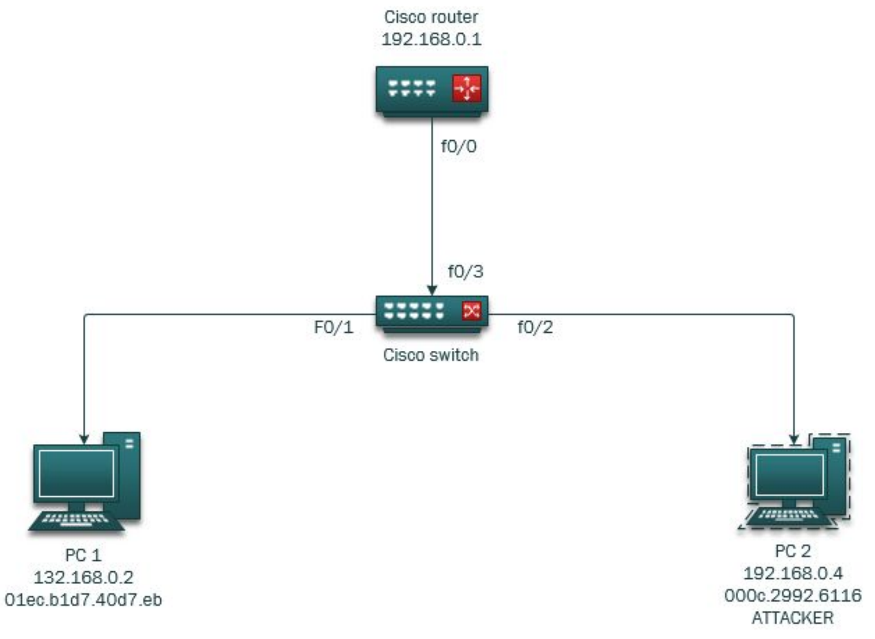
DHCP Snooping

Overview:

Attack→ In a *DHCP starvation attack*, the attacker sends a high number of DHCP DISCOVER packets with spoofed source MAC addresses. When the DHCP server begins responding, the available IP Addresses in the DHCP pool is quickly depleted, rendering the server useless. In addition, an attacker can then run a DHCP spoofing attack by setting up a rogue DHCP server to respond to new DHCP requests, which allows for seeing the traffic, relaying traffic to a gateway and even changing the destination to a malicious website.

Mitigation→ DHCP snooping is used to validate DHCP messages received from untrusted sources and to filter out those deemed invalid. For example if response packet received is (DHCPACK, DHCPNAK, or DHCPOFFER packet) on untrusted interface. It does this by building a DHCP snooping binding database which contains info about untrusted hosts with leased IP addresses.

LAB Topology



Successful Pings Between PC 1 & PC 2

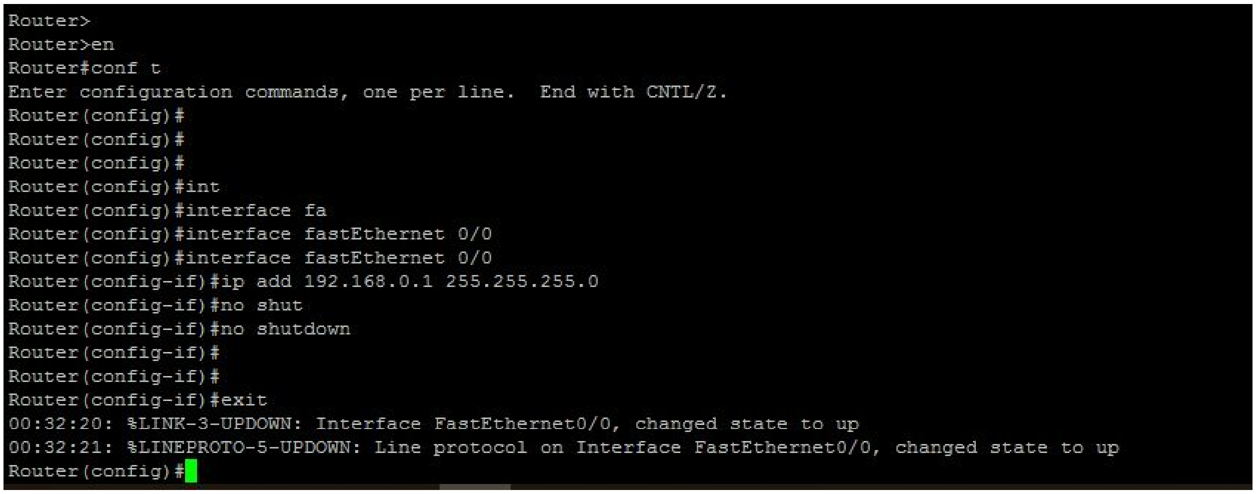
192.168.0.2	192.168.0.4

PART 1: Initial Setup

Steps to builder a dhcp server:

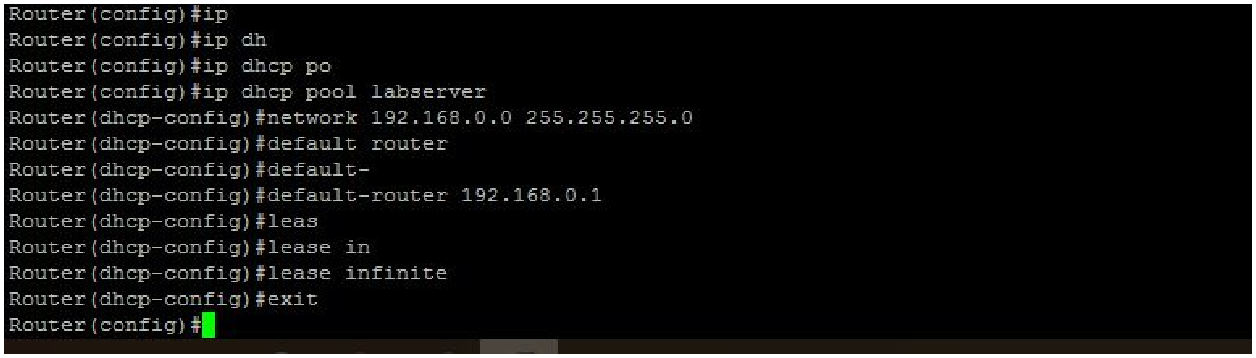
Configure Ip address for router
Build DHCP server on router
Enable the DHCP server
Check that hosts are receiving new DHCP addresses
Show ip DHCP binding

Step 1: Configure IP address for router



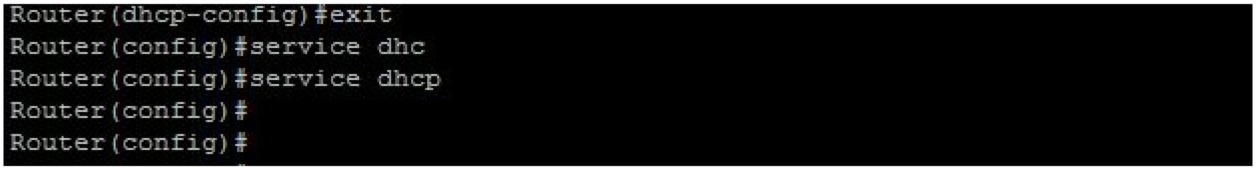
```
Router>
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#
Router(config)#int
Router(config)#interface fa
Router(config)#interface fastEthernet 0/0
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip add 192.168.0.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#no shutdown
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
00:32:20: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
00:32:21: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config)#
```

Step 2: Build DHCP server on router



```
Router(config)#ip
Router(config)#ip dh
Router(config)#ip dhcp po
Router(config)#ip dhcp pool labserver
Router(dhcp-config)#network 192.168.0.0 255.255.255.0
Router(dhcp-config)#default router
Router(dhcp-config)#default-
Router(dhcp-config)#default-router 192.168.0.1
Router(dhcp-config)#leas
Router(dhcp-config)#lease in
Router(dhcp-config)#lease infinite
Router(dhcp-config)#exit
Router(config)#
```

