Port Security and VLAN Hopping

Sumayyah Alahmadi [sfa8135@rit.edu](mailto:sfa8135@rit.edu)

Lab partner: Mugdha Deshmukh, [mud5545@rit.edu](mailto:mud5545@rit.edu)

CSEC.744.01

Professor Jonathan Weissman

**Table of contents**

1. Port Security………...……………………………………………………………….. 3
2. VLAN Hopping………...…………………………………………………………….. 4
3. Conclusion……………………………………………………………………………. 5
4. References ……………………………………………………………………………. 6
5. Port Security

Concept:

Switch mainly function based on context addressable memory CAM table wich contain both column MAC address and the corresponding switch port location.

This layer 2 switch help, help the switch direct the destination packet to the accosiated switch port. In CAM table, a fixed number of mac addrees and associated port can be entered. Oldest entites get delted

Attack:

For the cam overflow attack, the attacker try to fluid the switch port by thousands of mac address to disable the switch and make it work as a hub. In other words, when these random MAC address start to fluid the switch, the switch will delete the existance mak address and start to fill the CAM table. Then, after the table filled, every coming Mac address will be forword to every port in the switch. Thus, as attackers turn the switch to the hub, they can easily snooping and exposure the communication between different hosts connected that switch.

There is a couple tool that can perform this attack. In this report we are using the command macof using kali linux. This command mimic the attacker action by sending a lot of traffic to one or more port to the switch. In this report, we try the macof command twice. Once to simulate the attack and see the result and the other one is after doing the mitigation and make sure that the switch is not affected by this kind of attack.

Mitigation:

To each interface, we have to specify the allowed mac address so that we secure the network by preventing any intrusion or unauthorized mac address.

We use the following command for this purpose :

Switch(config-if) # switchport port-security

MAC address can be learned by switch port eathier statically or dynamically. In dynamic learning process, the switch port learned the MAC address as it comes and we can specify the number of allowed MAC address in each port, otherwise it will set to 1.

Also, it is better to specify the maximum number of mac address that is supposed to connected to each switch port, so that we make sure if CAM table overflow attack happen, the switch will not be flooded with more than the maximum number that we specified earlier.

Switch(config-if)# switchport port-security maximum *max-addr*

Other way for the switch to learn the Mac address is by statically assign one or more MAC address to interfaces following the command below

Switch(config-if)# switchport port-security mac-address *mac-addr*

In case the CAM overflow attack happen, we specify what reaction should the switch port follow. There are three reaction we can choose from in case the number of mac access the maximum number: shutdown, restricted or protect.

The shutdown is the most sever option that the port is completely shutdown and admin have to manually enable the port again. Unlike shutdown option, the restrict option does not disable the port, yet it drop all the extra coming packet and produce violation notification. Lastly, the protect is the less sever option. It let the packets drop without any notification. This option is not recommeneded to use. The following command let us shoes which option the switch should follow when violation happen.

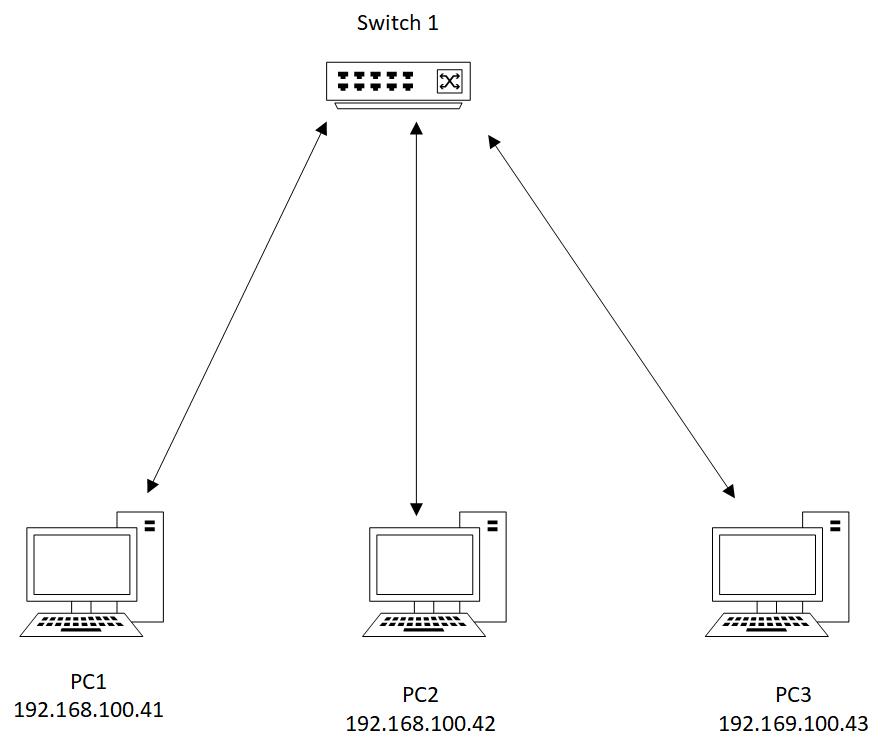
Switch(config-if) # switchport port-security violation {shutdown | restrict | protect}

To clear one of the port in switch from one mac address or all the entered mac address. We can apply the following command. The reason we do this is because we need to use the switch port for other host so we clear it if it in restrict or protect violation option

Switch# clear port-security dynamic [address *mac-addr* | interface *type mod/num*]

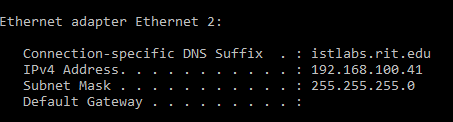
Practice:

We start up by setting up a topology, simulating the attack, do the mitigation, and try to do the attack again to make sure the switch port is secure. First we connected three devices to a switch PC1, PC2 and PC3.

