dns-spoofing

DNS Spoofing Attacks

```
MARK RODERICK SISR
```

🛡️ Définition de l’attaque DNS Spoofing

- **DNS Spoofing** (Domain Name System Spoofing, ou *usurpation DNS*) est une attaque qui consiste à **empoisonner les entrées d’un serveur DNS** afin de rediriger un utilisateur vers un site web malveillant contrôlé par l’attaquant.
- L’objectif est de tromper la victime en lui faisant croire qu’elle accède à un site légitime (banque, messagerie, réseau social…), alors qu’elle est en réalité sur une copie frauduleuse.

⚙️ Mécanisme de l’attaque

- L’attaquant modifie les **tables DNS** ou les **tables ARP** pour que la machine de la victime interroge un faux serveur DNS.
- Ce faux serveur renvoie une adresse IP frauduleuse correspondant au site piégé.
- L’utilisateur est alors redirigé sans s’en rendre compte vers une page contrôlée par l’attaquant.

Types DNS spoofing

- internet
- intranet
- proxy server
- dns cache poisoning*

⚙️ Phase 1 : Mise en place du « faux » serveur web (sur Kali)

Objectif : Configurer ta machine Kali pour accepter le trafic redirigé et afficher une page personnalisée.

Étapes

1. **Ouvrir un terminal** sur Kali.
2. **Démarrer le service Apache :**

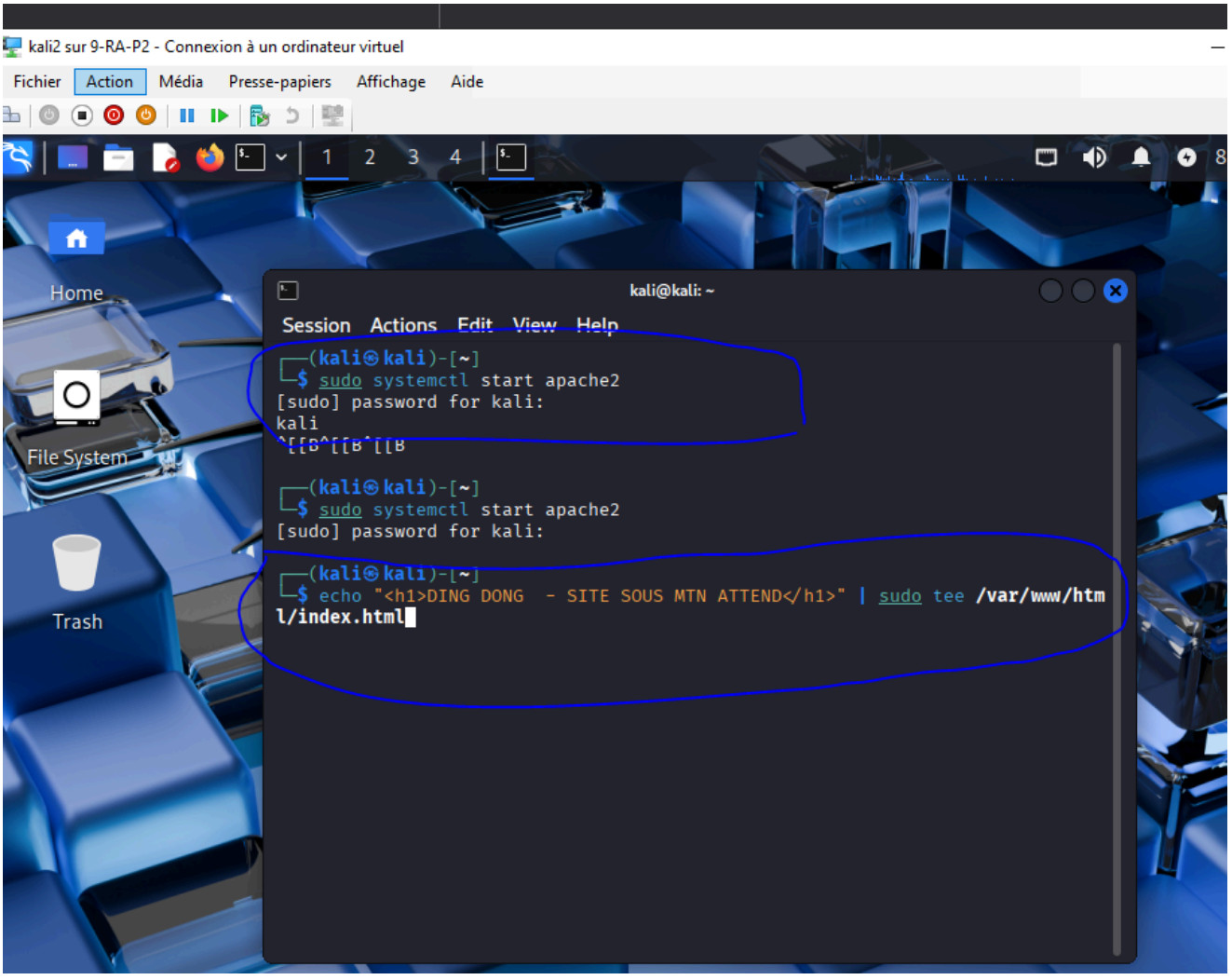
```
sudo systemctl start apache2
```

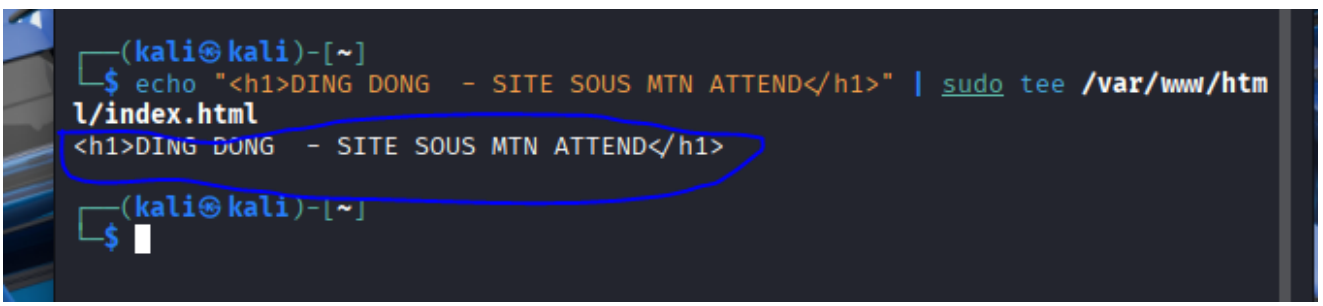
3. **Créer la page factice :**
   Cette commande remplace la page par défaut d'Apache par ton message personnalisé.

```
echo "<h1>DING DONG - SITE SOUS MTN ATTEND</h1>" | sudo tee
/var/www/html/index.html
```

🎯 Vérification

- Si l'utilisateur Windows redirigé voit le message **« SITE UNDER MAINTENANCE »**, cela prouve que la redirection DNS/ARP a fonctionné et que la session a bien été détournée dans le cadre du TP.



