Activité 7 – Réalisation d'une attaque de type DNS SPOOFING et propositions de contre-mesures

Propriétés	Description
Intitulé long	Ce TP a pour objectif de réaliser une attaque de type DNS SPOOFING et de proposer des contre-mesures.
Formation(s) concernée(s)	BTS Services Informatiques aux Organisations
Matière(s)	Bloc 3 SISR – Cybersécurité des services informatiques
Présentation	Dans ce TP, l'objectif est de simuler une attaque DNS SPOOFING et ainsi rediriger de façon transparente une victime sur une version malveillante d'un site.
Compétences	• Protéger les données à caractère personnel. • Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques. • Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service. • Assurer la cybersécurité d'une solution applicative.
Savoirs	• Typologie des risques et leurs impacts. • Cybersécurité : bonnes pratiques, normes et standards.
Prérequis	Connaissances de base concernant l'administration d'un système GNU/Linux, et la configuration des services Apache2 et bind9.
Outils	Kali, conteneurs sur Docker (Laboratoire n°2) https://forge.aeif.fr/btssio-labos-kali/lab2
Mots-clés	Kali, dns spoofing, analyse trames, empoisonnement arp, exploitation de vulnérabilités, remédiations, DNS, spoofing, hygiène numérique, respect des bonnes pratiques.
Durée	2 heures
Auteurs	Cécile Nivaggioni avec la relecture de Patrice Dignan et d'Apollonie Raffalli. Laboratoire sur Docker : Apollonie Raffalli avec les tests de Christelle Thiry

Préambule

Le TP proposé est uniquement à visée pédagogique. Son objectif est l'analyse de failles liées à l'usage de certains protocoles réseaux afin de proposer une amélioration de la sécurité informatique d'un système d'information et de l'hygiène numérique des étudiants. Il permet également l'acquisition de compétences associées au bloc 3 Cybersécurité SISR du BTS SIO.

Les outils abordés dans ce support sont uniquement utilisés à des fins éthiques (Ethical Hacking) et pédagogiques. Leur usage est formellement interdit en dehors de ce cadre sur un réseau tiers sans autorisation explicite.

Pour rappel, l'article 323-1 du code pénal stipule que le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

