Rapport sur le réseau et l’interception réseau

Tout d’abord pour parler d’interception de données sur un réseau il faut d’abord comprendre le principe de fonctionnement d’un réseau, le réseau n’est rien d’autres que l’interconnexion de plusieurs appareils entres eux afin de communique (transmettre l’information) et il repose essentiellement sur le modelé OSI (open system interconnections) ou le modèle TCP/IP

1. Le modèle OSI (open system interconnections) :

Il comprend 7 couches sur les quelles les données sont encapsules et chaque couche a une fonction

1. Physique :

Traite la transmission brute des données sous forme de signaux (fais référence au support de transmission)

1. Liaison de données :

Gere les communications, s’assure de la livraison grâce aux adresses mac

1. Réseau :

Achemine les paquets entre les réseaux, utilise les IP pour le routage

1. Transport :

Assure le transport entre les hôtes via TCP ou UDP

1. Session :

Gere les connections entre les applis

1. Présentation :

Formate les données pour la compréhension tels que les compressions, et chiffrement

1. Application :

Interface entre l’utilisateur et le réseau et fournit des services comme http, smtp

1. Le modèle TCP/IP :

Contrairement au modèle OSI, tcp est base sur l’implémentation pratique utilise dans internet et les réseaux ce modèle a 4 couches : Accès reseau, internet, transport, Application

1. Les paquets réseau :

Le fonctionnement des paquets réseau repose sur l’idée de découper les données en petits morceaux pour les transmettent efficacement, ils traversent plusieurs couches du modelés OSI

* Les paquets Ethernet (couche liaison) :

Les trames Ethernet sont forme de l’entête avec l’adresse mac source et destination, les types de protocole encapsule, la charge utile

* Les paquets IP (couche réseau) :

Il contient l’en-tête IP (adresse IP source et destination, version IP, TTL, etc), les données encapsulées

* Les paquets TCP (couche transport) :

Il contient le numéro de ports source et destination pour identifier les application, numéro de séquence et d’acquittement pour l’ordre des donnees, options de contrôle (flags comme SYN, ACK, FIN etc) pour les négociations de connexion

Apres la connaissance du fonctionnement d’un réseau nous allons passer à l’interception de données sur ce dernier

Pour intercepter les données nous devons dans un premier temps écouter (sniffer) le réseau pour voir et enregistrer les échanges effectuer a l’aide des outils comme **tcpdump** ou **wireshark** ensuite procéder a l’analyse soit manuellement ou a travers des scripts, nous pouvons même aller plus loin en injectant des paquets réseau manuellement soit pour usurpée l’identité d’un appareil ou pour injecter des payload pour exécuter des commandes ou exploiter des vulnérabilités connue, le meilleurs outil est un bibliothèque python très puissants appelé **SCAPY** qui peut injecter tous types de paquets réseau a travers des script python.