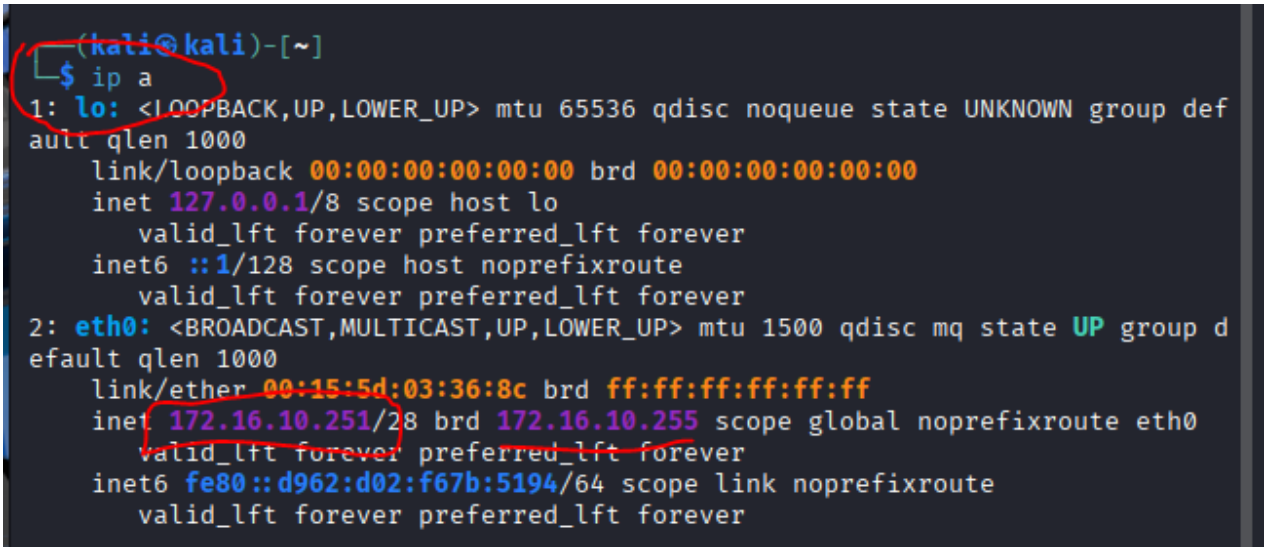


Phase 2: Configure & Execute the Attack (On Kali)

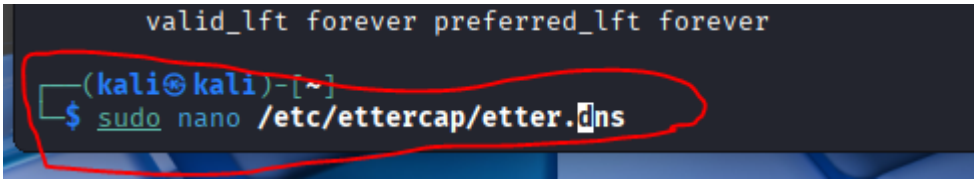
Now we configure **Ettercap** to redirect the specific domain to your Kali IP.

Step A: Configure the DNS File

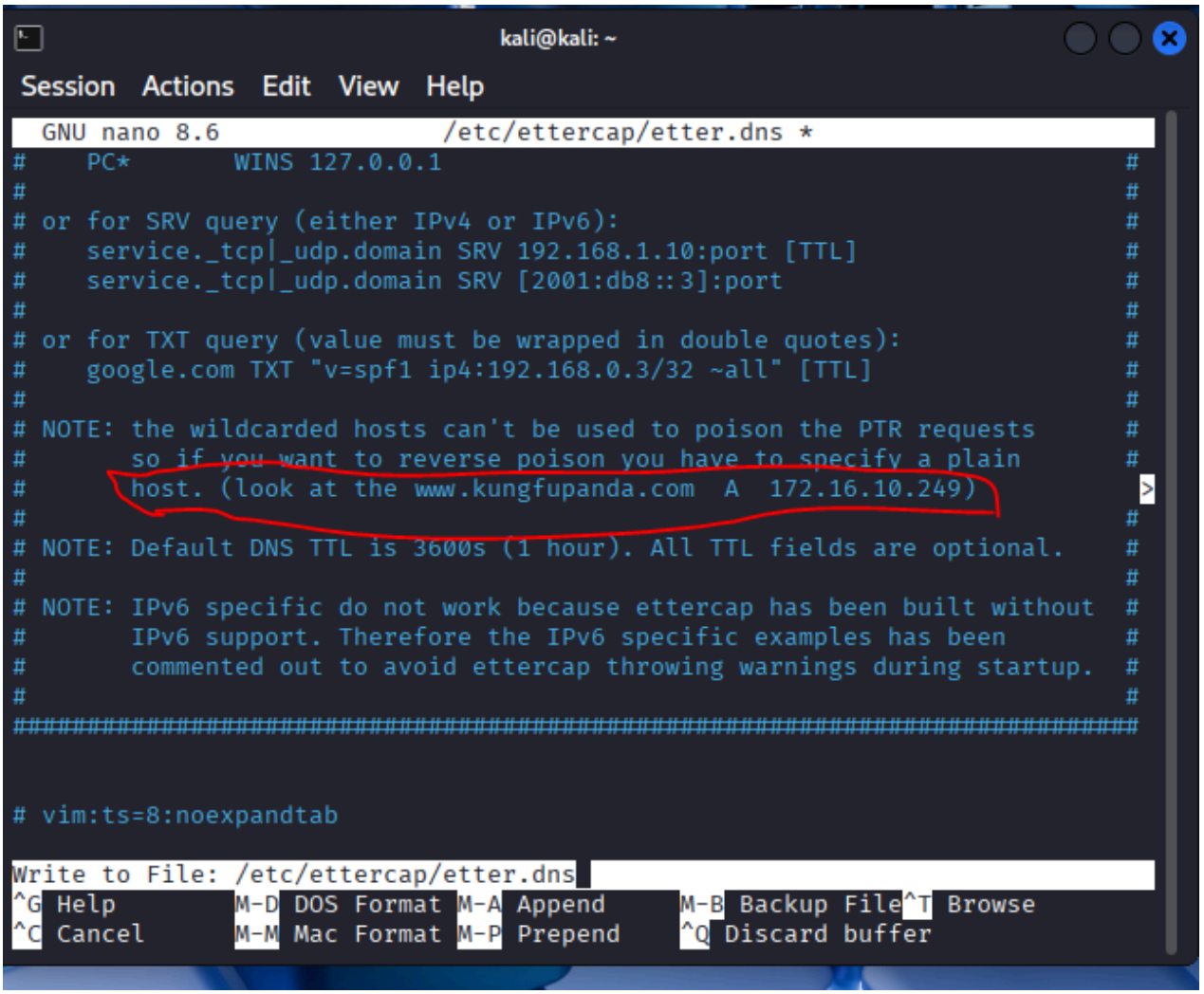
1. Find your Kali IP address:



2. Edit the Ettercap DNS config file:



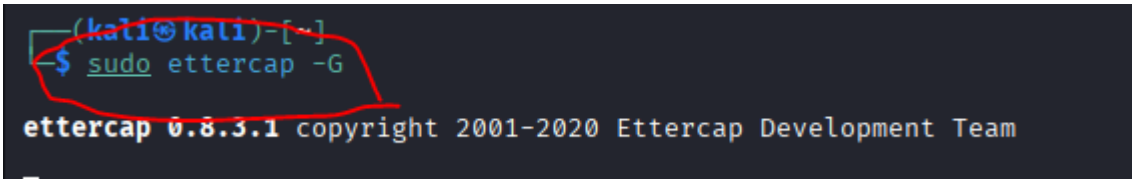
3. Scroll down to the section that looks like `microsoft.com`. Add a new line for your target website (e.g., xoxox or a simple HTTP site):