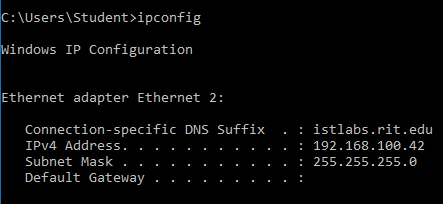


And here is the configuration for each device:

First IP for PC1:

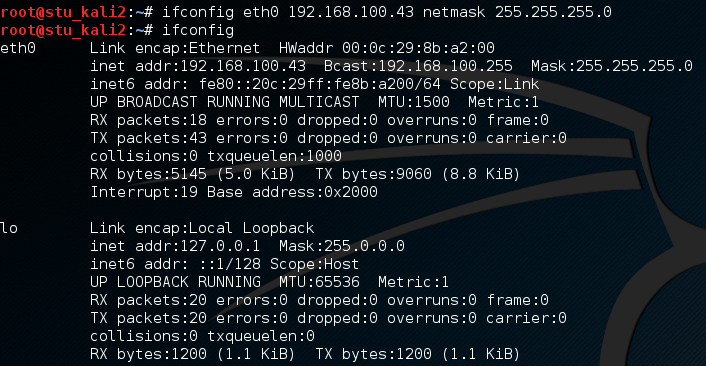


Then IP for PC2:

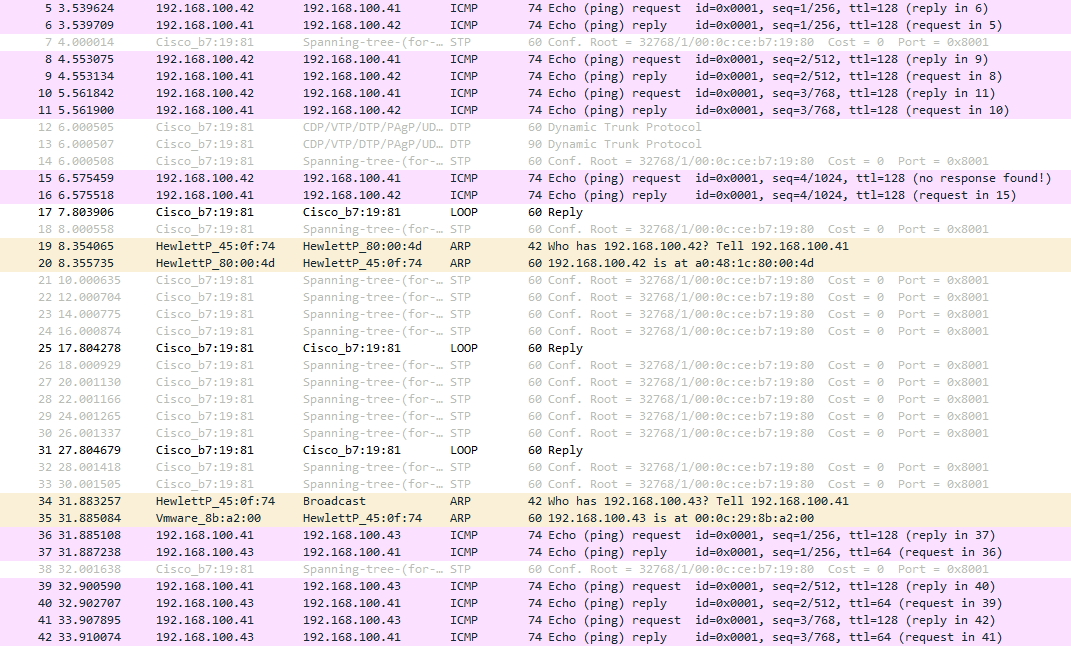


Then we set up Linux Kali Virtual machine in PC3 to perform the attack.

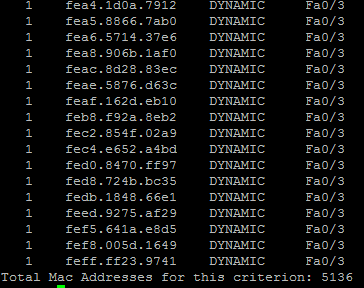
Here is the configuration



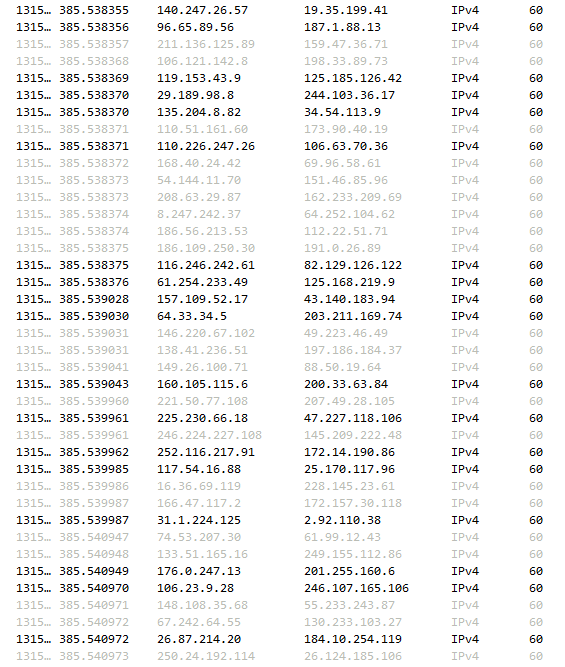
Using Wire Shark to show the connection between PC1 and PC2.



