DHCP Snooping

IP Source Guard

Dynamic ARP inspection

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. DHCP snooping……..……………………………………………………………….. 3
2. IP Source Guard………...…………………………………………………………….. 4
3. Dynamic ARP inspection ……………………………………………………………. 5
4. Conclusion……………………………………………………………………………. 5
5. References ……………………………………………………………………………. 6

DHCP Snooping

Concept:

The Dynamic Host Configuration Protocol (DHCP) server plays a major rule in network communication as it is responsible for assign IPs to each host in the network and provide other essential information like DNS server and default gateway address. When a host try to connect to the network for the first time, it sends a discover message for the DHCP trying to connect to the server. Then the legitimate DHCP server send an offer message to the host. Attacker can take advantages of these server by playing a role as DHCP server and send an offer to the host that appears as it comes from the authorized server. This rogue DHCP will send to the host his IP as the default router gateway. Thus, each time the host send a packet to the network outside its subnet, it goes through the attacker first then the attacker send it to the router gateway. The same happen when the router try to send information to the host, the attacker have the ability to view the packet before it sends it to the host. The user continues sending information as he or she thinks it goes directly to the router. This consider a man in-the-middle attack and it affects the confidentiality of the system and the integrity in case the attacker altered the message. Preventing the attacker from sending spoofed address is a significant mitigation for this attack. One way to assure the user wont be victim for this type of man in the middle attack, we can enable the DHCP snooping feature. Then determine one port in the switch as a trusted port while all other ports as untrusted, so that we can prevent the switch from connected to the rogue DHCP server. Only trusted port is connected to the legitimate DHCP server, and it is the only port allow to send discover and replay message. Coming packets from another ports is dropped by the switch, and that port will go through an automatic shutdown. The default configuration is that all the switch port are untrusted and has unlimited rate. In this report, we will simulate DHCP starvation attack which could be done by sending crazy amount of request to the DHCP server, so no more IPs left for the legitimate host.

Command:

First, we enable the DHCP snooping feature

* + Switch(config)# **ip dhcp snooping**

Determine which VLAN we will apply the DHCP server in

* + Switch(config)# **ip dhcp snooping vlan** *vlan-id* [*vlan-id*]

Configuring only one trusted port where is allowed to send reply message to a legitimate DHCP server

* + Switch(config)# **interface** *type mod/num*
  + Switch(config-if)# **ip dhcp snooping trust**

For the rest of switch ports, untrusted port, it is better to limit the traffic using this command Otherwise it sits to unlimited by default.

* + Switch(config)# **interface** *type mod/num*
  + Switch(config-if)# **ip dhcp snooping limit rate** *rate*

As the untrusted port drop the message, some information can be added to the option-82 request field to let the packet go through and reach legitimate DHCP server. Also, same information added in the DHCP reply to make sure the packet came from that switch.

* + Switch(config)# [**no**] **ip dhcp snooping information option**

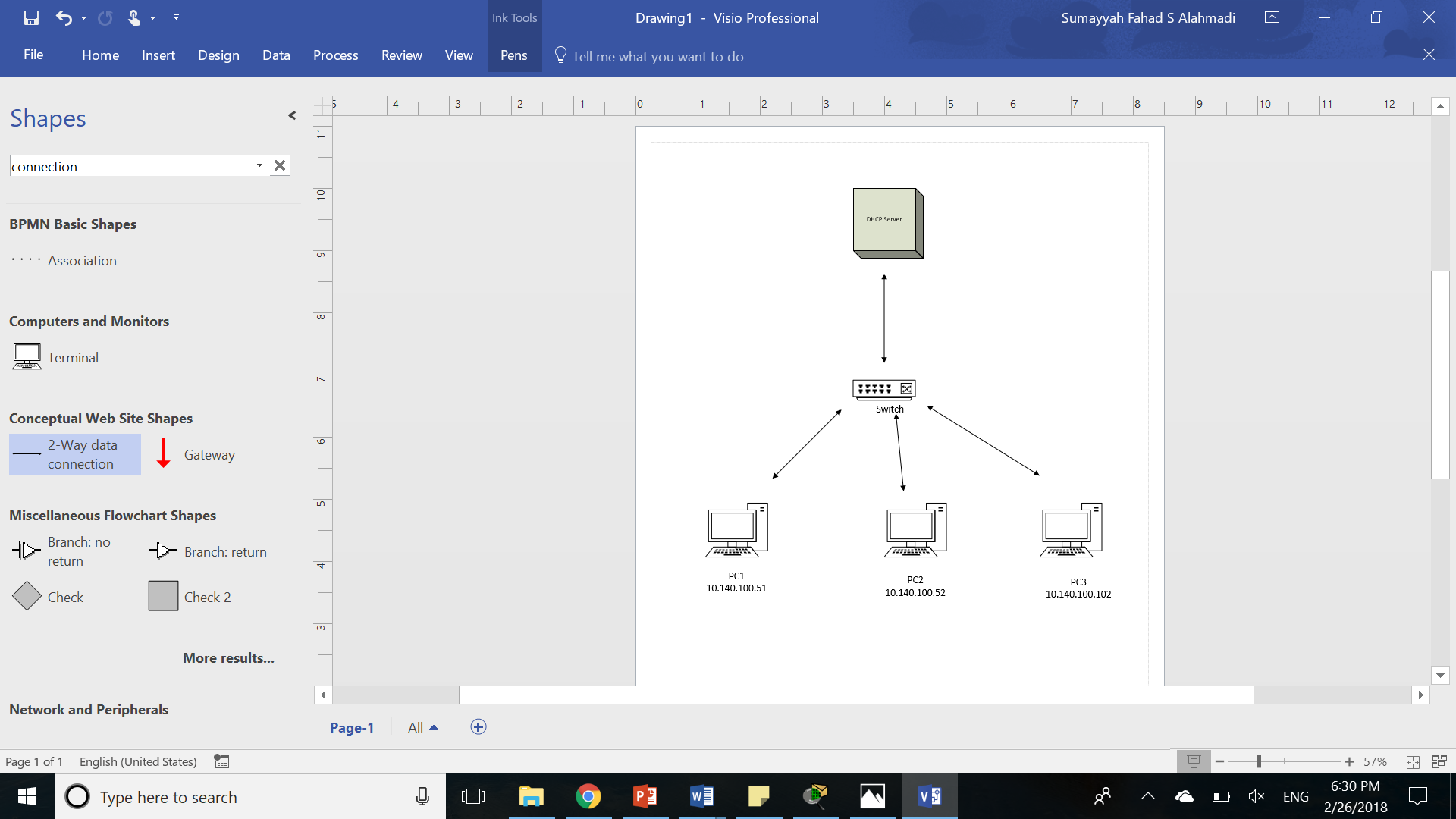
To view all the completed connections we can use the following command which show all connection saved in the switch memory database. Or view all recorded connection by added the word binding.

* + Switch# **show ip dhcp snooping** [**binding**]
  + To mitigate DHCP starvation attack that done by Yersinia, we use either p Switch(config)# **arp access-list acl-name**
  + Switch(config-acl)# **permit ip host** *sender-ip* **mac host** *sender-mac* [**log**]
  + Switch(config-acl)# **exit**

ort security for multiple MAC address or the following command for the same MAC address which verify that MAC address in the frame and DHCP reply is the same

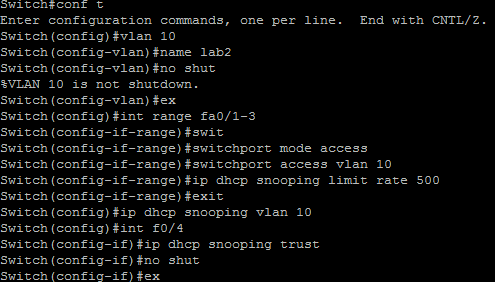
* + **ip** **dhcp snooping verify mac-address**

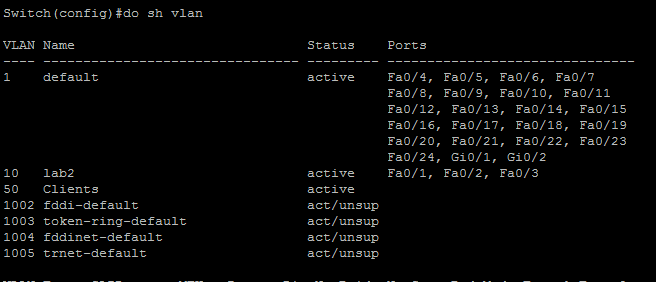
Topology:



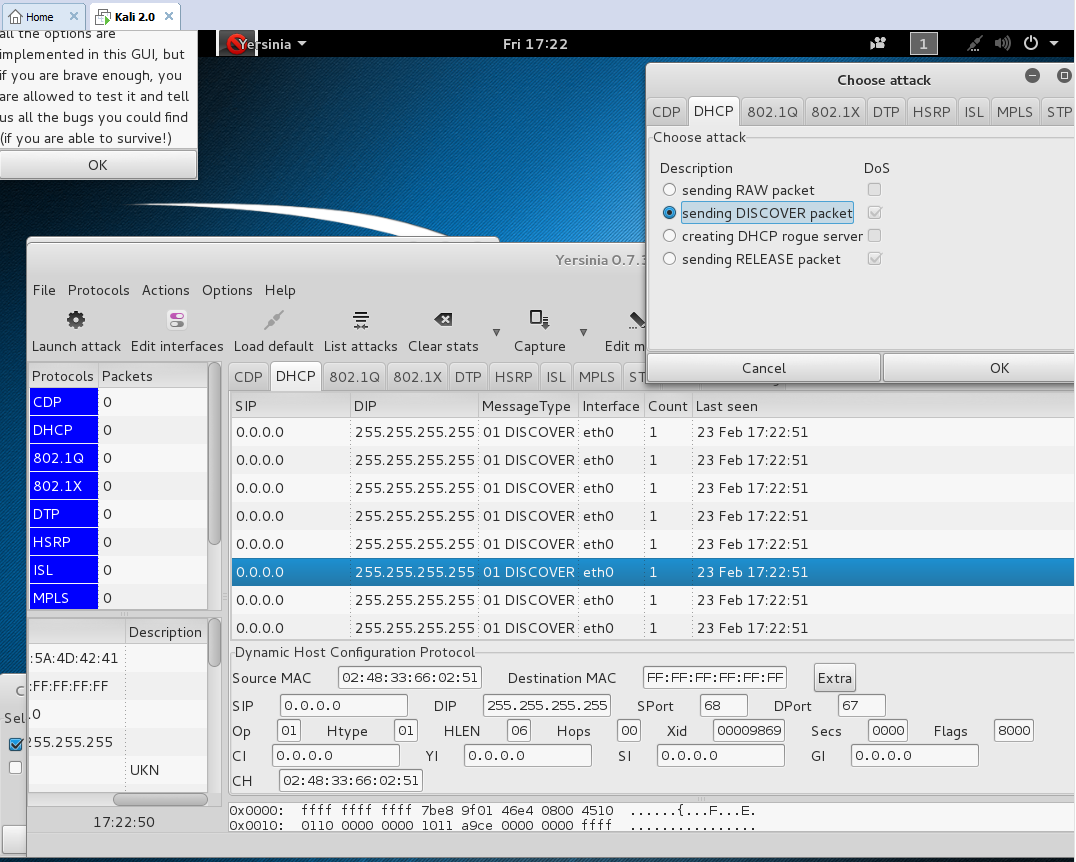
Implementation:

First we configured the VLAN 10

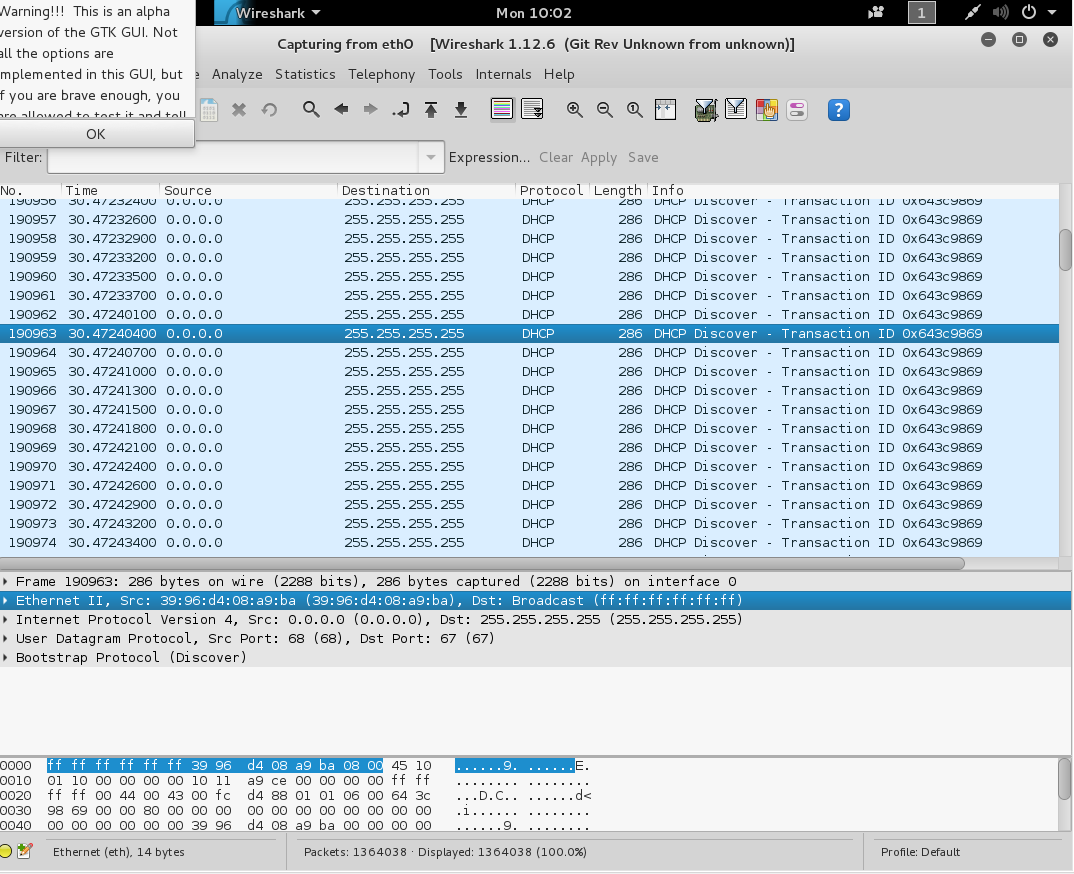


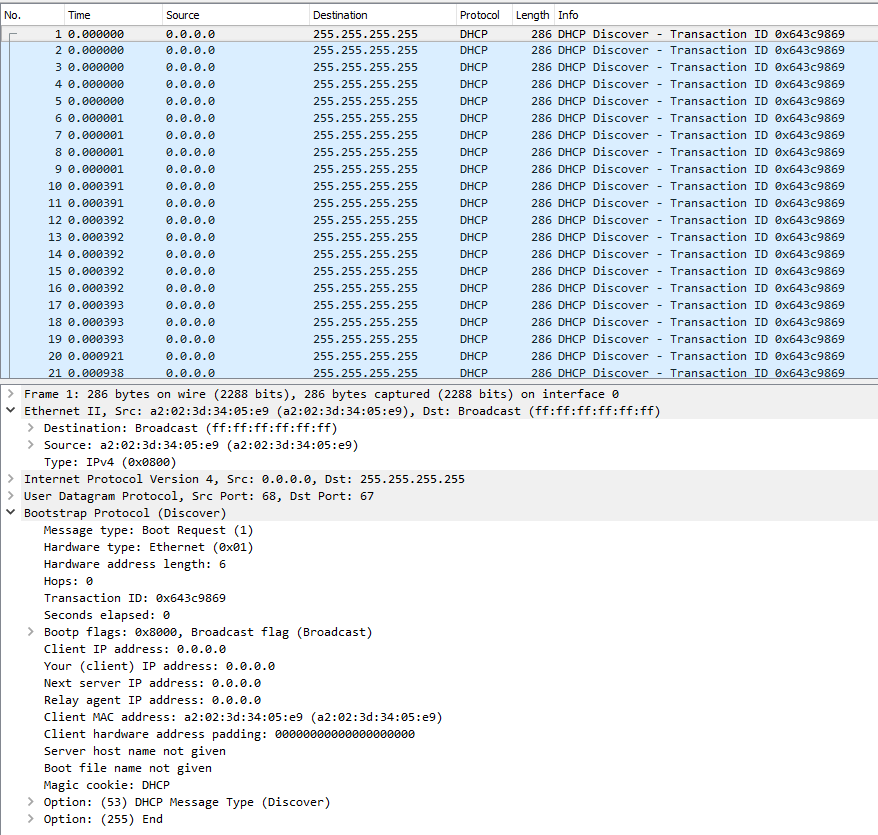


Using Yersinia to perform the attack

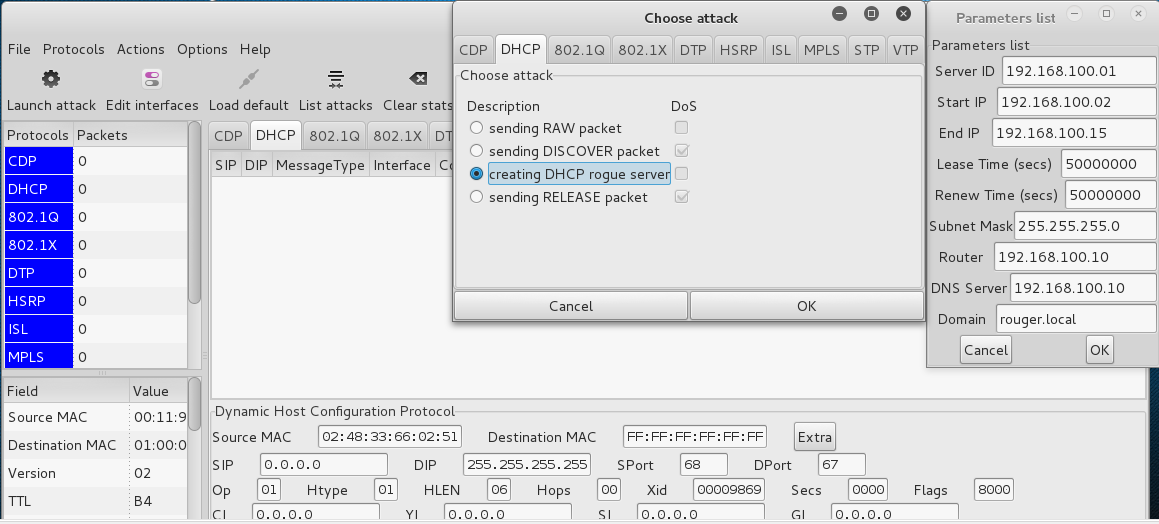


Attacker Wireshark

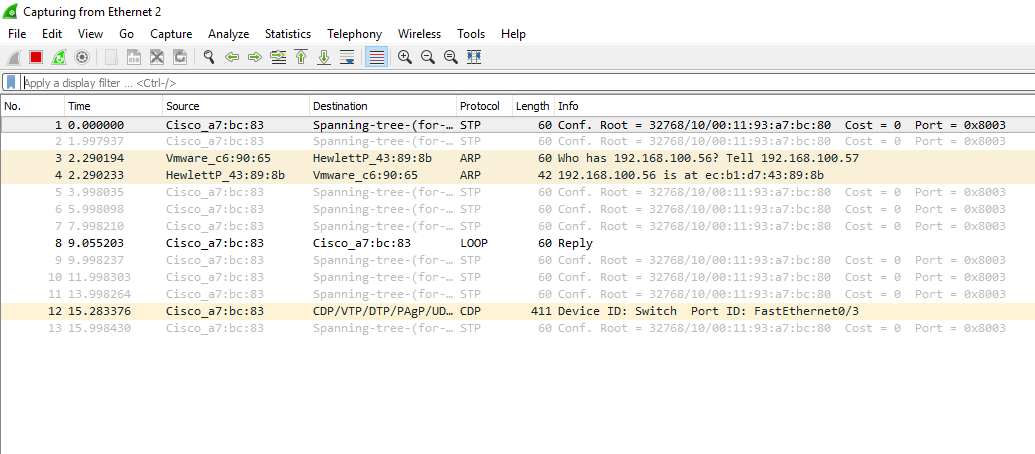
****victim wireshark

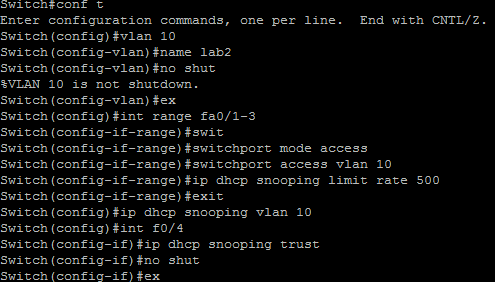


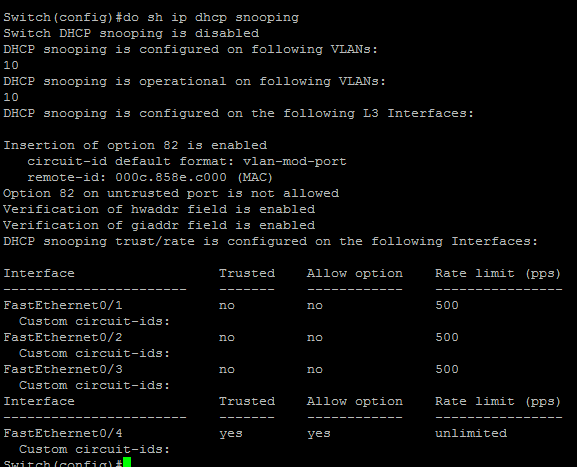
Performing DHCP rough server

****

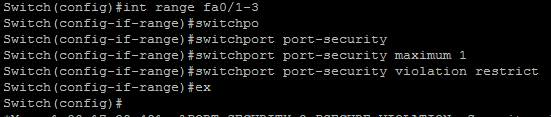
Attacker wireshark

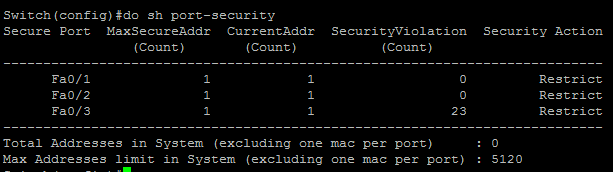
mitigation



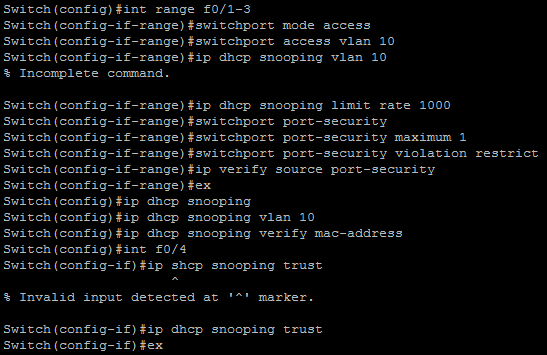


Enable port security

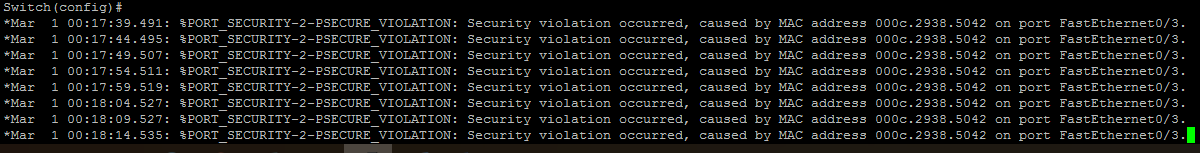




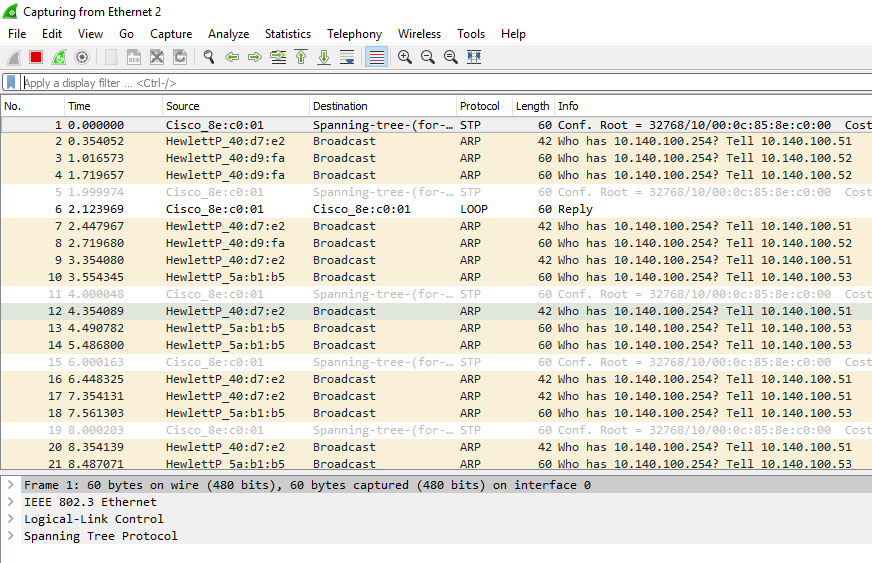
Enable dhcp snooping

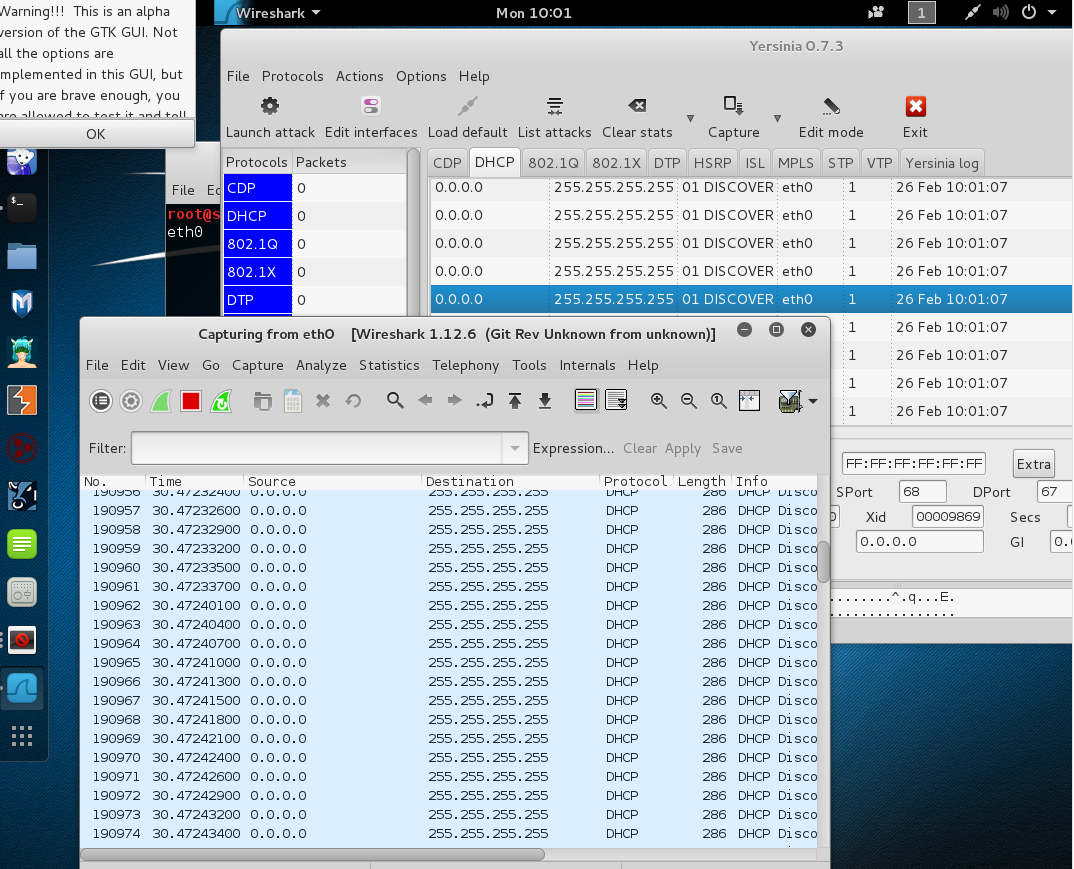


After the attack we see violation message



Wireshark after mitigation on victim and attacker





IP Source Guard

By default, each host has unique IP address that supposed to use in all network communication. Malicious hosts use different illegitimate IP address in its communication. The purpose of these malicious activity is to support denial of service attack because packets cannot return to the illegitimate IP address that is not really exist. This attack can be easy to detect if the illegitimate IP address was generated from VLAN the use different subnet. Nevertheless, attacking by using spoofed IP address that in the same supposed subnet is harder to discover. Therefore, implementing IP Source Guard in the switch is a significant step to recognize spoofed IP address from the same subnet and hinder upcoming communication.

In the previous section, we enabled the IP DHCP snooping, so now we have a database full of legitimate IP addresses and their associated MAC address. Thus, when a port receive a packet it compare its IP and MAC address to the ones in its database. If the switch find the exact similar IP and MAC address in its database, it will let the packet pass otherwise the switch will drop the packet. In order to enable IP source guard feature, we first have to enable port security and DHCP snooping.

Command:

First, enable IP source guard on specific interface in the switch:

* + Switch(config)# **interface** *type mod/num*
  + Switch(config-if)# **ip verify source** [**port-security**]

The following command is to configure a static IP address for those hosts that don’t use DHCP service.

