MINISTERE DE LA COMMUNAUTE FRANCAISE

ADMINISTRATION GENERALE DE L'ENSEIGNEMENT

ENSEIGNEMENT DE PROMOTION SOCIALE

DOSSIER PEDAGOGIQUE

UNITE D'ENSEIGNEMENT

FORMATION CONTINUE : NETWORK SECURITY

ENSEIGNEMENT SUPERIEUR DE TYPE COURT
DOMAINE : SCIENCES

CODE : 7532 13 U32 D1

CODE DU DOMAINE DE FORMATION : 710
DOCUMENT DE REFERENCE INTER-RESEAUX

Approbation du Gouvernement de la Communauté française du
sur avis conforme du Conseil général

FORMATION CONTINUE : NETWORK SECURITY

ENSEIGNEMENT SUPERIEUR DE TYPE COURT

1. FINALITÉS DE L'UNITÉ D'ENSEIGNEMENT

1.1. Finalités générales

Dans le respect de l'article 7 du décret du 16 avril 1991 organisant l'enseignement de promotion sociale de la Communauté française, cette unité de formation 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 d'enseignement vise à permettre à l'étudiant :

- ♦ de mettre en œuvre concepts associés à la « gestion du risque », les problèmes de vulnérabilités et de menaces courantes des réseaux ;
- ♦ de configurer un réseau sur base d'une situation donnée, de réaliser les terminaisons des différents types de câblages et connecteurs ;
- ♦ de résoudre les problèmes courants de sécurité associés aux technologies et configurations réseaux.

2. CAPACITES PREALABLES REQUISES

2.1. Capacités

Pour l'introduction à la sécurité des systèmes d'information :

En respectant les consignes liées à l'évaluation,
dans le respect du temps imparti,
sous la forme demandée et dans un local défini :

- ♦ d'expliquer différents concepts liés à la sécurisation des systèmes d'information et de communication ;
- ♦ d'identifier des outils et des technologies de sécurisation des systèmes d'information et de communication appropriés dans un scénario ou un contexte ;

2.2. Titre pouvant en tenir lieu

Attestation de réussite de l'unité d'enseignement « Formation continue : Introduction à la sécurité des systèmes d'information », code N° 7532 10 U32 D1, classée dans l'enseignement supérieur de type court.

3. ACQUIS D'APPRENTISSAGE

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

en disposant du matériel informatique nécessaire (routeur, switches, câbles informatiques, ordinateur serveur et ordinateurs clients éventuellement virtualisés, ...), de l'outillage adéquat, de la documentation requise et d'un réseau,
en suivant les consignes,
de manière individuelle ou dans un travail d'équipe ;
sur base d'un scénario donné par le chargé de cours et reprenant les technologie, le matériel, les contraintes,…. explicités dans un cahier de charges,

- de configurer l'adressage, switch, pare-feu et autres matériels utiles ;
- d'assurer le monitoring, d'analyser et de résoudre les problèmes courants de sécurité associés aux technologies réseaux ;
- de mettre en place la gestion du changement et en établir un rapport (sources documentaires) ;

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

- le degré de pertinence des solutions retenues,
- du respect du temps alloué,
- du degré de cohérence de sa justification,
- du degré de clarté et de précision du vocabulaire technique.

4. PROGRAMME

L'étudiant sera capable :

4.1. Technique informatique et sécurité :

- Expliquer les fonctions et usages de différents dispositifs réseaux ;
- Comparer les usages de services et d'applications réseaux ;
- Expliquer les caractéristiques et les différences de technologies WAN diverses ;

