# Rapport d'incident de cybersécurité : analyse du trafic réseau

|  |
| --- |
| Partie 1 : rédigez une synthèse relative au problème découvert dans le journal de trafic DNS et ICMP |
| Le protocole UDP révèle que le serveur DNS est hors service ou inaccessible. Comme le montrent les résultats de l'analyse du réseau, la réponse d'écho ICMP a renvoyé le message d'erreur « port udp 53 inaccessible ». Le port 53 est généralement utilisé pour le trafic du protocole DNS. Il est fort probable que le serveur DNS ne réponde pas. |
|

|  |
| --- |
| Partie 2 : expliquez l'analyse des données effectuée et proposez une solution à mettre en œuvre |
| L'incident s'est produit ce jour à 13 h 23. Des clients ont appelé l'entreprise pour informer l'équipe informatique qu'ils avaient reçu le message « port de destination inaccessible » lorsqu'ils avaient tenté d'accéder au site Web. Les spécialistes de la sécurité réseau au sein de l'entreprise enquêtent en ce moment sur le problème afin que les clients puissent à nouveau accéder au site Web. Dans le cadre de notre enquête, nous avons effectué des tests de reniflage de paquets à l'aide de tcpdump. Nous avons constaté dans le fichier journal correspondant que le port 53 (DNS) était inaccessible. L'étape suivante consiste à déterminer si le serveur DNS est hors service ou si le trafic vers le port 53 est bloqué par le pare-feu. Le serveur DNS peut être hors service en raison d'une attaque par déni de service réussie ou d'une erreur de configuration. |