Man-in-the-Middle

Objective: The goal of this lab is to perform a DHCP starvation attack using the tool Yersinia and introduce a rogue DHCP server. The attack works by sending a large number of DHCP requests to the legitimate DHCP server, quickly using up all available IP addresses in its pool. Once the DHCP server that was configured on the router can no longer assign IPs, a rogue DHCP server is created to respond to new client requests. This rogue server assigns IP addresses and sets network configurations allowing it to intercept and potentially control network traffic. This lab helps demonstrate how attackers can exploit weaknesses in DHCP to gain access to or interfere with network communications.

Abstract: This lab demonstrates a DHCP starvation attack using Yersinia and setting up a rogue DHCP server to intercept client traffic. To prevent this DHCP snooping is configured on the network switch, blocking rapid unauthorized DHCP responses and protecting the integrity of IP address assignment.

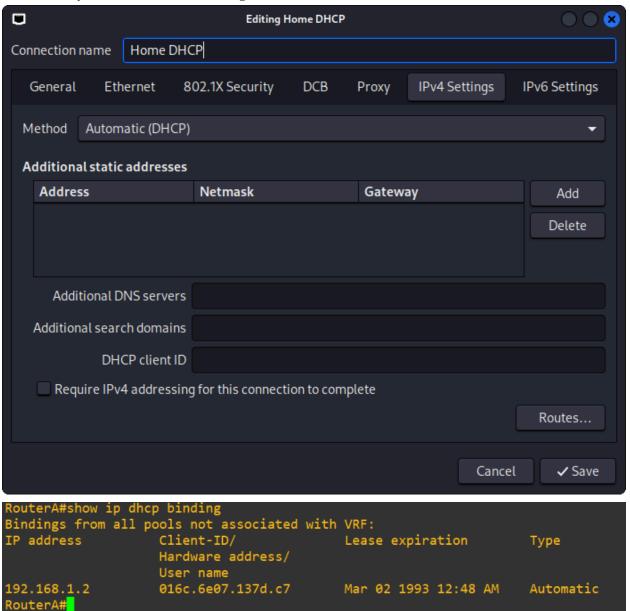
Equipment: Raspberry Pi (Kali Linux), Yersinia, 3560 Switch, 2811 Router, and PuTTy

Steps:

1. Create a DHCP Pool on the 2811 router (RouterA)

```
ip dhcp excluded-address 192.168.1.254
!
ip dhcp pool Home
  network 192.168.1.0 255.255.255.0
  default-router 192.168.1.254
!
!
!
```

2. Verify that the **DHCP** is working



3. Start the **DHCP Starvation Attack**



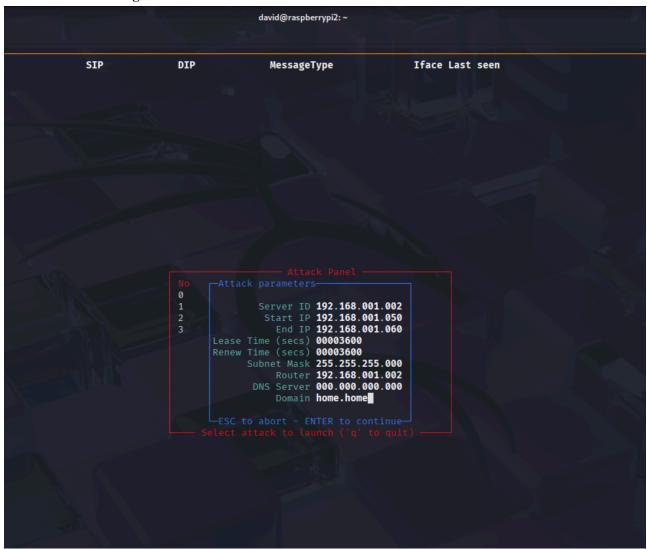
4. Check on the status of the ip bindings

```
RouterA#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address
                    Client-ID/
                                             Lease expiration
                                                                     Type
                    Hardware address/
                    User name
                    016c.6e07.137d.c7
                                                                     Automatic
192.168.1.2
                                            Mar 02 1993 12:48 AM
192.168.1.3
                    04dd.b374.4e38
                                            Mar 01 1993 01:10 AM
                                                                     Automatic
192.168.1.4
                    b857.2079.c55b
                                            Mar 01 1993 01:10 AM
                                                                     Automatic
192.168.1.5
                    3e57.972f.6d66
                                            Mar 01 1993 01:10 AM
                                                                     Automatic
192.168.1.6
                    7aaa.2c25.9e98
                                            Mar 01 1993 01:10 AM
                                                                     Automatic
192.168.1.7
                    e2ef.012d.e5c3
                                            Mar 01 1993 01:10 AM
                                                                     Automatic
192.168.1.8
                    52d2.db3f.3586
                                            Mar 01 1993 01:10 AM
                                                                     Automatic
192.168.1.9
                    a6b2.4579.3440
                                            Mar 01 1993 01:10 AM
                                                                     Automatic
                                            Mar 01 1993 01:10 AM
192.168.1.10
                    9257.a804.2582
                                                                     Automatic
192.168.1.11
                    8e73.246f.6873
                                            Mar 01 1993 01:10 AM
                                                                     Automatic
                    e2aa.824e.4b0e
                                            Mar 01 1993 01:10 AM
192.168.1.12
                                                                     Automatic
192.168.1.13
                    76b1.1c4f.9a02
                                            Mar 01 1993 01:10 AM
                                                                     Automatic
                                                                     Automatic
192.168.1.14
                    106a.2616.b408
                                            Mar 01 1993 01:10 AM
192.168.1.15
                    52a1.4139.c057
                                            Mar 01 1993 01:10 AM
                                                                     Automatic
192.168.1.16
                    f8dc.9558.c58d
                                            Mar 01 1993 01:10 AM
                                                                     Automatic
192.168.1.17
                    fa13.1d3c.5e32
                                            Mar 01 1993 01:10 AM
                                                                     Automatic
                                            Mar 01 1993 01:10 AM
192.168.1.18
                    7eb8.a335.d2ce
                                                                     Automatic
                                            Mar 01 1993 01:10 AM
192.168.1.19
                    3a42.a550.d1cb
                                                                     Automatic
192.168.1.20
                    34a5.2708.1ced
                                            Mar 01 1993 01:10 AM
                                                                     Automatic
 --More--
```

