Mininet

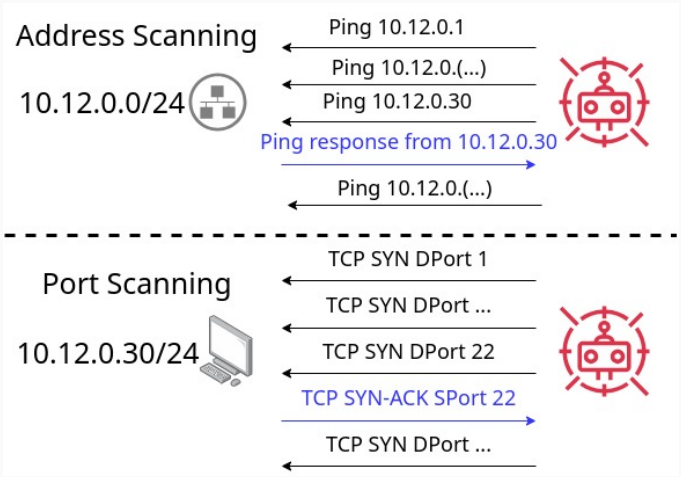
Manuel Dias Group 38

16/05/2025

UCLouvain

Network Scan

Attack

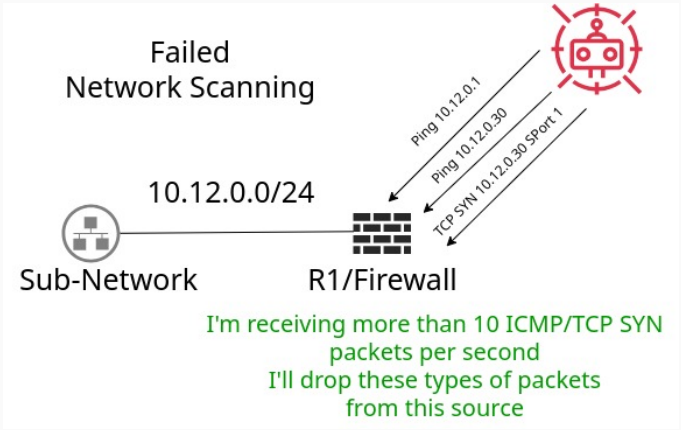


Send ICMP Requests to all the addresses of a given sub-domain

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

Save the addresses and their open ports

Defense

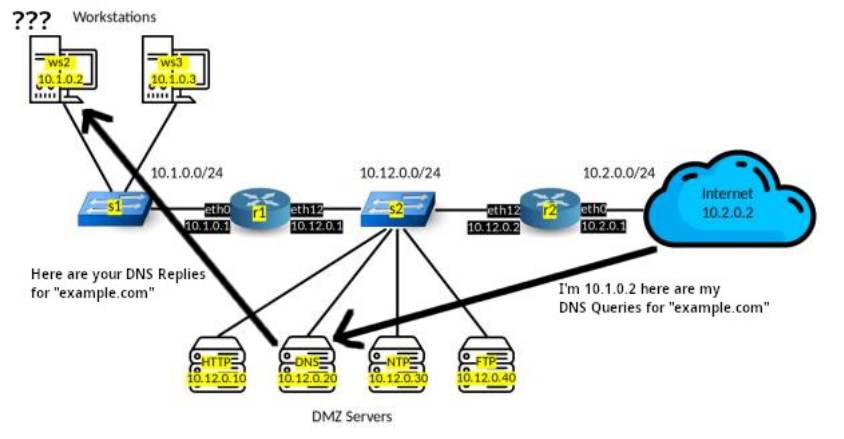


Send ICMP Requests/TCP SYN Packets to all the addresses of a given sub-domain

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

Dns Reflection

Attack

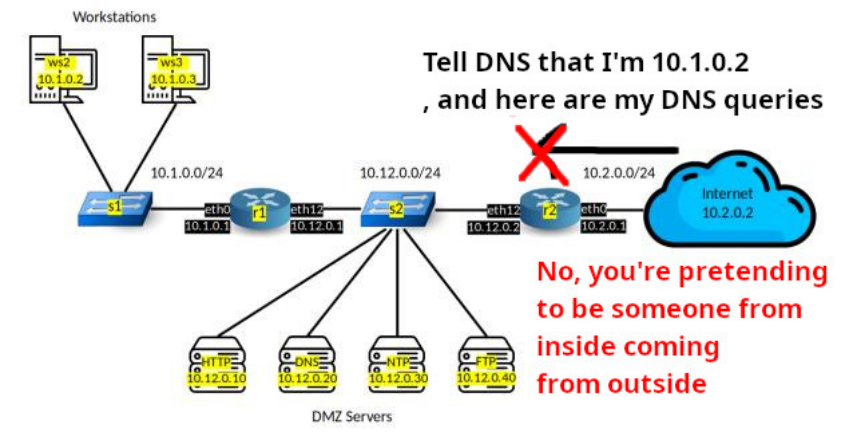


Send Dns Requests in the name of the victim

DNS Server processes and sends response to the victim