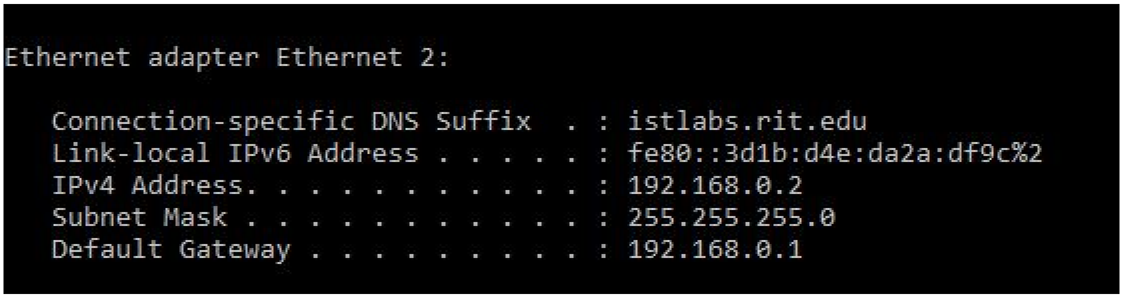
Step 3: Enable the DHCP server



```
Router(dhcp-config)#exit
Router(config)#service dhc
Router(config)#service dhcp
Router(config)#
Router(config)#
```

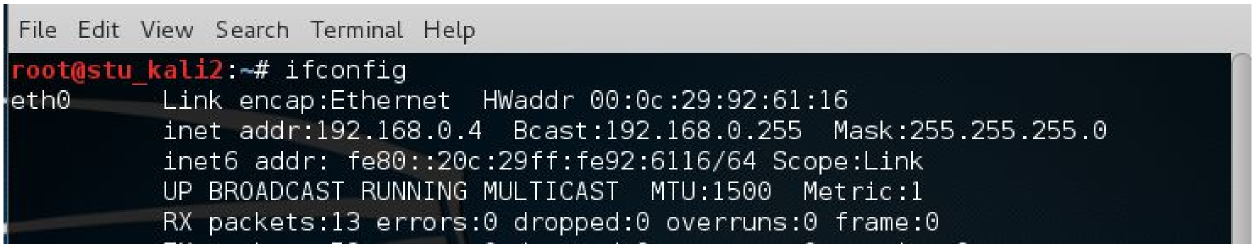
Step 4: Ensure that both computers in the topology are receiving the correct DHCP addresses

PC1



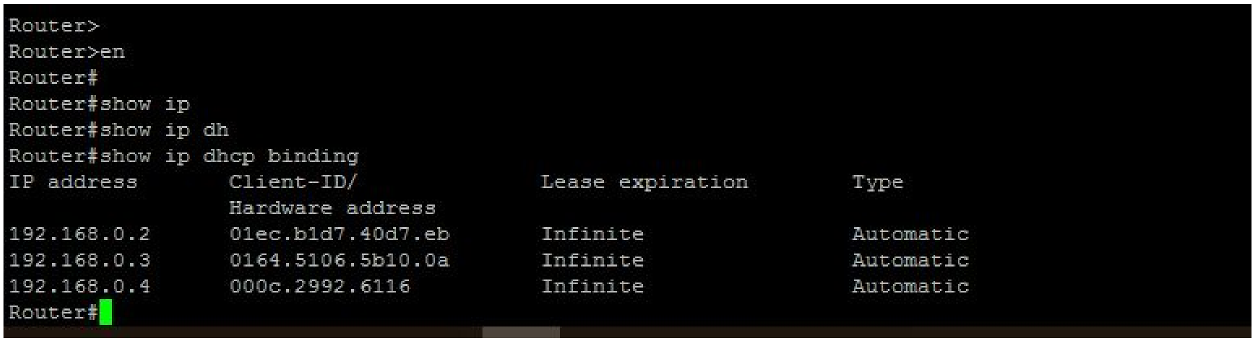
```
Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : istlabs.rit.edu
   Link-local IPv6 Address . . . . . : fe80::3d1b:d4e:da2a:df9c%2
   IPv4 Address. . . . . . . . . . . : 192.168.0.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

PC2



