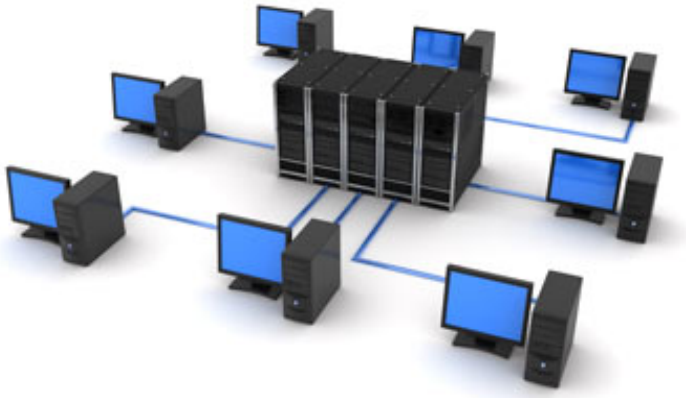
MAN IN THE MIDDLE



Man in the middle **consiste en capturar la información intercambiada entre cliente y servidor ilegítimamente**

1.

INTRODUCCIÓN

INTRODUCCIÓN

- Man In The Middle captura y reenvía la comunicación de forma transparente
- Uso de ARP Spoofing para la realización del ataque
- Servidor <-> Atacante <-> Cliente

2.

ARP PROTOCOL

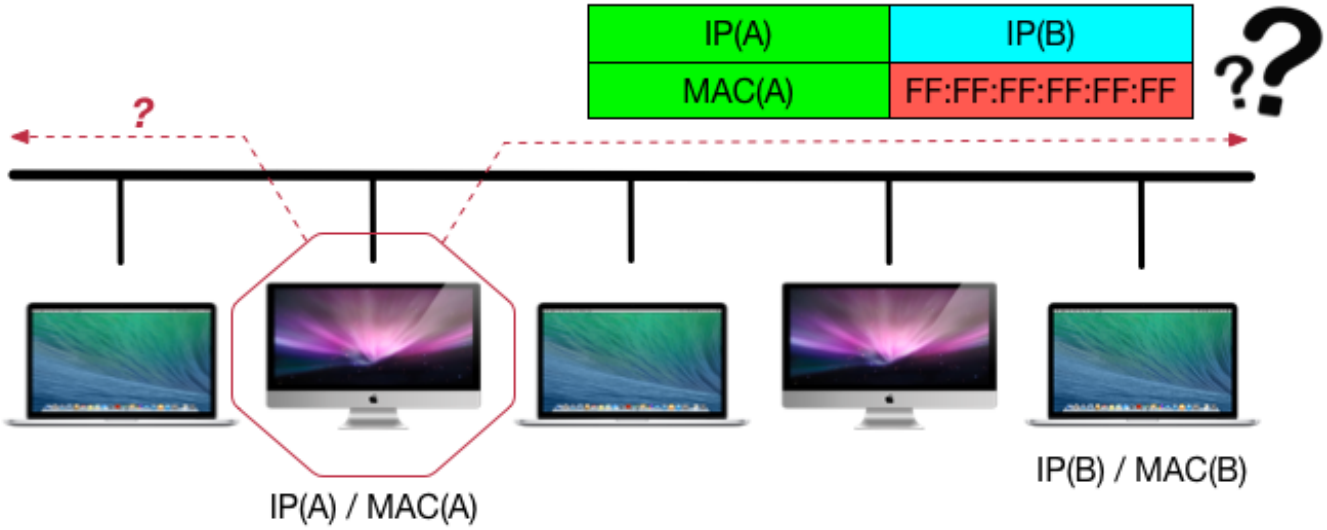
PROTOCOLO ARP

- Su objetivo es conocer la MAC correspondiente a una dirección IP
- Tabla *"caché ARP"* para almacenarlas