Then by using kali linux in the VM we do the CAM overflow attack using Macof. We notice here there are a lot of mac address fluded. More than the capasity of the switch



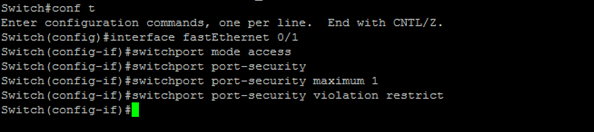
This is during the attack. Wireshark running while macof fludding the switch with many mac addresss

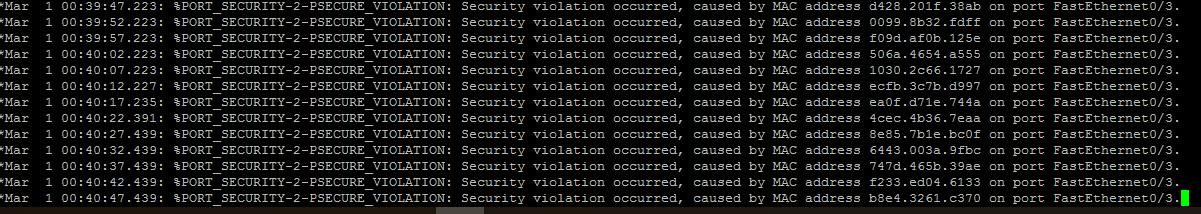


Then we try to resolve the problem by using the following command to mitigate the attack: switchport port-security

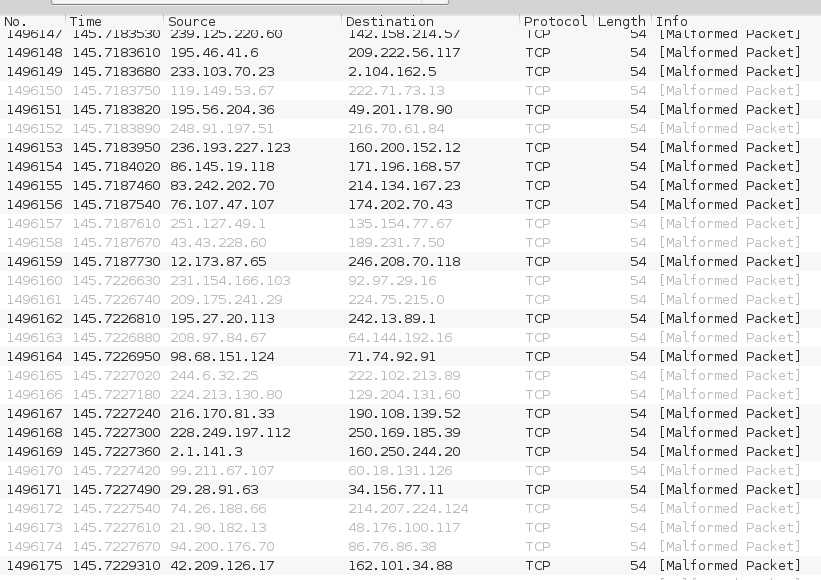


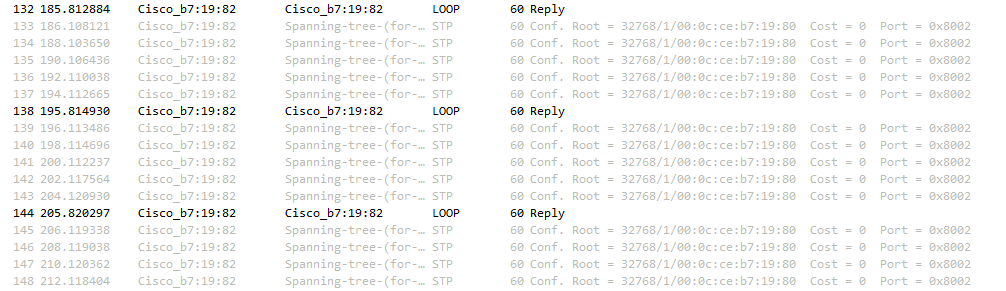
As explained above we need to specific the maximum number that allowed for the switch port and in case of violation we chose “restrict” as what we prefer the switch to do in case of CAM overflow attack. Restrict option notify admin by message for the violation

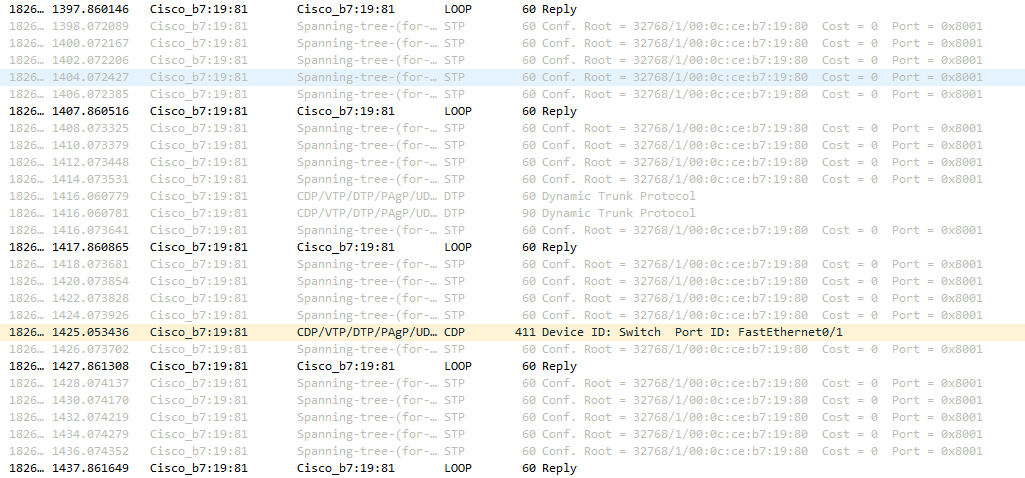




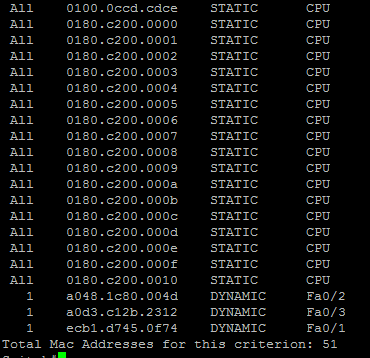
After mitigation, we try the attack again. However, Switch don’t accept any more unexpected packet. It showen here by malformed packet