```
root@stu_kali2:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:92:61:16
          inet addr:192.168.0.4  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe92:6116/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13 errors:0 dropped:0 overruns:0 frame:0
```

Step 5: show IP DHCP binding [Shows PC1, PC2 & KALI linux VM running on PC2]



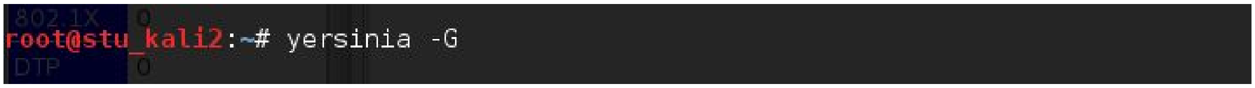
```
Router>
Router>en
Router#
Router#show ip
Router#show ip dh
Router#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.0.2      01ec.b1d7.40d7.eb       Infinite                Automatic
192.168.0.3      0164.5106.5b10.0a       Infinite                Automatic
192.168.0.4      000c.2992.6116          Infinite                Automatic
Router#
```

PART 2 : Launch DHCP Starvation Attack

The basic steps to run exploit:

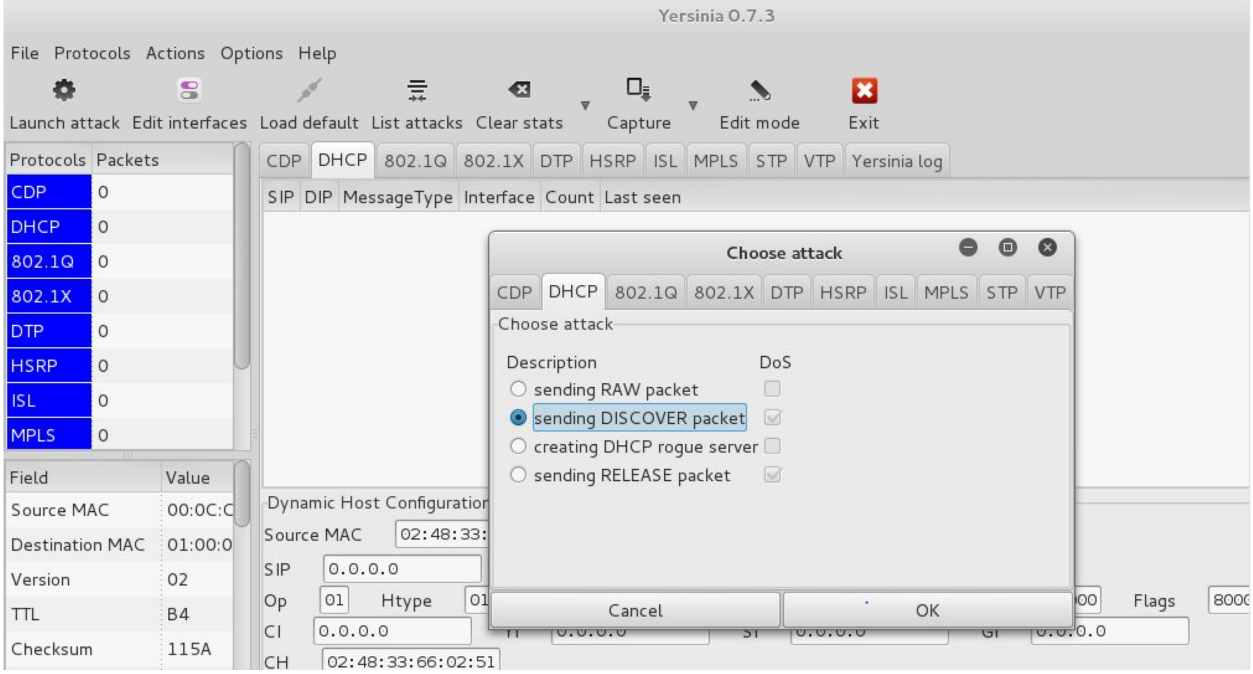
Step 1: Set up an attacker machine. [PC 2] on a Kali Linux VM
Step 2: Use the tool Yersinia to generate large number of DHCP discover packets
Results A: Sh ip dhcp binding   [Overload the routers DHCP server pool]
Results B Sh ip dhcp binding   [Full DHCP server pool]
Results C: Sh ip dhcp server statistics [# of leases]
Note: Not in the this lab (run rogue dhcp server to sniff network traffic)

Step 1: Open/Run Yersinia