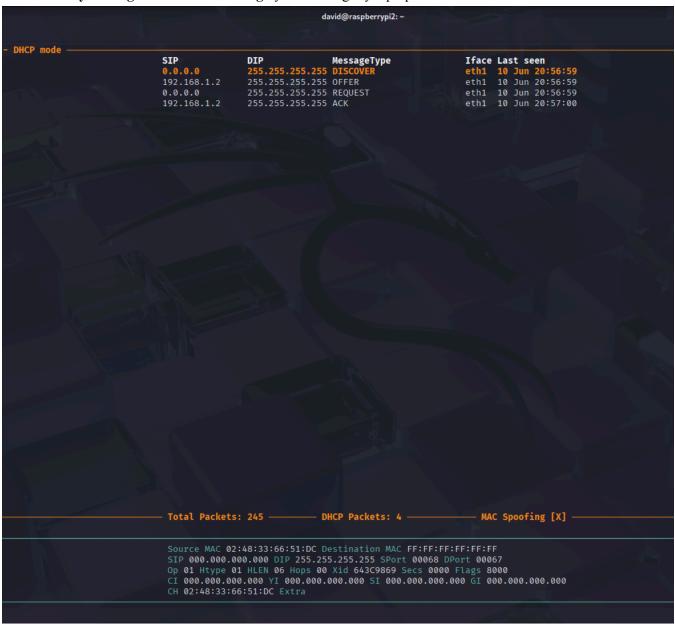
5. Make sure the **pool is fully exhausted**

```
RouterA#show ip dhcp pool
Pool Home :
Utilization mark (high/low)
                                : 100 / 0
Subnet size (first/next)
                                : 0 / 0
                                : 254
Total addresses
Leased addresses
                                : 253
Excluded addresses
                                : 1
Pending event
1 subnet is currently in the pool :
Current index
                      IP address range
                                                           Leased/Excluded/Total
0.0.0.0
                      192.168.1.1
                                       - 192.168.1.254
                                                                          / 254
RouterA#
```

6. Create the rogue DHCP Server



7. **Verify the rogue DHCP is working** by connecting my laptop to the network



```
C:\Users\ddiaz>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 6:

Connection-specific DNS Suffix .: home.home
Link-local IPv6 Address . . . . : fe80::4964:bef1:4990:7c31%55
IPv4 Address . . . . . . : 192.168.1.50
Subnet Mask . . . . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.2
```

8. To test the Man-in-the-Middle attack I will telnet to my router and capture sensitive information

Password:

ccna

RouterA>
e
e
n
n
n

Password:
ccna

RouterA#

9. In order to prevent this, I will configure ip DHCP snooping and limit the rate to 10 packets per second

```
switcha(config)#ip dhcp snooping
switcha(config)#ip dhcp snooping vlan 1
switcha(config)#int g1/0/1
switcha(config-if)#ip dhcp snooping limit rate 10
switcha(config-if)#exit
```

10. I commenced the attack again but now ip DHCP should stop it from being overflown

```
switcha(config)#

Jun 13 14:33:41.636: %DHCP_SNOOPING-4-DHCP_SNOOPING_ERRDISABLE_WARNING: DHCP Snooping received 10 DHCP packets on interface Gi1/0/1

Jun 13 14:33:41.636: %DHCP_SNOOPING-4-DHCP_SNOOPING_RATE_LIMIT_EXCEEDED: The interface Gi1/0/1 is receiving more than the threshold set

Jun 13 14:33:41.636: %PM-4-ERR_DISABLE: dhcp-rate-limit error detected on Gi1/0/1, putting Gi1/0/1 in err-disable state

Jun 13 14:33:42.639: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to down

Jun 13 14:33:43.638: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to down
```

11. Lastly, I trusted the port that is connected to the router and disabled option 82 to get authenticate DHCP exchanges

```
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
DHCP snooping is operational on following VLANs:
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is disabled
   circuit-id default format: vlan-mod-port
   remote-id: acf5.e6f1.0500 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
                                      Allow option
                                                      Rate limit (pps)
Interface
                           Trusted
GigabitEthernet1/0/1
                                                      10
                           no
                                      no
  Custom circuit-ids:
GigabitEthernet1/0/5
                                                      unlimited
                           yes
                                      yes
  Custom circuit-ids:
switcha(config)#
```