* + Switch(config)# **ip source binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *type mod/num*

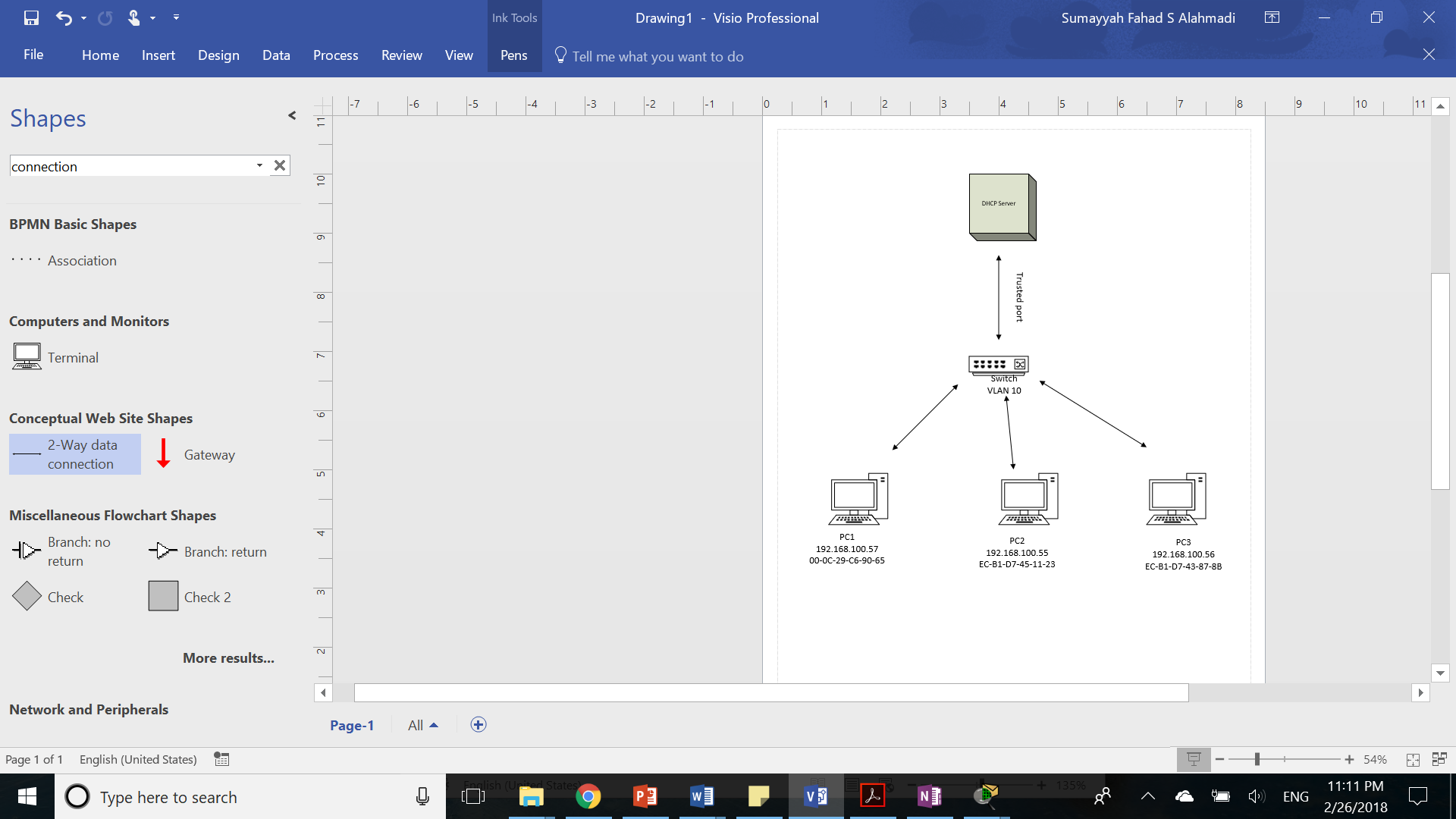
Next, checking the status of IP source guard

* + Switch# **show ip verify source** [**interface** *type mod/num*]

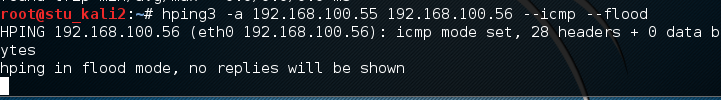
Furthermore, you can check the data inside the IP source binding database by using the command bellow

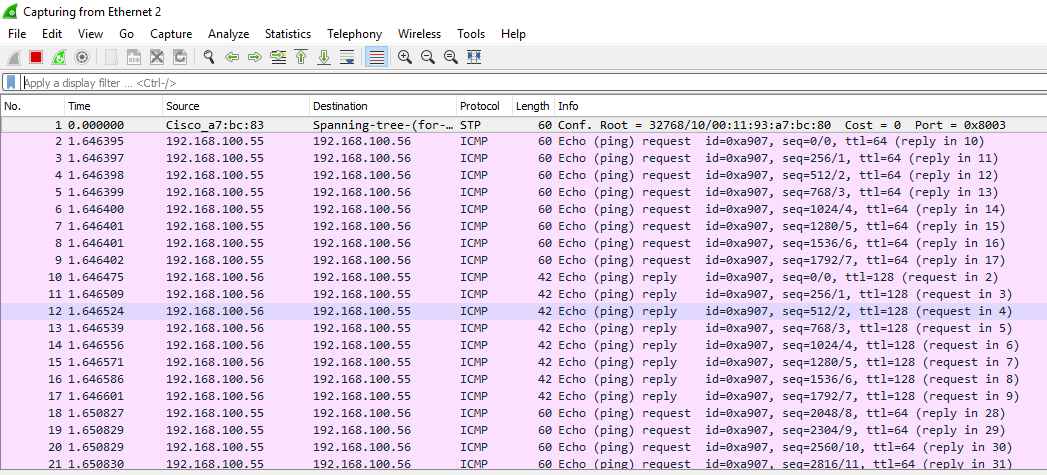
* + Switch# **show ip source binding** [*ip-address*] [*mac-address*] [**dhcp-snooping** | **static**] [**interface** *type mod/num*] [**vlan** *vlan-id*]

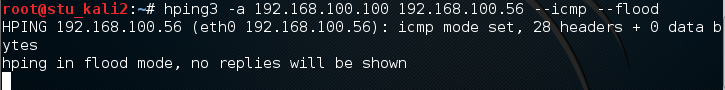
Topology:

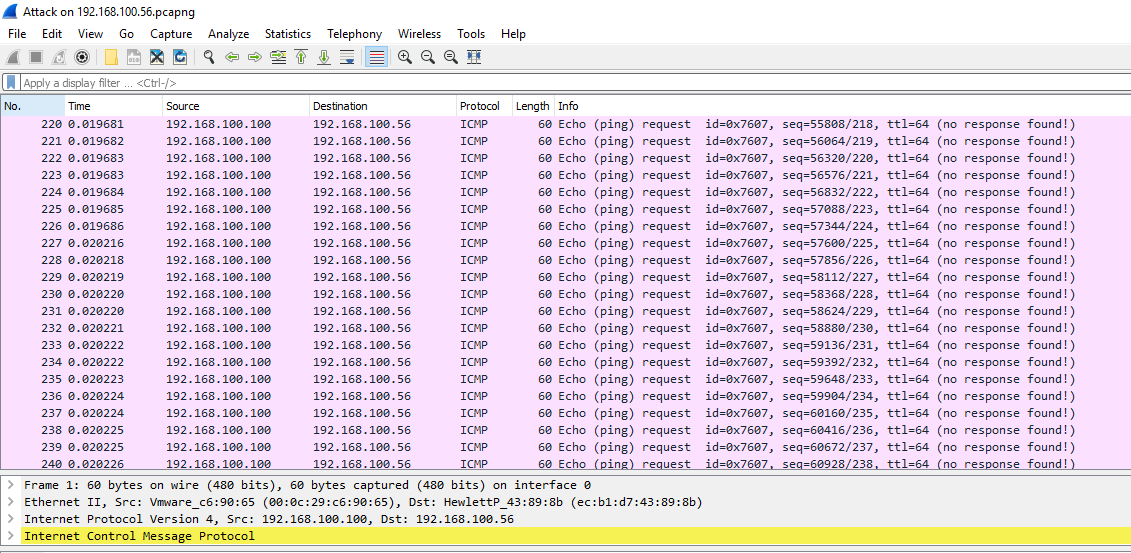


Implementation:

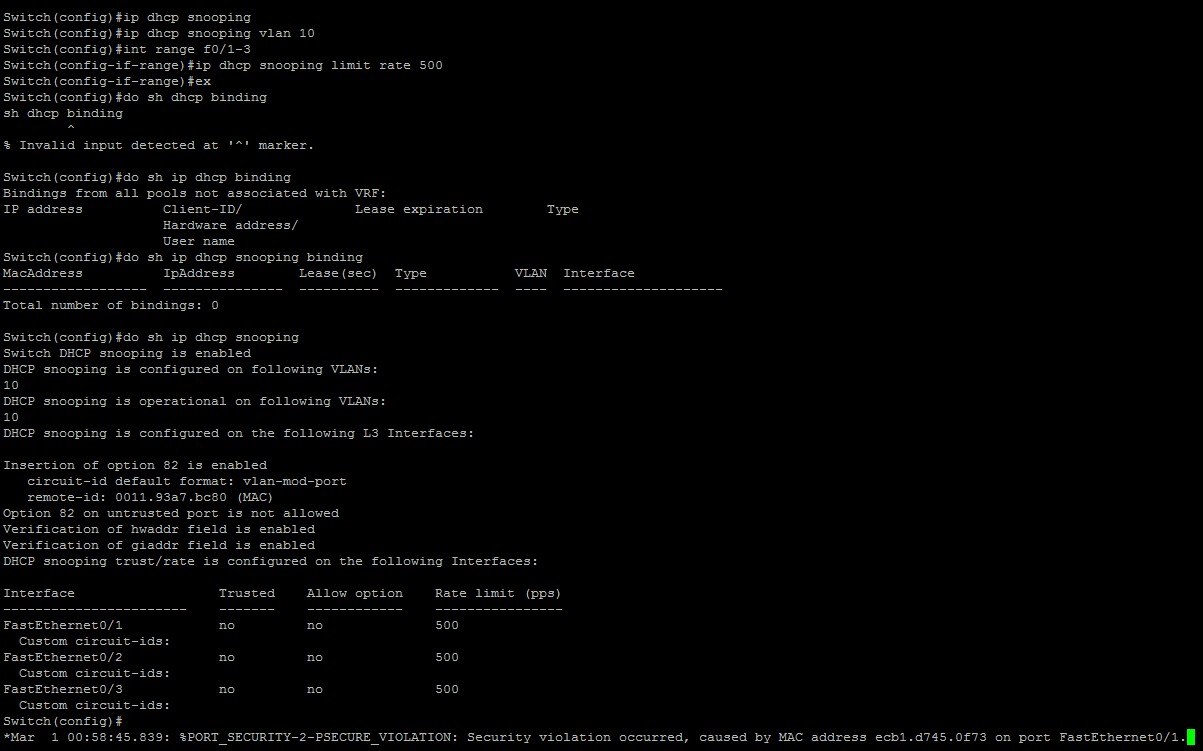


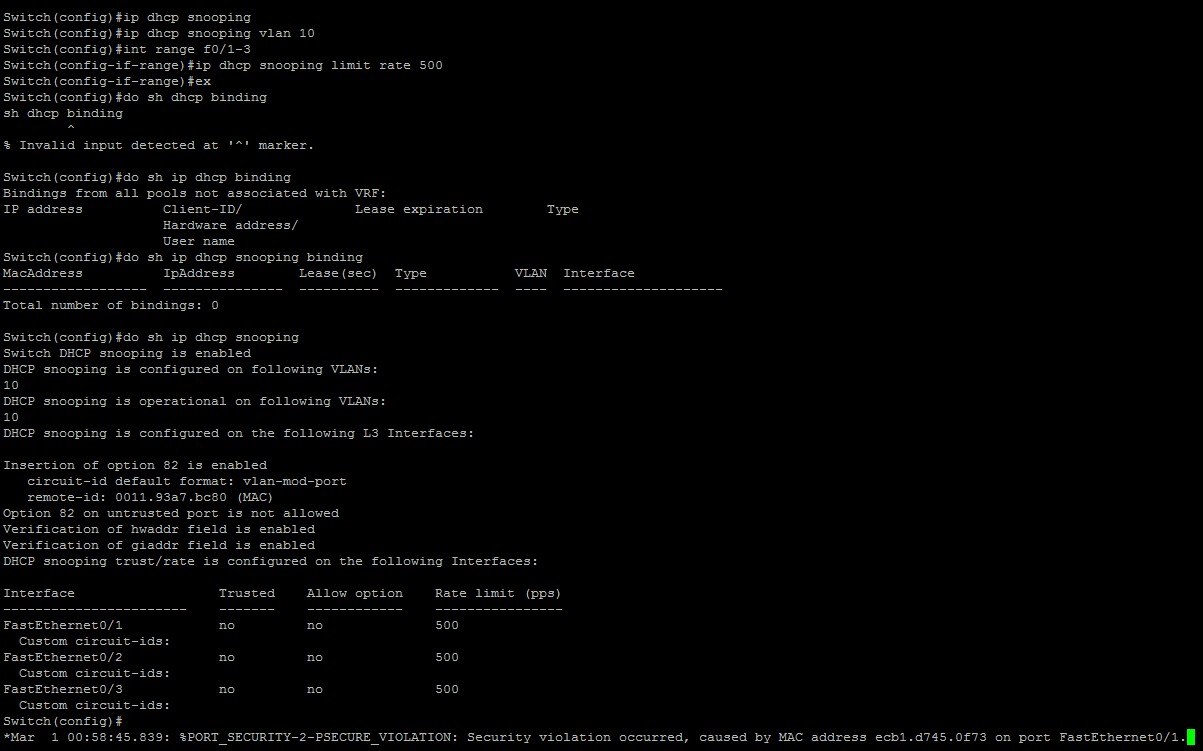


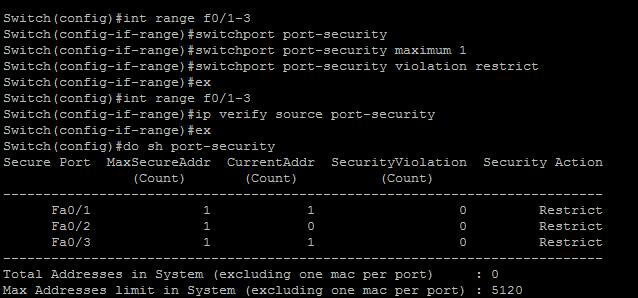


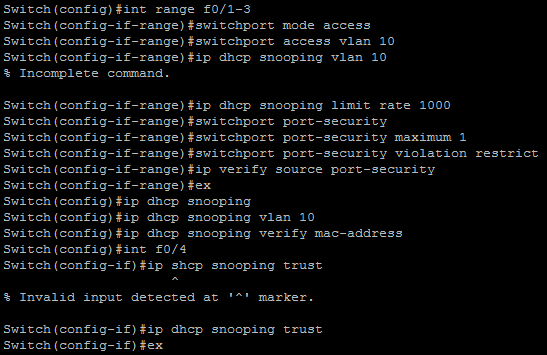


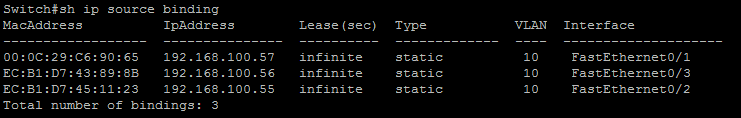
Mitigation

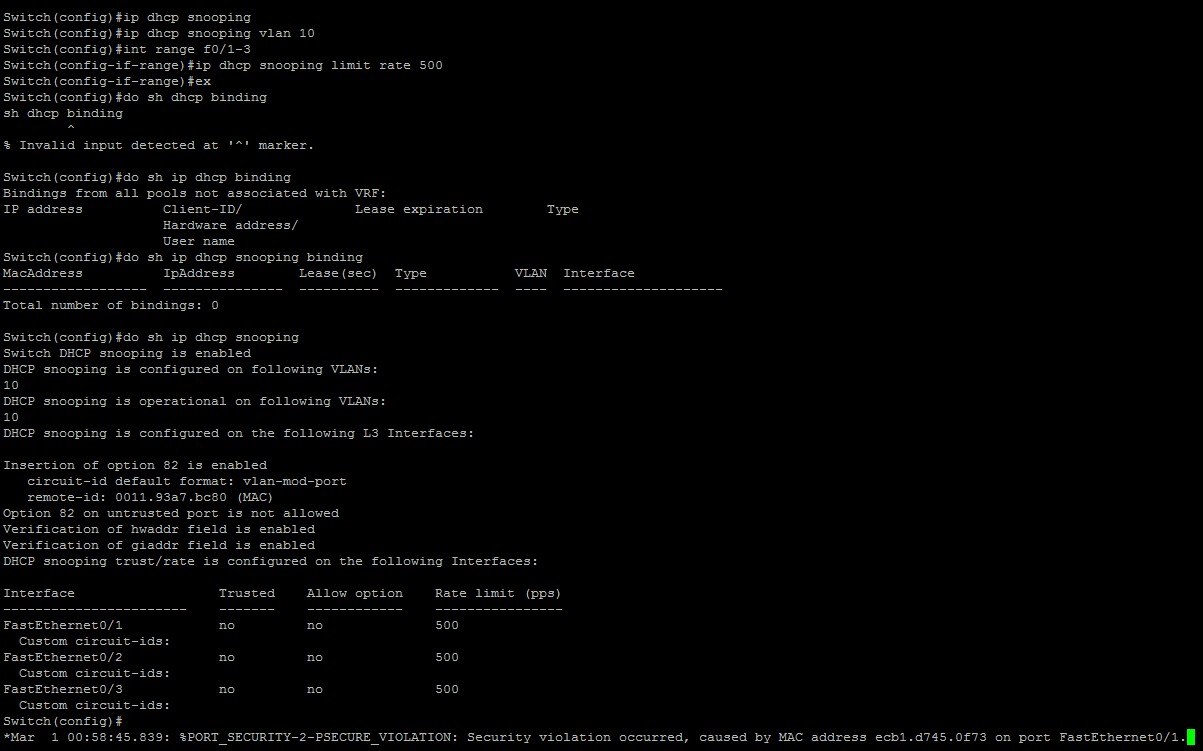


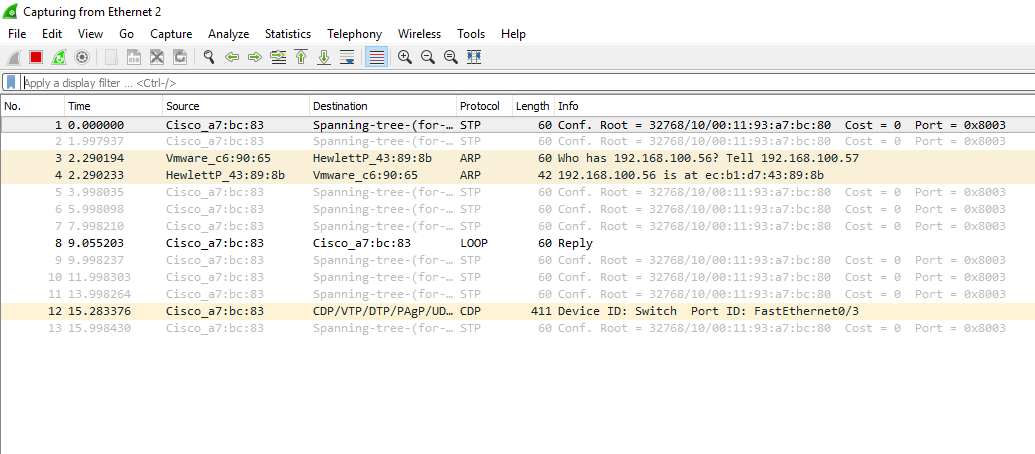


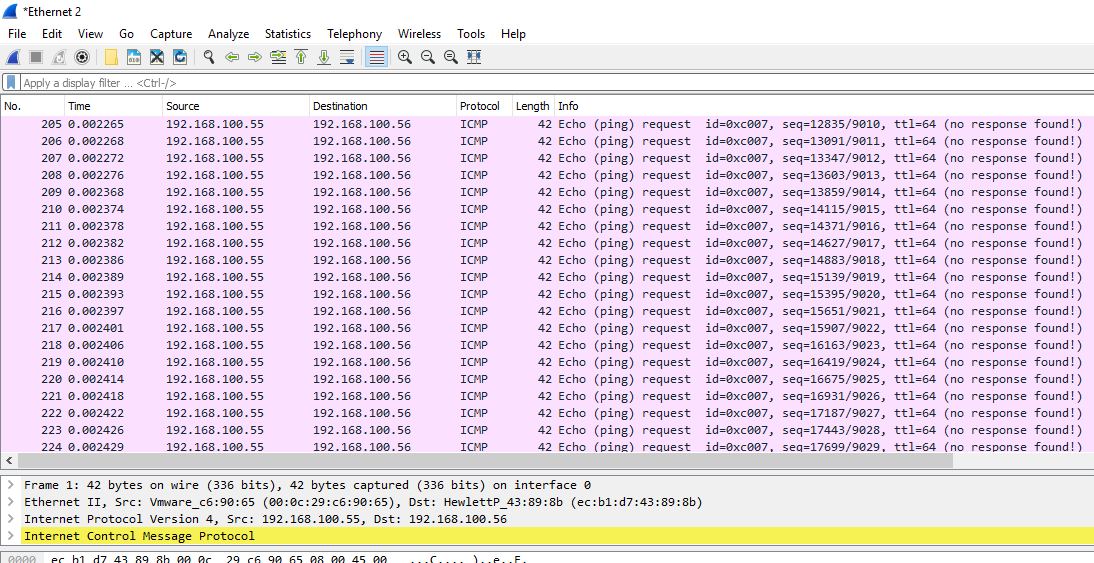




****







Dynamic ARP Inspection

Concept:

In layer 2, host need to find a way to direct traffic. In some cases, the host does not know the MAC address of the destination host, so the host try to find MAC address by searching on its based on its IP address. Using Address Resolution Protocol (ARP), the host is able to send a broadcast message looking for a MAC address of the target based on its IP address. When the message has received to a host that have the same IP, the target host send its MAC address. The attacker can take advantages of this situation by sending fake ARP reply pretending that its his IP address. Thus, when the victim host send a broadcast by specific IP, it receives an incorrect MAC address. As the victim host has no idea that it has the malicious host MAC address, the victim host will send packets to the attacker thinking it is an intended destination host. To prevent this type of an attack which called ARP poising attack, we will be implementing Dynamic ARP Inspection (DAI) which will classify the switch ports as trusted and untrusted. ARP