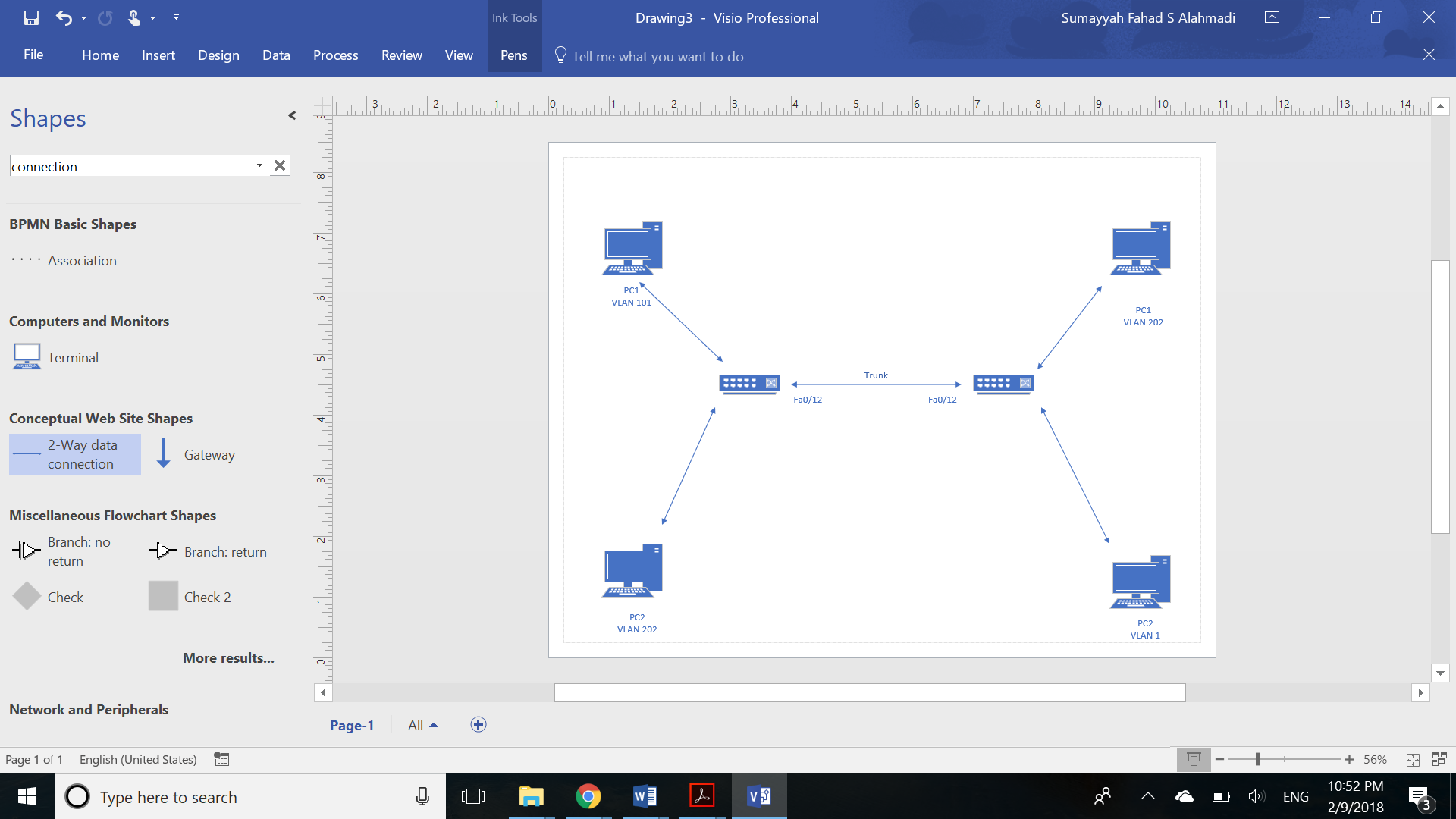


Last screenshot show that is all ststic and 3 dynamic and the max port security after the mitigation

