NOTIONS DE BASES

Les menaces et attaques passant par le réseau sont généralement de deux types :

- **Menaces passives sur les réseaux** : activités comme Network Sniffing (reniflage réseau) et l'idle scan (méthode de balayage des ports TCP), conçues pour intercepter le trafic passant par le réseau.
- **Menaces actives sur les réseaux** : activités telles que les attaques par déni de service (DoS, Denial of Service) et les injections SQL, où l'auteur tente d'exécuter des commandes pour perturber le fonctionnement normal du réseau.

Liste (non exhaustive) des attaques passives les plus fréquentes en Cyber :

- Network Sniffing (Reniflage réseau) – Capture des trames à des fins d'analyse
- Scan de port (balayage de port) – Scan par Ping – TCP Half open – TCP Connect – UDP – Balayage furtif
- Analyse de trafic

Liste (non exhaustive) des attaques actives les plus fréquentes en Cyber :

- Le phishing (hameçonnage) et le spear-phishing (harponnage)
- Les attaques par logiciel malveillant (malware)
- Le déni de service (DoS) et par déno de service distribué (DDOS)
- L'attaque par Drive by Download (téléchargement furtif)
- L'attaque de l'homme au milieu ou MitM
- Le piratage de compte
- La fraude au président ou Faux Ordre de Virement (FOVI)

SCAN DE PORT

DEFINITION : Un scanner de ports est un programme informatique qui analyse les ports réseau pour déterminer leur statut : ouvert, fermé ou filtré. Ces outils sont très utiles pour diagnostiquer un problème de réseau ou de connectivité. Toutefois, ils permettent aussi aux attaquants de détecter des points d'infiltration possibles et d'identifier les appareils utilisés sur votre réseau, comme le pare-feu, serveurs proxy ou serveurs VPN.

Un scanner de ports envoie un paquet réseau TCP ou UDP demandant à un port quel est son statut. Trois réponses sont possibles :

- **Ouvert, accepté** : l'ordinateur répond et demande s'il peut faire quelque chose pour vous.
- **Fermé, n'écoute pas** : l'ordinateur répond que le port est en cours d'utilisation et indisponible pour le moment.
- **Filtré, ignoré, bloqué** : l'ordinateur ne répond pas du tout.

TEST : Utilisation des l'outils « **Advanced IP Scanner** » et « **Advanced port Scanner** »

NETWORK SNIFFER + ANALYSE DE TRAFIC

DEFINITION : Le reniflement est une technique de surveillance et de capture de tous les paquets de données d'un réseau à l'aide d'outils logiciels ou matériels. Il permet aussi à un attaquant d'observer et d'accéder à l'intégralité du trafic réseau cible à partir d'un point donné.
Le reniflement de paquets permet à l'attaquant de collecter des informations telles que le trafic de messagerie, la configuration des routeurs, le trafic DNS, les sessions de chat, etc.
Une fois les paquets capturés, il faudra analyser celui-ci avec un outil permettant de lire le code.
Il existe deux types d'attaques:

- ***Reniflement passif*** : Il s'agit de renifler un réseau à travers un concentrateur (obsolète de nos jours)
- ***Reniflement actif :***Il est utilisé pour renifler un réseau basé sur un commutateur
  - Inondation MAC ou Attaques MAC (voire II) ?
  - Empoisonnement DNS
  - Empoisonnement ARP ou Attaque par usurpation d'ARP
  - Attaques par DHCP
  - Vol de port de commutateur
  - Attaque par usurpation d'identité

ATTENTION AUX PROTOCOLES VULNERABLES : Telnet – Imap – HTTP – SMTP – FTP etc.

LA SOLUTION : le **S** = HTTPS – SMTPS – etc.

TEST : Utilisation de l'outil « **WireShark** »

FOCUS SUR LE DENI DE SERVICE

DEFINITION : Une attaque par déni de service (DoS) est une attaque ciblée qui inonde délibérément un réseau de fausses requêtes dans le but de perturber les activités de l'entreprise. Lors d'une attaque DoS, les utilisateurs sont incapables d'effectuer des tâches courantes et nécessaires, comme accéder à la messagerie électronique, à des sites web, à des comptes en ligne ou à d'autres ressources gérées par un ordinateur ou un réseau compromis. Si la plupart des attaques DoS n'entraînent pas de perte de données et sont généralement résolues sans versement de rançon, elles coûtent du temps, de l'argent et d'autres ressources à l'entreprise pour le rétablissement des activités stratégiques.

CONCEPT : Une attaque DoS consiste le plus souvent à inonder l'hôte ou le réseau ciblé de demandes de services illégitimes. Elle se caractérise par l'utilisation d'une fausse adresse IP qui empêche le serveur d'authentifier l'utilisateur. Le traitement de cette vague de fausses requêtes submerge le serveur, provoquant son ralentissement et parfois même son plantage, et empêche les utilisateurs légitimes d'y accéder. Pour qu'une attaque de ce type soit fructueuse, le cyberattaquant doit disposer de plus de bande passante que sa cible.

La principale différence entre une attaque par déni de service distribué (DDoS) et une attaque DoS réside dans l'origine de l'attaque. Une attaque DDoS est lancée de façon orchestrée depuis de multiples emplacements et par plusieurs systèmes en même temps, tandis qu'une attaque DoS est isolée par nature.

FOCUS SUR LE DENI DE SERVICE

TYPES D'ATTAQUES : Il existe deux types principaux d'attaques DoS : celles qui font planter les services web et celles qui les inondent. Ces deux catégories sont à leur tour subdivisées en plusieurs sous-ensembles, qui varient selon les méthodes utilisées par le cyberadversaire, l'équipement ciblé et la méthode d'évaluation de l'attaque.

1. **Débordement de mémoire tampon (buffer overflow)** : Le débordement ou dépassement de mémoire tampon est la forme la plus fréquente d'attaque DoS. Dans ce type d'exploit, le cyberadversaire dirige vers une adresse IP plus de trafic que le système n'est à même de traiter. La machine ciblée consomme alors toutes les mémoires tampons disponibles ou la totalité des régions de la mémoire de stockage qui conservent temporairement les données pendant leur transfert au sein du réseau. Un débordement de mémoire tampon se produit lorsque le volume de données dépasse la bande passante disponible, notamment l'espace disque, la mémoire ou le processeur, ce qui provoque un ralentissement des performances et le plantage du système.
2. **Attaques par inondation (flood attacks)** : Les attaques par inondation consistent à envoyer au système un volume de trafic impossible à gérer par le serveur, ce qui provoque son ralentissement et parfois son arrêt. Les attaques par inondation les plus fréquentes sont les suivantes :

- **Les attaques par inondation ICMP,** communément appelées attaques smurf ou ping, exploitent des terminaux réseaux mal configurés. Dans ces attaques, les cyberadversaires déploient des paquets frauduleux, ou fausses adresses IP, qui envoient une commande ping à chaque terminal connecté au réseau ciblé sans attendre de réponse. La gestion par le réseau de cette augmentation du trafic provoque un ralentissement, voire l'arrêt, du système.
- **Une attaque par inondation SYN** consiste à envoyer une demande de connexion à un serveur, sans jamais établir cette connexion avec l'hôte. Ces demandes continuent d'inonder le système jusqu'à ce que tous les ports ouverts soient saturés, ce qui empêche les utilisateurs légitimes d'accéder au serveur.