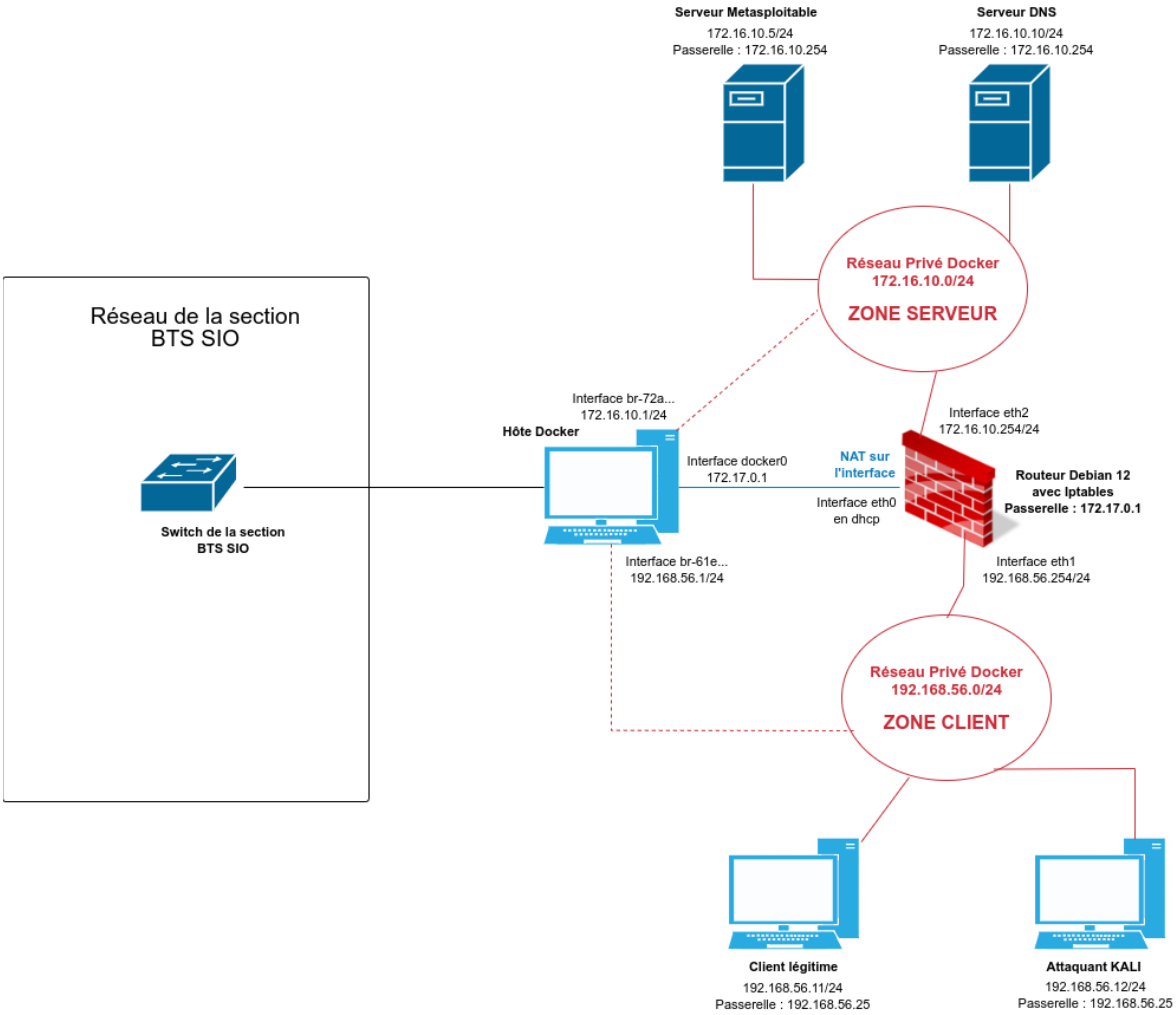
Plateforme utilisée

Le TP qui vous est proposé utilise le laboratoire 2 contenant 5 conteneurs pré-configurées. **Pour rappel :**

Machine	Nom de domaine pleinement qualifié	Configuration réseau	Applications et services
Serveur sous Debian 12	srvssh.local.sio.fr	Adresse IPv4 : 172.16.10.10/24 Passerelle : 172.16.10.254 Serveur DNS : 172.16.10.10	Service OpenSSH port 22/TCP Service DNS Bind port 53/UDP
Client sous Debian 12	clissh.local.sio.fr	Adresse IPv4 : 192.168.56.11/24 Passerelle : 192.168.56.254 Serveur DNS : 172.16.10.10	Environnement de bureau XFCE Service XRDP port 3389/TCP Client OpenSSH
Attaquant sous Kali Linux	kali.local.sio.fr	Adresse IPv4 : 192.168.56.12/24 Passerelle : 192.168.56.254 Serveur DNS :172.16.10.10	Environnement de bureau XFCE Service XRDP port 3389/TCP Metasploit Netfilter/Iptables
Routeur sous Debian 12	routeur.local.sio.fr	Adresses IPv4 : eth0 – DHCP eth1 – 192.168.56.254/24 eth2 – 172.16.10.254 Serveur DNS : 172.16.10.10	Netfilter/Iptables
Serveur Metasploitable	srvm.local.sio.fr	Adresse IPv4 : 172.16.10.5/24 Passerelle : 172.16.10.254 Serveur DNS : 172.16.10.10	Service OpenSSH port 22/TCP Service Web port 80:TCP (site « mutillidae »)

Toutes les machines sont accessibles en SSH (sur le port 22 à partir de l'hôte qui les héberge) et à partir de l'extérieur.

La machine Kali Linux et le client Debian bénéficient d'une interface graphique accessible via un bureau à distance (protocole RDP sur le port 3389 à partir de l'hôte qui les héberge) et à partir de l'extérieur.



