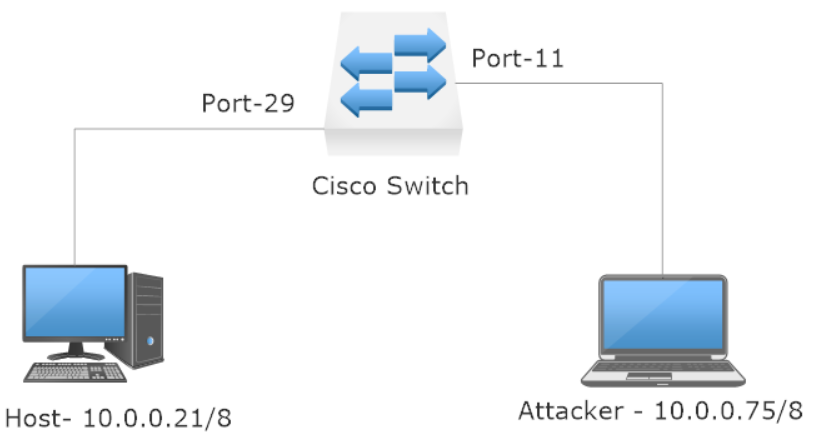
**Port Security – Attack & Mitigation**

**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.

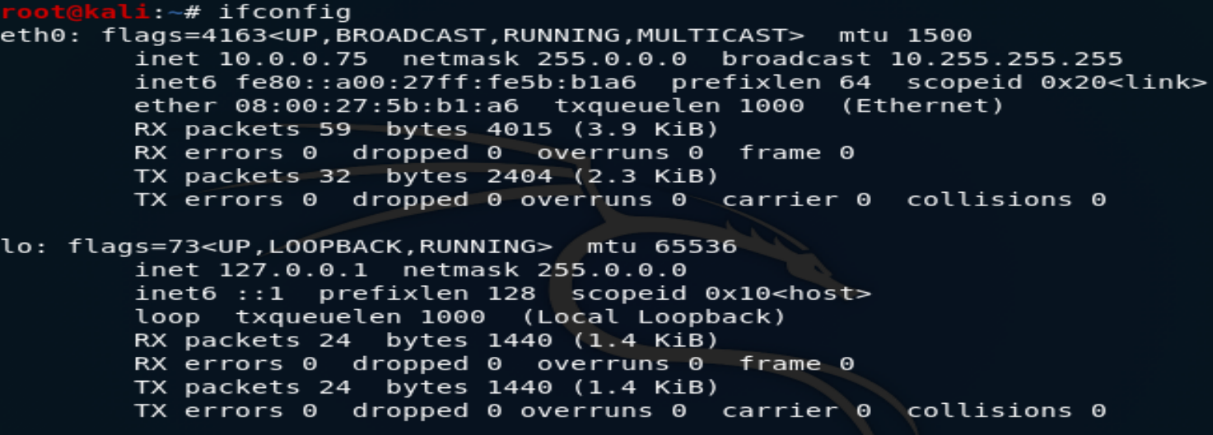
To emulate a real-world scenario, a lab setup was created as shown below and implement both attack and its mitigation.



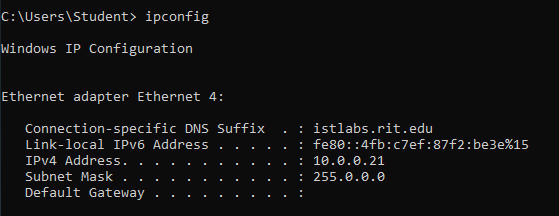
Below are screenshots that show both how the attacker can exploit this particular vulnerability and also how as a network administrator, one can mitigate this by deploying port security in switch.

