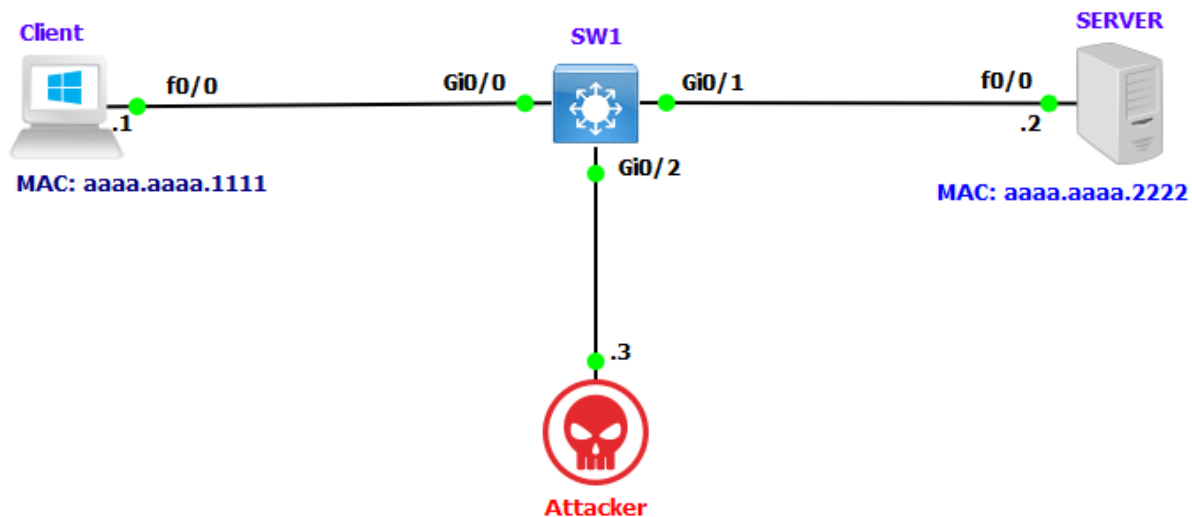
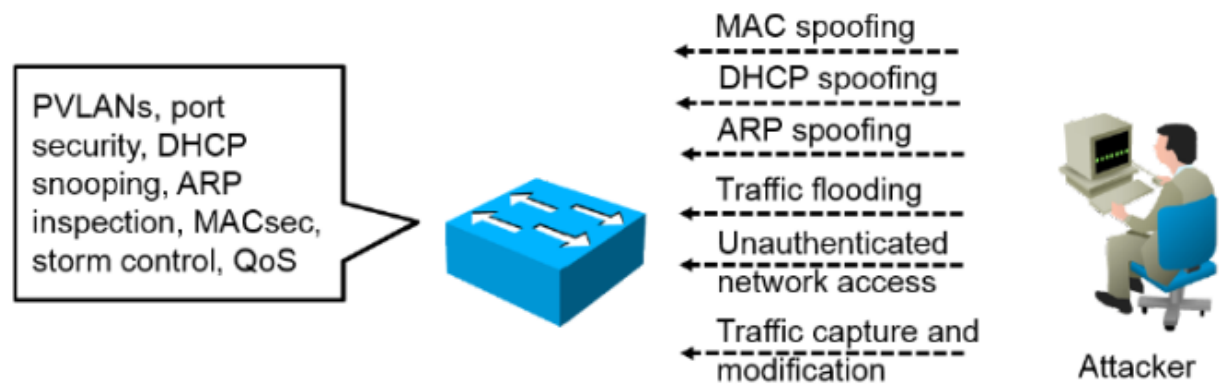


Layer 2 Attacks:

- o Most end-user devices connect to the network via Layer 2 access switches.
- o End devices such as Computers, Printers, IP Phones, and other hosts etc.
- o As a result, the Cisco switches can present a network security risk.
- o The Cisco Switches are subject to attack from malicious internal users.
- o Switches provide many security features to block internal attacks.
- o Security of Layer 2 is aims to mitigate Man in the Middle Attacks (MITM).