- Comparer les différentes topologies réseaux et les modèles logiques de connectivité, (à titre d'exemple : Mesh, Bus, Ring, P2P, Client-Server, ...) ;
- Comparer les formes d'implémentations d'infrastructure. (à titre d'exemple : WAN, MAN, LAN, WLAN, ...) ;
- Expliquer les concepts et protocoles essentiels de routages ;
- Identifier les éléments essentiels des technologies unifiées de communication (à titre d'exemple : VoIP, QoS, ...) ;
- Comparer les technologies cloud et la virtualisation ;
- Expliquer et comparer les outils et techniques de monitoring
- Sur base d'un scénario, utiliser des technologies et outils adéquats de support à la gestion des configurations (à titre d'exemple : Archivage, Backups, Baselines, Documentation, etc.) ;
- Expliquer l'importance de la mise en place de segmentation des réseaux ;
- Expliquer les mécanismes, processus et différents types de mises à jour et correctifs logiciels ;
- Comparer les différents concepts associés à la « gestion du risque » ;
- Comparer les vulnérabilités et les menaces courantes des réseaux ;
- Identifier et décrire les terminaisons des différents types de câblages et connecteurs ;
- Enoncer et expliquer les rôles, caractéristiques et paramètres principaux des services et applications réseaux courants (à titre d'exemple : DHCP, DNS, Proxy, Reverse Proxy, NAT, Port Forwarding) ;
- Comparer les contrôles de sécurité physique ;
- Expliquer les objectifs et rôles des différents modèles de contrôle d'accès aux réseaux ;
- Expliquer et résumer les concepts fondamentaux de forensiques ;
- Sur base d'un scénario, expliquer et mettre en place une méthodologie de résolution de problèmes réseaux ;
- Sur base d'un scénario, analyser et interpréter les résultats produits par les outils de résolutions de problèmes ;
- Sur base d'un scénario, analyser et résoudre les problèmes courants associés aux technologies :
    - sans fil,
    - de câbles cuivrés,
    - de fibre optique,
    - WAN ;
- Sur base d'un scénario, analyser et résoudre les problèmes réseaux courants ;
- Sur base d'un scénario, analyser et résoudre les problèmes courants de sécurité associés aux technologies réseaux ;
- Analyser un scénario et déterminer la couche du modèle OSI correspondante ;
- Expliquer les concepts fondamentaux de la théorie des réseaux ;

- Sur base d'un scénario, mettre en place les standards réseaux sans fil appropriés (wpa2, portail captif, …) ;
- Sur base d'un scénario, mettre en place les standards réseaux câblés appropriés ;
- Sur base d'un scénario, mettre en place les « policies » et procédures appropriées dans la gestion des réseaux ;
- Résumer les pratiques essentielles de sécurité (safety) des personnes dans un environnement (Système anti-incendie, HVAC, Sécurité du réseau électrique, etc.) ;
- Expliquer les fondamentaux des procédures de gestion du changement (maintenance documentaire) ;
- Comparer les ports et protocoles réseaux courants (http, https, netbios, pop, imap, smtp, sip, tcp, udp, ...) ;

4.2. Laboratoire informatique et sécurité :

en disposant du matériel informatique nécessaire (routeur, switches, câbles informatiques, ordinateur serveur et ordinateurs clients éventuellement virtualisés, ...), de l'outillage adéquat, de la documentation requise et d'un réseau,

- Mettre en place et configurer les services et applications réseaux courants (à titre d'exemple : DHCP, DNS, Proxy, Reverse Proxy, NAT, Port Forwarding) ;
- Mettre en place et établir correctement les terminaisons des différents types de câblages et connecteurs avec les outils appropriés ;
- Sur base d'un scénario donné, mettre en place et configurer les schémas d'adressage adéquats ;
- Sur base d'un ensemble de contraintes et d'exigences, mettre en place un réseau élémentaire ;
- Sur base d'un scénario, utiliser les outils de monitoring appropriés pour faire fonctionner le réseau ou maintenir une qualité de réseau ;
- Sur base d'un scénario, analyser les mesures et les rapports d'outils de monitoring et de mesure de performance ;
- Sur base d'un scénario, configurer un switch et ses fonctionnalités appropriées ;
- Installer et configurer les infrastructures LAN sans fil et implémenter les technologies appropriées associées aux dispositifs sans fil ;
- Sur base d'un scénario, mettre en place les techniques de hardening réseau ;
- Sur base d'un scénario, mettre en place et configurer un pare-feu fondamental ;
- Sur base d'un scénario, analyser et résoudre les problèmes courants associés à une des technologies :
    - sans fil,
    - de câbles cuivrés,
    - de fibre optique,
    - WAN ;

- Sur base d'un scénario, mettre en place et configurer les équipements aux bons endroits en utilisant les "best practices" (gestion du câblage, gestion du refroidissement et air flow, étiquettage, ...) ;
- Sur base d'un scénario, configurer et appliquer les ports et protocoles appropriés. (à titre d'exemple : ftp, snmp, ssh, telnet, dns, dhcp, tftp, smb, rdp).

5. CHARGE(S) DE COURS

Un enseignant ou un expert.

L'expert devra justifier de compétences issues d'une expérience professionnelle actualisée dans le domaine en relation avec le programme du présent dossier pédagogique.

6. CONSTITUTION DES GROUPES OU REGROUPEMENT

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

7. HORAIRE MINIMUM DE L'UNITE D'ENSEIGNEMENT

7.1. Dénomination du cours	**Classement**	**Code U**	**Nombre de périodes**
Technique informatique et sécurité	CT	B	48
Laboratoire informatique et sécurité	CT	S	48
7.2. Part d'autonomie		P	24
Total des périodes			120
Nombre d'ECTS			8