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

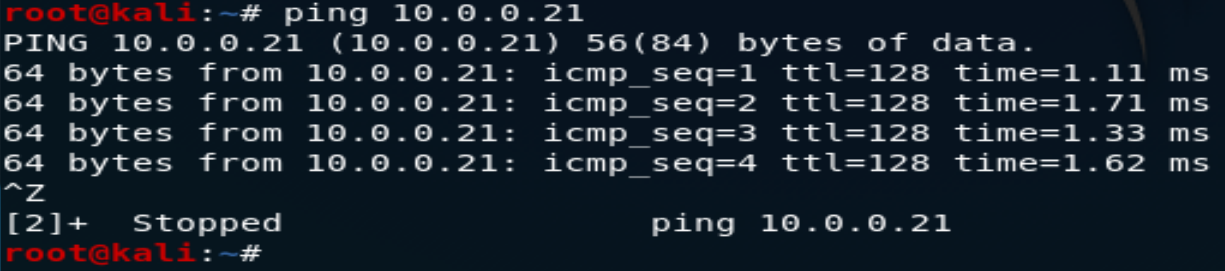
**CAM Overflow attack:**



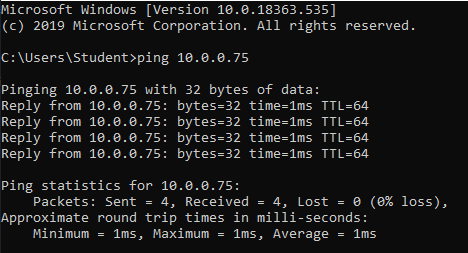
**IP of Attacker’s system**



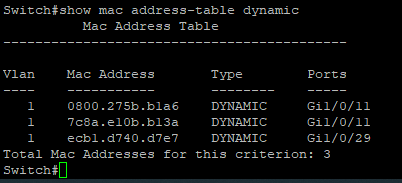
**IP address of host machine**



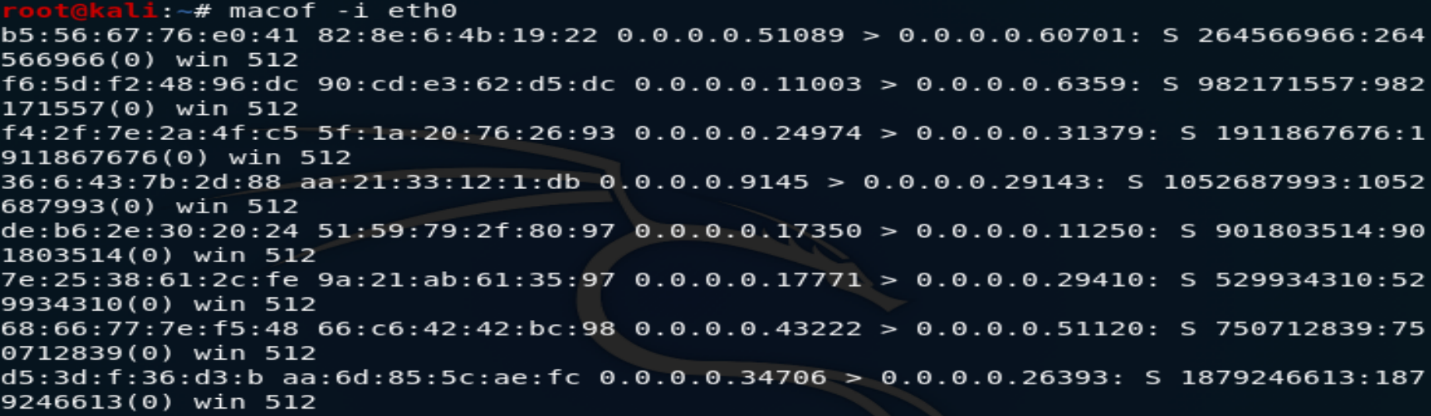
**Ping successful from Attacker to host machine which proves proper switch connection**



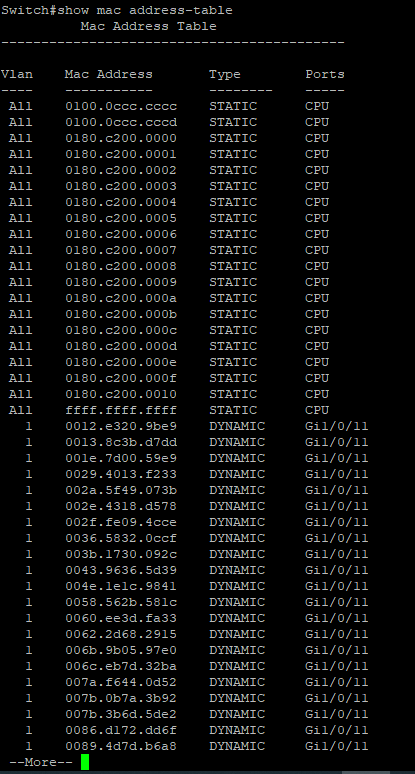
**Same is true from other side i.e. host to attacker’s machine**



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

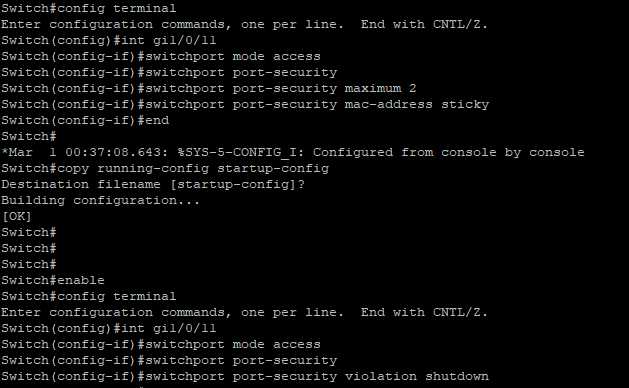


**Running the macof command for CAM overflow attack on switch at port 11**

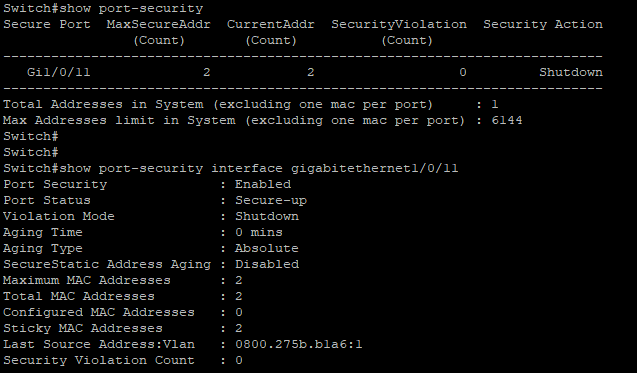


**Above is the MAC address table after attack. Clearly, the table is being flooded with random MAC addresses on a single port. (port 11)**

