BTS Services informatiques aux organisations

Session 2013

E4 – Conception et maintenance de solutions informatiques
Coefficient 4

DESCRIPTION D'UNE SITUATION PROFESSIONNELLE

Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐

PARCOURS SISR ☒ **PARCOURS SLAM** ☐

NOM et prénom du candidat : ROYER Christopher **N° candidat :**

Contexte de la situation professionnelle N°2 :

Hôpital Pédiatrique de Nice (Lenval)

La Fondation Lenval est un hôpital pédiatrique privé à but non lucratif. Elle est spécialisée dans les soins destinés aux enfants et aux adolescents. Comme suite à la fusion de la pédiatrie du CHU en 2010, une entité a été créée en **G**roupement de **C**oordination **S**anitaire (GCS) sous le nom d'Hôpitaux pédiatriques de Nice CHU-LENVAL.

Intitulé de la situation professionnelle

Mise en œuvre d'une détection d'intrusion avec SNORT.

Période de réalisation : Avril 2013 **Lieu :** Hôpital Lenval (Nice)

Modalité : ☒ Individuelle ☐ En équipe

Principale(s) activité(s) concernée(s)

A1.1.1 Analyse du cahier des charges d'un service à produire
La mise en place de notre service émane d'un besoin spécifique. Comment surveiller les échanges de la connexion internet de l'hôpital.

A1.1.2 Étude de l'impact de l'intégration d'un service sur le système informatique
En ajoutant ce nouveau service, nous avons étudié son utilité et vérifié qu'il peut être intégré dans notre infrastructure réseau. Et sans ouvrir une faille de sécurité.

A1.2.3 Évaluation des risques liés à l'utilisation d'un service
En mettant en place cette nouvelle solution, nous nous sommes assurés qu'il n'ouvrira pas de brèches de sécurités. Un moyen a été trouvé pour sécuriser notre nouveau service.

A1.2.4 Détermination des tests nécessaires à la validation d'un service
Afin d'être certains que notre solution fonctionne nous effectuerons des tests en interne, en utilisant divers logiciels que pourrait être utilisé par une personne mal intentionnée.

A3.1.3 Prise en compte du niveau de sécurité nécessaire à une infrastructure
Cette nouvelle solution a été mise en place pour augmenter la sécurité entre le réseau de l'hôpital Lenval et la connexion internet. Elle va servir à se prémunir contre les attaques extérieures.

A3.2.1 Installation et configuration d'éléments d'infrastructure
L'ensemble des trames réseaux sont envoyées sur le poste qui fera office de superviseur de la connexion internet.

A4.1.3 Conception ou adaptation d'une base de données
Elle sera mise en place en suivant les recommandations de la documentation et nous servira à sauvegarder nos traces de l'activité néfaste.

A5.2.4 Étude d'une technologie, d'un composant, d'un outil ou d'une méthode
Pour comprendre le mode de fonctionnement du logiciel, de la documentation a été nécessaire entre les sources officiels de l'éditeur et celles qui se trouvent sur internet.

Conditions de réalisation (ressources fournies, résultats attendus)

Ressources : Documentation officiels SNORT et documentations issues d'internet.

Résultats attendus : Le nouveau service doit permettre de détecter les signes d'intrusions présents sur la ligne internet de l'hôpital et de pouvoir garder une trace des éventuelles attaques.

Productions associées

- Installation LibpCap, LibdNet et DAQ
- Installation MySQL
- Installation Apache et module PHP
- Installation Base
- Installation OinkMaster

Modalités d'accès aux productions :

Le dossier est disponible via les adresses :
http://minu.me/8s2x ou **http://sdrv.ms/11Ht4ge** (*Aucune authentification n'est nécessaire*)
Le projet est disponible dans le dossier « **Situation 2 - Détection d'intrusion** » puis « **Détection d'intrusion avec SNORT.pdf** »
Sont également présents via le lien : les documentations, les fichiers de configurations.

Description :

La situation initiale :

L'hôpital Lenval dispose d'une connexion internet en fibre optique de 8Mega pour son propre réseau et celui de Santa-Maria. De plus, le serveur d'E-mail (Exchange) utilise cette connexion pour envoyer les courriers depuis internet.

Le besoin :

Afin de garantir la sécurité de cette connexion à internet et pour garder une trace du trafic néfaste, un système de détection d'intrusion va être mis en place. Le but est de pouvoir surveiller toutes les données qui circulent entre le routeur du FAI et le Pare-Feu de l'hôpital.

Matériels & logiciels utilisés :

Pour mettre en place notre IDS nous avons utilisé un poste reconditionné de marque Fujitsu Siemens (Processeur doubleur cœur et 2GO de mémoire vive, disque dur de 160 GO). Le système d'exploitation choisi sera du Linux avec une interface graphique permettant de voir les résultats directement sur la machine.

Le logiciel utilisé qui va permettre de récupérer nos activités sera **SNORT**, il comprendra l'installation d'une base de données pour recueillir nos attaques recensées. Une interface graphique sera installée pour mieux voir les activités.

De ce fait, cette installation ne reposera que sur des logiciels libres.