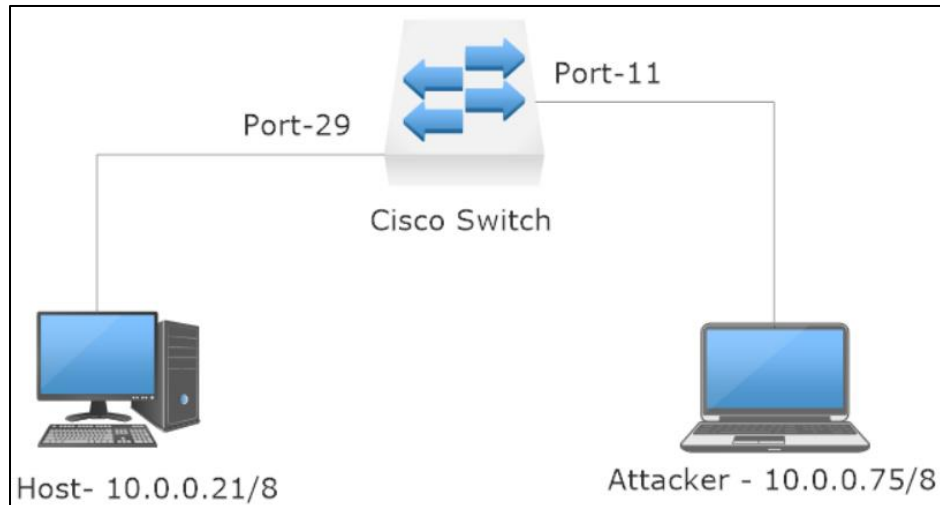


Port Security – Attack & Mitigation

Port Security – a layer 2 attack mitigation for CAM Overflow attack where the attacker, floods switch on a particular port with multiple MAC addresses to store in the CAM table which eventually fills the switch's memory and converting switch to behave like a hub.

To emulate a real-world scenario, a lab setup was created as shown below and implement both attack and its mitigation.



Below are screenshots that show both how the attacker can exploit this particular vulnerability and also how as a network administrator, one can mitigate this by deploying port security in switch.

First, we'll see how attacker can use simple Linux commands to attack and perform CAM overflow attack.

CAM Overflow attack:

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.75 netmask 255.0.0.0 broadcast 10.255.255.255
    inet6 fe80::a00:27ff:fe5b:bla6 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:5b:bl:a6 txqueuelen 1000 (Ethernet)
    RX packets 59 bytes 4015 (3.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 32 bytes 2404 (2.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

IP of Attacker's system

```
C:\Users\Student> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 4:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : 
    IPv4 Address. . . . . : 10.0.0.21
    Subnet Mask . . . . . : 255.0.0.0
    Default Gateway . . . . . :
```

IP address of host machine

```

root@kali:~# ping 10.0.0.21
PING 10.0.0.21 (10.0.0.21) 56(84) bytes of data.
64 bytes from 10.0.0.21: icmp_seq=1 ttl=128 time=1.11 ms
64 bytes from 10.0.0.21: icmp_seq=2 ttl=128 time=1.71 ms
64 bytes from 10.0.0.21: icmp_seq=3 ttl=128 time=1.33 ms
64 bytes from 10.0.0.21: icmp_seq=4 ttl=128 time=1.62 ms
^Z
[2]+  Stopped                  ping 10.0.0.21
root@kali:~#

```

Ping successful from Attacker to host machine which proves proper switch connection

```

Microsoft Windows [Version 10.0.18363.535]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Student>ping 10.0.0.75

Pinging 10.0.0.75 with 32 bytes of data:
Reply from 10.0.0.75: bytes=32 time=1ms TTL=64
Reply from 10.0.0.75: bytes=32 time=1ms TTL=64
Reply from 10.0.0.75: bytes=32 time=1ms TTL=64
Reply from 10.0.0.75: bytes=32 time=1ms TTL=64

Ping statistics for 10.0.0.75:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

```

Same is true from other side i.e. host to attacker's machine

```

Switch#show mac address-table dynamic
      Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       0800.275b.b1a6   DYNAMIC   Gil/0/11
1       7c8a.e10b.b13a   DYNAMIC   Gil/0/11
1       ecbl.d740.d7e7   DYNAMIC   Gil/0/29
Total Mac Addresses for this criterion: 3
Switch#

