SAE5.Cyber03 : Etude et installation d'un système IDS/IPS pour un centre hospitalier

Un hôpital souhaite munir son réseau informatique d'un système de détection et prévention d'intrusion pour se prémunir des risques internes et des attaques externes. Le réseau informatique de l'hôpital est composé de trois types de terminaux :

- Des stations de travail utilisables par le personnelle hospitalier par un service d'authentification centralisé.
- Un réseau opérationnel composé de terminaux de contrôle des équipements hospitaliers : assistance respiratoire, …
- Des serveurs de BDD (données médicales), d'authentification, de messagerie et web.

Par manque de moyens, l'hôpital penche pour une solution IDS/IPS logicielle. Vous êtes chargé d'étudier, installer et tester une solution IDS/IPS performante et gratuite.

Etape 1 : étude

- Etudier les solutions IDS/IPS du marché et en extraire une liste de 4 solutions dont absolument « Security Onion »
- Etablir une étude comparative des solutions retenues.
- Sélectionner une solution et établir une présentation devant les décideurs pour la défendre

Durée : deux journées,

Livrable : document d'étude (3 pages max) + présentation de 5 minutes l'après-midi du 2ème jour

Etape 2 : déploiement

- Etablir l'architecture réseau de la solution (infrastructure réseaux et serveurs) nécessaire à son implémentation en décrivant la position du IDS/IPS (passive IDS avec port mirror, out-of-band IPS, inline IPS, etc.). Une gestion du cloisonnement des différentes parties du réseau doit être proposés (règles de pare-feu).
- Installer et configurer l'infrastructure matérielle et les outils logiciels (notamment la solution IDS) choisis
- Définir un plan de test du fonctionnement
- Etablir un rapport de test des services

Durée deux jours

Livrable : schéma de l'architecture choisi (une figure), rapport de test (2 pages max) à la fin du 4ème jour (avant 17h00).

Etape 3 : supervision

- Etablir un document succinct relatant les métriques de qualité à surveiller et le type d'attaques à surveiller
- Etablir un document succinct relatant les mécanismes de sécurité à implémenter

Durée : 1 jour et demi

Livrable : document des métriques surveillés à fournir l'après-midi de journée du lundi de la semaine 2.

Etape 4 : démonstration

L'objectif de cette étape est de préparer une démonstration à réaliser devant les décideurs sur les capacités du système mis en place pour la détection d'attaques

- Préparer deux scénarios d'attaque sur le système informatique de l'hôpital (SQL injection, Fast DNS Fluxing ou autre) incluant la description de la Blue Team et de la Red Team.

- Par une démonstration, montrez comment le système adopté permet de répondre à la problématique de sécurité

Durée : 3 jours

Livrable : Présentation du scénario d'attaque et des résultats de détection et de correction le jeudi de la semaine 2.