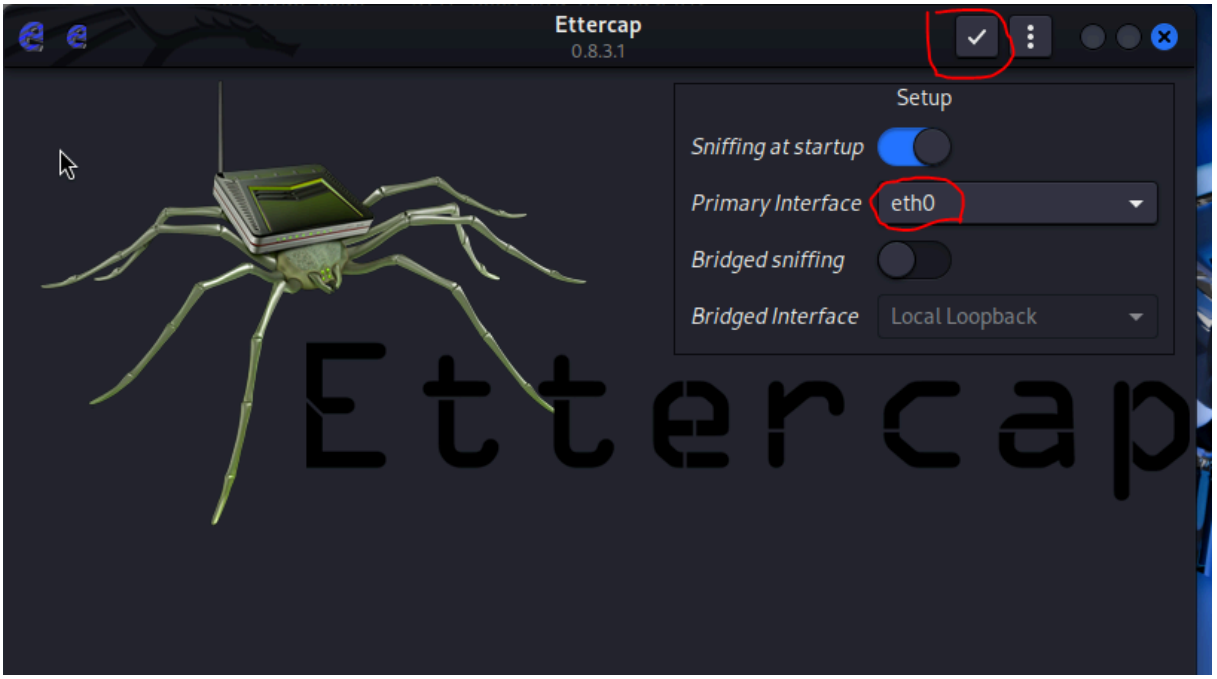
4. Save and exit (`Ctrl+O` , `Enter` , `Ctrl+X`).

Step B: Run Ettercap (GUI)

1. Launch Ettercap in graphical mode:

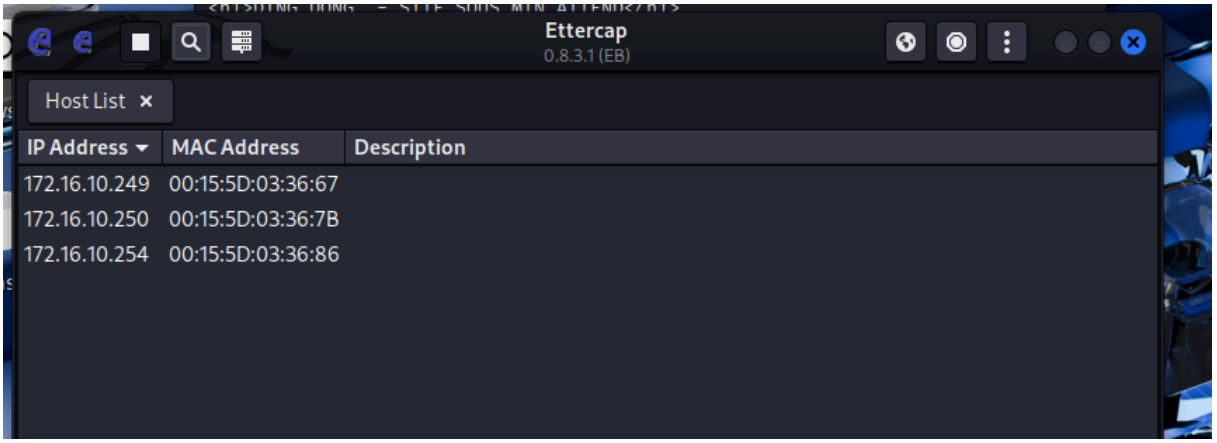


2. **Start Sniffing:**
   - In the setup screen, ensure your primary interface (usually `eth0`) is selected.

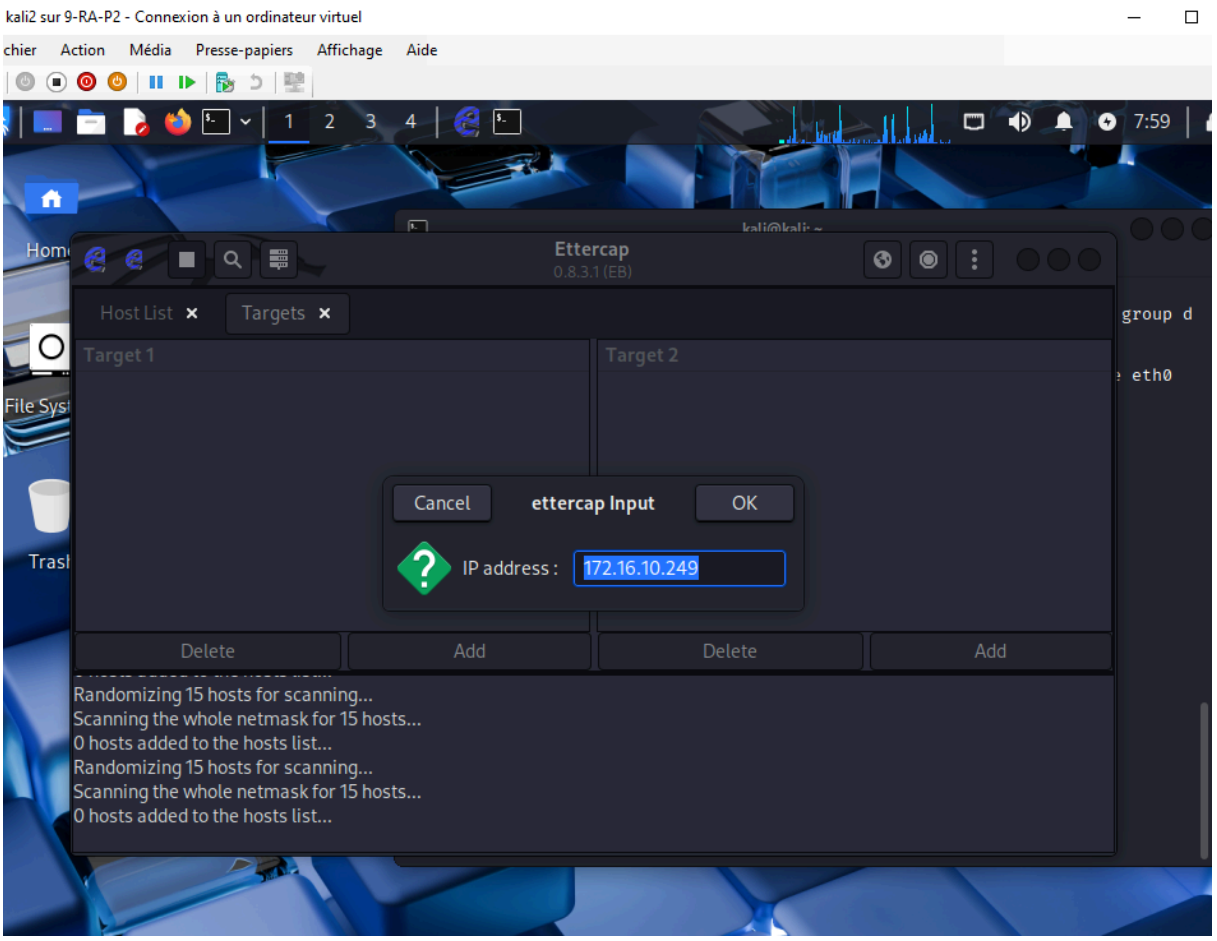


   - Click the **Accept (✔)** button in the top right.

