Mininet

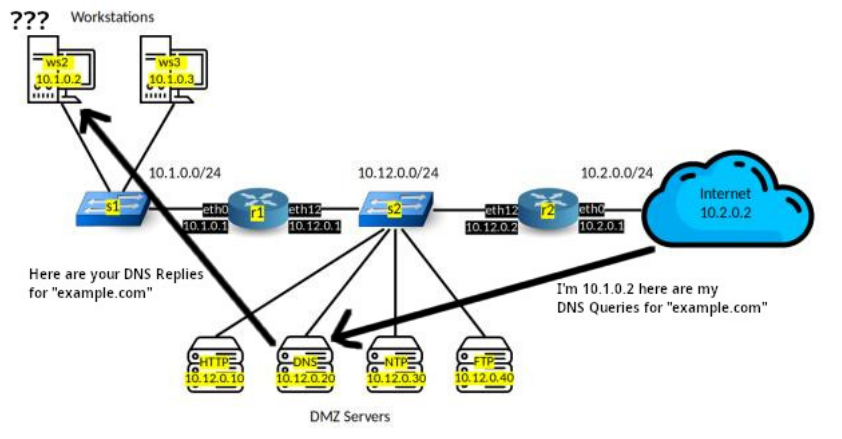
Manuel Dias

16/05/2025

UCLouvain

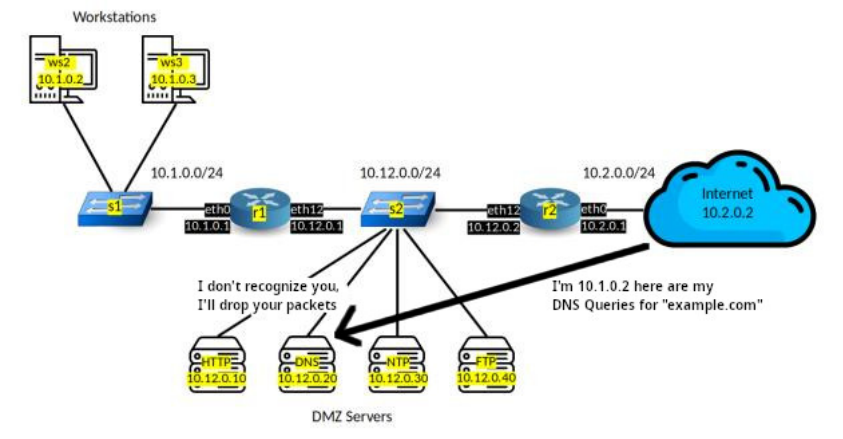
Dns Reflection

Attack



- Send Dns Requests in the name of the victim
- DNS Server processes and sends response to the victim
- Victim is overloaded with Traffic becoming Unavailable

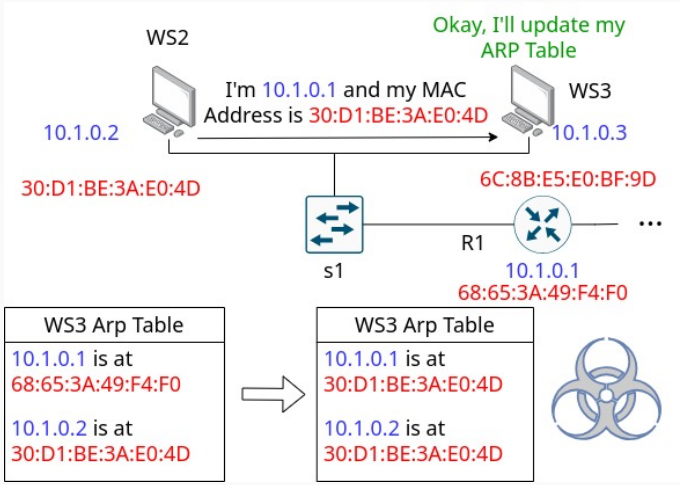
Defense



- Send Dns Requests in the name of the victim
- DNS Server doesn't recognize the source of the request meaning it's spoofed so it
- Drops the packet

