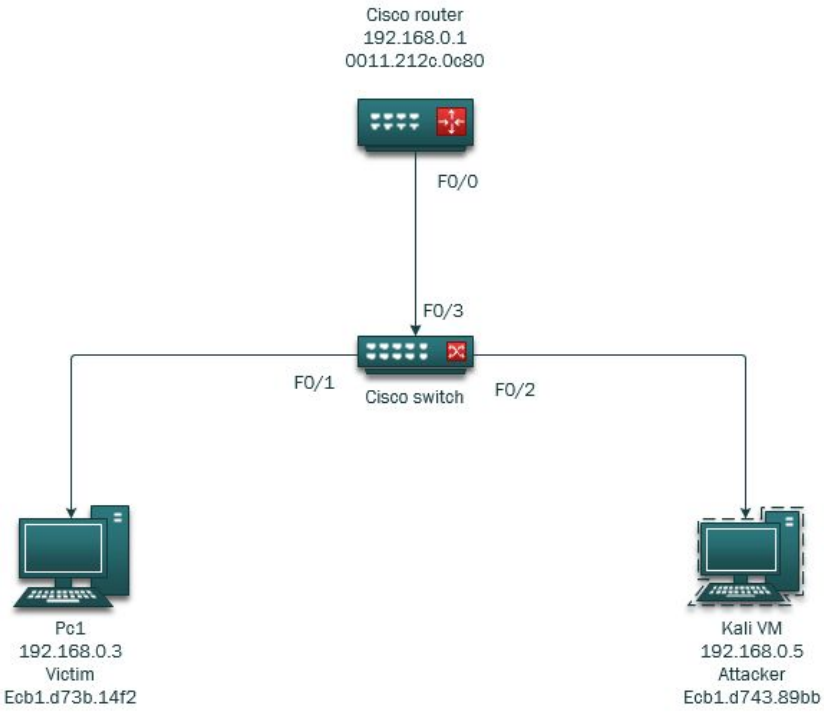
IP Source Guard

Overview:

Attack→ In a IP/Address Spoofing Attack, or more specifically[to this lab], a non-blind spoofing attack, an attacker steals the source IP address of a victim and pretends to be a legitimate user on the same LAN. In more detail, the attack is accomplished by corrupting a connection and re-setting it based on correct sequence and acknowledgement numbers with the attack machine. A successful attack can allow for capturing/redirecting traffic, gaining privileged access to servers & DOS.

Mitigation → IP source guard is used to detect and stop address spoofing attacks. The switch must have a way to look up MAC addresses and find out what IP addresses are associated with them. IPSG does this by utilizing the DHCP snooping database and static IP source binding entries [For this lab: It is static IP source bindings]. If DHCP snooping is configured and enabled, the switch learns the MAC and IP addresses of hosts that use DHCP. If the address is something other than the one learned or statically configured, the switch drops the packet.

LAB Topology

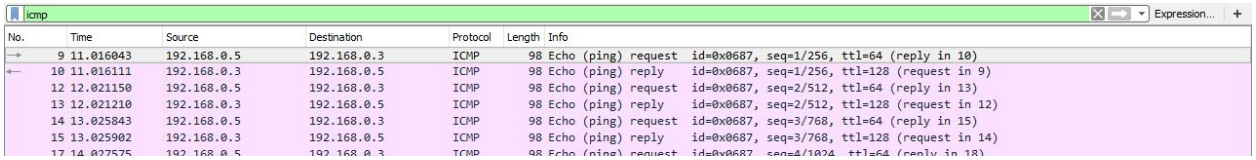


PART 1: Initial Setup

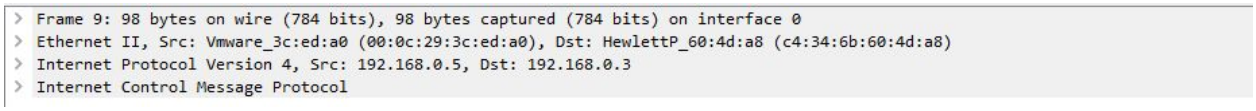
Successful pings between attack machine and PC1