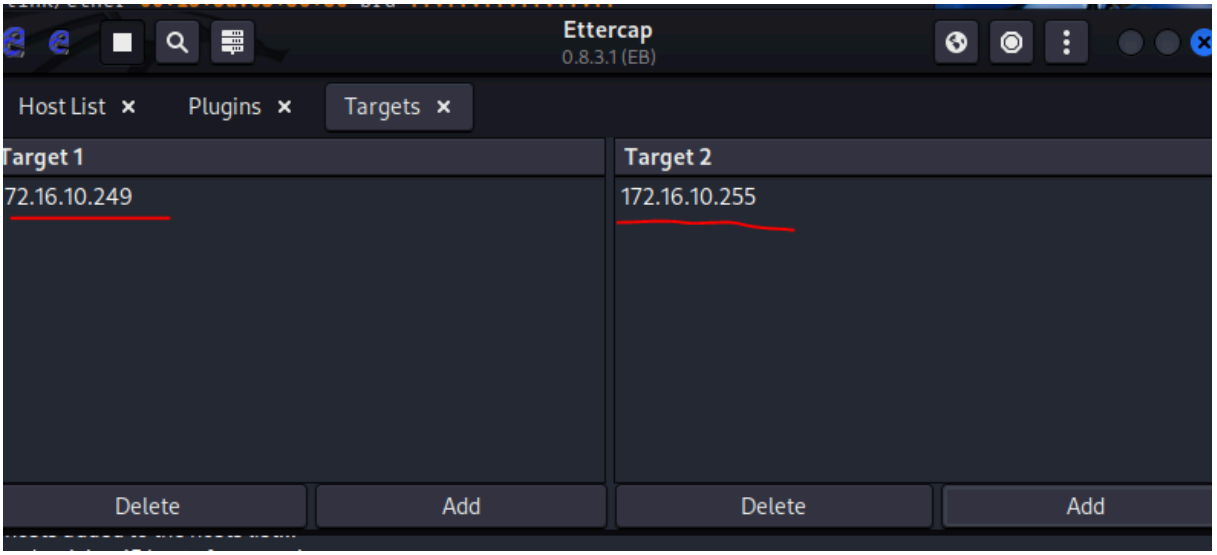
3. **Scan for Victims:**
   - Click the **Search Icon** (magnifying glass) or go to **Hosts** > **Scan for Hosts**.
   - After the scan finishes, click the **List Icon** (next to the magnifying glass) to see the Host List.



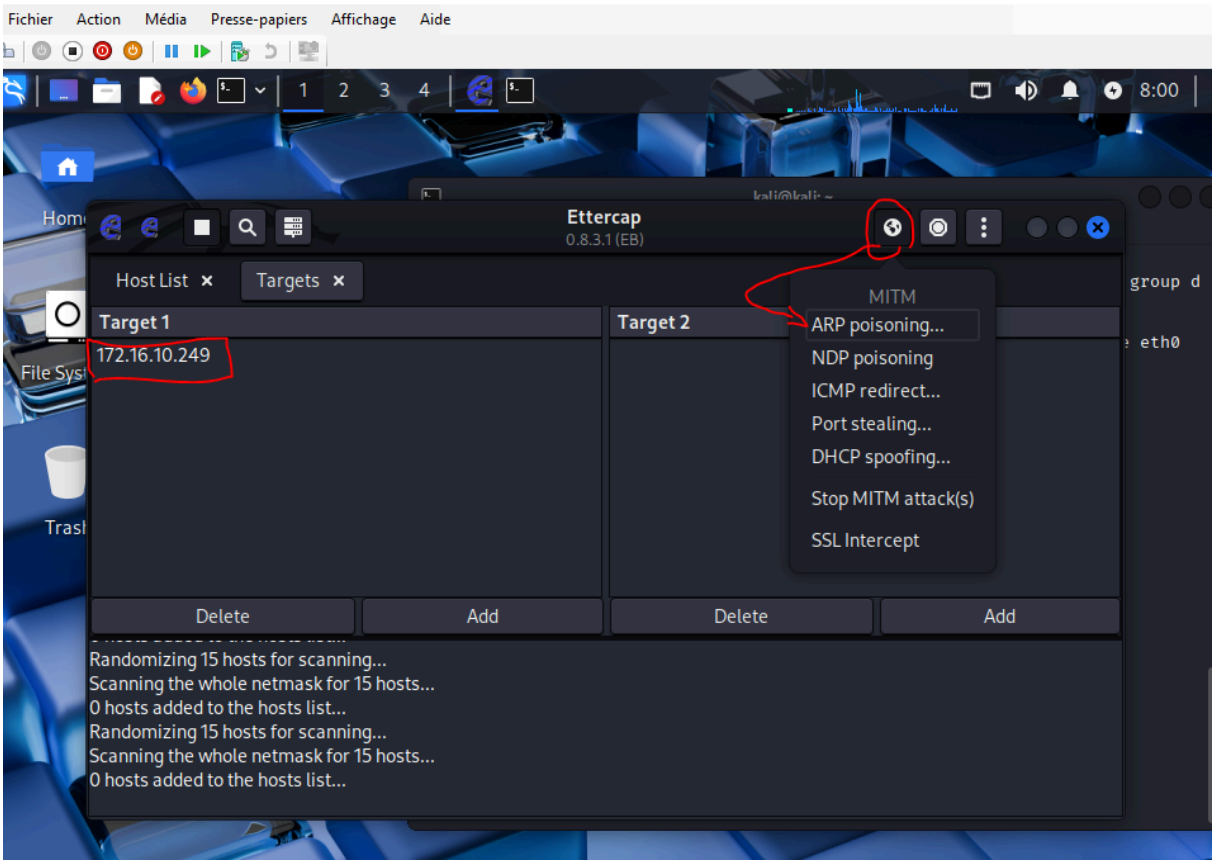
4. **Set Targets:**
   - Select the debian IP **-> Click** Add to Target 1**.