Victim is overloaded with Traffic becoming Unavailable

Defense



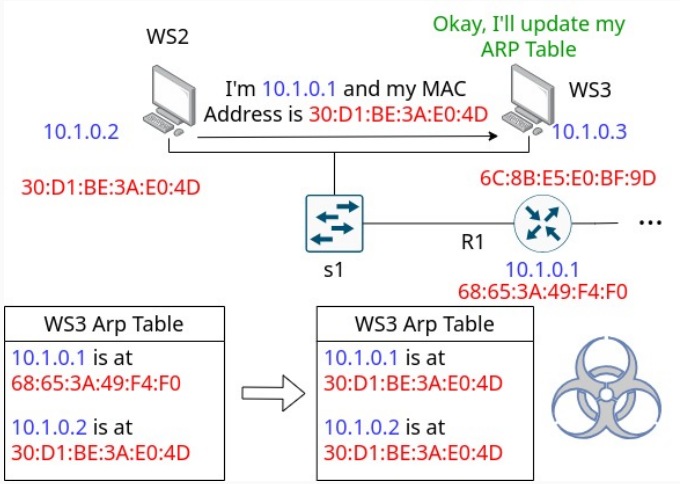
Send Dns Requests in the name of the victim

R2 Blocks outside traffic coming from spoofed internal IP's

R1 sets a limit rate for DNS Responses

Arp Poisoning

Attack

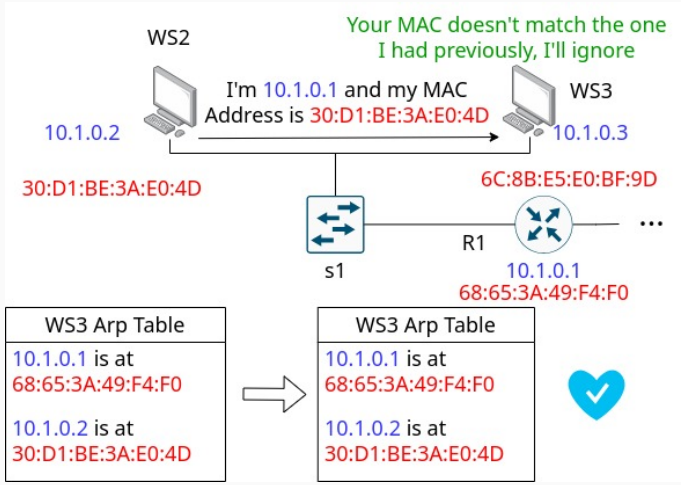


Send Spoofed ARP packet saying that our MAC Address matches the Default Gateway's

Victim Updates it's ARP Table with wrong MAC Address

Attacker receiver all the traffic coming out of Victim

Defense



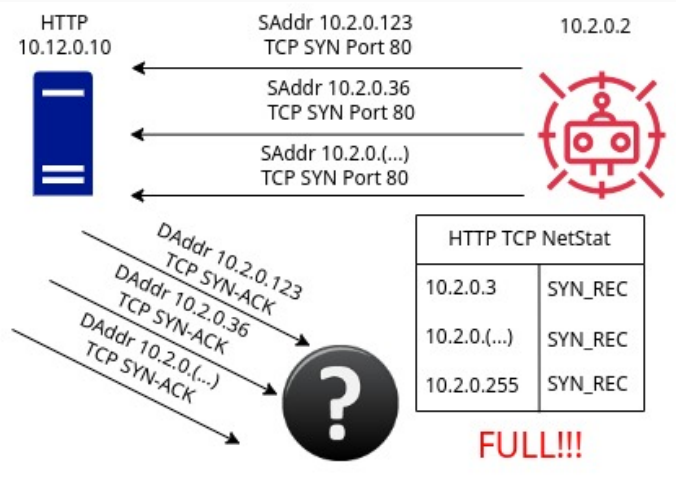
Send Spoofed ARP packet saying that our MAC Address matches the Default Gateway's