```
root@stu_kali2:~# yersinia -G
```

Step 2: Launch Yersinia Attack with DHCP Discover packets



Yersinia 0.7.3
File Protocols Actions Options Help
Launch attack
Edit interfaces
Load default
List attacks
Clear stats
Capture
Edit mode
Exit
CDP DHCP 802.1Q 802.1X DTP HSRP ISL MPLS STP VTP Yersinia log
SIP DIP MessageType Interface Count Last seen
Choose attack
CDP DHCP 802.1Q 802.1X DTP HSRP ISL MPLS STP VTP
Cancel
OK

Protocols	Packets
CDP	0
DHCP	0
802.1Q	0
802.1X	0
DTP	0
HSRP	0
ISL	0
MPLS	0

Field	Value
Source MAC	00:0C:C
Destination MAC	01:00:0
Version	02
TTL	B4
Checksum	115A

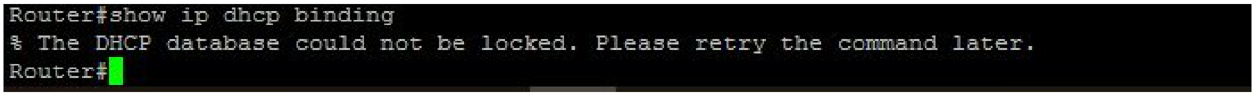
Choose attack