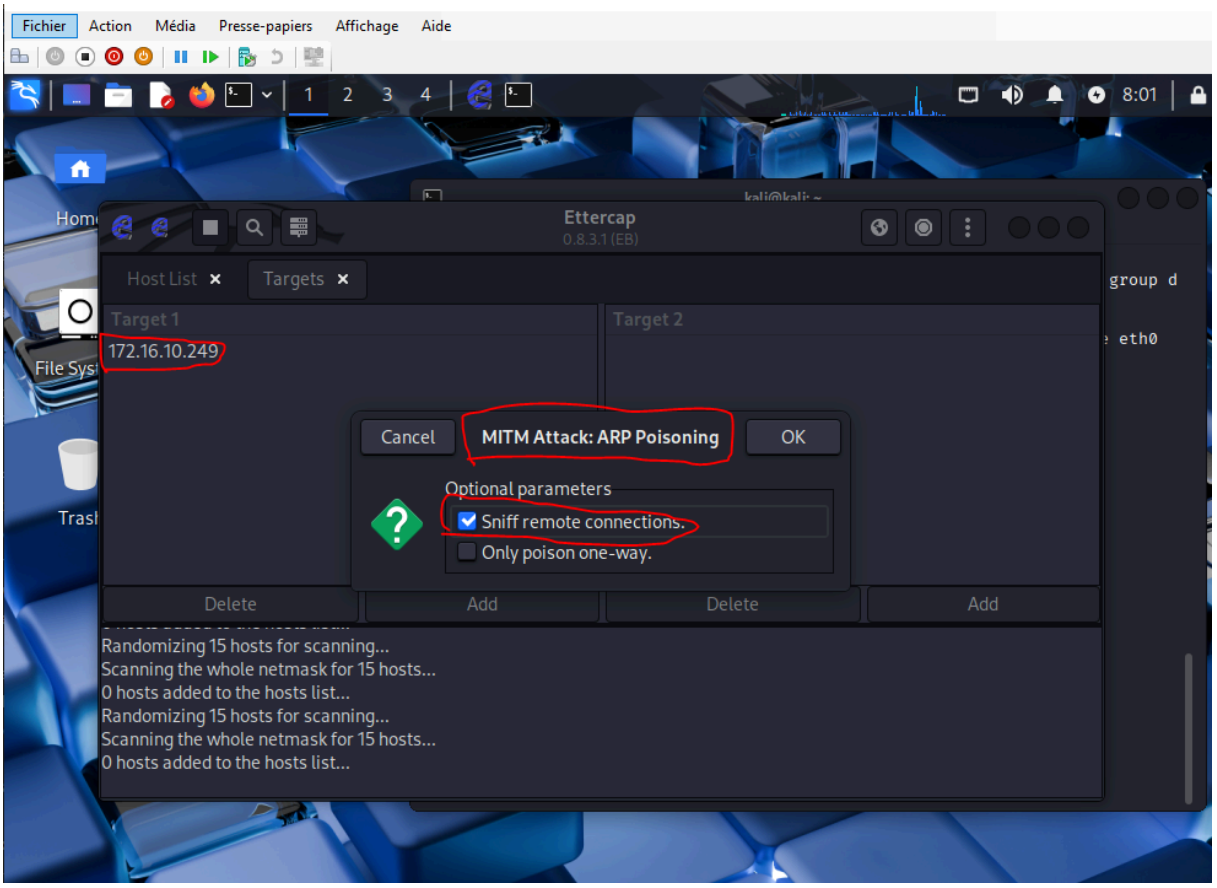
- Select the **Gateway/Router IP** -> Click **Add to Target 2**.



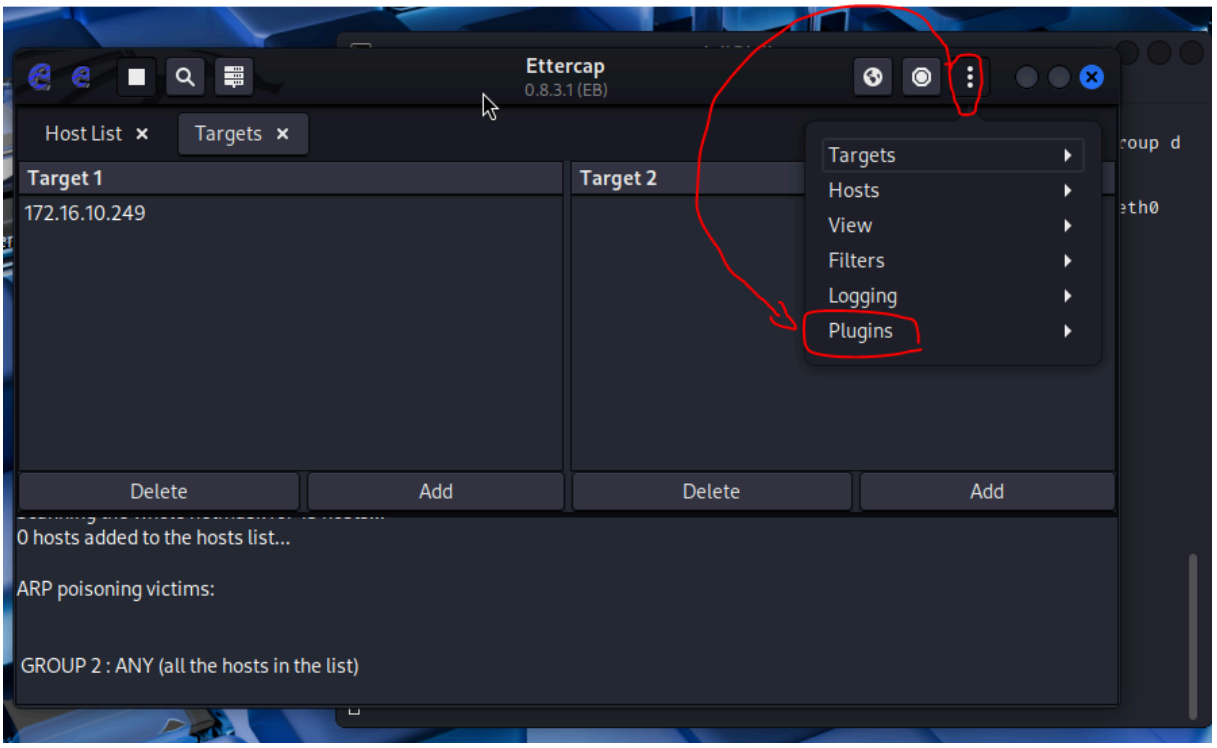
5. **Start ARP Poisoning (Man-in-the-Middle):**
   - Click the **MITM Menu** (icon looks like a planet/network) -> Select **ARP Poisoning**.