192.168.0.5	**192.168.0.3**

Wireshark capture of successful ping from Attack machine [PC2] → PC1



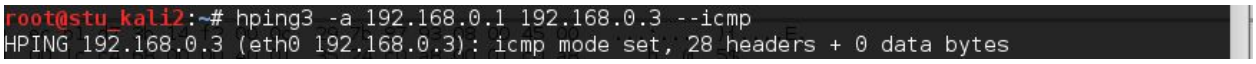
Wireshark capture of IPV4 SRC and DST for ping from [pc2 → pc1]



NOTE: The IP address of the ***source*** is **192.168.0.5**

PART 2: Launch Non-Blind Address Spoofing Attack

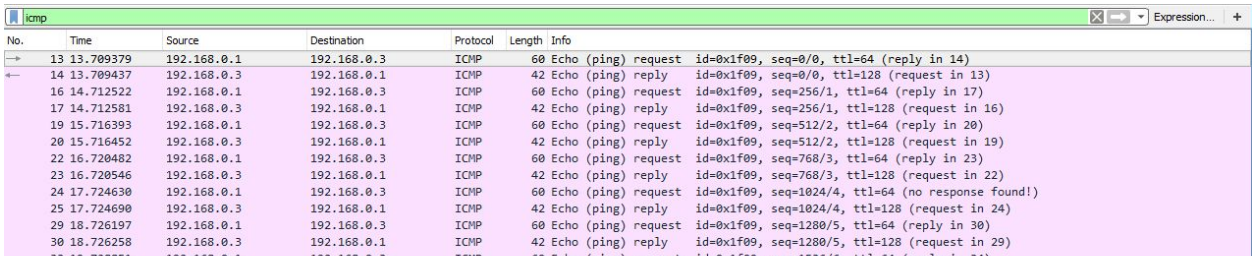
Hping3 command from Kali VM Machine [192.168.0.5]



Command Breakdown

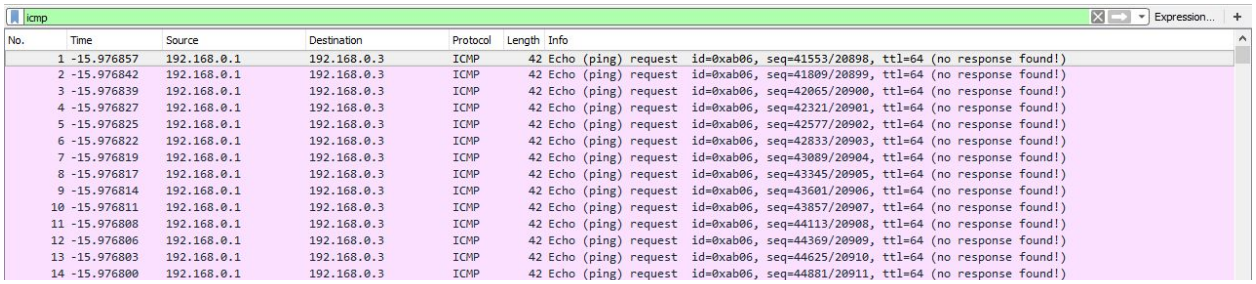
-a is to spoof the source address
192.168.0.1(first address in command) = source address
192.168.0.3(second address in command) = who we're pinging
Icmp = desired protocol

Wireshark capture during IP spoofing attack from victim PC 1 [192.168.0.3]
Note: Ping behavior appears normal [request/reply]