Description	DoS
○ sending RAW packet	□
● sending DISCOVER packet	☑
○ creating DHCP rogue server	□
○ sending RELEASE packet	☑

Dynamic Host Configuration

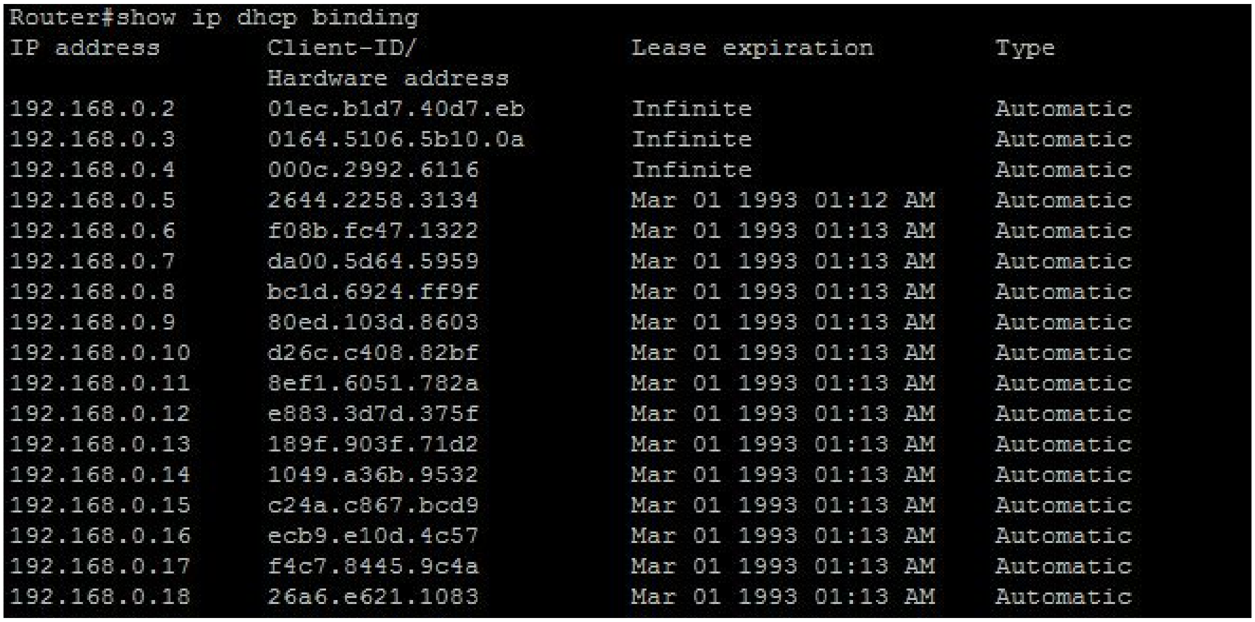
Source MAC 02:48:33:
SIP 0.0.0.0
Op 01 Htype 01
CI 0.0.0.0
CH 02:48:33:66:02:51
Flags 8000
00
YI 0.0.0.0 SI 0.0.0.0 GI 0.0.0.0

Results A: Show ip dhcp binding during DHCP starvation attack[Overload DHCP server pool]



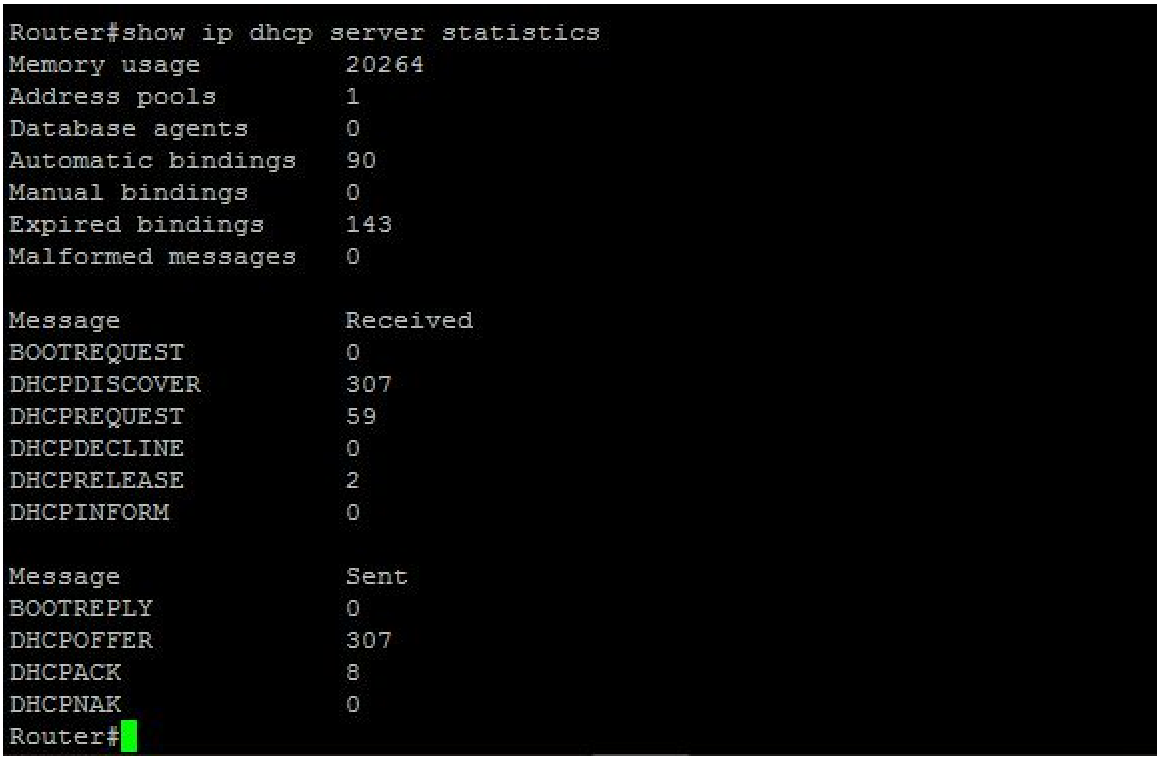
```
Router#show ip dhcp binding
% The DHCP database could not be locked. Please retry the command later.
Router#
```

Results B: Show ip dhcp binding after DHCP starvation attack



