Ilyas TUNAY

Ibrahim DBOUK

Métriques de qualité et attaques à surveiller

Dans ce document nous verrons donc les informations nécessaires relatant les métriques de qualité à surveiller et le type d'attaques à surveiller pour le réseau informatique que nous mettons en place. Cela permettra d'avoir une base solide pour la sécurité du réseau de l'hôpital.

Concernant les métriques à surveiller :

- La solidification des mots de passes

Nous allons commencer simplement, avec la gestion des mots de passes. Il est impératif d'avoir une utilisation solide des mots de passes. Ils doivent inclure des combinaisons avec des lettres majuscules et minuscules, de caractères, de chiffres. De plus, des outils pour analyser la force du mot de passe peuvent être utilisés tel que RoboForm.

- Contrôle d'accès physique

En vue de l'architecture mise en place et toute l'implémentation de sécurité pour le réseau informatique. Pour cela plusieurs aspects peuvent être mis en place :

- Gestion d'accès par badge
- Caméra de surveillance
- Système d'alarme
- Formation du personnel

- Mises à jour et Sauvegardes :

Il faut toujours faire en sorte d'avoir tous les systèmes et toutes les applications à jours, pour éviter certaines interruptions et maintenir une architecture complète et sécurisée. De plus, pour plus de sécurité, il faut souvent effectuer des sauvegardes pour éviter toutes pertes de données.

- Analyse des incidents + Délai de réaction

Il faut faire en sorte d'analyser le pourcentage de résolution suite à des incidents qui ont été réussis par rapport au nombre total d'incidents détectés, pour évaluer l'efficacité du système.

En plus des analyses des incidents, il faut prendre en compte le temps de réaction du système face à ces incidents, analyser la rapidité de détection et réaction.

- Surveiller la bande passante

Il est essentiel de surveiller la bande passante pour évaluer la capacité du réseau. On pourra détecter des activités inhabituelles, agir efficacement sur le réseau informatique et donc garantir une performance optimale du réseau.

- Analyse de faux positifs et négatifs :

Cela concerne le fait d'avoir un résultat, une caractéristique apparente suite à un test alors qu'elle ne l'est pas (faux positifs). Puis, le fait d'avoir un résultat, une caractéristique non apparente à la suite d'un test alors qu'elle l'est en réalité (faux négatifs). Par exemple si notre système IDS/IPS Suricata alerte une authentification bloqué sur un site qui est finalement légitime, cela est un faux positif. Au contraire, si notre système suite à un scan de réseau ne détecte aucune anomalie alors qu'il y en a une, il faut identifier cela comme un faux négatif.

Il faut analyser ces éléments qui permettront d'évaluer la sécurité du réseau et des filtrages mis en place.

<u>Concernant le type d'attaques à surveiller :</u>

- Attaques par force brute

Commençons par voir simple, l'attaque par force brute. Comme nous l'avons vue tout à l'heure dans les métriques à surveiller, il faut mettre des mots de passe solide. Un mot de passe simple peut engendrer un attaquant qui en s'authentifiant, peut tomber sur le bon mot de passe. Il faut surveiller les tentatives de connexion répétées.

- Injections SQL

Notre base de données peut être infectés. Il faut donc surveiller la base de données, les entrées d'utilisateurs, pour éviter que celle-ci soit affectée, et engendrer par exemple une intrusion de données et des fuites d'informations.

- Attaques de phishing

Il faut être vigilant aux tentatives de tromperie visant à obtenir des informations qui sont confidentielles. Il faut surveiller les mails suspects, les URL ou message que nous voyons qui peuvent être malveillants.

- Attaques DDos

Ces attaques cible directement un service du réseau telle qu'un site web pour les rendre indisponibles. Pour éviter ce type d'attaque, surveiller le trafic du réseau pour détecter et réagir à certaines anomalies.

- Attaque Man-in-the-middle (MITM)

Cette attaque permet à un attaquant d'intercepter des données, des communications, entre deux machines qui discutes par exemple. Cette attaque peut être résolu lorsque l'attaquant utilise par exemple de faux certificat SSL/TLS, il faut donc surveiller constamment les certificats, si des changements, des anomalies s'effectue.

En somme, ces attaques sont importantes à surveiller dans le réseau informatique en raison de leur présence fréquente et leur effet de gravité qu'il peut engendrer. En effet, surtout dans un réseau d'hôpital où il y a beaucoup de données qui sont sensibles, il faut se préparer et être formés à toute éventualités.