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

Ignores the ARP Change request

Syn Flooding

Attack

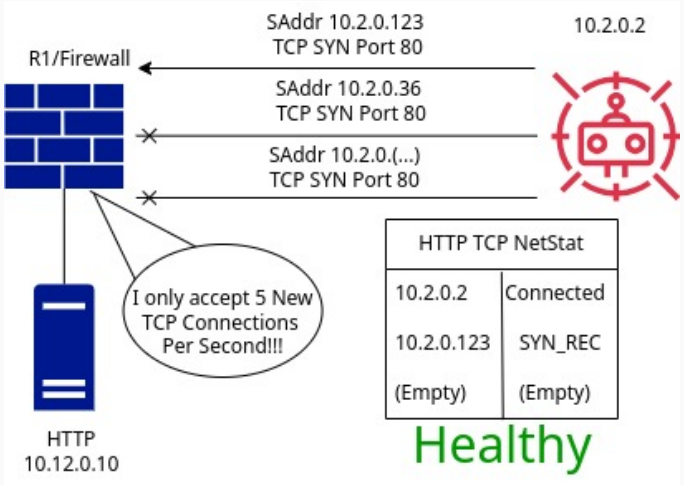


Send spoofed TCP SYN packets to a victim's open port

Victim adds the tcp connections

Victim sends SYN-ACKS that will never get be answered leaving the connections table full

Defense



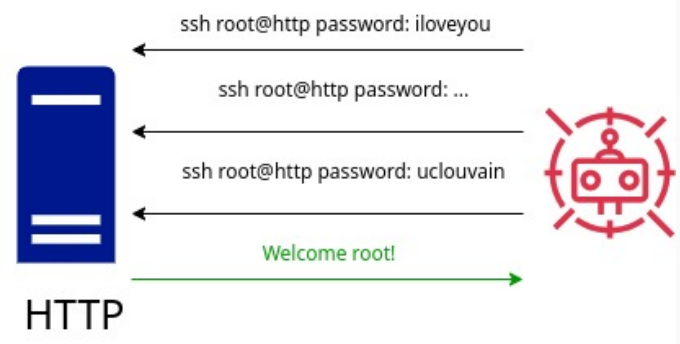
Send spoofed TCP SYN packets to a victim's open port

Firewall sets a limit of 5 new TCP Connections per second

Victim might send unanswerable SYN-ACKS but not enough to block new legitimate connections

SSH Bruteforce

Attack

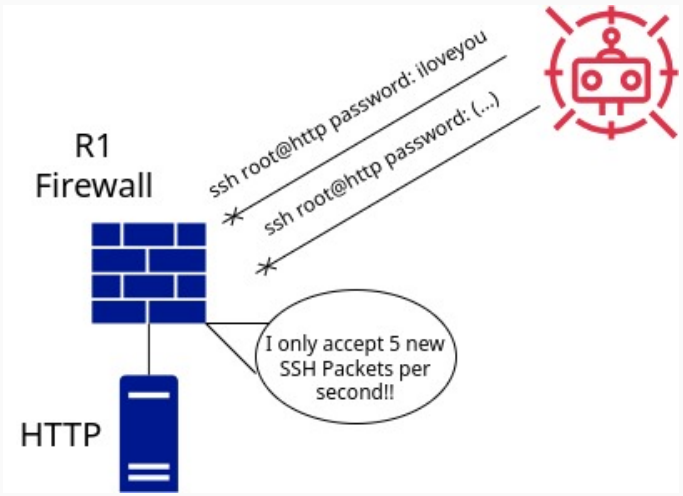


Try to ssh login with every password in a list

Eventually find correct credentials

Login and profit

Defense



Try to ssh login with every password in a list

Firewall blocks the attempt because it surpasses the threshold