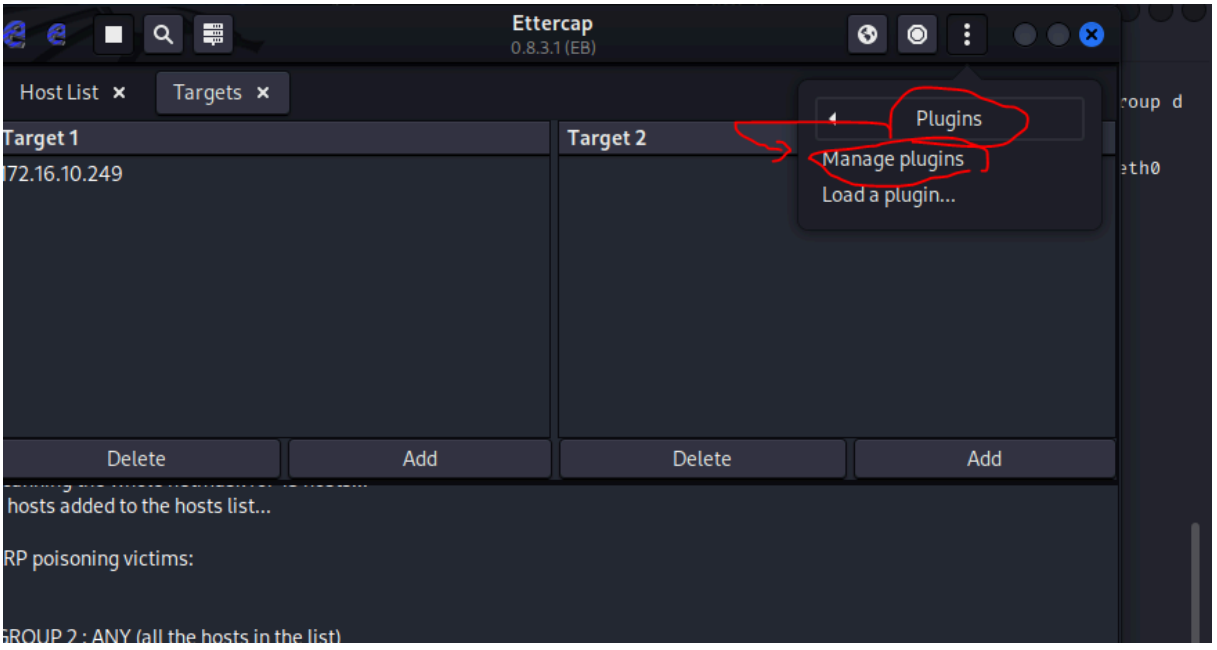


- Check the box **"Sniff remote connections"** and click **OK**.

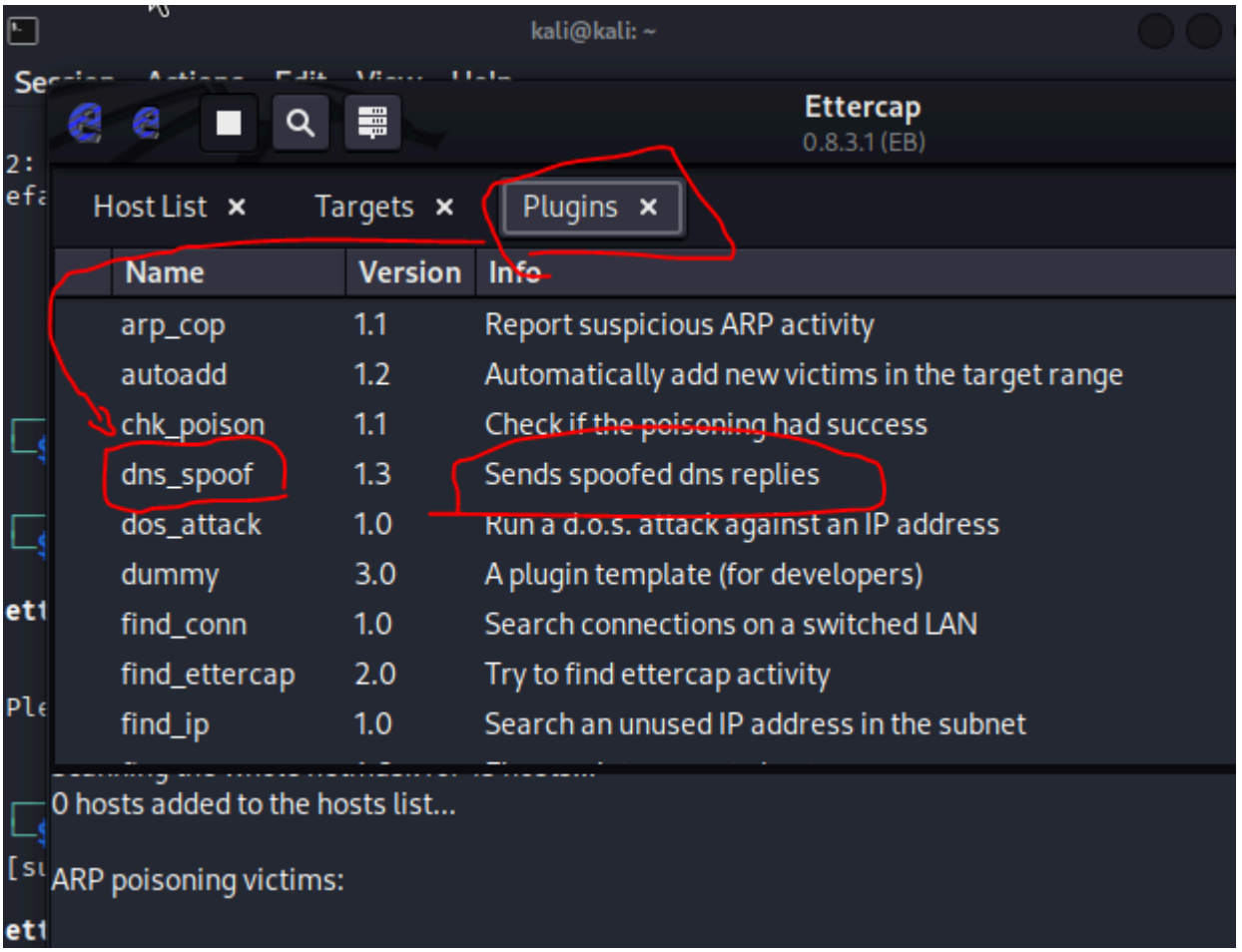


6. **Activate DNS Spoofing:**
   - Click the **3-Dots Menu** (top right) -> **Plugins** -> **Manage Plugins**.

