**IoT : PROTOCOLES TCP, UDP et FTP**

Ici nous allons lister les attaques phares donc peuvent subir les protocoles TCP, UDP et FTP et proposer éventuellement quelques mesures de sécurité pour pallier à cela.

1. **Le protocole TCP**

**Attaque SYN Flood :** C’est une attaque qui consiste à envoyer un grand nombre de paquets SYN(Synchronisation) à une cible, dans le but de saturer sa mémoire tampon et de la rendre indispensable aux utilisateurs légitimes. Elle exploite une faiblesse dans le processus de connexion TCP à trois voies ou le serveur doit maintenir un état de connexion pour chaque demande entrante.

**Attaque Man-In-The-Middle (MITM) :** Cette attaque consiste à intercepter et à modifier les paquets TCP échangés entre deux parties, dans le but de voler les données ou modifier les informations. Elle exploite une faiblesse dans le chiffrement des données en usurpant l’adresse IP de l’une des parties

**Attaque TCP reset**: Elle consiste à envoyer un paquet RST (réinitialisation) à une cible, dans le but de fermer une connexion TCP existante de manière inattendue. Elle peut se produire en exploitant une faiblesse dans la séquence de numérisation des paquets TCP

**Attaque TCP prédiction de séquence :** Cette attaque consiste à prédire la séquence de numérotation des paquets échanges entre deux parties. Comme faiblesse, cette information peut être utilisée pour usurper l’identité d’une partie ou pour compromettre la sécurité d’une connexion TCP.

**Attaque TCP Hijacking :** Cette attaque consiste à usurper l’identité d’une partie en modifiant les paquets TCP échanges entre deux parties, dans le but de voler les données ou modifier des informations sensibles. Elle peut se produire en exploitant une faiblesse de l’authentification ou la validation des données.

**Règles de sécurité pour TCP**

Il est recommandé de mettre en place les mesures de sécurité telles que l’utilisation de pare-feu, de VPN, de chiffrement de bout en bout et de vérifier l’intégralité des données

1. **Le protocole UDP**

**Attaque UDP Flood**: elle consiste à envoyer un grand nombre de paquets UDP à une cible dans le but de saturer sa bande passante et de la rendre indisponible aux utilisateurs légitimes. Cette attaque peut être réalisée en utilisant des botnets ou des machine zombies.

**Attaque UDP Spoofing**: Elle consiste à usurper l’adresse IP d’une partie en modifiant les paquets UDP échanges entre deux parties. Cette attaque peut être réalisée en exploitant une faiblesse dans la validation des données ou en utilisant les techniques de falsification d’adresse IP.

**Règles de sécurité pour UDP**

Il est recommandé de mettre en place des mesures de sécurité telles que l’utilisation des pares-feux, la limitation du trafic UDP, la mise en place des listes blanches d’adresses IP autorisées et la vérification de l’intégrité des données.

1. **Le protocole FTP**

**Attaque par force brute** : Elle consiste à essayer toutes les combinaisons possibles de noms d’utilisateurs et des mots de passe pour se connecter à un serveur FTP, dans le but d’obtenir un accès non autorisé à des fichiers sensibles ou de modifier des informations.

**Attaque de renifleur de paquets :** Elle consiste à analyser les paquets FTP échangés entre deux parties, dans le but de voler les données sensibles telles que les noms d’utilisateurs et les mots de passe.

**Attaque par Déni de Service (DoS) :** Elle consiste à envoyer un grand nombre de requêtes FTP au serveur, dans le but de la saturer et de le rendre indisponibles aux utilisateurs légitimes

**Règles de sécurité pour FTP**

Il est recommandé de mettre en place des mesures de sécurité telles que l’utilisation des pares-feux, la mise en place des protocoles d’authentification forts, la limitation des autorisations d’accès sur les fichiers et les dossiers.