LAB 2 : Les attaques réseaux

Objectifs

Le but ce lab est d'acquérir une connaissance élémentaire des différents types d'attaques qui peuvent menacer les réseaux.

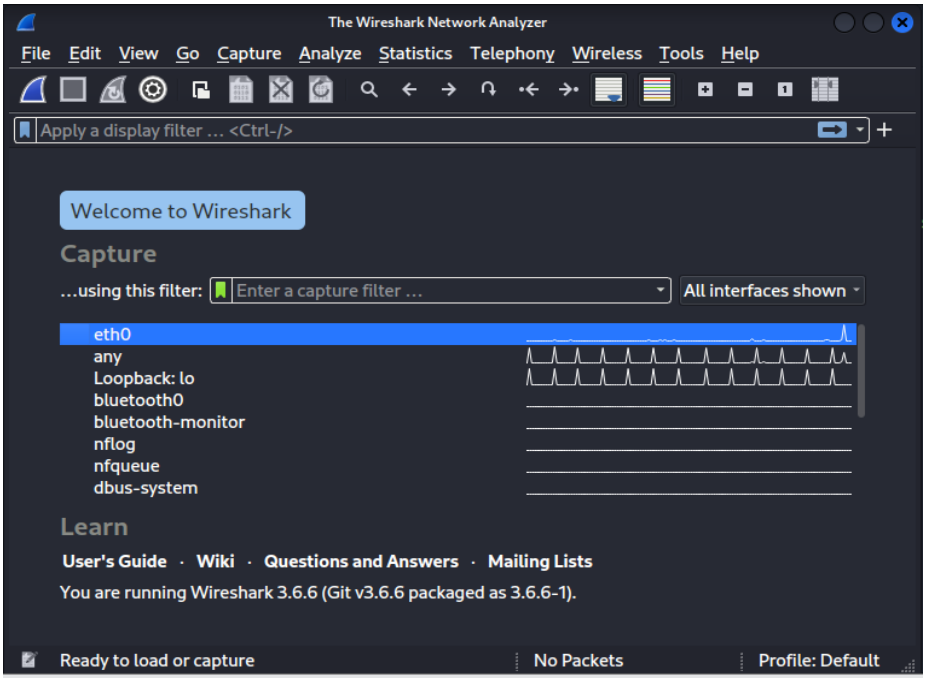
Rendu

Vous êtes invités à remettre, sur votre Google Classroom, Un fichier avec les commandes que vous avez lancées et les résultats obtenus avec capture d'écran. Un seul rendu est à remettre par groupe.

1. Attaque Sniffing

L'objectif de ce cette attaque est de sniffer la communication entre deux machins afin d'intercepter le trafic. Pour lancer la capture du trafic nous allons utiliser le logiciel Wireshark sur Kali avec la commande :

```
$ wireshark
```



Menu Capture > eth0 > Cliquer sur Start. Il faut ensuite chercher dans les différentes trames les données désirées (@IP, protocole, port….)

2. L' ARP spoofing

Le programme arpspoof est un forgeur de paquets. Cette commande permet aussi l'interception du trafic et dans un réseau local. Elle est utilisée comme suit :

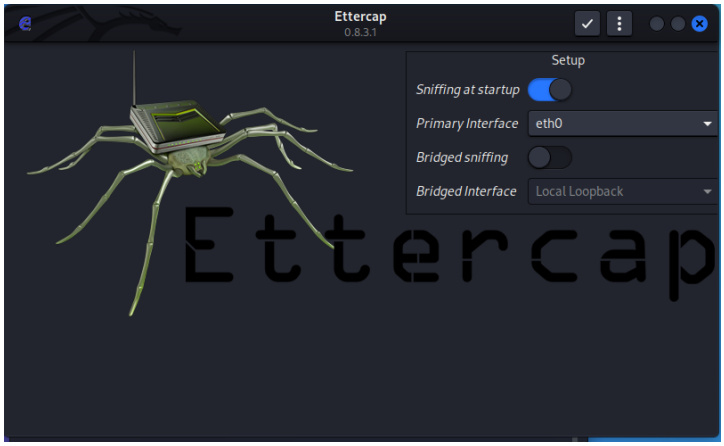
- Il faut commencer par lancer des pings entre tous les machines (minimums 3 machines) de votre réseau.
- Afficher la table arp de machine victime avec la commande **$ arp -a**.
- Lancer l'attaque arpspoof avec la commande suivante :