DHCP SERVER Configuration
SERVER(config)# interface FastEthernet0/0
SERVER(config-if)# mac-address aaaa.aaaa.2222
SERVER(config-if)# ip address 192.168.1.2 255.255.255.0
SERVER(config-if)# no shutdown
SERVER(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.100
SERVER(config)#ip dhcp pool TEST
SERVER(dhcp-config)#network 192.168.1.0 /24
SERVER(dhcp-config)#default-router 192.168.1.2
SERVER# show ip dhcp binding

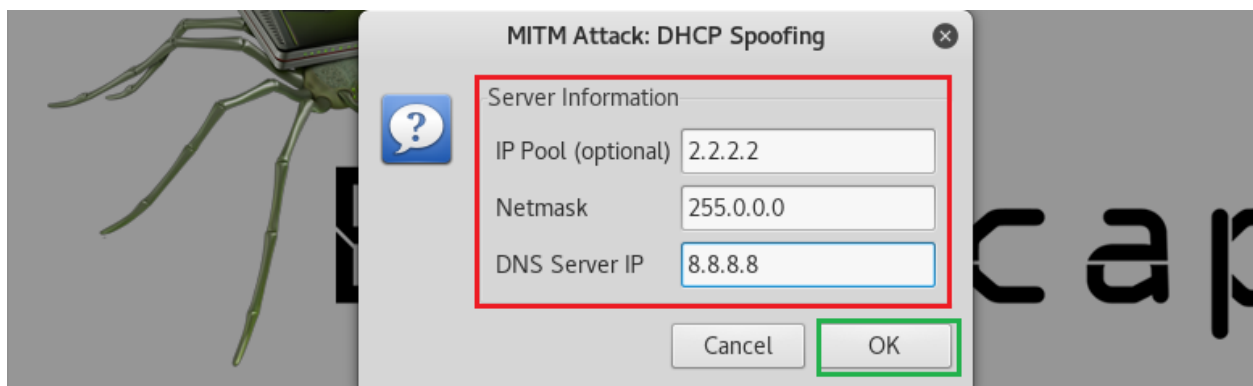
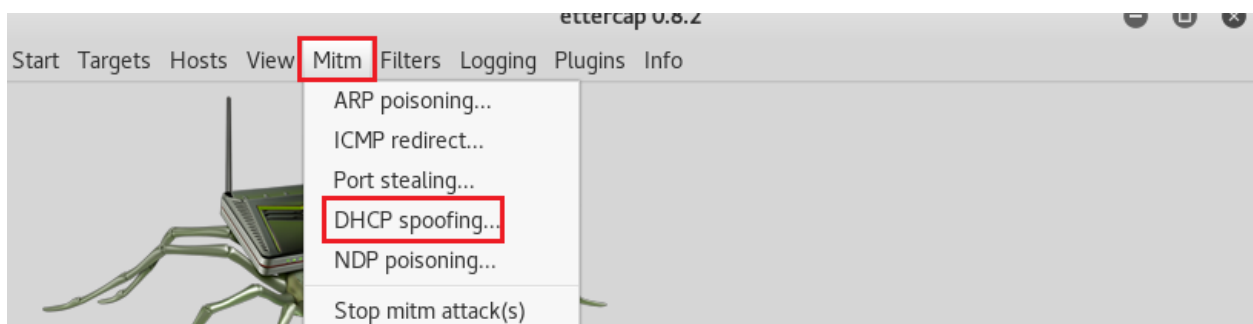
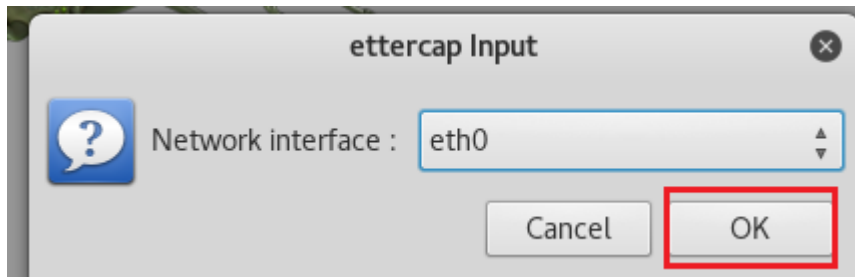
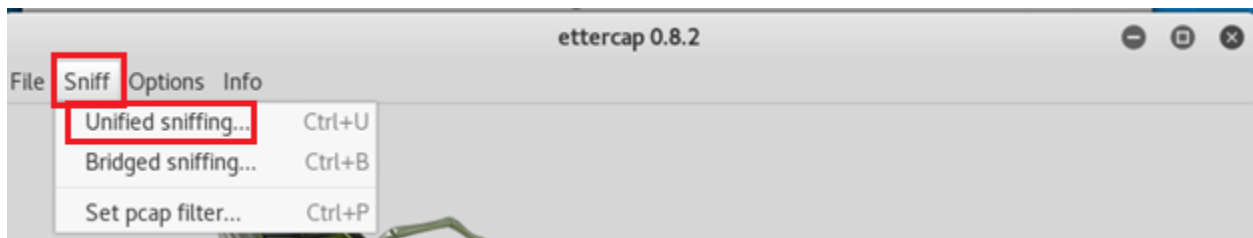
DHCP Client Configuration
Client(config)# interface FastEthernet0/0
Client(config-if)# mac-address aaaa.aaaa.1111
Client(config-if)# ip address 192.168.1.1 255.255.255.0
Client(config-if)# no shutdown
Client(config)# interface FastEthernet0/0
Client(config-if)#no ip address
Client(config-if)#ip address dhcp
Client# show ip int br

