MINISTERE DE LA COMMUNAUTE FRANCAISE

ADMINISTRATION GENERALE DE L'ENSEIGNEMENT

ENSEIGNEMENT DE PROMOTION SOCIALE

DOSSIER PEDAGOGIQUE

UNITE D'ENSEIGNEMENT

FORMATION CONTINUE : HOST SECURITY

ENSEIGNEMENT SUPERIEUR DE TYPE COURT
DOMAINE : SCIENCES

CODE : 7532 11 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 : HOST 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 sécuriser des ordinateurs et leur système d'exploitation.

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 la documentation requise et d'un réseau,
face à un système informatique installé ou à installer, des consignes précises lui étant communiquées,
à partir de cas concrets,
dans les deux environnements du programme,

- De mettre en pratique et vérifier les principes, outils et technologies de sécurisation des hôtes (clients, serveurs, …) ;
- D'expliquer et de justifier les choix et solutions proposées.

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 utilisé.

4. PROGRAMME

L'étudiant sera capable :

en disposant du matériel informatique nécessaire (routeur, switches, câbles informatiques, ordinateur serveur et ordinateurs clients éventuellement virtualisés, ...), de la documentation requise et d'un réseau,
les deux environnements Microsoft/Windows et Linux/Unix ci-dessous sont incontournables, mais les compétences de host security peuvent être interprétées dans le contexte dans un ou plusieurs environnements additionnels.

Expliquer, mettre en pratique et vérifier :

- les principes centraux de la sécurité (à titre d'exemple : CIA, Risk, Threat modeling, …) ;
- Expliquer et mettre en pratique les principes de sécurité physiques (à titre d'exemple : sécurité du site, dispositifs détachables, contrôles d'accès, dispositifs mobiles, …) ;

- Expliquer et mettre en pratique les principes de sécurité du web (à titre d'exemple : paramètre de sécurité du navigateur, site web sécurisé, ...) ;
- Expliquer et mettre en pratique les principes de sécurité des systèmes sans fil ;
- Expliquer et mettre en pratique les principes d'authentification des utilisateurs ;
- Expliquer et mettre en pratique les principes de permissions ;
- Expliquer et mettre en pratique les policies de gestion des mots de passe ;
- Expliquer et mettre en pratique les policies d'audit ;
- Expliquer et mettre en pratique les mécanismes de chiffrement (à titre d'exemple : EFS, bitlocker, TPM, ...) ;
- Expliquer les malwares et vulnérabilités correspondantes (à titre d'exemple : Buffer overflow; viruses, polymorphic viruses; worms; Trojan horses; spyware; ransomware; adware; rootkits; backdoors; zero day attacks) ;
- Expliquer et mettre en pratique les modèles Access Control (à titre d'exemple : DAC, MAC, RBAC et ABAC …) ;
- Expliquer et mettre en pratique les principes de pare-feu ;
- Expliquer et mettre en pratique les principes d'isolation des réseaux ;
- Expliquer et mettre en pratique les principes des protocoles de sécurité (à titre d'exemple : Protocol spoofing ; IPsec ; tunneling ; DNSsec ; network sniffing ; denial-of-service (DoS) attacks) ;
- Expliquer et mettre en pratique les mécanismes de protection des clients ;
- Expliquer et mettre en pratique les mécanismes de protection des emails ;
- Expliquer et mettre en pratique les mécanismes de protection des serveurs (à titre d'exemple : séparation des services, renforcement, contrôle des mises à jour, secure DNS, etc.) ;
- Expliquer et mettre en pratique les infrastructures à base de certificats et de clef publique (à titre d'exemple : X.509, pki, autorité, revocation, pem, openssl, libressl, pkcs, TLS, HTTPD mod_ssl, MITM, ...) ;
- Expliquer et mettre en pratique les systèmes de fichiers chiffrés (à titre d'exemple : LUKS, dm-crypt, ecryptfs, pam, ...) ;
- Expliquer et mettre en pratique les systèmes de résolution de nom et leurs composantes de sécurité (à titre d'exemple : DNSSEC, DANE, BIND, TSIG, ...) ;
- Expliquer et mettre en pratique les mécanismes de renforcement de sécurité des hôtes (à titre d'exemple : BIOS, GRUB, sysctl, exec-shield, ASLR, ...) ;
- Expliquer et mettre en pratique les mécanismes de détection d'intrusion basé sur l'hôte ;
- Expliquer et mettre en pratique les mécanismes de gestion des utilisateurs et de l'authentification ;
- Expliquer et mettre en pratique les modèles Access Control (à titre d'exemple : DAC, MAC, RBAC et ABAC …) ;
- Expliquer et mettre en pratique les systèmes de fichiers réseaux et leur sécurité ;
- Expliquer et mettre en pratique le renforcement sécuritaire des réseaux ;
- Expliquer et mettre en pratique les mécanismes de détections d'intrusions de réseaux ;

- Expliquer et mettre en pratique les mécanismes de filtrage des paquets ;
- Expliquer et mettre en pratique les mécanismes de réseaux privés virtuels ;

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**
Laboratoire informatique et sécurité	CT	S	80
7.2. Part d'autonomie		P	20
Total des périodes			**100**
Nombre d'ECTS			**6**