```
Router#show ip dhcp binding
IP address        Client-ID/              Lease expiration        Type
                  Hardware address
192.168.0.2       01ec.b1d7.40d7.eb       Infinite                Automatic
192.168.0.3       0164.5106.5b10.0a       Infinite                Automatic
192.168.0.4       000c.2992.6116          Infinite                Automatic
192.168.0.5       2644.2258.3134          Mar 01 1993 01:12 AM    Automatic
192.168.0.6       f08b.fc47.1322          Mar 01 1993 01:13 AM    Automatic
192.168.0.7       da00.5d64.5959          Mar 01 1993 01:13 AM    Automatic
192.168.0.8       bc1d.6924.ff9f          Mar 01 1993 01:13 AM    Automatic
192.168.0.9       80ed.103d.8603          Mar 01 1993 01:13 AM    Automatic
192.168.0.10      d26c.c408.82bf          Mar 01 1993 01:13 AM    Automatic
192.168.0.11      8ef1.6051.782a          Mar 01 1993 01:13 AM    Automatic
192.168.0.12      e883.3d7d.375f          Mar 01 1993 01:13 AM    Automatic
192.168.0.13      189f.903f.71d2          Mar 01 1993 01:13 AM    Automatic
192.168.0.14      1049.a36b.9532          Mar 01 1993 01:13 AM    Automatic
192.168.0.15      c24a.c867.bcd9          Mar 01 1993 01:13 AM    Automatic
192.168.0.16      ecb9.e10d.4c57          Mar 01 1993 01:13 AM    Automatic
192.168.0.17      f4c7.8445.9c4a          Mar 01 1993 01:13 AM    Automatic
192.168.0.18      26a6.e621.1083          Mar 01 1993 01:13 AM    Automatic
```

Results C: Show ip dhcp server statistics [307 addresses leased out]



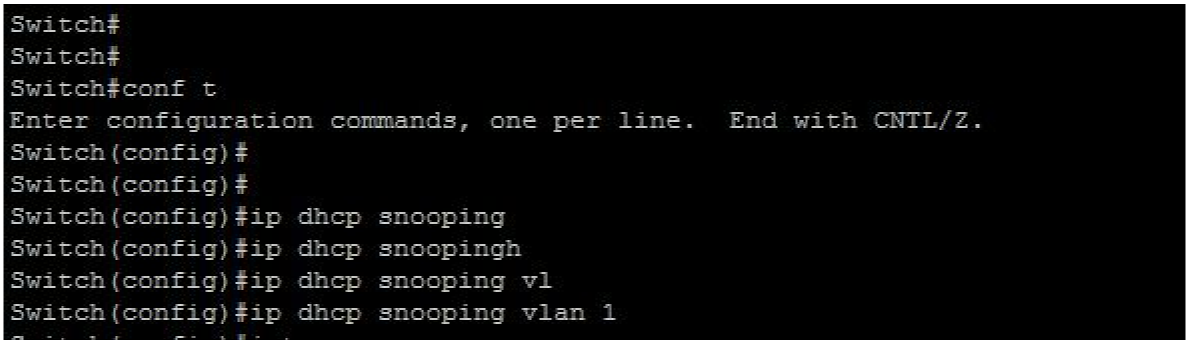
```
Router#show ip dhcp server statistics
Memory usage          20264
Address pools         1
Database agents       0
Automatic bindings    90
Manual bindings       0
Expired bindings      143
Malformed messages    0