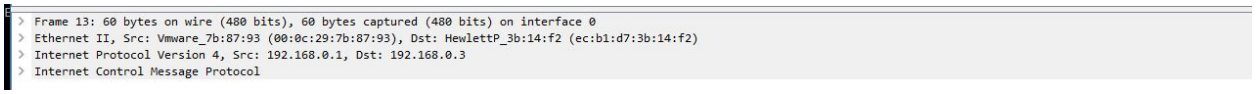
No.	Time	Source	Destination	Protocol	Length	Info
13	13.709379	192.168.0.1	192.168.0.3	ICMP	60	Echo (ping) request id=0x1f09, seq=0/0, ttl=64 (reply in 14)
14	13.709437	192.168.0.3	192.168.0.1	ICMP	42	Echo (ping) reply id=0x1f09, seq=0/0, ttl=128 (request in 13)
16	14.712522	192.168.0.1	192.168.0.3	ICMP	60	Echo (ping) request id=0x1f09, seq=256/1, ttl=64 (reply in 17)
17	14.712581	192.168.0.3	192.168.0.1	ICMP	42	Echo (ping) reply id=0x1f09, seq=256/1, ttl=128 (request in 16)
19	15.716393	192.168.0.1	192.168.0.3	ICMP	60	Echo (ping) request id=0x1f09, seq=512/2, ttl=64 (reply in 20)
20	15.716452	192.168.0.3	192.168.0.1	ICMP	42	Echo (ping) reply id=0x1f09, seq=512/2, ttl=128 (request in 19)
22	16.720482	192.168.0.1	192.168.0.3	ICMP	60	Echo (ping) request id=0x1f09, seq=768/3, ttl=64 (reply in 23)
23	16.720546	192.168.0.3	192.168.0.1	ICMP	42	Echo (ping) reply id=0x1f09, seq=768/3, ttl=128 (request in 22)
24	17.724630	192.168.0.1	192.168.0.3	ICMP	60	Echo (ping) request id=0x1f09, seq=1024/4, ttl=64 (no response found!)
25	17.724690	192.168.0.3	192.168.0.1	ICMP	42	Echo (ping) reply id=0x1f09, seq=1024/4, ttl=128 (request in 24)
29	18.726197	192.168.0.1	192.168.0.3	ICMP	60	Echo (ping) request id=0x1f09, seq=1280/5, ttl=64 (reply in 30)
30	18.726258	192.168.0.3	192.168.0.1	ICMP	42	Echo (ping) reply id=0x1f09, seq=1280/5, ttl=128 (request in 29)

Wireshark capture during IP spoofing attack from Attacker machine [192.168.0.5]
NOTE: No replies coming back from 192.168.0.3, only the request being sent out from 0.1



No.	Time	Source	Destination	Protocol	Length	Info
1	-15.976857	192.168.0.1	192.168.0.3	ICMP	42	Echo (ping) request id=0xab06, seq=41553/20898, ttl=64 (no response found!)
2	-15.976842	192.168.0.1	192.168.0.3	ICMP	42	Echo (ping) request id=0xab06, seq=41809/20899, ttl=64 (no response found!)
3	-15.976839	192.168.0.1	192.168.0.3	ICMP	42	Echo (ping) request id=0xab06, seq=42065/20900, ttl=64 (no response found!)
4	-15.976827	192.168.0.1	192.168.0.3	ICMP	42	Echo (ping) request id=0xab06, seq=42321/20901, ttl=64 (no response found!)
5	-15.976825	192.168.0.1	192.168.0.3	ICMP	42	Echo (ping) request id=0xab06, seq=42577/20902, ttl=64 (no response found!)
6	-15.976822	192.168.0.1	192.168.0.3	ICMP	42	Echo (ping) request id=0xab06, seq=42833/20903, ttl=64 (no response found!)
7	-15.976819	192.168.0.1	192.168.0.3	ICMP	42	Echo (ping) request id=0xab06, seq=43089/20904, ttl=64 (no response found!)
8	-15.976817	192.168.0.1	192.168.0.3	ICMP	42	Echo (ping) request id=0xab06, seq=43345/20905, ttl=64 (no response found!)
9	-15.976814	192.168.0.1	192.168.0.3	ICMP	42	Echo (ping) request id=0xab06, seq=43601/20906, ttl=64 (no response found!)
10	-15.976811	192.168.0.1	192.168.0.3	ICMP	42	Echo (ping) request id=0xab06, seq=43857/20907, ttl=64 (no response found!)
11	-15.976808	192.168.0.1	192.168.0.3	ICMP	42	Echo (ping) request id=0xab06, seq=44113/20908, ttl=64 (no response found!)
12	-15.976806	192.168.0.1	192.168.0.3	ICMP	42	Echo (ping) request id=0xab06, seq=44369/20909, ttl=64 (no response found!)
13	-15.976803	192.168.0.1	192.168.0.3	ICMP	42	Echo (ping) request id=0xab06, seq=44625/20910, ttl=64 (no response found!)
14	-15.976800	192.168.0.1	192.168.0.3	ICMP	42	Echo (ping) request id=0xab06, seq=44881/20911, ttl=64 (no response found!)