```

Before attack- Switch CAM table shows 3 MAC addresses (there are 2 MAC addresses on port 11 because attacker used virtual machine)

```

root@kali:~# macof -i eth0
b5:56:67:76:e0:41 82:8e:6:4b:19:22 0.0.0.0.51089 > 0.0.0.0.60701: S 264566966:264
566966(0) win 512
f6:5d:f2:48:96:dc 90:cd:e3:62:d5:dc 0.0.0.0.11003 > 0.0.0.0.6359: S 982171557:982
171557(0) win 512
f4:2f:7e:2a:4f:c5 5f:1a:20:76:26:93 0.0.0.0.24974 > 0.0.0.0.31379: S 1911867676:1
911867676(0) win 512
36:6:43:7b:2d:88 aa:21:33:12:1:db 0.0.0.0.9145 > 0.0.0.0.29143: S 1052687993:1052
687993(0) win 512
de:b6:2e:30:20:24 51:59:79:2f:80:97 0.0.0.0.17350 > 0.0.0.0.11250: S 901803514:90
1803514(0) win 512
7e:25:38:61:2c:fe 9a:21:ab:61:35:97 0.0.0.0.17771 > 0.0.0.0.29410: S 529934310:52
9934310(0) win 512
68:66:77:7e:f5:48 66:c6:42:42:bc:98 0.0.0.0.43222 > 0.0.0.0.51120: S 750712839:75
0712839(0) win 512
d5:3d:f:36:d3:b aa:6d:85:5c:ae:fc 0.0.0.0.34706 > 0.0.0.0.26393: S 1879246613:187
9246613(0) win 512

```

Running the macof command for CAM overflow attack on switch at port 11

```
Switch#show mac address-table
Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
All     0100.0ccc.cccc   STATIC  CPU
All     0100.0ccc.cccd   STATIC  CPU
All     0180.c200.0000   STATIC  CPU
All     0180.c200.0001   STATIC  CPU
All     0180.c200.0002   STATIC  CPU
All     0180.c200.0003   STATIC  CPU
All     0180.c200.0004   STATIC  CPU
All     0180.c200.0005   STATIC  CPU
All     0180.c200.0006   STATIC  CPU
All     0180.c200.0007   STATIC  CPU
All     0180.c200.0008   STATIC  CPU
All     0180.c200.0009   STATIC  CPU
All     0180.c200.000a   STATIC  CPU
All     0180.c200.000b   STATIC  CPU
All     0180.c200.000c   STATIC  CPU
All     0180.c200.000d   STATIC  CPU
All     0180.c200.000e   STATIC  CPU
All     0180.c200.000f   STATIC  CPU
All     0180.c200.0010   STATIC  CPU
All     ffff.ffff.ffff   STATIC  CPU
1       0012.e320.9be9   DYNAMIC Gi1/0/11
1       0013.8c3b.d7dd   DYNAMIC Gi1/0/11
1       001e.7d00.59e9   DYNAMIC Gi1/0/11
1       0029.4013.f233   DYNAMIC Gi1/0/11
1       002a.5f49.073b   DYNAMIC Gi1/0/11
1       002e.4318.d578   DYNAMIC Gi1/0/11
1       002f.fe09.4cce   DYNAMIC Gi1/0/11
1       0036.5832.0ccf   DYNAMIC Gi1/0/11
1       003b.1730.092c   DYNAMIC Gi1/0/11
1       0043.9636.5d39   DYNAMIC Gi1/0/11
1       004e.1e1c.9841   DYNAMIC Gi1/0/11
1       0058.562b.581c   DYNAMIC Gi1/0/11
1       0060.ee3d.fa33   DYNAMIC Gi1/0/11
1       0062.2d68.2915   DYNAMIC Gi1/0/11
1       006b.9b05.97e0   DYNAMIC Gi1/0/11
1       006c.eb7d.32ba   DYNAMIC Gi1/0/11
1       007a.f644.0d52   DYNAMIC Gi1/0/11
1       007b.0b7a.3b92   DYNAMIC Gi1/0/11
1       007b.3b6d.5de2   DYNAMIC Gi1/0/11
1       0086.d172.dd6f   DYNAMIC Gi1/0/11
1       0089.4d7d.b6a8   DYNAMIC Gi1/0/11
--More--
```

Above is the MAC address table after attack. Clearly, the table is being flooded with random MAC addresses on a single port. (port 11)

Port Security – Mitigation for CAM Overflow Attack

```
Switch#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int gil/0/11
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 2
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#end
Switch#
*Mar 1 00:37:08.643: %SYS-5-CONFIG_I: Configured from console by console
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
Switch#
Switch#
Switch#enable
Switch#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int gil/0/11
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security violation shutdown
```