has Access Control List ACL which will compare the upcoming traffic data to untrusted port with an already existing ones. This ACL created either statically or by DHCP snooping database while packet in trusted port doesn’t need any further chucking. In case the information in the ARP reply doesn’t match the ones in the untrusted port database, the switch will intercept the message and produce alert message.

Command:

Configuration command for enabling dynamic ARP inspection in a VLAN

* + Switch(config)# **ip arp inspection vlan** *vlan-range*

Configuration command for selecting trusted port, otherwise it is untrusted by default.

* + Switch(config)# **interface** *type mod/num*
  + Switch(config-if)# **ip arp inspection trust**

Configuration command for listing the allowed IP address statically

* + Switch(config)# **arp access-list acl-name**
  + Switch(config-acl)# **permit ip host** *sender-ip* **mac host** *sender-mac* [**log**]
  + Switch(config-acl)# **exit**

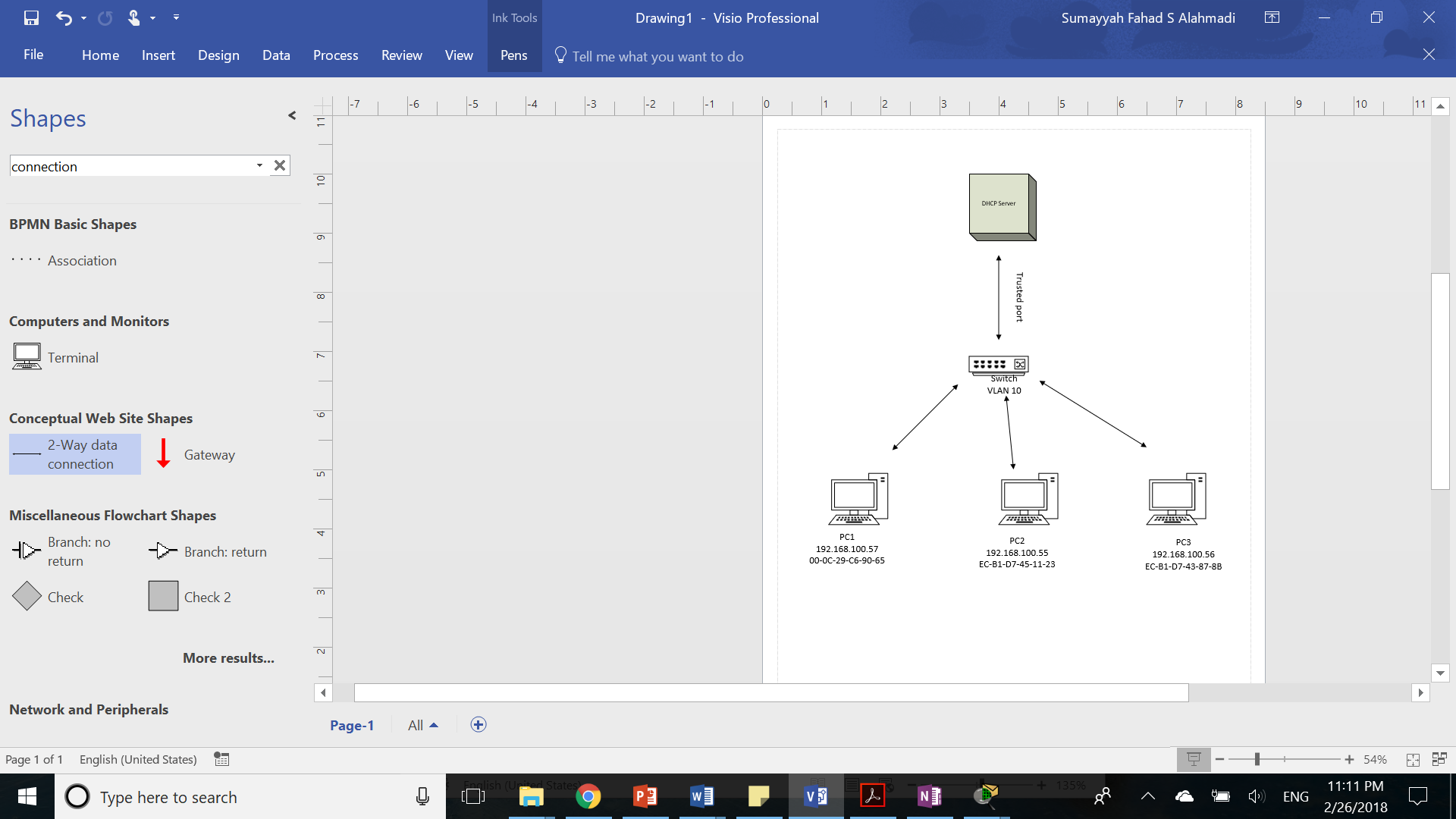
After we figure out the access command list we implemented to dynamic ARP inspection

* + Switch(config)# **ip arp inspection filter** *arp-acl-name* **vlan** *vlan-range* [**static**]

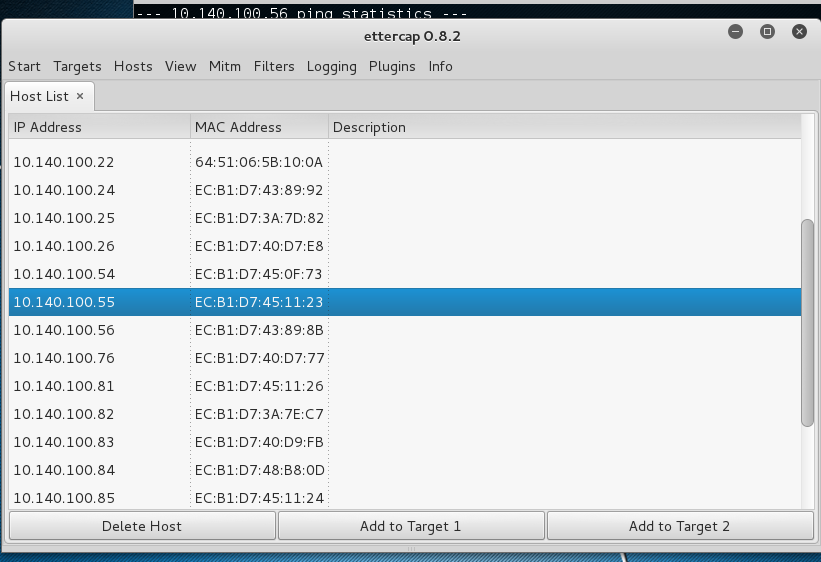
Configuration command for enabling dynamic ARP inspection validation which comes in handy for making sure that the address in the ARP reply coming from the same claimed host.