Voici les comptes, les mots de passe et les numéros de ports **accessibles de l'extérieur**, vous permettant d'accéder aux différents conteneurs :

Intitulé de la machine	**Nom d'utilisateur**	**Mot de passe**	**Ports SSH**	**Port RDP**
Serveur sous Debian 12	etusio	Fghijkl1234*	12222	
Client sous Debian 12	etusio	Fghijkl1234*	22222	23389
Attaquant sous Kali Linux 2023.3	etusio	Fghijkl1234*	32222	33389
Routeur sous Debian 12	etusio	Fghijkl1234*	42222	
Serveur Metasploitable	msfadmin	msfadmin	52222	

Lorsque des commandes nécessitant des privilèges administrateurs seront utilisées, il sera nécessaire d'utiliser la commande **sudo**.

```
etusio@srvssh:~$ sudo service ssh restart
```

Voici une représentation logique de la maquette proposée dans le cadre de ce laboratoire :

- Lancer le laboratoire : **bash gestion_lab2.sh -c**
- Vérifier que les 5 conteneurs sont actifs : **docker ps**

```
CONTAINER ID   IMAGE                               COMMAND                  CREATED       STATUS              PORTS
                                   NAMES
dd0866a4c36d   tleemcjr/metasploitable2            "sh -c '/bin/service…"   6 days ago    Up About a minute
                                   metasploitable-lab2
4136eb106769   aporaf/kalirolling:lab2             "/lib/systemd/system…"   6 days ago    Up About a minute   22/tcp, 3389/tcp
                                   kali-lab2
e879e10e57a3   aporaf/clientdebian12:lab2          "/lib/systemd/system…"   6 days ago    Up About a minute   22/tcp, 3389/tcp
                                   client-lab2
7c1ef0ce2e65   aporaf/serveurdebian12:lab2         "/lib/systemd/system…"   6 days ago    Up About a minute   22/tcp, 53/tcp, 53/udp
                                   serveur-lab2
13a1ffaae620   aporaf/routeurdebian12:lab2         "/lib/systemd/system…"   6 days ago    Up About a minute   0.0.0.0:12222->12222/tcp, :::12222->12222/tcp, 0.0.0.0:22222->22222/tcp, :::22222->22222/tcp
, 0.0.0.0:23389->23389/tcp, :::23389->23389/tcp, 0.0.0.0:32222->32222/tcp, :::32222->32222/tcp, 0.0.0.0:33389->33389/tcp, :::33389->33389/tcp, 0.0.0.0:52222->52222/tcp, :::52222->52222/tcp, 0.0.0.0:
42222->22/tcp, :::42222->22/tcp    routeur-lab2
```

Évolution du laboratoire

L'attaque de type DNS SPOOFING consiste à corrompre le cache DNS de la victime afin de fausser les associations entre les noms et les adresses IP des sites visités. Ainsi, lorsque la victime se rendra sur un site, elle se retrouvera face à une copie de ce site.
Ce type d'attaque peut par exemple permettre à une personne malveillante de récupérer des informations de connexion (identifiant et mot de passe) en cas d'authentification sur le site falsifié.

Pour ce TP, nous considérerons que la victime (client légitime sous Debian 12) **souhaite se rendre sur le site www.local.sio.fr,** hébergé par le serveur srvm.local.sio.fr (conteneur Docker Serveur Metasploitable).

Configuration du service web

Actuellement le site www.local.sio.fr n'existe pas, le service web du serveur srvm.local.sio.fr est à configurer.
Pour simuler le site, une page index.html affichant « Bienvenue sur le site du BTS SIO » doit être créée dans un répertoire « sitesio » à la racine du service web.

↗ Configurez le service web.

↗ Testez l'accès au site à partir du navigateur du client sous debian (machine virtuelle DebClient 2) en utilisant l'adresse IP du serveur web.

Configuration du service DNS

Ce site doit pouvoir être joignable via l'URL http://www.local.sio.fr.

↗ Configurez le serveur DNS pour déclarer le nom pleinement qualifié www.local.sio.fr.