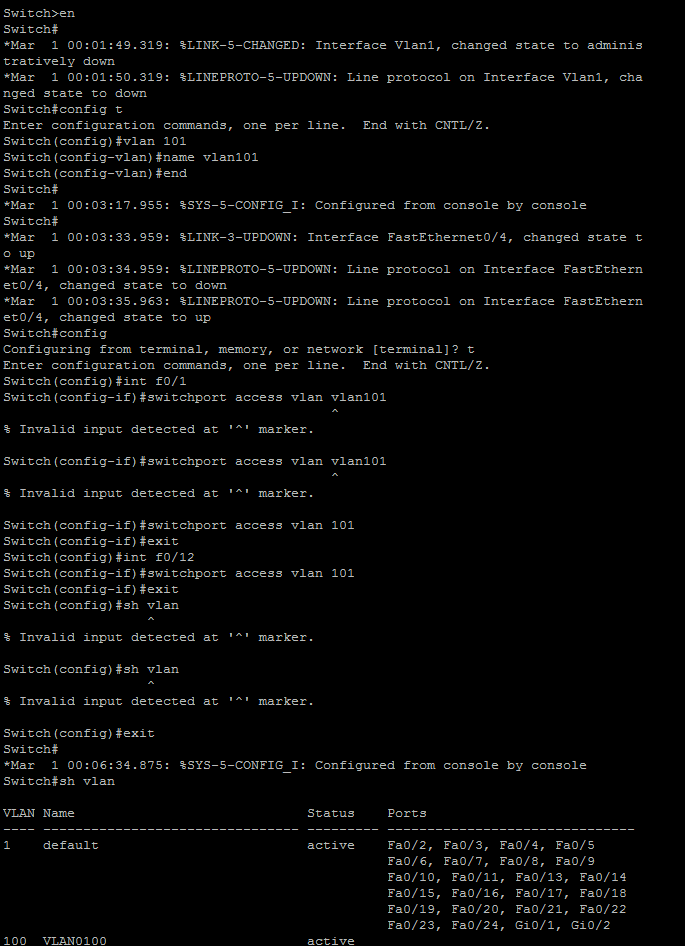


1. VLAN Hopping

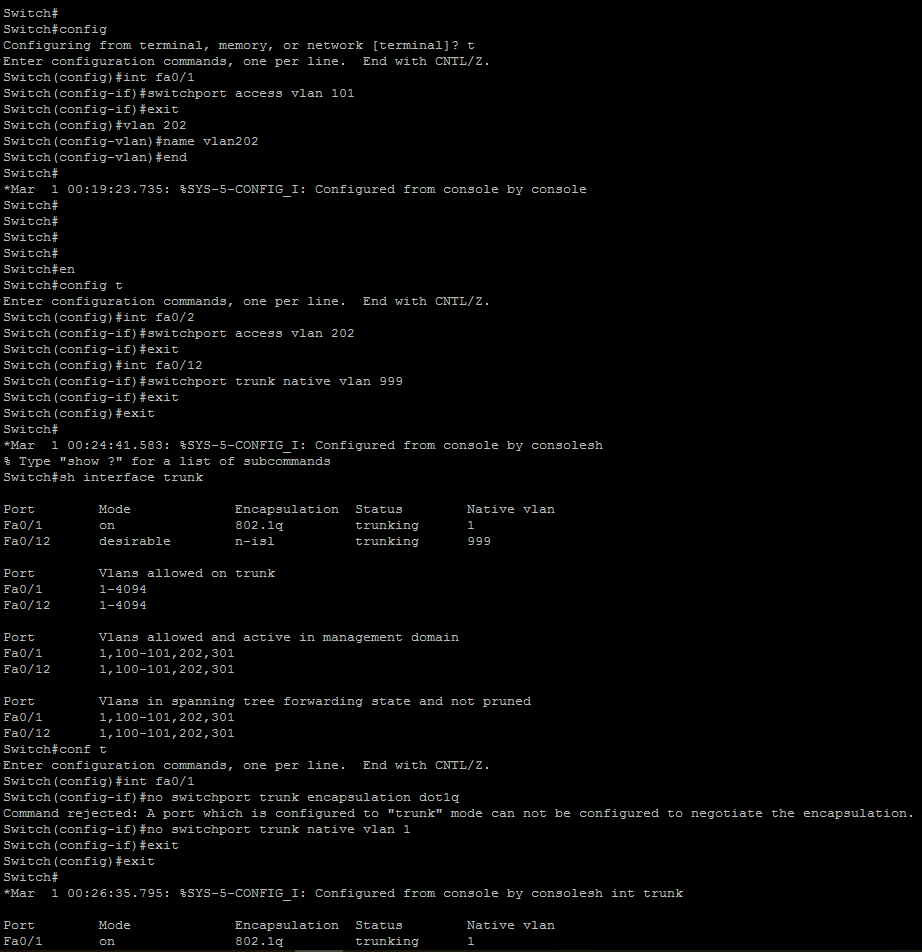
VLAN hopping is basically a pc in specific VLAN connect with other pc in different VLAN by unauthorized way. There are two methods to do vlan hopping first double tag and switch spoofing. Using protocol 802.1q to perform the double tag by double encapsulation. During this attack. A packet going from to one VLAN to another VLAN is tagged with two header. The first header is decapsulate by the first switch then it directed to the second header which will decapsulate by a second switch. Consequently, the transmited packet is going to another VLAN that is not supposed to connect to. To avoid having multiple links between every VLAN, using trunk as a one link that connect many VLAN which benefit the system user but it can misused by the attacker to hop between VLAN and breach the system spoofing. Using encapsulation and native VLAN command is the best way to mitigate this attack.