Arp Poisoning

Attack

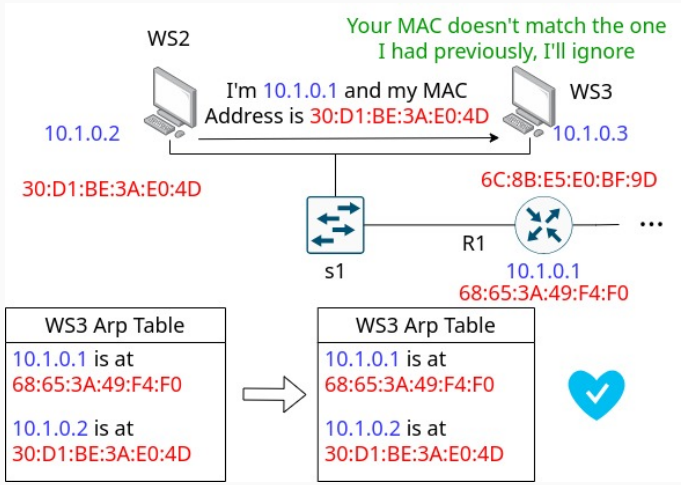


Send Spoofed ARP packet saying that our MAC Address matches the Default Gateway's

Victim Updates it's ARP Table with wrong MAC Address

Attacker receiver all the traffic coming out of Victim

Defense



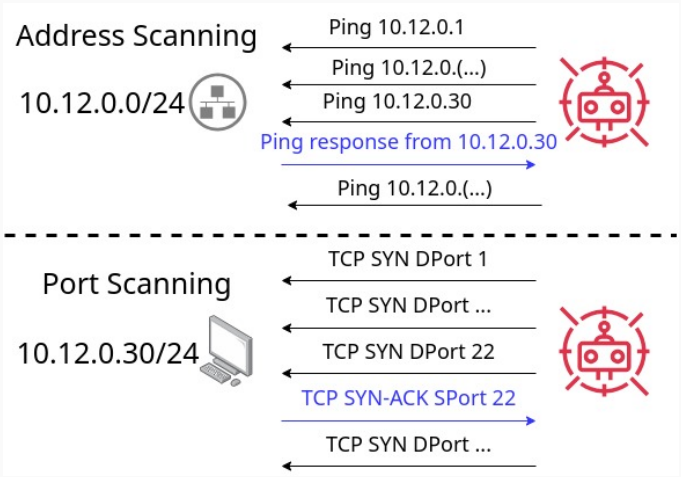
Send Spoofed ARP packet saying that our MAC Address matches the Default Gateway's

Victim checks it's ARP Table for changes in the MAC

Ignores the ARP Change request

Network Scan

Attack

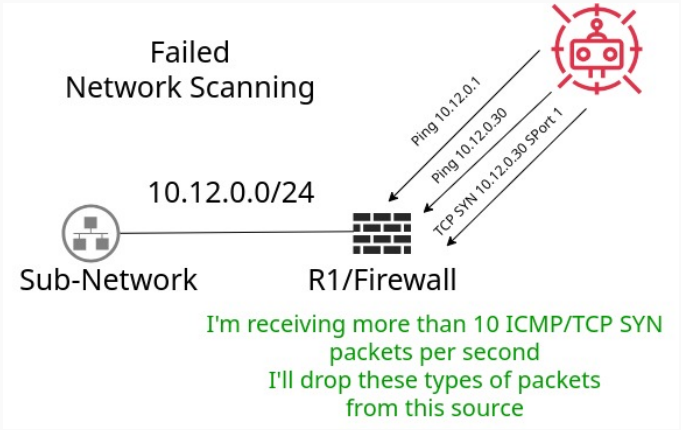


Send ICMP Requests to all the addresses of a given sub-domain

Send TCP SYN packets to all of the found Hosts that responded

Save the addresses and their open ports

Defense



Send ICMP Requests/TCP SYN Packets to all the addresses of a given sub-domain

Firewall sees that the amount of these type of packets that were received surpasses the threshold so it drops