↗ Utilisez une commande ***nslookup*** à partir du client sous debian (machine virtuelle DebClient 2) pour vérifier et valider votre configuration.

Réalisation de l'attaque

Découverte des hôtes et services présents sur un réseau local

En tant qu'attaquant, la première étape consiste en général à recueillir des informations sur le réseau dans lequel nous nous trouvons. Ainsi, à l'aide de l'outil nmap présent sur Kali Linux, il est possible de réaliser un scan des réseaux logiques locaux :

```
etusio@kali:~$ nmap -sP 192.168.56.0/24
etusio@kali:~$ nmap -sP 172.16.10.0/24
```

Puis de scanner les différents hôtes afin de savoir quels ports sont ouverts sur ceux-ci et quels services sont proposés. Par exemple, sur la zone des serveurs :

```
etusio@kali:~$ nmap -sV 172.16.10.5
etusio@kali:~$ nmap -sV 172.16.10.10
etusio@kali:~$ nmap -sV 172.16.10.254
```

Le scan du serveur 172.16.10.10 montre que le service DNS (bind) est à l'écoute sur le port 53

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-09 02:06 EDT
Nmap scan report for srvdns.local.sio.fr (172.16.10.10)
Host is up (0.00028s latency).
Not shown: 998 closed ports
PORT     STATE    SERVICE  VERSION
22/tcp   open     ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
53/tcp   open     domain   ISC BIND 9.11.5-P4-5.1+deb10u2 (Debian Linux)
```

Une commande **nslookup** permet par exemple de voir le domaine géré par ce serveur DNS :

```
nslookup 172.16.10.10
10.10.16.172.in-addr.arpa       name = srvdns.local.sio.fr.
```

Dans ce TP nous allons nous intéresser au domaine local.sio.fr et plus précisément sur www.local.sio.fr qui pointe vers le site du BTS SIO.

Préparation de la machine pirate sous kali

Mise en place du site pirate

La machine pirate sous Kali (machine virtuelle KaliAttanquant 2) va tenter de se faire passer pour le site http://www.local.sio.fr.
Pour cela, elle doit disposer d'un service web opérationnel avec une copie du site.

Pour différencier le site pirate du site officiel, le site pirate n'affichera non pas « Bienvenue sur le site du BTS SIO » mais « Bienvenue sur le site NON OFFICIEL du BTS SIO ».

- Configurez le service web Apache2 sous Kali pour mettre en ligne la version pirate du site.

- Testez l'accès au site pirate à partir du navigateur du client sous debian en utilisant l'adresse IP du serveur web.

Attention : le service Apache2 n'est pas automatiquement lancé au démarrage de l'attaquant Kali.

Configuration du DNS SPOOFING

Pour configurer le DNS SPOOFING via l'outil Ettercap (déjà installé sur Kali) il faut modifier les fichiers /etc/ettercap/etter.conf et /etc/ettercap/etter.dns.

Dans /etc/ettercap/etter.conf, vous devez :

- ➔ modifier les valeurs de « ec_uid » et « ec_gid » à 0 pour permettre un fonctionnement via le compte « root » ;
- ➔ décommenter les 4 lignes « iptables » (lignes 179, 180, 183 et 184) pour activer les redirections de trames :

```
[privs]
ec_uid = 0 # nobody is the default
ec_gid = 0 # nobody is the default


redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport
%port -j REDIRECT --
to-port %rport"
redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport
%port -j REDIRECT --
to-port %rport"

redir6_command_on = "ip6tables -t nat -A PREROUTING -i %iface -p tcp --dport
%port -j REDIRECT --
to-port %rport"
redir6_command_off = "ip6tables -t nat -D PREROUTING -i %iface -p tcp --dport
%port -j REDIRECT --
to-port %rport"
```

Dans /etc/ettercap/etter.dns ,vous devez ajouter la section suivante :