* + Switch(config)# **ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]}

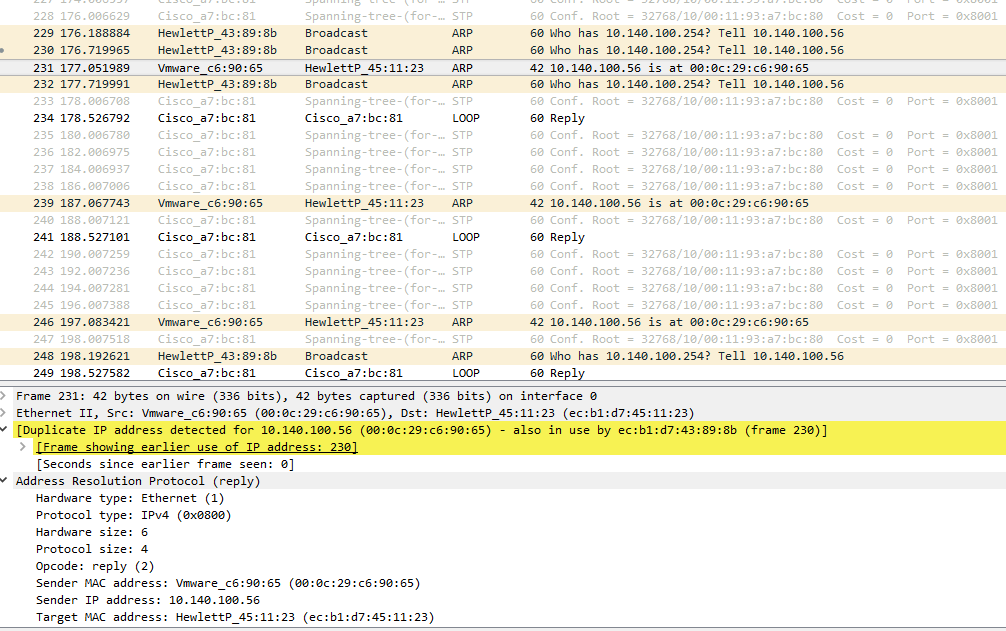
Topology:



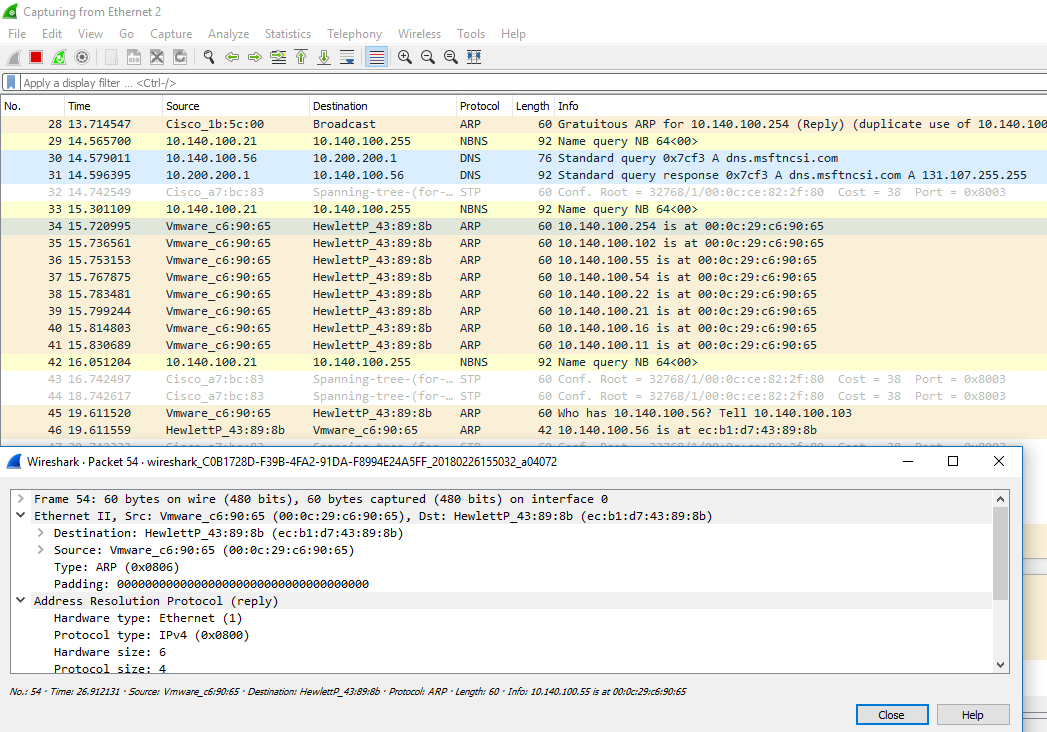
Implementation:



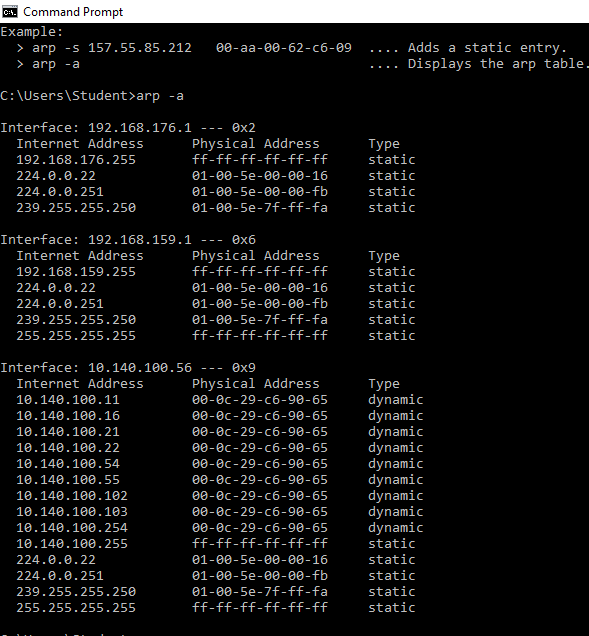
attacker machine

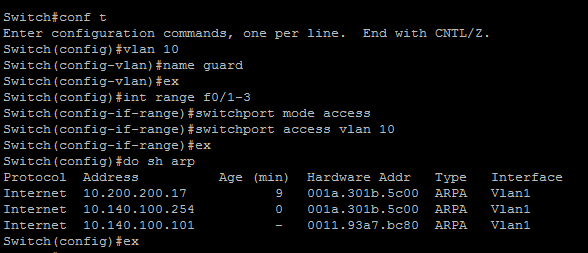


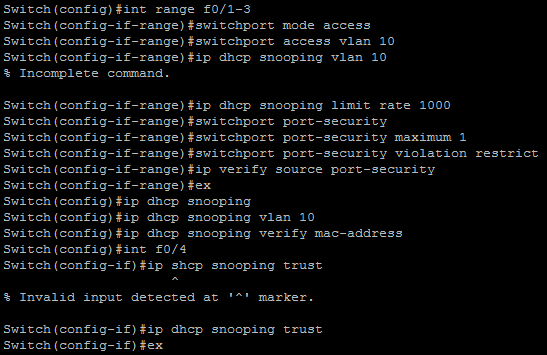
victim machine

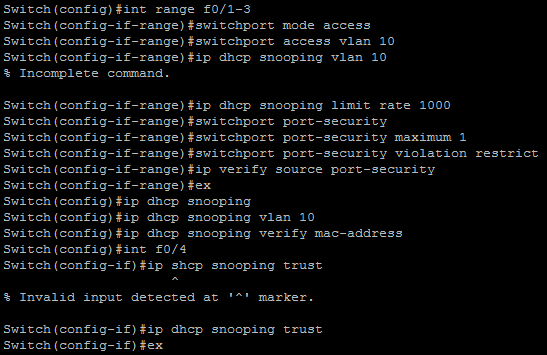


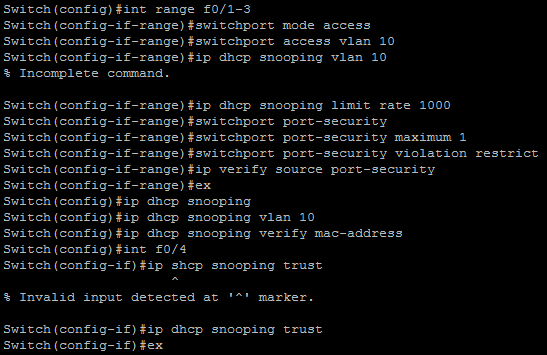
after the attack:

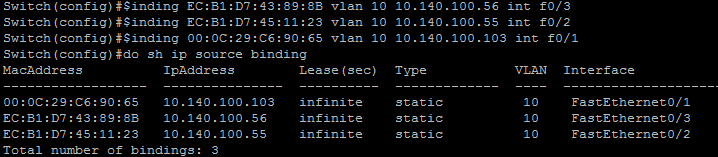


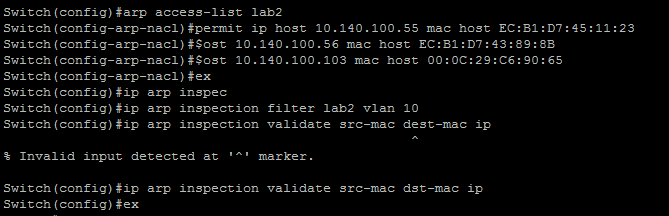


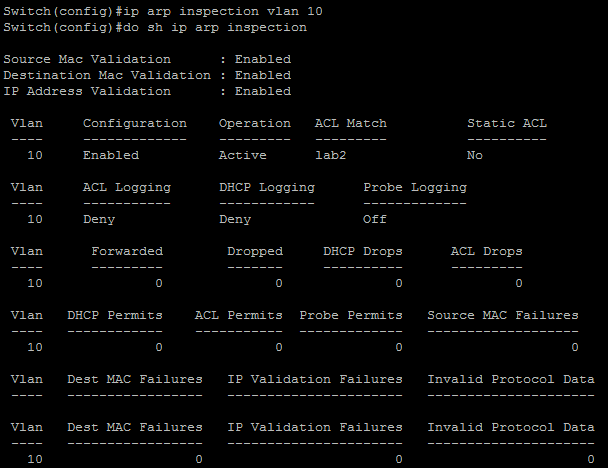




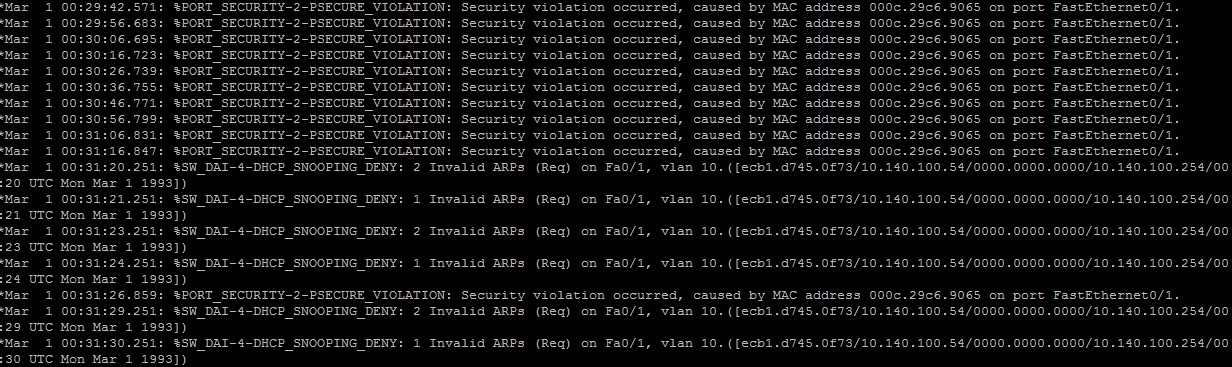




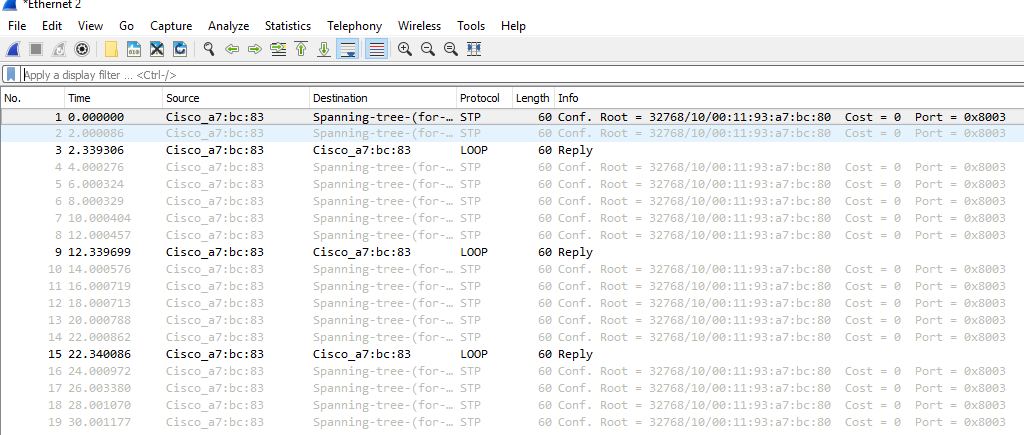




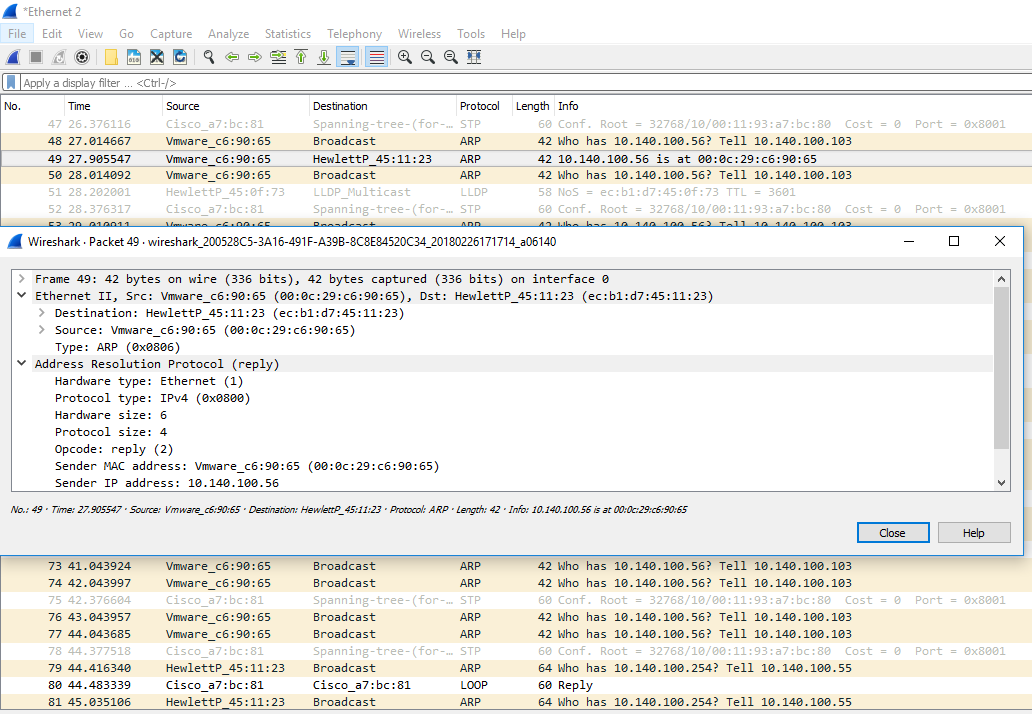
after mitigation

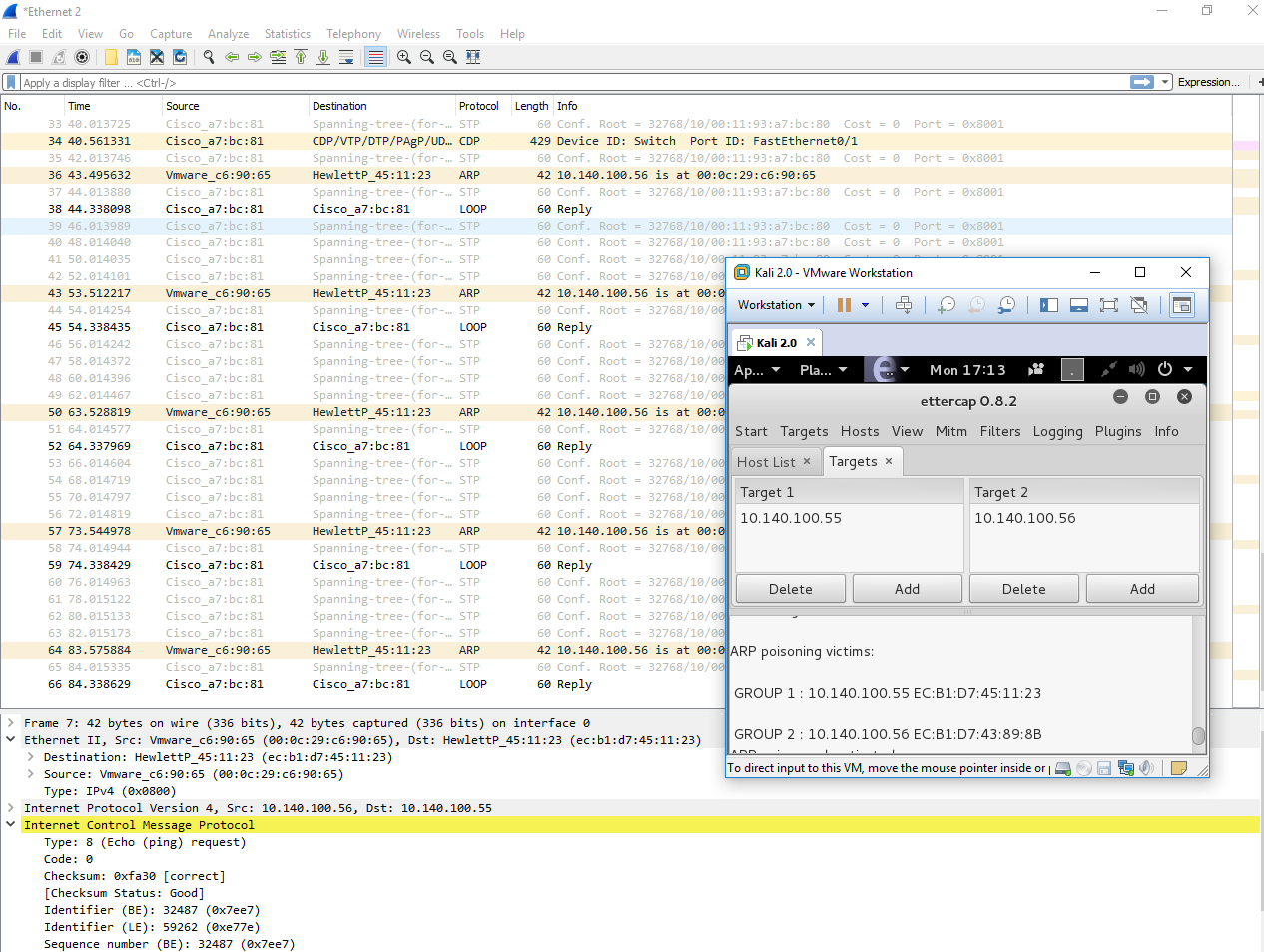


victim machine after mitigation:

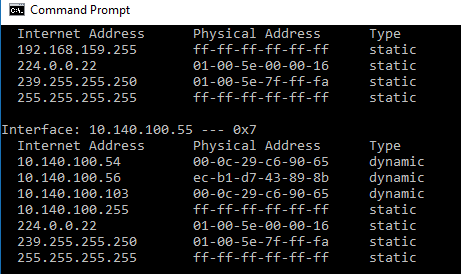


attacker machine after mitigation





after mitigation:



Conclusion

To summarize, in this report, we indicate three security mechanism: DHCP snooping, IP source guard and dynamic ARP inspection. All the three mentioned technics are essential to avoid man in the middle attack and mitigate the risk of any malicious threat. The common factor in these Cisco catalyst features is that it prevents the user from sending information to the attacker instead of sending it to the router gateway. In the spoofing attack, attacker try to fool the user using some tricks so that they can expose the packet before sending it back to the router gateway. Usually victim users have no idea that their information has been sent to a malicious host before going to the router. These kind of attacks allows the attacker to view the user information and break the confidentiality of the message. Also, when the router tries to send packets to the host, the attacker can analyze or alert the packet before it arrives to the intended destination. Therefore, using these technique is significant to mitigate the risk and assure the security of all user’s information.

Reference

* Switch security slides
* Catalyst 6500 Release 12.2SY Software Configuration Guide - IP Source Guard [Cisco Catalyst 6500 Series Switches]. (2016, August 29). Retrieved February 26, 2018, from <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SY/configuration/guide/sy_swcg/ip_source_guard.html>