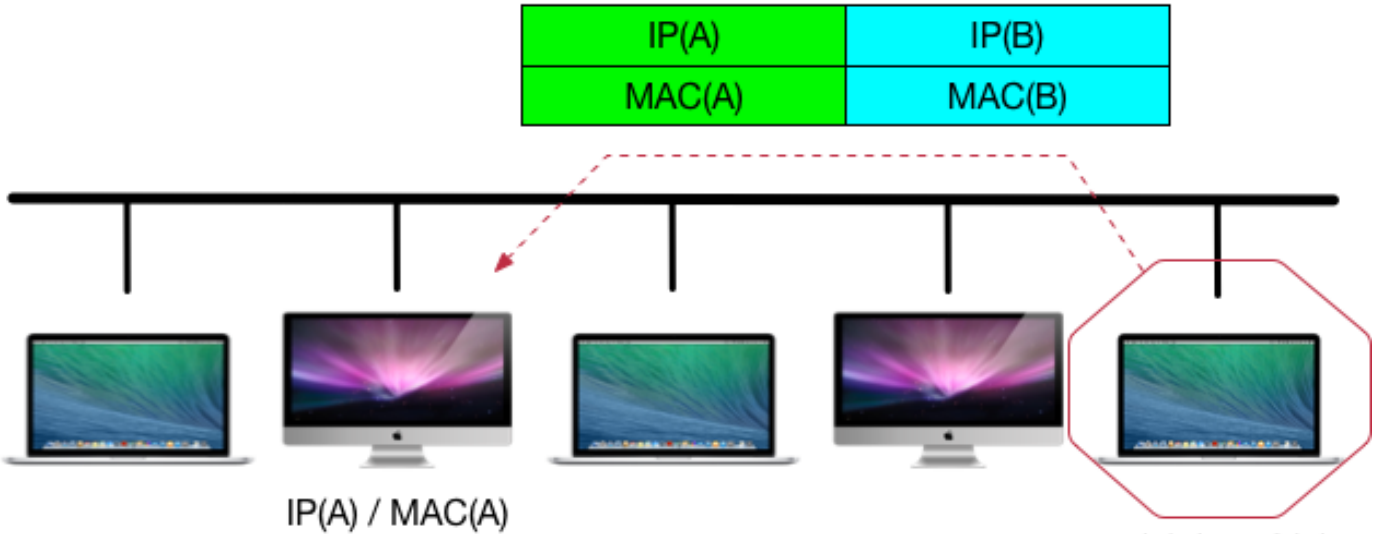
INTERNET ADDRESS	*PHYSICAL ADDRESS*
192.168.1.1	00-1B-57-C1-6E-B4
192.168.1.255	FF-FF-FF-FF-FF-FF
192.168.1.25	00-11-43-DE-91-15
…	…

ARP REQUEST

- Difusión: ***FF:FF:FF:FF:FF:FF***



ARP REPLY



3.

ARP SPOOFING

ENVENENAMIENTO ARP

CLIENTE
172.16.1.130

MAC 1

MAC 2

SERVIDOR
172.16.1.129

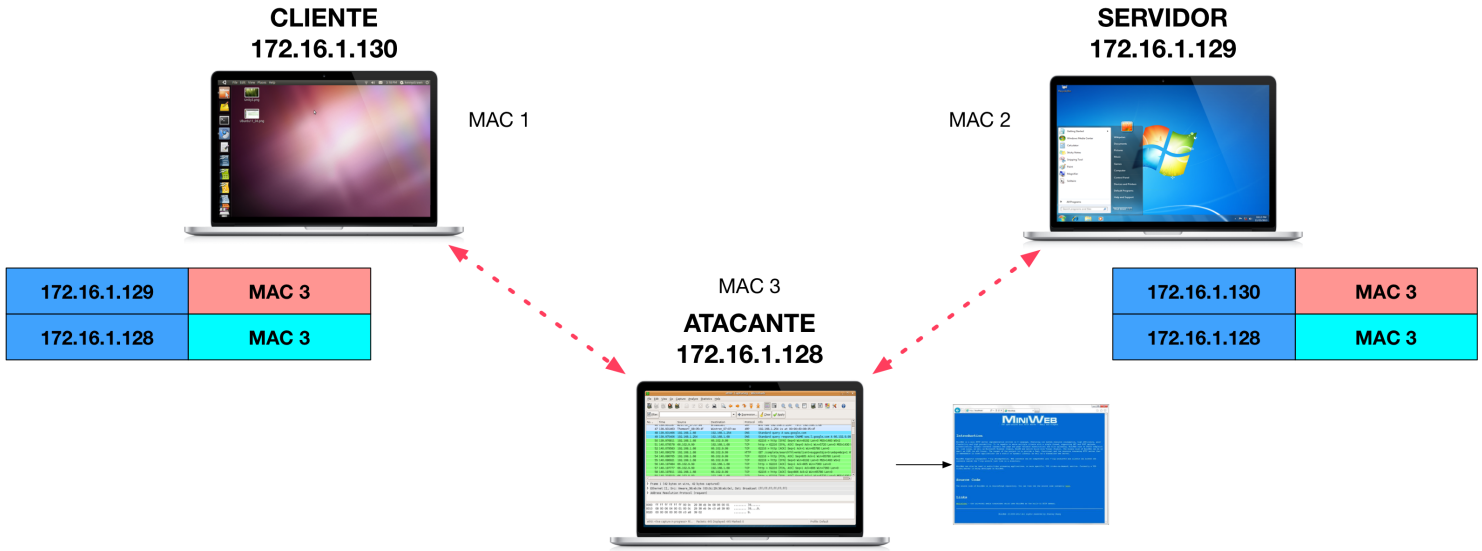
172.16.1.129	MAC 2
172.16.1.128	MAC 3

172.16.1.130	MAC 1
172.16.1.128	MAC 3

MAC 3

ATACANTE
172.16.1.128

ENVENENAMIENTO ARP



4.

PREVENCIÓN

DHCP-SNOOPING

Para protegerse de este ataque se usará *DHCP-snooping* que asocia ***interfaz-MAC-IP-VLAN*** sobre puertos fiables.

- Con ARP-protect contrastará los *arp* que escucha con la tabla y el conmutador se encargará de autorizar o bloquear el tráfico.
- Se configura el rango de direcciones para asignar las IPs
- Una vez tienen las IPs, se activará la protección con:

  # arp-protect validate ip

  # arp-protect vlan 1

DHCP-SNOOPING