```
#Spoofing DNS du site du BTS SIO
local.sio.fr  A  <IP-de-l'attaquant>
*.local.sio.fr  A  <IP-de-l'attaquant>
www.local.sio.fr  PTR  <IP-de-l'attaquant>
```

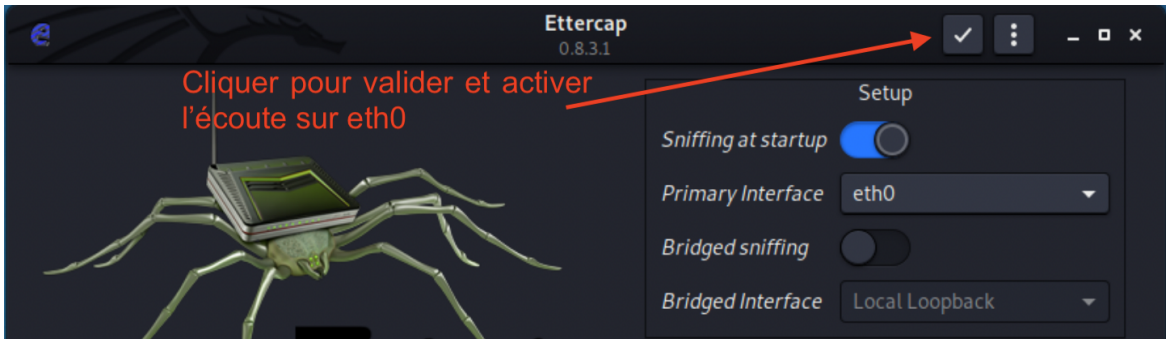
↗ Configurez ettercap sur l'attaquant Kali.

Configuration d'un arp poisoning via ettercap

La prochaine étape consiste à effectuer un positionnement MITM avec **Ettercap**. Cela a déjà été réalisé dans des activités précédentes en utilisant les lignes de commande.
Dans cette activité, nous allons utiliser la version graphique de **Ettercap**.

↗ Rappelez en quoi consiste une attaque ARP POISONING (ou ARP SPOOFING).

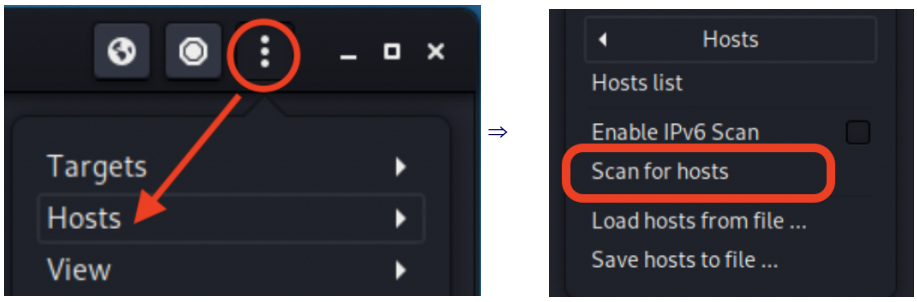
Lancez l'outil ettercap-graphical et vérifiez que l'interface d'écoute est bien eth0 :



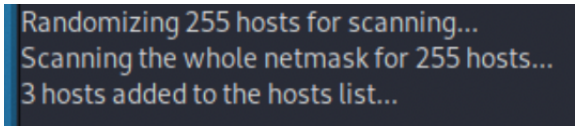
Vous devez obtenir l'affichage suivant :

Scannez le réseau.

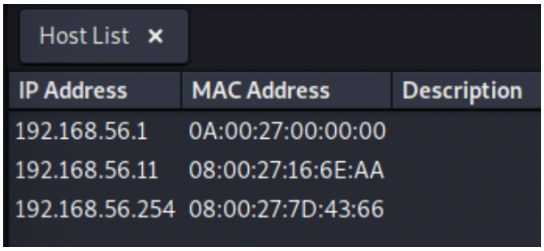
Il faut scanner le réseau afin de découvrir les hôtes disponibles. Pour cela, il faut cliquer sur le sous-menu « Scan for hosts » du menu « Hosts ».



3 hôtes devraient être scannés :



