrire les modèles OSI et TCP-IP :
  - associer la fonction des hub, switch et routeur aux couches du modèle OSI ;

- décrire la structure d'une trame Ethernet ;
- décrire le principe de l'encapsulation des données ;
- citer les caractéristiques de différents médias utilisés sur un réseau local et comparer ces medias ;
- citer et caractériser le matériel qui constitue le réseau (interface réseau, hub, switch, routeur, ...) ;
- décrire la fonction du protocole ARP et utiliser la commande arp ;
- décrire le principe et le fonctionnement du CSMA-CD ;

- décrire l'adressage de réseaux :
  - décrire la structure de l'adressage IP (classes, masques, sous-réseaux) ;
  - décrire et illustrer le VLSM ;

- décrire et configurer un réseau local commuté :
  - citer les caractéristiques de différents médias utilisés sur un réseau local et comparer ces medias ;
  - citer et caractériser le matériel qui constitue le réseau (interface réseau, hub, switch, routeur, ...) ;
  - décrire la fonction du protocole ARP et utiliser la commande arp ;
  - décrire le principe et le fonctionnement du CSMA-CD ;
  - configurer un réseau local sous IP (adresse, masque, passerelle) ;
  - décrire le fonctionnement des switches (commutateurs) ;
  - définir, décrire et configurer des VLANs ;
  - définir, décrire et configurer le routage inter-VLANs ;

- configurer un inter-réseau :
  - interconnecter un minimum de trois réseaux IP à l'aide de routeurs ;

- décrire et configurer le routage :
  - caractériser et configurer des protocoles de routage à vecteur de distance et à états de liens ;

- contrôler le trafic réseau :
  - décrire et configurer des listes de contrôle d'accès basées sur l'adresse IP source, l'adresse IP du destinataire et le service utilisé ;
  - contrôler la diffusion de mises à jour de routage sur une interface (désactivation).

2.2. Titre pouvant en tenir lieu

Attestation de réussite de l'unité de formation « SWITCHING, ROUTAGE et TECHNOLOGIES WANs » CODE N°: 29 83 02 U31 D2 classée dans l'enseignement technique supérieur de type court, **ou** être en possession d'une certification Cisco CCNA.

3. HORAIRE MINIMUM DE L'UNITE DE FORMATION

3.1. Dénomination du cours	Classement	Code U	Nombre de périodes
Laboratoire de maintenance informatique : sécurité des réseaux par système d'exploitation sécurisé	CT	S	64
3.2. Part d'autonomie		P	16
Total des périodes			**80**

4. PROGRAMME

L'étudiant sera capable :

en disposant du matériel informatique nécessaire (routeurs avec IOS adéquats, switches, câbles informatiques, ...), de la documentation requise et d'une station informatique opérationnelle connectée à Internet, par l'intermédiaire de travaux pratiques,

- de maîtriser des savoirs sur la sécurité des réseaux et de leurs composants en développant les notions suivantes :
  - la définition des besoins, des buts, des éléments clés et des enjeux majeurs de la sécurité des réseaux,
  - la définition des différents types de vulnérabilités, de menaces et d'attaques en se basant sur les protocoles définis dans le modèle OSI,
  - la conception et l'implémentation d'un modèle de sécurité basé sur les étapes de sécurisation, de surveillance, de test, d'épreuve et de conception de règles de sécurité bien définies,
  - la définition des différents éléments qui composent les architectures sécurisées des réseaux telles que l'authentification, les pare-feux, les réseaux privés virtuels, les systèmes de détection d'intrusions, la récolte, la gestion et l'audit des messages d'activité, les différents guides de sécurité publiés par les constructeurs,
  - la définition et la distinction des notions d'intégrité des données, de confidentialité des données et d'authentification des données,
  - la définition des principes de cryptage des données encapsulées, du cryptage des en-têtes de données et du cryptage de mots de passe,
  - l'identification des différents algorithmes de cryptage en les classant par leur force et leur niveau d'utilisation dans les protocoles de sécurité,
  - l'identification des solutions commerciales et libres de sécurité des réseaux parmi les domaines de l'authentification, des pare-feux, des réseaux privés virtuels, des systèmes de détection d'intrusion, de récolte, de gestion et d'audit des messages d'activité ;
- de maîtriser la sécurité de base des routeurs et des switches en développant les notions suivantes :
  - le contrôle et l'administration des différents accès aux machines sécurisées par la définition de comptes, de privilèges, de mots de passe et de messages d'accueils,
  - la désactivation de tout service réseau qui n'est pas nécessaire notamment les protocoles de routage, ARP, ICMP, NTP, SNMP, DNS, Telnet et les protocoles de partage de fichiers et d'imprimantes,
  - la sécurisation du périmètre des machines par le contrôle du trafic entrant et sortant, la translation d'adresses (NAT), le filtrage des mises à jour de routage, le filtrage des messages ICMP et par l'utilisation de solutions pare-feux,

