# Exemple d'activité : analyser les attaques de réseaux

|  |
| --- |
| Section 1 : indiquez le type d'attaque susceptible d'avoir provoqué  l'interruption du réseau |
| Le message d'erreur relatif au délai d'attente de connexion du site Web peut indiquer une attaque par déni de service (DoS). Les journaux montrent que le serveur Web cesse de répondre lorsqu'il est surchargé de demandes de paquets SYN. Il pourrait s'agir d'une attaque par déni de service (DoS) de type inondation SYN. |

|  |
| --- |
| 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 (three-way handshake) a lieu à l'aide du protocole TCP. Le protocole de communication se compose de trois étapes :   1. Un paquet SYN est envoyé d'un périphérique source à un périphérique de destination, demandant une connexion. 2. Le périphérique de destination répond au périphérique source par un paquet SYN-ACK afin d'accepter la demande de connexion. Le périphérique de destination réservera des ressources pour que le périphérique source puisse se connecter. 3. Un dernier paquet ACK est envoyé par le périphérique source au périphérique de destination pour accuser réception de l'autorisation de connexion.   Dans le cas d'une attaque par inondation SYN, un acteur malveillant envoie un grand nombre de paquets SYN en même temps, ce qui submerge les ressources disponibles du serveur pour réserver la connexion. Lorsque cela se produit, aucune ressource de serveur n'est disponible pour accepter les demandes de connexion TCP légitimes.  Les journaux indiquent que le serveur Web est submergé et qu'il n'est pas en mesure de traiter les demandes SYN des visiteurs. Le serveur n'est pas en mesure d'ouvrir une connexion aux nouveaux visiteurs. Ces derniers reçoivent un message d'erreur (délai d'attente de connexion). |