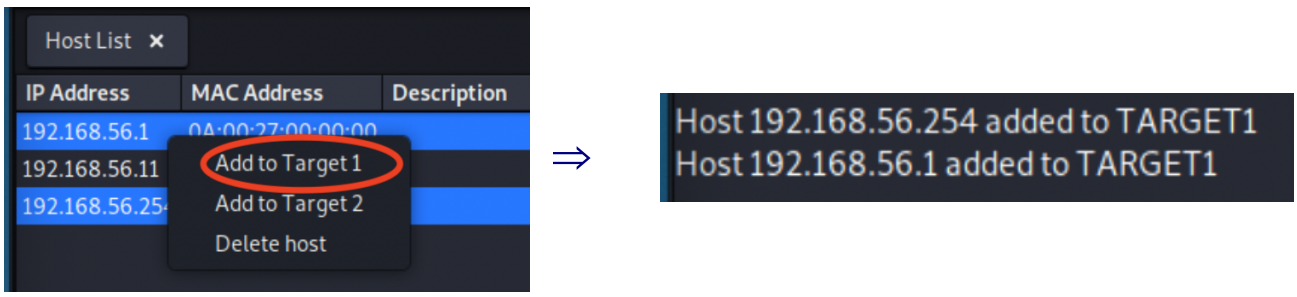
Pour afficher la liste des hôtes, il faut cliquer sur le sous-menu « Host List » du menu « Hosts » :



Deux cibles (« target ») doivent être définies :

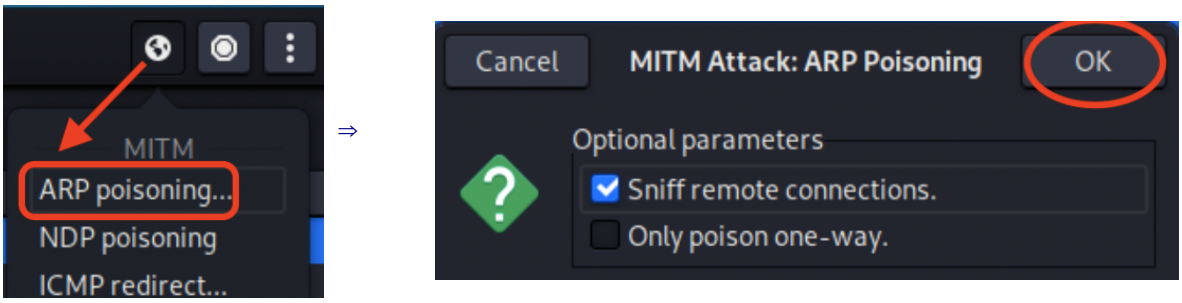
- la première correspond à la machine victime (192.168.56.1) ;
- la seconde correspond à la passerelle (192.168.56.254). C'est cette sélection qui permettra de réaliser le positionnement MITM. La passerelle correspond au routeur OpenBSD (machine virtuelle RouteurOpenBSD 2).

Pour cela, il faut sélectionner les 2 hôtes concernés, faire un clique droit et choisir « Add to Target1 » :

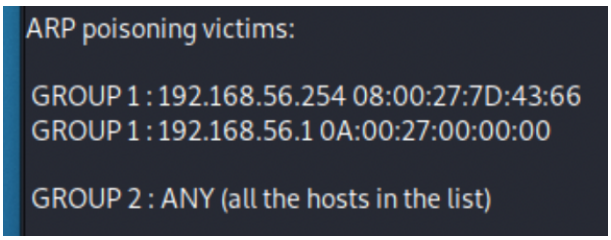


Lancez l'ARP Poisoning (empoisonnement de cache ARP).

Pour cela, il faut cliquer sur le sous-menu « ARP Poisoning » du sous-menu « Mitm » (icône « planete terre » en haut à droite), vérifier que l'option « Sniff remote connections » est activée et valider :

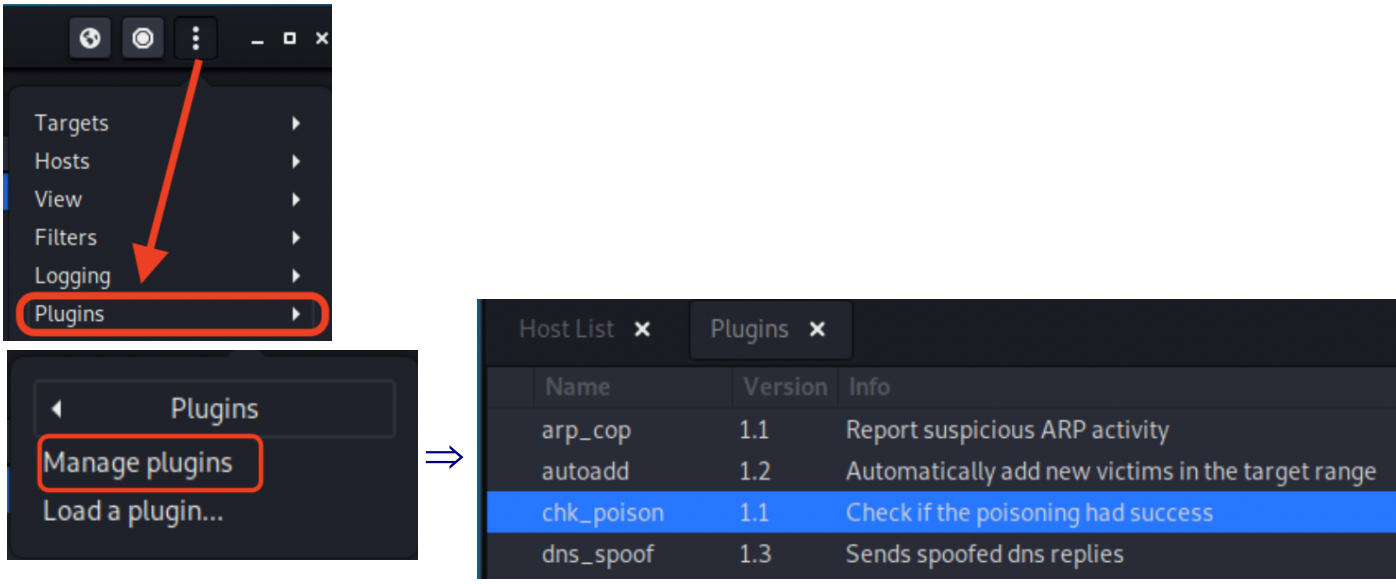


Vous devriez obtenir un affichage du type :

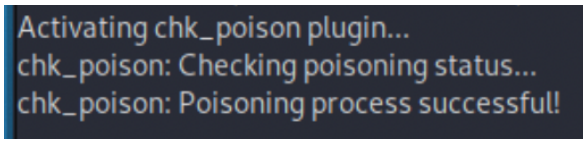