- l'administration et la collecte des événements enregistrés,
- la mise à jour des systèmes d'exploitation,
- la configuration des machines de manière sécurisée notamment via le protocole d'accès à distance sécurisé SSH (Secure Shell),
- la sécurisation de l'accès aux réseaux commutés locaux en étudiant les attaques de couche 2 du modèle OSI et en implémentant les protocoles de sécurité propres aux commutateurs ;

- d'élaborer les listes d'accès (ACL) et les listes d'accès basées sur des contextes (CBAC) en développant les notions suivantes :
  - l'optimisation, la création, l'application, l'édition et le diagnostic des listes d'accès et des règles d'inspection du trafic,
  - la définition et la conception des différents types de solutions de filtrage du trafic basées sur les protocoles IP, TCP/UDP et les protocoles applicatifs,
  - l'identification et l'autorisation du trafic exclusivement sollicité,
  - la conception et l'implémentation des modèles de pare-feux ;

- de maîtriser et d'utiliser les concepts d'« Authorization », « Authentication » et « Accounting » (AAA) pour sécuriser les accès réseau en développant les notions suivantes :
  - la définition de la sécurité des réseaux par la mise en œuvre des concepts d'authentification, d'autorisation et de comptabilisation des accès,
  - l'introduction dans la conception d'architecture des réseaux des trois principes d'authentification, d'autorisation et de comptabilisation des accès,
  - la définition et la mise en œuvre du principe de l'authentification à travers la correspondance simple d'un nom d'utilisateur et d'un mot de passe clair ou crypté,
  - la définition et la mise en œuvre du principe de l'authentification par clés d'encryption partagées, publiques et privées,
  - la définition et la mise en œuvre du principe de l'authentification par la distribution de clés d'authentification par des serveurs logiciels ou matériels et l'émission de requêtes par des clients matériels ou logiciels,
  - la définition et la mise en œuvre des services d'authentification de type TACACS+, RADIUS et KERBEROS,
  - la définition et la mise en œuvre des services d'authentification à travers un service proxy WEB et par le protocole HTTPS ;

- de préciser et d'utiliser les concepts de détection d'intrusion (IDS), de surveillance et de gestion des routeurs en développant les notions suivantes :
  - la définition des signatures d'attaque et de tentatives d'intrusions,
  - la définition et la mise en œuvre des réponses à donner aux attaques et aux tentatives d'intrusions,
  - la conception, la mise en œuvre et la vérification d'un système de détection d'intrusions,
  - la consultation des messages d'activités d'un système de détection d'intrusions,
  - la définition du niveau de sévérité des messages d'activités d'un système de détection d'intrusions,
  - la conception, la mise en œuvre et la vérification d'un service des messages d'activités d'un système de détection d'intrusion via un service SYSLOG,

