Voici une liste des attaques courantes visant le protocole TCP et leurs solutions potentielles :

1. Attaques SYN Flood

Solution : Les solutions possibles comprennent l'utilisation de pare-feu pour filtrer les paquets SYN, l'utilisation de seuils de détection de SYN Flood pour bloquer les adresses IP malveillantes, et l'augmentation de la taille de la table de connexion pour gérer des volumes élevés de connexions SYN.

2. Attaques de réinitialisation TCP (TCP Reset Attack)

Solution : Les solutions possibles comprennent la mise en place d'un système de vérification de la source des connexions TCP, l'utilisation de pare-feu pour bloquer les paquets RST malveillants, et l'utilisation de techniques de chiffrement pour empêcher la manipulation des paquets TCP.

3. Attaques de modification de séquence TCP (TCP Sequence Number Attack)

Solution : Les solutions possibles comprennent l'utilisation de techniques de chiffrement pour protéger les numéros de séquence TCP, l'utilisation de pare-feu pour bloquer les paquets malveillants, et la mise en place de mécanismes de vérification d'intégrité de paquets pour détecter les paquets malveillants.

4. Attaques de détournement de session TCP (TCP Session Hijacking)

Solution : Les solutions possibles comprennent l'utilisation de techniques de chiffrement pour protéger les sessions TCP, la mise en place de mécanismes d'authentification pour vérifier l'identité des parties impliquées dans la session, et la mise en place de mécanismes de vérification d'intégrité pour détecter la manipulation des paquets.

5. Attaques de fenêtre TCP (TCP Window Size Attack)

Solution : Les solutions possibles comprennent l'utilisation de mécanismes de régulation de flux pour limiter le taux de paquets entrants, l'augmentation de la taille de la fenêtre TCP pour gérer des volumes élevés de paquets, et la mise en place de seuils de détection pour bloquer les paquets malveillants.

6. Attaques de déni de service (DoS) TCP

Solution : Les solutions possibles comprennent l'utilisation de pare-feu pour filtrer les paquets malveillants, la mise en place de mécanismes de régulation de flux pour limiter le taux de paquets entrants, et l'utilisation de techniques de surveillance pour détecter et bloquer les attaques DoS.

7. Attaques de fragmentation TCP (TCP Fragmentation Attack)

Solution : Les solutions possibles comprennent l'utilisation de pare-feu pour bloquer les paquets malveillants, la mise en place de mécanismes de vérification d'intégrité pour détecter la manipulation des paquets, et l'utilisation de techniques de surveillance pour détecter et bloquer les attaques de fragmentation TCP.