Le plugin « chk_poison » permet de vérifier le succès de l'empoisonnement.

Pour cela, il faut cliquer sur le sous-menu « Manage the plugins » du menu « Plugins ». Un double clic sur le plugin doit afficher un message confirmant le succès de l'opération :



Vous devriez obtenir un affichage du type :



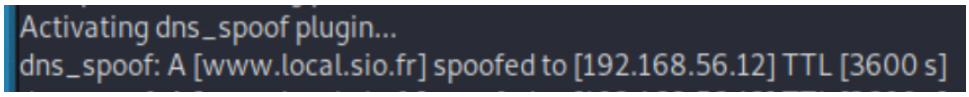
Vérifiez sur le client que la machine pirate est bien la passerelle du trafic.

Lancement de l'attaque DNS SPOOFING

Maintenant que le positionnement MITM est opérationnel, vous pouvez lancer le DNS SPOOFING.
Pour cela, il faut double cliquer sur le plugin « dns_spoof ».

↗ Lancez le plugin « dns_spoof ».

À partir de maintenant, lorsque la victime va consulter le site du BTS SIO (http://www.local.sio.fr), la requête va être automatiquement redirigée vers le site pirate, et des logs de ce type doivent s'afficher sur Ettercap :



↗ Visitez, à partir du client, le site du BTS SIO et vérifiez que le site pirate s'affiche.

Proposition de contre-mesures

Q1. Proposez des contre-mesures pour éviter ou pour limiter une telle attaque.