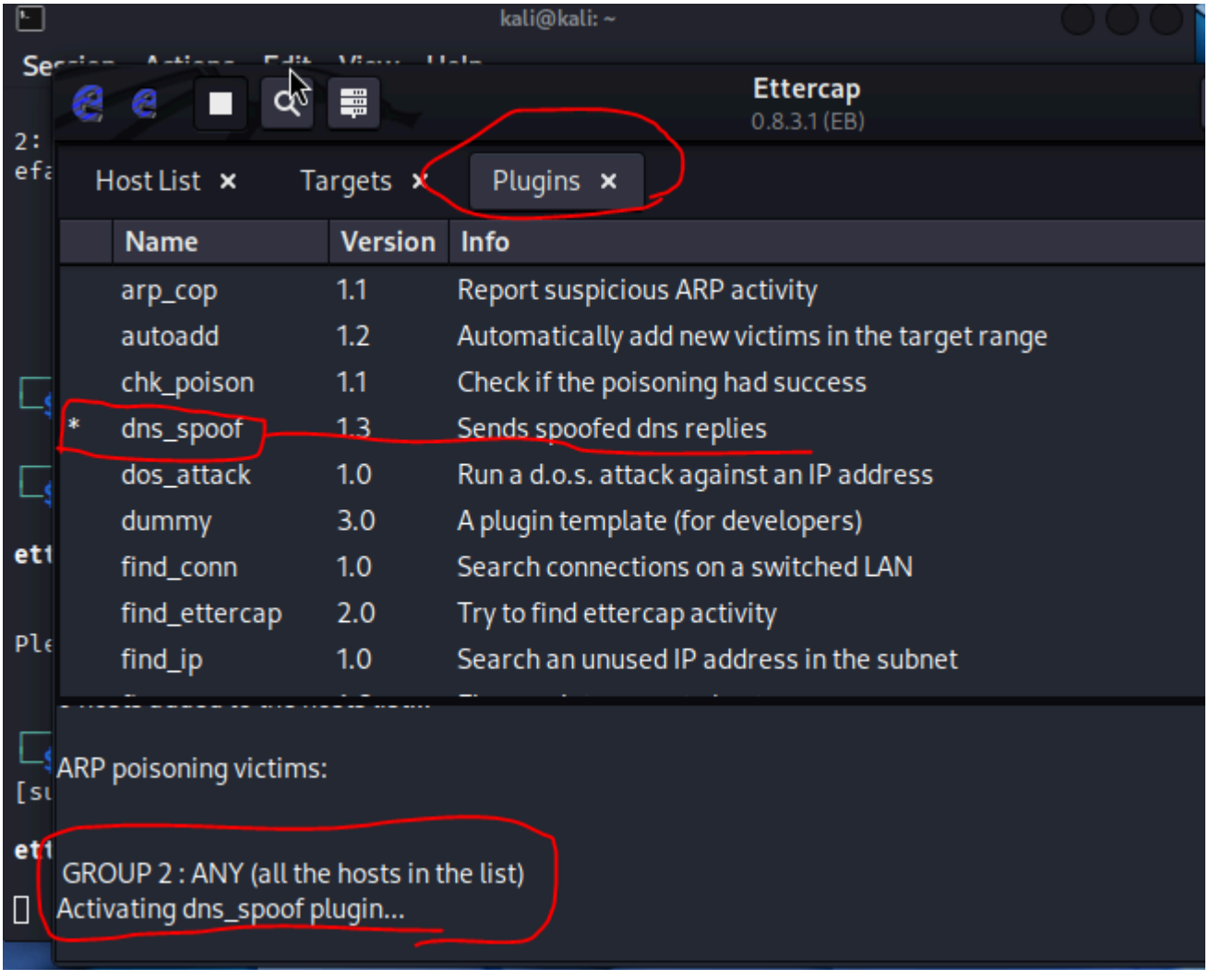




- Find `dns_spoof` in the list.
- **Double-click it**. You must see a small `*` (asterisk) appear next to it. This means it is ACTIVE.



doucle click dns_spoof



Phase 2: Victim Validation (Debian VM)

Goal: Prove the attack is working using the Debian terminal.

Since the victim is now Debian, you cannot use `ipconfig`. Use these Linux-specific commands instead.

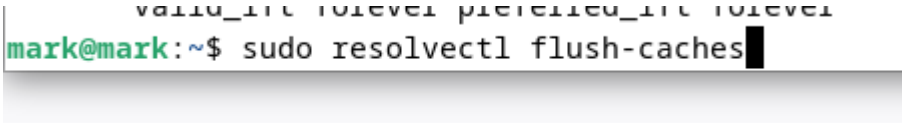
1. Flush DNS Cache (Debian)

Linux does not always cache DNS the same way Windows does. If you need to force a refresh:

Bash

```
# For modern Debian (using systemd-resolved):
sudo resolvectl flush-caches

# OR simply restart the networking service:
sudo systemctl restart networking
```



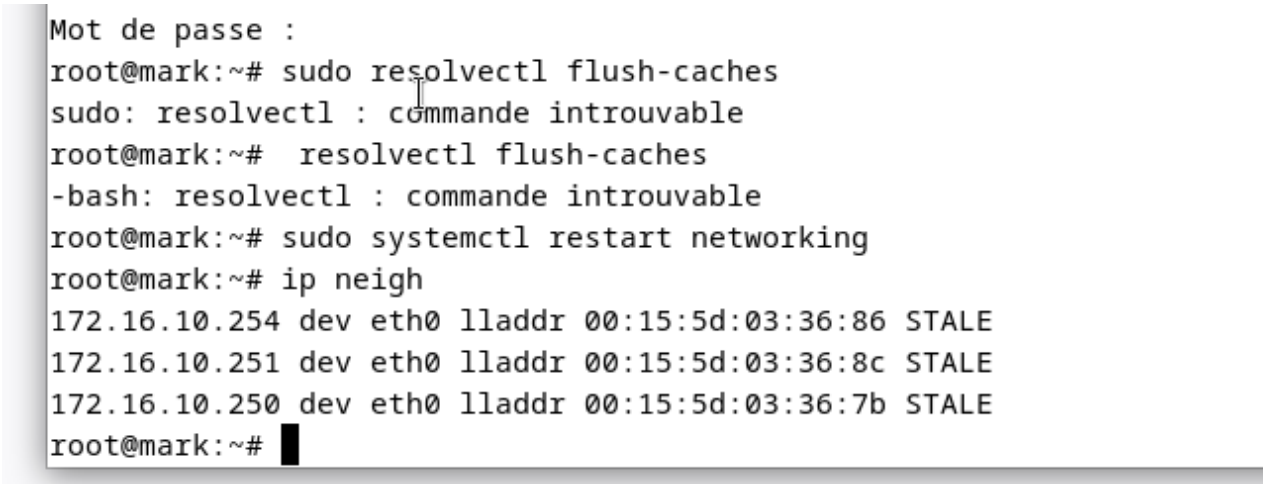
2. Verify ARP Poisoning (The "Man-in-the-Middle")

Check if the Gateway's MAC address has changed to the Kali MAC address.

Bash

```
# Show the ARP table (Neighbors)
ip neigh
```

- *Look for the Gateway IP.* The MAC address listed next to it should now match your **Kali machine's MAC address**.



DEUXIEME ESSAY

```
mark@mark:~$ su -
Mot de passe :
root@mark:~# sudo systemctl restart restart
Failed to restart restart.service: Unit restart.service not found.
root@mark:~# sudo systemctl restart restart networking
Failed to restart restart.service: Unit restart.service not found.
root@mark:~# sudo resolvectl flush-caches
sudo: resolvectl : commande introuvable
root@mark:~# resolvectl flush-caches
-bash: resolvectl : commande introuvable
root@mark:~# sudo systemctl restart networking
root@mark:~# ip neigh
172.16.10.251 dev eth0 lladdr 00:15:5d:03:36:8c STALE
172.16.10.250 dev eth0 lladdr 00:15:5d:03:36:8c REACHABLE
172.16.10.254 dev eth0 lladdr 00:15:5d:03:36:8c REACHABLE
root@mark:~#
```

3. Vérification du DNS Spoofing

Objectif : Vérifier où Debian pense que le domaine `www.kungfupanda.com` est situé.

Commande Bash

```
# Envoyer 4 paquets ICMP vers le site
ping -c 4 www.kungfupanda.com
```

```
root@mark:~# ping -c 4 www.kungfupanda.com
PING kungfupanda.com (44.232.96.25) 56(84) bytes of data.

--- kungfupanda.com ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3080ms

root@mark:~#
```

Interprétation des résultats

- **Succès :** L'adresse IP renvoyée dans la réponse doit être **l'IP de ta machine Kali** (celle de l'attaquant dans le scénario), et non l'adresse IP réelle du site sur Internet.

4. Vérification de la page Web

Objectif : Tester directement dans le terminal si la redirection DNS est effective, sans ouvrir de navigateur.

Commande Bash

```
# Récupérer le contenu de la page web
```

```
curl http://www.kungfupanda.com
```

Interprétation des résultats

- **Succès :** Le terminal doit afficher :

  ```
  <h1>DING DONG - SITE SOUS MTN ATTEND</h1>
  ```

⚠️ Note importante concernant Firefox (Debian)

Si vous utilisez le navigateur **Firefox** sur Debian pour tester, il se peut que cela échoue même si les commandes dans le terminal fonctionnent.

