SEC001 - Sécurisation d'un parc informatique d'une PME

Mis à jour le 17-02-2022

Code : SEC001

Unité d'enseignement de type cours

6 crédits

Volume horaire de référence (+/- 10%) : **50 heures**

Responsabilité nationale :
EPN05 - Informatique / Véronique LEGRAND

Contact national :

EPN05 - Informatique
2 rue Conté
accès 33.1.13B
75003 Paris
01 40 27 28 21
Mmadi Hamida
hamida.mmadi@lecnam.net

Présentation

Prérequis

Avoir suivi et validé les UE NFA086 (ex-NFA070), NFA071, NFA077 (ex-NFA072), NFA088 (ex-NFA073) , NFA085 (ex-NFA074) et NFA087 (ex-NFA076 puis NFA078), ou pouvoir justifier de l'acquisition des compétences correspondantes au travers de son expérience professionnelle.

Objectifs pédagogiques

monter en compétence par rapport à une évolution du métier des techniciens de maintenance réseaux ou des postes de travail vers les bases de la remédiation et des bonnes pratiques de la cybersécurité

Compétences

Connaitre le modèle menace, mesure, vulnérabilité, attaque, cible et contremesures.

Connaitre les menaces sur le poste de travail et les réseaux.

Connaitre les vulnérabilités : déni de service, intrusion, injection de code ....

Connaitre les opérations de durcissement sur le poste de travail.

Sécuriser des postes de travail par l'installation d'antivirus, de pare feu ...

Connaitre les menaces et vulnérabilités ouvertes avec la mise en réseau.

Connaitre les bonnes pratiques du poste de travail : usurpation mac address et modification.

Configurer des serveurs DN interne plutôt qu'externes.

Configurer un client HTTPS.Sauvegarder des données et les restaurer : politique, support de sauvegardes, architectures.

Connaitre les menaces et vulnérabilités ouvertes sur internet.

Connaitre les bonnes pratiques sur les périphériques : disques durs effacés d'imprimante.

Configurer une adresse publique IP, protocole via IPSec-installation poste de travail : VPN II/III/V

Programme

Contenu

I/ INTRODUCTION

LES BASES DE LA CYBERSECURITE

Objectif général : comprendre les enjeux de sécurité informatique lors des phases d'installation et de

maintenance pour le poste de travail local et en réseau :

- décrire le modèle menace, mesure, vulnérabilité, attaque, cible et contre-mesures ;

- montrer les vulnérabilités en général : déni de service, intrusion, injection de code ....

- décrire et montrer une ou deux menaces /vulnérabilités/ exploits/attaques ;

- comprendre la notion de politiques de sécurité et de bonnes pratiques :

• montrer l'organisation de la PSSI et énumérer les principales bonnes pratiques,

• manipuler quelques bonnes pratiques dans l'entreprise : consulter, décrire, diffuser,

• mettre en place une bonne pratique dans l'entreprise : exemple : « Mot de passe ».

II/ SECURITE DU POSTE DE TRAVAIL

1 – LES MENACES ET VULNERABILITES DU POSTE DE TRAVAIL

- Montrer les vulnérabilités sur le poste de travail : déni de service, intrusion, injection de code ....

- Montrer le panorama des vulnérabilités les plus courantes du poste de travail ;

- Poste de travail et les Virus / Hoax …

2 – LES MESURES DE SECURITE SUR LE POSTE DE TRAVAIL

Montrer le durcissement d'un poste de travail : quelques bonnes pratiques

- Operating System : Windows et Linux ;

- Registre ;

- Droits ;

- Mots de passe : BIOS, Machine locale, Mode commande : SUDO, …

- Applications.

III/ SECURITE DE LA MISE EN RESEAU

1 – LES MENACES ET VULNERABILITES OUVERTES DU FAIT DE LA MISE EN RESEAU

- Montrer le panorama des vulnérabilités les plus courantes lors de la mise en réseau : clé WIFI ...