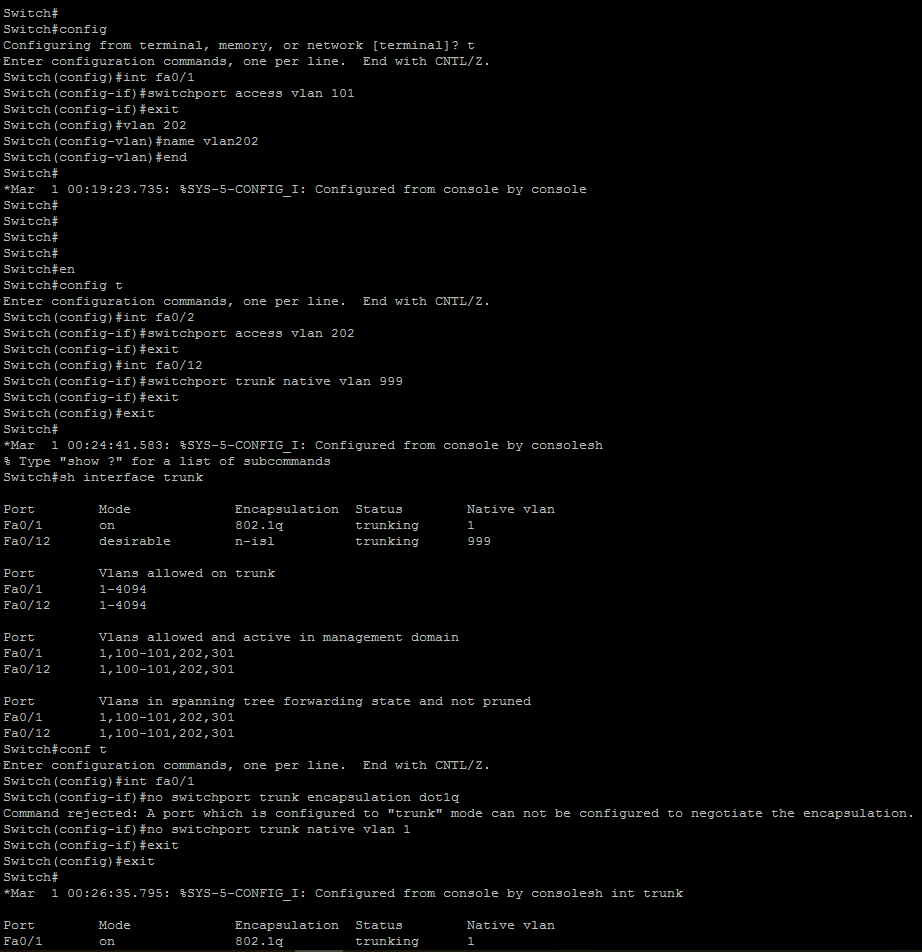
First we create VLAN 101



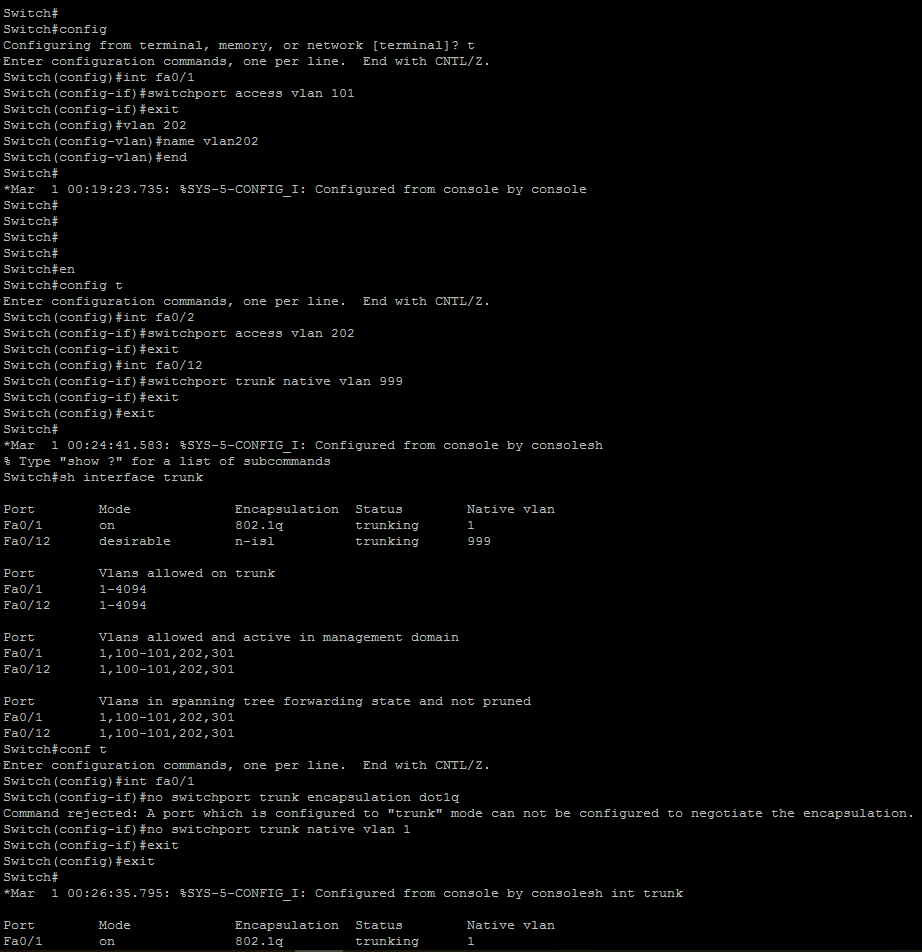
Then create another vlan and give it the number 202



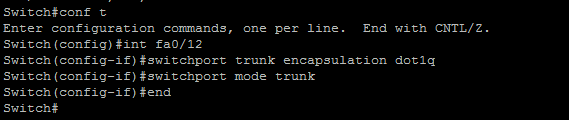
Then assign fa0/1 as an interface port for the VLAN

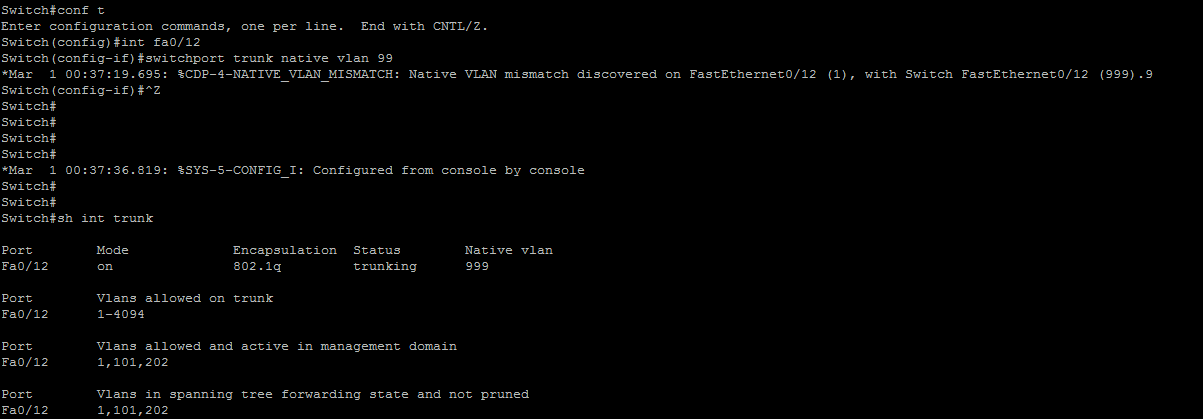


Assign an interface port fa0/2 to VLAN 202, and connect the trunk port to fa0/12. Also connect native VLAN 999 to the trunk.