- la conception, la mise en œuvre et la vérification d'un service de gestion et d'administration réseau sécurisé tel que SNMP version 3 ;

- de maîtriser et d'utiliser les réseaux privés virtuels entre sites à l'aide de routeurs en développant les notions suivantes :
  - la définition, la conception, la mise en œuvre et le diagnostic des modèles d'architecture des réseaux privés virtuels, notamment les modèles site à site,
  - l'identification, le classement et la définition des protocoles de conception de tunnels de réseaux privés virtuels en les plaçant dans le modèle OSI,
  - la définition et l'implémentation du protocole IKE (Internet Key Exchange) dans le processus préalable à l'échange des données sur un tunnel IPSec,
  - la définition d'une méthode de distribution de clés de manière manuelle ou via un serveur d'authentification,
  - la définition d'une méthode d'authentification soit par des clés déjà partagées, soit par des signatures RSA utilisées par un certificat digital,
  - la définition correcte des éléments du réseau privé virtuel et l'application les règles appropriées de routage, notamment sur des routeurs NAT,
  - la définition des règles de négociation du réseau privé virtuel par un algorithme de cryptage des messages (DES ou 3DES),
  - la définition de l'algorithme vérifiant l'intégrité des messages (SHA-1 ou MD5),
  - la définition de la méthode d'authentification dans un contexte d'échange non sécurisé,
  - la définition du temps de vie d'une authentification d'hôtes dans un réseau privé virtuel,
  - l'identification, la définition et l'implémentation des protocoles nécessaires en fonction du type de trafic tels que ESP (Encaspulating Security Payload) et AH (Authentication Header),
  - l'installation et la configuration d'un logiciel client de réseau privé virtuel ;

- de configurer un accès client distant sécurisé (utilisateurs mobiles ou télétravailleurs) en appliquant les notions suivantes :
  - la définition, la conception, la mise en œuvre et le diagnostic des modèles d'architecture des réseaux privés virtuels, notamment les modèles client-serveur,
  - l'identification, le classement et la définition des protocoles de conception de tunnels pour les accès distants dans les réseaux privés virtuels,
  - l'utilisation et la mise en œuvre d'un client VPN distant et la mise en œuvre du serveur VPN,
  - la description et l'analyse des différentes phases de fonctionnement d'un client VPN,
  - la mise en œuvre et le fonctionnement d'un système central de gestion d'un réseau VPN,
  - l'intégration du système de gestion des VPN dans un gestionnaire général de réseau.

5. CAPACITES TERMINALES

Pour atteindre le seuil de réussite, l'étudiant sera capable :

en disposant du matériel informatique nécessaire (routeurs, switches, câbles informatiques, ...), de la documentation requise et d'une station informatique opérationnelle connectée à Internet,

- de démontrer la compréhension des concepts et notions développés dans le cadre de cette unité de formation en répondant à un questionnaire ;
- de résoudre via un laboratoire, une étude de cas concrétisant au minimum les notions théoriques suivantes :
  - la conception et la réalisation d'un VPN,
  - une procédure d'identification et de cryptage,
  - l'implémentation d'une procédure de défense,
- de remédier à un dysfonctionnement provoqué.

Pour la détermination du degré de maîtrise, il sera tenu compte des critères suivants :

- l'exhaustivité des informations dans l'étude de cas,
- la méthodologie mise en œuvre pour répondre à un dysfonctionnement provoqué,
- la pertinence de l'interprétation des différentes démarches et des résultats,
- les degrés d'autonomie et d'autoformation atteints,
- l'utilisation judicieuse du vocabulaire informatique.

6. CHARGE DE COURS

Le chargé de cours sera un enseignant ou un expert.

L'expert justifiera de compétences particulières issues d'une expérience professionnelle actualisée en relation avec le programme du cours concerné.

7. CONSTITUTION DES GROUPES OU REGROUPEMENT

Il est recommandé de ne pas dépasser plus d'un étudiant par poste de travail.