- Aborder un cas pratique : usurpation « mac address » par le biais de sa modification lors de la

configuration de la carte réseau...

Premières mesures : le durcissement du poste local.

2 – LES MESURES DE SECURITE DU FAIT DE LA MISE EN RESEAU

Premières mesures : le durcissement du poste local :

- activation/désactivation de l'antivirus, règles de firewall local …

- stratégies de mots de passe ;

- la base de registre sous Windows sous Windows XP et Windows 7 ;

- les Clés CLSID, les SID ;

- les clés à surveiller.

Autres mesures :

- les bonnes pratiques Windows et Linux en réseau ;

- montrer le principe de la sécurisation des réseaux ;

- configurer la sécurité du poste de travail en réseau :

• Fonctionnement des permissions NTFS,

• Différences entre autorisations de partages et permissions NTFS,

• Mise en place des stratégies de groupes vis à vis de la sécurité,

• Protéger le fichier de mot de passe : montrer la localisation des droits NTFS et de fichier

password,

- Configurer des serveurs DNS internes versus externes ;

- Protéger les scripts de login de serveurs Windows ;

- bonnes pratiques sur les périphériques :

• disque durs d'imprimantes effacés,

• clé USB …

IV/ SECURITE OPERATIONNELLE

1 – INTRODUCTION AU MAINTIEN OPERATIONNEL DES CONDITIONS DE SECURITE

- phases de la sécurité opérationnelle ;

- qu'est-ce qu'un SOC ;

- description des conditions de sécurité ;

- les outils de supervision de la sécurité ;

2 – INCIDENT DE SÉCURITÉ

- Equipements, consoles d'administration de la sécurité, notion de SIEM ;

- Règles de corrélation pour configurer les équipements de détection : login ;

- Failed et intrusion ;

- Configuration d'un firewall : règles ;

- Configuration d'un IDS : règles.

V/ SECURITE ET INTERNET

1 – LES MENACES ET VULNERABILITES OUVERTES SUR INTERNET

- Décrire les menaces et vulnérabilités du fait de l'interconnexion du SI avec internet.

2 – LES MESURES DE SECURITE SUR L'UTILISATION ET L'INSTALLATION DES OUTILS INTERNET

- Bonnes pratiques sur les périphériques : disque durs effacés d'imprimante ;

- Configurer une adresse publique IP, protocole via IPSec-installation poste de travail : VPN II/III/V ;

- Notion de politique de sécurité de base : le firewall et les règle ;

- Décrire les premières mesures de l'accès du poste de travail à Internet :

• montrer le principe des architectures informatiques sécurisées,

• montrer le politique de sécurité de base :

O Expliquer la notion de flux et de zone de coupure

O Configurer le firewall et les règles

• configurer la sécurité du poste de travail Windows et Linux sur Internet :

O Configurer une adresse publique IP,

O Configurer protocole via IPSec

O Configurer le poste de travail : VPN II/III/V

O Client VPN

O Proxy sur le poste client

• configurer la sécurité des postes de travail Windows et Linux sur Internet :

O Antivirus

O Signature électronique et certificat sur le poste de travail

- Décrire les architectures sécurisées de sites web et leurs configurations :

• montrer le principe de la sécurité des serveurs d'accès à Internet :

O Proxy web

O Reverse proxy

O Portail captif

O Filtrage mail

VI/ SECURITE D'UN SITE WEB

1 – LES MENACES ET VULNERABILITES LIEES AU DEVELOPPEMENT WEB

Décrire les menaces et vulnérabilités sur les applications des serveurs WEB :

- mode de codage ;

- balises.

2 – LES MESURES DE SECURITE D'UN SITE WEB

- Bonnes pratiques du codage HTML/CSS : exemple : convention de nommage des classes CSS ;

- Redirections externes versus statiques (PHP, GET...) ;

- Obfuscation ;

- Bonnes pratiques de la configuration d'un serveur WEB ;

- Recommandations ANSSI pour la sécurisation des sites WEB.