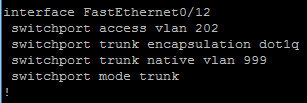


Connecting the trunk to port fa0/12

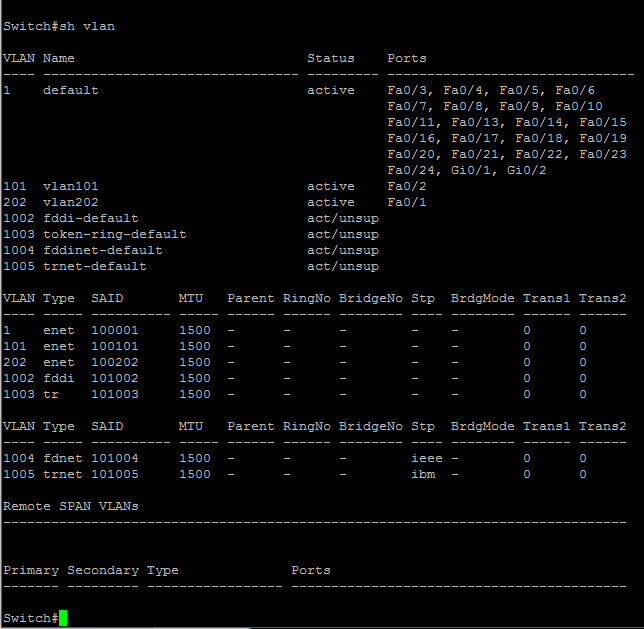
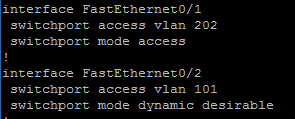




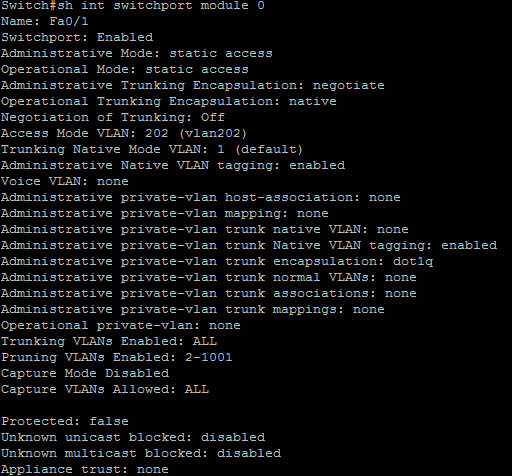
Connect the other Vlan to fa0/12



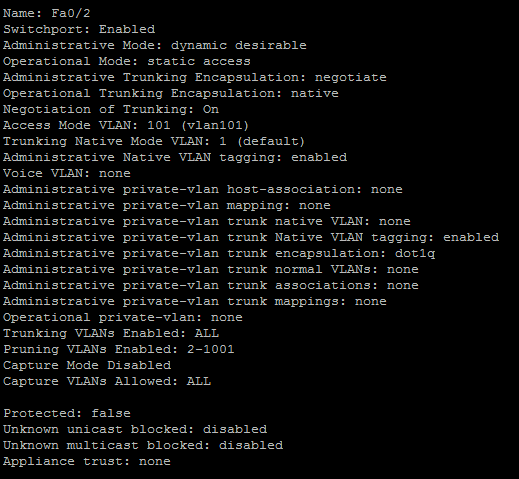
As we see here port fa0/1 is in VLAN 202 and fa0/2 is in VLAN 101



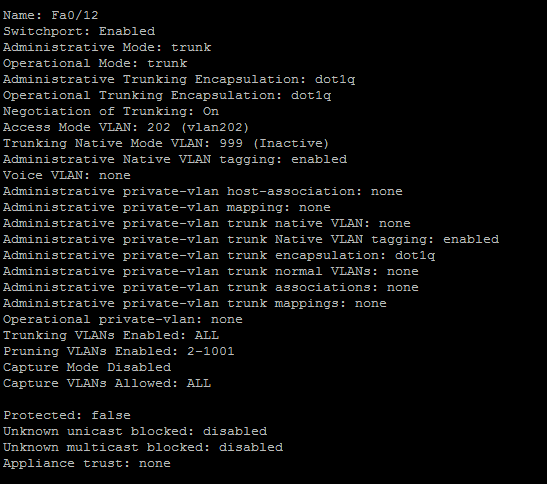
Using show command to check the status of the ports