[redacted]

- Vérifier la table arp au niveau de machine cible en citant vos remarques.

4. Man In The Middle attaque

- Lancer Ettercap en introduisant la commande **# ettercap –G** et suivre les étapes suivantes :



- Accepter et passer
- Menu Hosts>Scan for hosts
- Host List >Add to target 1 (passerelle) et add to Target 2 (machine cible)
- menu MITM> ARPpoisoning
- Lancer urlsnarf sur kali avec la commande **#urlsnarf**
- Faire une recherche sur le navigateur de la machine cible.
- Vérifier la fenêtre de urlsnarf.

5. Attaque de déni de service (DoS) : synflooding

Pour cette attaque nous allons utiliser l'utilitaire **hping3. hping3** est un outilréseau capable d'envoyer des paquets TCP/IP sur commande (forgeur de paquet) et d'afficher lesréponses de la cible comme le programme ping le fait. La commande à exécuter pour mettre hors service un serveur web est la suivante :

```
Hping3 10.0.0.2 -I eth0 -i u1 -S --rand-source -p 80 &
```

Solutions contre l'attaque synflooding :

- Modifier la configuration par défautdesparamètres TCP (nombre de connexion par unité de temps).
- le filtrage par firewall (pare-feu) qui réalise une stateful inspection.
- IDS/IPS.

6. L'attaque social engineering

Lancer l'attaque social engineering sur kali et suivre les choix suivants :

1- Social-Engineering Attacks
2- Website Attack Vectors
3- Credential Harvester Attack Method
4- Web Template
5- Maitre l'adresse IP de la machine kali

7. Password attacks: John the Ripper

Pour ce TP nous allons créer trois utilisateurs avec trois mots de passe comme le montre le tableau ci- dessous :

Utilisateur	Mot de passe
admin	admin
admin2	4a1
admin3	Qp@

Les mots de passes utilisés ont des degrés de complexité différents. Pour la création de ces utilisateurs, nous allons utiliser la commande **htpassword**. Cette commande va permettre la création d'un nouvel utilisateur et le stockage de ses paramètres d'authentification cryptés dans un fichier donné. Pour la création des trois utilisateurs nous allons faire comme suit :

```
htpasswd -cb /test admin
admin htpasswd -b /test
admin2 3a1 htpasswd -b
/testadmin3 Qp@
```

Remarque :

- Les paramètres d'authentification seront stocké dans le fichier /test.
- L'option -c permet de créer le fichier destination.
- L'option -b permet la création de l'utilisateur.

A ce stade, si on affiche le contenu du fichier /test, on remarque que son contenu est crypté. Nous allons par la suite craquer les mots de passes enregistrés dans le fichier /test grâce au logiciel John The Ripper (JTR). C'est un logiciel libre de cassage de mot de passe, utilisé notamment pour tester la sécurité d'un mot de passe. Pour réaliser cette attaque nous devons exécuter les commandes suivantes :

```
cd /pentest/passwords/jtr
./john /test
```

Solutions contre les attaques de mots de passes :

- La mise en place d'une politique de gestion de mots de passes : choix du mot passe (combinaison de chiffres, lettres minuscule et majuscule et de caractères spéciaux), duréede vie et stockage (jamais en claire sur un disque dure ou un papier)
- Les moyens d'authentification forte (**One time password** OTP, les cartes à puces, labiométrie …)