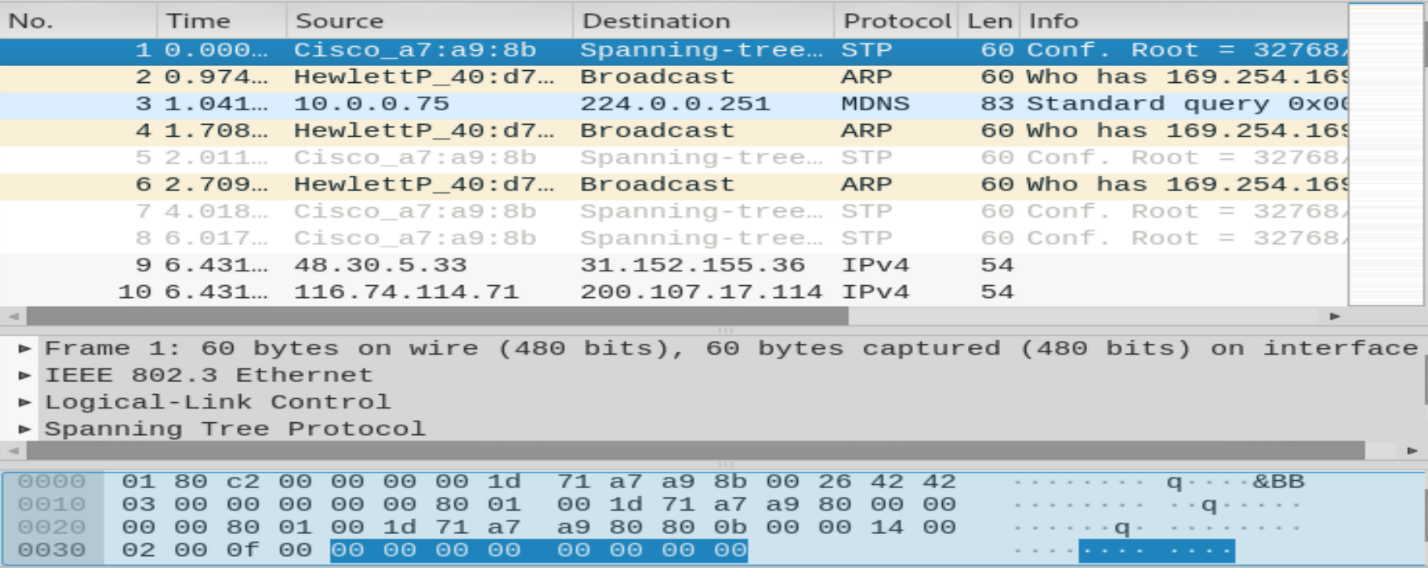
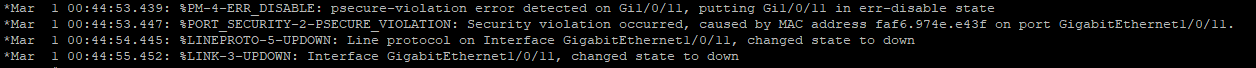
**Port Security – Mitigation for CAM Overflow Attack**



**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.**



**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.**

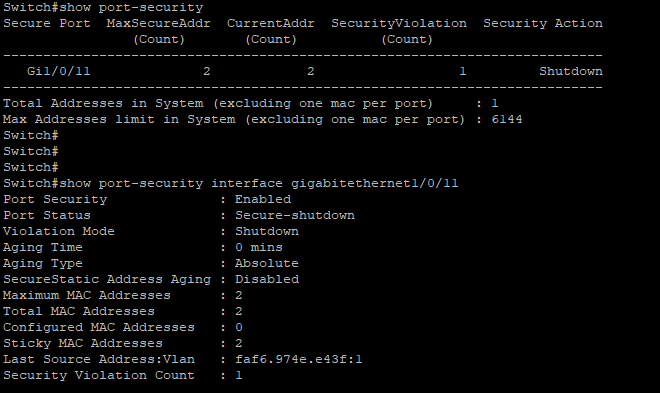


**\**

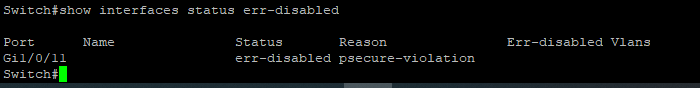
**When the attacker’s machine executed macof command again, this time attack was successfully mitigated and wireshark captures show that how random mac addresses were flooded onto the switch through a single port.**

**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.**



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



**We can also see what interfaces ae 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.