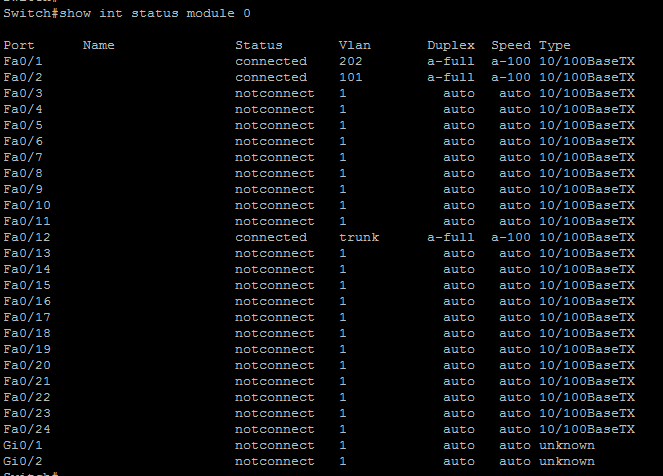


Fa0/2

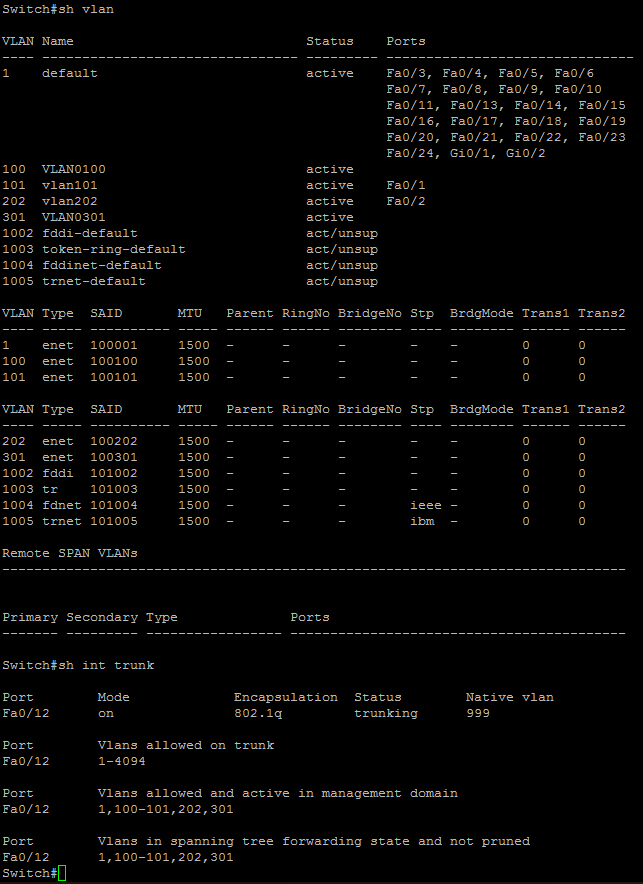


Fa0/12

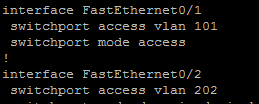


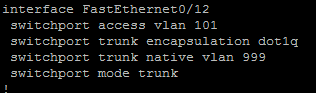


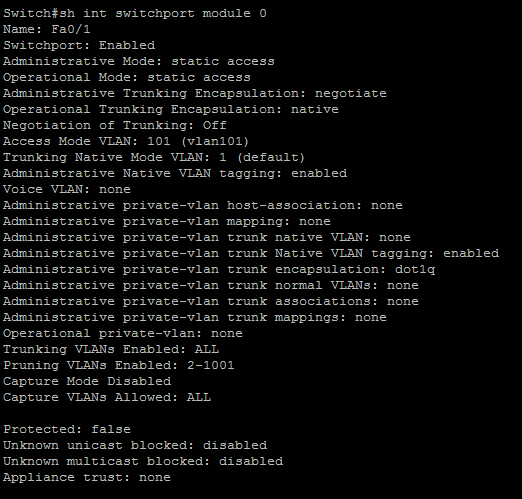
Here is a screenshot from the other switch where port fa0/1 connect to vlan 101 and port fa0/2 connect vlan202



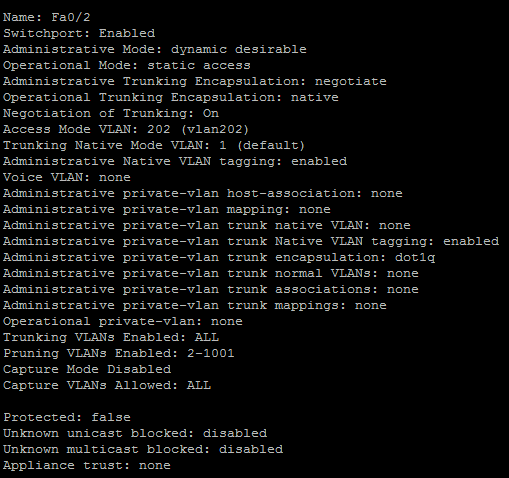
Screenshot from the other switch



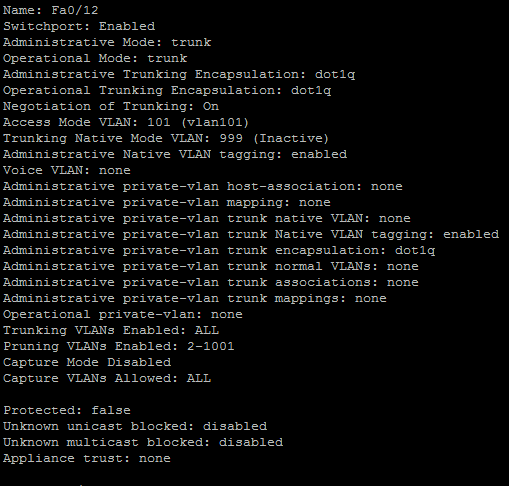




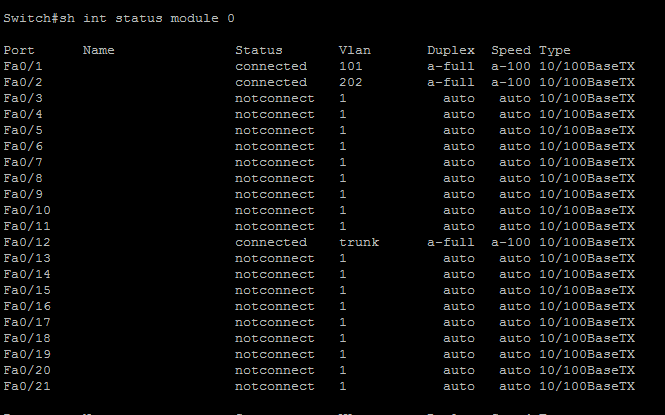
Interface port fa2/1



Fa0/12



All the port: 1,2,12



1. Conclusion

In summary, there are many attack and vulnerability in network layer. Fixing error and mitigate risk is a useful way to prevent attacker from having unauthorized access and breach to a sensitive data. In this report, we explained in detail two of the most known vulnerability and their mitigation. Port security make sure that all the ports are connected to legitimate and expected MAC address. VLAN hopping is when an attacker connect to another VLAN that is not authorized to connect to. Also, we prove that by using specific mitigation we can reduce the impact of these two attacks.

1. References

Lectures slide