Rapport d’incident de cybersécurité : analyse du trafic réseau

Partie 1 : Synthèse du problème découvert dans le journal de trafic DNS et ICMP

Le journal de trafic DNS et ICMP révèle que le serveur DNS responsable de la résolution des noms de domaine en adresse IP est actuellement indisponible ou inaccessible.

Cette conclusion découle de l’analyse de réseau, qui a détecté des réponses ICMP indiquant que le “port UDP 53 inaccessible”.

Le port 53 est le port standard utilisé par le service DNS pour traiter les requêtes de résolution de noms de domaine. L’inaccessibilité du port 53 indique que le serveur DNS ne répond pas aux requêtes entrantes.

Partie 2 : Explication de l’analyse des données effectuée et proposition de solutions à mettre en oeuvre

L’incident a été signalé pour la première fois à 13h24 après que plusieurs clients ont rapporté être incapables d’accéder au site web “yummyrecipesforme.com”, recevant un message d’erreur “port de destination inaccessible”.

L’analyse du trafic réseau a révélé que le problème est lié à l’inaccessibilité du serveur DNS, spécifiquement via le port UDP 53. Les logs DNS et ICMP montrent que des requêtes DNS sont envoyées au serveur DNS (adresse IP 203.0.113.2) sur le port 53, mais le serveur DNS ne répond pas, générant des messages d’erreur ICMP “port UDP 53 inaccessible”.

Analyse des données :

- Protocole concerné : Le protocole UDP est utilisé pour les requêtes DNS.
- Port affecté : Le port 53, port standard pour le service DNS, est inaccessible.

- Cause possible : L'inaccessibilité du serveur DNS peut être due à plusieurs facteurs, notamment :
    - erreur de configuration du serveur DNS : Une erreur dans la configuration du serveur DNS peut empêcher le serveur de répondre aux requêtes.
    - Attaque par déni de service (DDoS) : Le serveur DNS peut être victime d'une attaque DDoS qui le surcharge et l'empêche de répondre aux requêtes.
    - Panne du serveur DNS : Le serveur DNS peut être hors service en raison d'une panne matérielle ou logicielle

Solutions possibles :

- Vérification de la configuration du serveur DNS : Il est recommandé de vérifier la configuration du serveur DNS pour s'assurer qu'il est correctement configuré et qu'il n'y a pas de problèmes de configuration.
- Vérification des règles du pare-feu : L'équipe de sécurité devrait analyser les règles du pare-feu pour s'assurer que le trafic UDP sur le port 53 n'est pas bloqué de manière incorrecte.
- Protection contre les attaques DDoS : La mise en place d'une solution de protection contre les attaques DDoS est recommandée pour protéger le serveur DNS des attaques futures.
- Solution de secours pour la résolution DNS : Il est important d'avoir une solution de secours pour la résolution DNS afin de garantir l'accès aux sites web en cas de défaillance du serveur DNS principal.

Conclusion :
L'analyse du trafic réseau indique que le serveur DNS est inaccessible, ce qui empêche les clients d'accéder au site web. Les solutions proposées permettront de diagnostiquer et de résoudre le problème, en garantissant la disponibilité du service DNS et l'accès au site web.