Wireshare capture showing IPV4 SRC has changed from VMware to [192.168.0.1]
NOTE: The address of [0.5] attack machine was spoofed/redirected to the [0.1] router



PART 3 : Attack Mitigation

Steps to Mitigation:

Step 1: Configure Ip dhcp snooping globally & for for vlan 1 Set ip dhcp snooping trust on switch ports Set ip verify source on port 2
Step 2: Configure switchport port-security & ip verify source port-security
Step 3: Ip source binding commands for all switch ports
check: Sh ip verify source
check: Sh ip source binding
Results: Check Wireshark on attacker PC [Kali VM]

Step1:
Configure Ip dhcp snooping globally & for for vlan 1
Set ip dhcp snooping trust on switch ports

Set ip verify source on port 2

```
Switch(config)#
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#int fa0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#int fa0/2
Switch(config-if)#ip dhcp snooping limit rate 10
Switch(config-if)#exit
Switch(config)#int fa0/2
Switch(config-if)#ip verify source
Switch(config-if)#int fa0/3
Switch(config-if)#ip dhcp snooping limit 10
                                         ^
% Invalid input detected at '^' marker.

Switch(config-if)#ip dhcp snooping limit rate 10
Switch(config-if)#ip verify source
Switch(config-if)#
```

Step 2: Configure switchport port-security & ip verify source port-security

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/2
Switch(config-if)#switchport port-security
Command rejected: FastEthernet0/2 is a dynamic port.
Switch(config-if)#int fa0/3
Switch(config-if)#switchport port-security
Command rejected: FastEthernet0/3 is a dynamic port.
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#ip verify source port-security
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#ip verify source port-security
Switch(config-if)#exit
```

Step 3: Ip source binding commands for all switch ports

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip source binding ecb1.d73b.14f2 vlan 1 192.168.0.3 int fa0/1
Switch(config)#ip source binding ecb1.d743.89bb vlan 2 192.168.0.5 int fa0/2
Switch(config)#ip source binding ecb1.d743.89bb vlan 1 192.168.0.5 int fa0/2
Switch(config)#ip source binding 0011.212c.0c80 vlan 1 192.168.0.1 int fa0/3
Switch(config)#
```

Check: Sh ip verify source

```
Switch#sh ip verify source
Interface  Filter-type  Filter-mode  IP-address      Mac-address       Vlan
---------  -----------  -----------  --------------  ----------------  ----
Fa0/1      ip-mac       inactive-trust-port
Fa0/2      ip-mac       active       192.168.0.5     EC:B1:D7:43:89:BB  1
Fa0/3      ip-mac       active       192.168.0.1     00:11:21:2C:0C:80  1
Switch#
```

Check: Sh ip source binding

```
Switch#
Switch#sh ip source binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
EC:B1:D7:3B:14:F2   192.168.0.3      infinite    static          1     FastEthernet0/1
00:11:21:2C:0C:80   192.168.0.1      infinite    static          1     FastEthernet0/3
EC:B1:D7:43:89:BB   192.168.0.5      infinite    static          1     FastEthernet0/2
Total number of bindings: 3

Switch#
```

Results:

hping3 address spoof attack stops working in wireshark & kali terminal after IPSG configs made