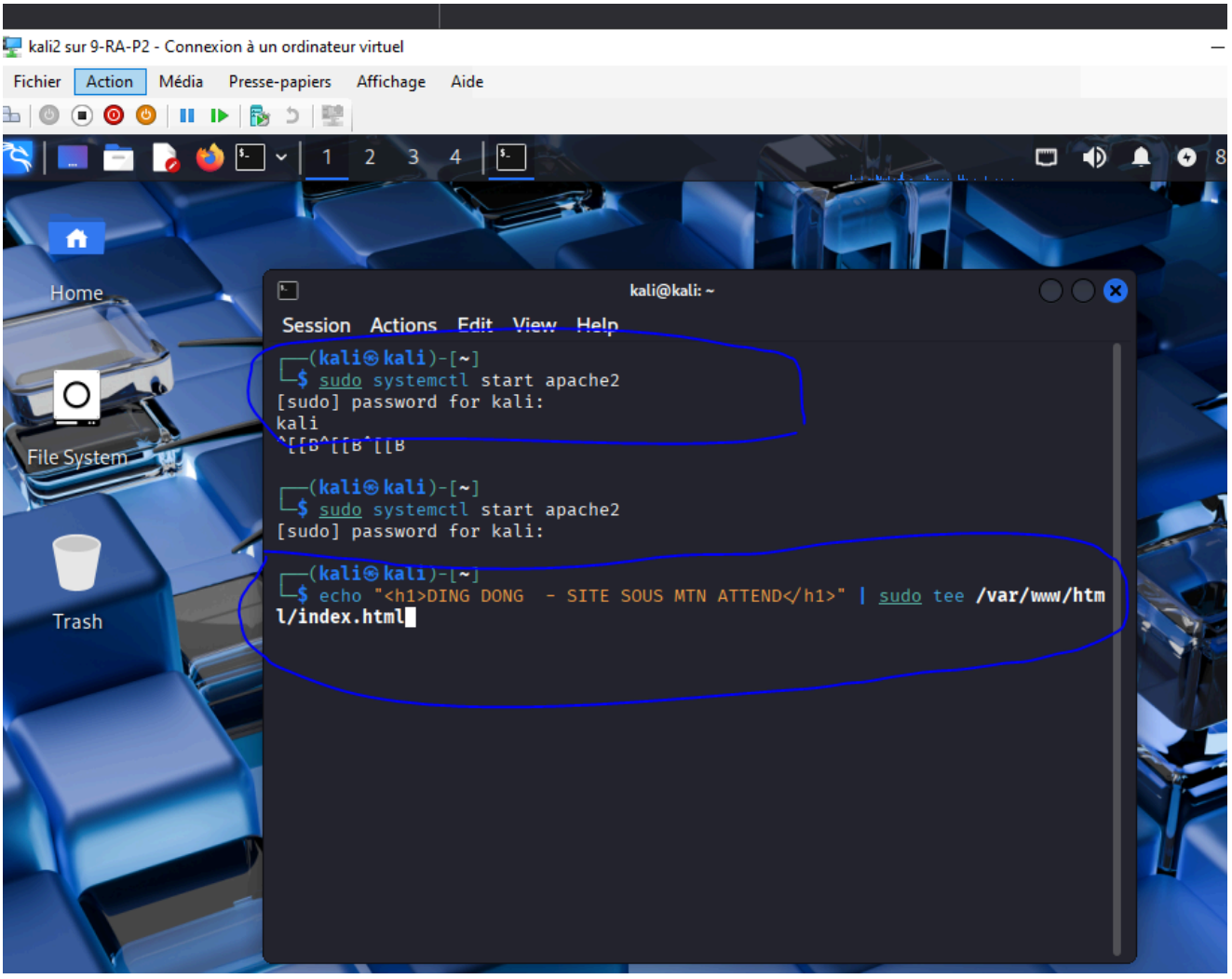
- **Pourquoi :** Firefox utilise souvent le mécanisme **DNS over HTTPS (DoH)**, qui contourne les paramètres DNS locaux (et donc votre attaque).
- **Solution :** Dans Firefox → Paramètres → Paramètres réseau → **désactivez** l'option « *Activer DNS over HTTPS* » afin que le test fonctionne correctement dans le cadre du laboratoire.

🎥 Ressource pédagogique

Une vidéo explicative montre les mécanismes de l'**ARP poisoning** de manière visuelle, ce qui aide à comprendre pourquoi la table `ip neigh` change pendant la simulation.

How ARP Poisoning Works // Man-in-the-Middle

tp



Classement au niveau de gravité et vraisemblance

- ***Gravité : Élevée à Critique (niveau 3–4)***
  - Parce que l'attaque peut mener au vol de données sensibles (mots de passe, informations bancaires) et à l'installation de malwares.
  - Dans un contexte professionnel ou institutionnel, l'impact est critique.
- ***Vraisemblance : Moyenne (niveau 2–3)***
  - L'attaque est techniquement réalisable, surtout sur des réseaux Wi-Fi publics ou mal sécurisés.
  - Elle demande toutefois un certain niveau de compétence (ARP poisoning, configuration d'un faux serveur DNS).
  - Dans un environnement bien protégé (DNSSEC, VPN, surveillance réseau), la probabilité est plus faible.

🛡️ Mesures techniques pour les administrateurs

- **Activer DNSSEC (Domain Name System Security Extensions)** : ajoute une signature cryptographique aux enregistrements DNS pour garantir leur authenticité.
- **Surveiller les réseaux internes** : détecter les anomalies dans les tables ARP ou les résolutions DNS.

- **Configurer correctement les serveurs DNS** : limiter les mises à jour non autorisées et appliquer des règles de sécurité strictes.
- **Utiliser des solutions de sécurité réseau** : pare-feu, IDS/IPS (systèmes de détection/prévention d'intrusion) pour repérer les attaques.

La protection repose sur **la vigilance des utilisateurs** (ne pas se laisser piéger par un faux site) et sur **des mécanismes techniques** comme DNSSEC qui empêchent la falsification des enregistrements DNS.

88888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888

ACTIVER HHTPS ON KALI
To simulate an HTTPS site, you need to enable the **SSL module** on your Kali Apache server and create a **self-signed certificate**. This is necessary because modern browsers on your Debian client will automatically try to upgrade `google.com` or `facebook.com` to a secure connection.

1. Enable HTTPS on Kali

Run these commands in your Kali terminal to set up the secure server:

1. Enable the SSL Module:

   sudo a2enmod ssl
2. Activate the Default SSL Site:

   sudo a2ensite default-ssl
3. Restart Apache to apply changes:

   sudo systemctl restart apache2

Now, your Apache server is listening on both **Port 80 (HTTP)** and **Port 443 (HTTPS)**.

---

2. Update your HTML for both ports

Apache uses different directories or configurations for HTTP and HTTPS by default. To ensure your "Maintenance" page shows up on both, verify your file is in the correct place:

- Ensure your code is in `/var/www/html/index.html` .
- The default SSL configuration usually points to the same folder.

---

3. Testing on the Debian Machine

When you visit a spoofed site like `https://google.com` from the Debian client:

1. **The Certificate Warning:** The browser will show a "Your connection is not private" warning. This is **normal** in a simulation.
2. **Why?** Because your Kali machine is providing a "self-signed" certificate that isn't officially verified by Google.
3. **Action:** Click **Advanced** and then **Proceed to [site] (unsafe)**. You will then see your "DING DONG" maintenance page over a secure (HTTPS) connection.

---

4. Summary of Common Simulation Sites

Here are the simple `.com` sites you can add to your `/etc/ettercap/etter.dns` file to test this:

Site	Record Type	Kali IP
google.com	A	172.16.10.250
bing.com	A	172.16.10.250
example.com	A	172.16.10.250
test.com	A	172.16.10.250

> **Note**
>
> Ensure your Kali IP matches the one in your ip neigh output (e.g., 172.16.10.250).

Would you like me to show you how to check the Apache error logs on Kali if the page doesn't load at all on the Debian side?