Above is the snapshot of how port security is being configured on port 11 and setting violation as shutdown. Whenever, port 11 violates port security, that port will be shutdown and the switch will no longer listen on that port.

```
Switch#show port-security
Secure Port    MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)          (Count)          (Count)
-----
   Gil/0/11           2             2             0             Shutdown
-----
Total Addresses in System (excluding one mac per port)    : 1
Max Addresses limit in System (excluding one mac per port) : 6144
Switch#
Switch#
Switch#show port-security interface gigabitethernet1/0/11
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 2
Total MAC Addresses    : 2
Configured MAC Addresses : 0
Sticky MAC Addresses   : 2
Last Source Address:Vlan : 0800.275b.bla6:1
Security Violation Count : 0
```

Here, we can see that port security is enabled and no violation has been recorded yet. We can also see what security action is set currently in case of violation. Port-status is currently up and secured. Maximum MAC addresses allowed on that port is 2.

No.	Time	Source	Destination	Protocol	Len	Info
1	0.000...	Cisco_a7:a9:8b	Spanning-tree...	STP	60	Conf. Root = 32768
2	0.974...	HewlettP_40:d7...	Broadcast	ARP	60	Who has 169.254.169
3	1.041...	10.0.0.75	224.0.0.251	MDNS	83	Standard query 0x00
4	1.708...	HewlettP_40:d7...	Broadcast	ARP	60	Who has 169.254.169
5	2.011...	Cisco_a7:a9:8b	Spanning-tree...	STP	60	Conf. Root = 32768
6	2.709...	HewlettP_40:d7...	Broadcast	ARP	60	Who has 169.254.169
7	4.018...	Cisco_a7:a9:8b	Spanning-tree...	STP	60	Conf. Root = 32768
8	6.017...	Cisco_a7:a9:8b	Spanning-tree...	STP	60	Conf. Root = 32768
9	6.431...	48.30.5.33	31.152.155.36	IPv4	54	
10	6.431...	116.74.114.71	200.107.17.114	IPv4	54	

▶ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface
▶ IEEE 802.3 Ethernet
▶ Logical-Link Control
▶ Spanning Tree Protocol

0000	01 80 c2 00 00 00 00 1d	71 a7 a9 8b 00 26 42 42 q....&BB
0010	03 00 00 00 00 00 80 01	00 1d 71 a7 a9 80 00 00 q.....
0020	00 00 80 01 00 1d 71 a7	a9 80 80 0b 00 00 14 00 q.....
0030	02 00 0f 00 00 00 00 00	00 00 00 00 00 00 00 00

```

00:44:53.439: %PM-4-ERR_DISABLE: psecure-violation error detected on Gi1/0/11, putting
00:44:53.447: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused
00:44:54.445: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/11,
00:44:55.452: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/11, changed state to down

```

When the attacker's machine executed macof command again, this time attack was successfully mitigated and wireshark captures show that how random mac addresses were flooded onto the switch through a single port.

Above, is the system log message that was generated due to security violation on port 11. The port went under err-disabled state and port 11 status was changed to down.

Below is the capture of port security status after the attack.

```

Switch#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
          (Count)          (Count)          (Count)
-----
   Gi1/0/11             2             2             1             Shutdown
-----
Total Addresses in System (excluding one mac per port)    : 1
Max Addresses limit in System (excluding one mac per port) : 6144
Switch#
Switch#
Switch#
Switch#show port-security interface gigabitethernet1/0/11
Port Security          : Enabled
Port Status            : Secure-shutdown
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 2
Total MAC Addresses    : 2
Configured MAC Addresses : 0
Sticky MAC Addresses   : 2
Last Source Address:Vlan : faf6.974e.e43f:1
Security Violation Count : 1

```

We can see that security violation count is 1 now and port status is secure-shutdown.

```
Switch#show interfaces status err-disabled

Port      Name      Status      Reason      Err-disabled Vlans
Gi1/0/11  err-disabled psecure-violation

Switch#
```

We can also see what interfaces are under err-disabled state, the reason for err-disabled is also listed as psecure-violation.

Conclusion:

The port status can be changed back to normal after running “shut”, “no shut” command from the network administrator. This successfully demonstrates how in real life we can mitigate such CAM overflow attacks. The switch functionality is not hampered and attacker cannot disrupt the flow of traffic.