Message               Received
BOOTREQUEST           0
DHCPDISCOVER          307
DHCPREQUEST           59
DHCPDECLINE           0
DHCPRELEASE           2
DHCPINFORM            0

Message               Sent
BOOTREPLY             0
DHCPOFFER             307
DHCPACK               8
DHCPNAK               0
Router#
```

PART 3 : Attack Mitigation

Steps to mitigation:

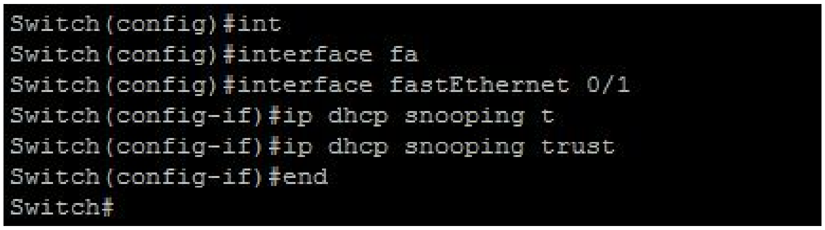
Step 1: Enable IP DHCP snooping on the switch
Step 2: Ip dhcp snooping trust for port switch 1
Step 3: IP dhcp snooping trust for port switch 3
Step 4: Enable port security on switch interfaces
See Results: Show ip dhcp binding after port security and dhcp snooping is enabled

Step1: Enable IP DHCP snooping on the switch



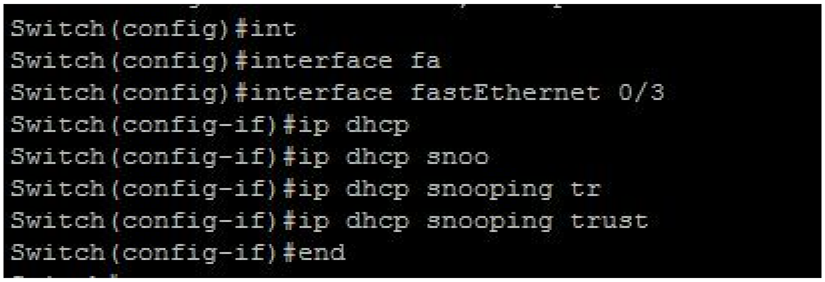
```
Switch#
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snoopingh
Switch(config)#ip dhcp snooping vl
Switch(config)#ip dhcp snooping vlan 1
```

Step 2: Ip dhcp snooping trust for port switch 1



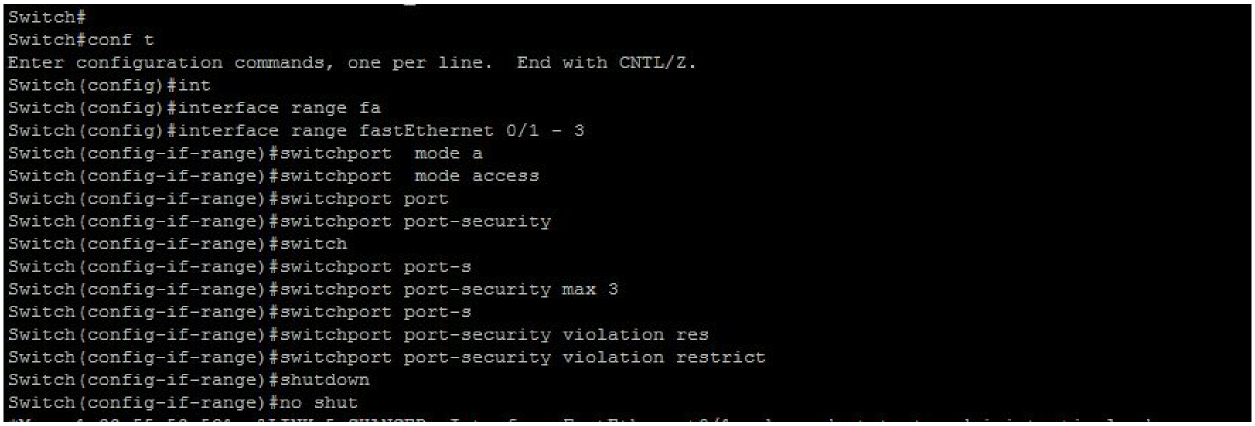
```
Switch(config)#int
Switch(config)#interface fa
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#ip dhcp snooping t
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#end
Switch#
```

Step 3: IP dhcp snooping trust for port switch 3



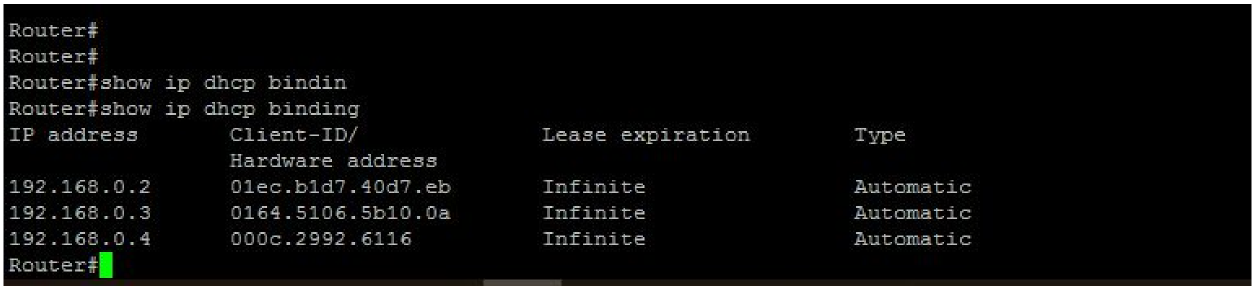
```
Switch(config)#int
Switch(config)#interface fa
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#ip dhcp
Switch(config-if)#ip dhcp snoo
Switch(config-if)#ip dhcp snooping tr
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#end
```

Step 4: Enable port security on switch interfaces



```
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int
Switch(config)#interface range fa
Switch(config)#interface range fastEthernet 0/1 - 3
Switch(config-if-range)#switchport  mode a
Switch(config-if-range)#switchport  mode access
Switch(config-if-range)#switchport port
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switch
Switch(config-if-range)#switchport port-s
Switch(config-if-range)#switchport port-security max 3
Switch(config-if-range)#switchport port-s
Switch(config-if-range)#switchport port-security violation res
Switch(config-if-range)#switchport port-security violation restrict
Switch(config-if-range)#shutdown
Switch(config-if-range)#no shut
```

Results: Show ip dhcp binding after port security and dhcp snooping is enabled



```
Router#
Router#
Router#show ip dhcp bindin
Router#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.0.2      01ec.b1d7.40d7.eb       Infinite                Automatic
192.168.0.3      0164.5106.5b10.0a       Infinite                Automatic
192.168.0.4      000c.2992.6116          Infinite                Automatic
Router#
```