Rapport d’incident de cybersécurité - Attaque par inondation SYN

Section 1 : Indiquez le type d’attaque susceptible d’avoir provoqué l’interruption du réseau

Notre analyse a débuté suite à une alerte automatique signalant une anomalie avec le serveur web, entraînant des erreurs de délai de connexion pour les visiteurs du site. L’utilisation de Wireshark pour examiner le trafic a révélé une quantité inhabituellement élevée de requêtes TCP SYN provenant d’une adresse IP unique inconnue, indiquant une attaque SYN flood.
Ce type d’attaque de déni de service (DoS) est caractérisé par l’envoi massif de requêtes SYN dans le but de saturer les capacités du serveur à établir de nouvelles connexions, empêchant les utilisateurs légitimes d’accéder au site.

Section 2 : Expliquez en quoi l’attaque est à l’origine du dysfonctionnement du site web

Lorsque les visiteurs du site web tentent d’établir une connexion avec le serveur web, un protocole de communication en trois étapes, connu sous le nom de “three way handshake”, se déroule, utilisant le protocole TCP. Ce processus est vital pour le fonctionnement sécurisé et fiable des communications sur Internet. Il se compose des étapes suivantes :

- SYN : Un paquet SYN est envoyé d’un périphérique source à un périphérique de destination, demandant une connexion (ex: lignes 47,55,63,69 du journal)
- SYN ACK : Le périphérique de destination répond au périphérique source par un paquet SYN ACK afin d’accepter la demande de connexion et réserver des ressources (ex: lignes 48, 56,65)
- ACK : Un dernier paquet ACK est envoyé par le périphérique source au périphérique de destination pour accuser réception de l’autorisation de connexion (ex : lignes 49,58, 67).

Dans le cas d'une attaque par inondation SYN, un acteur malveillant submerge le serveur avec un volume excessif de paquet SYN (ex : lignes 52,57,59,..., etc. Toutes les lignes rouges dans le journal). Le serveur, incapable de gérer ce volume de requêtes, est dépassé et ne peut plus répondre aux nouvelles connexions légitimes.

Ce dysfonctionnement a les conséquences suivantes pour l'entreprise :

- Perte de productivité : Les employés ne peuvent pas accéder au site web pour effectuer leurs tâches, ce qui réduit l'efficacité et engendre des pertes de temps.
- Manque à gagner : Les clients potentiels ne peuvent pas accéder au site web pour consulter les offres et effectuer des réservations, ce qui entraîne une perte de revenus.
- Dommages à la réputation : L'indisponibilité du site web nuit à l'image de marque de l'entreprise et peut entraîner une perte de confiance chez les clients.

Solutions :

- Pare-feu avec protection DDoS : La mise en place d'un pare-feu capable de détecter et de bloquer les attaques DDoS, notamment les attaques SYN flood, est essentielle pour protéger le serveur web.
- Systèmes de détection d'intrusion (IDS) : Un IDS permet de surveiller le trafic réseau et de détecter des activités suspectes, telles que les attaques SYN flood, ce qui permet une réaction rapide.
- Configuration du serveur : Le serveur web doit être configuré pour gérer efficacement les connexions TCP et limiter le nombre de connexions simultanées.