SW1 Configuration
SW1(config)#interface range GigabitEthernet 0/0- 2
SW1(config-if-range)#switchport
SW1(config-if-range)#switchport access vlan 1
SW1(config-if-range)#no shutdown
SW1(config)#interface vlan 1
SW1(config-if)#ip address 192.168.1.10 255.255.255.0
SW1(config-if)#shutdown
SW1(config-if)#no shutdown

Client#show ip int br						
Interface	IP-Address	OK?	Method	Status	Protocol	
FastEthernet0/0	192.168.1.101	YES	DHCP	up	up	
FastEthernet1/0	unassigned	YES	NVRAM	administratively down	down	

SERVER#show ip dhcp binding						
Bindings from all pools not associated with VRF:						
IP address	Client-ID/ Hardware address/ User name	Lease expiration			Type	
192.168.1.101	0063.6973.636f.2d61. 6161.612e.6161.6161. 2e31.3131.312d.4661. 302f.30	Mar 02 2002 12:06 AM			Automatic	

Rogue DHCP Server:



```
Client(config-if)#do show ip int br
Interface      IP-Address    OK? Method Status Protocol
FastEthernet0/0 2.2.2.2       YES DHCP   up         up
FastEthernet1/0 unassigned    YES NVRAM   administratively down down
```

DHCP Snooping:

- o DHCP snooping is a security feature acts like a firewall between trusted & untrusted.
- o DHCP snooping is like a firewall between untrusted hosts & trusted DHCP servers.
- o DHCP snooping use trusted source to reply DHCP offer message.
- o DHCP snooping will drop DHCP messages from a DHCP server that is not trusted.
- o DHCP snooping rate-limits DHCP traffic from trusted and untrusted sources.
- o DHCP snooping keep binding database, which is untrusted hosts with leased IPs.
- o DHCP snooping binding database validate subsequent requests from untrusted hosts.
- o DHCP snooping Can be enable to disabled per VLAN basis.
- o DHCP snooping feature is inactive on all VLANs by default,
- o DHCP snooping device insert **DHCP option No 82 Relay Agent Information Option.**
- o DHCP Snooping to prevent a man-in-the middle attack on the network.
- o DHCP Snooping uses a mechanism of trusted and untrusted sources.
- o DHCP Snooping is L 2 security switch feature to blocks unauthorized DHCP servers.
- o DHCP snooping feature identifies Switch Ports as "trusted" and "untrusted".
- o DHCP Untrusted interfaces where clients are connected cannot source DHCP messages.
- o DHCP trusted interfaces where Server are connected source all types of DHCP messages.
- o DHCP Snooping provides protection from DHCP starvation & Rogue DHCP Server attacks.

DHCP Snooping Configuration SW1	
SW1(config)#ip dhcp snooping	
SW1(config)#ip dhcp snooping vlan 1	
SW1(config)#interface GigabitEthernet 0/1	
SW1(config-if)#ip dhcp snooping trust	
SW1(config-if)# no ip dhcp snooping information option	
SW1(config)#interface GigabitEthernet 0/1	
SW1(config-if)# ip dhcp snooping limit rate 100	
SW1(config)#interface range GigabitEthernet 0/0, GigabitEthernet 0/2	
SW1(config-if)# ip dhcp snooping limit rate 20 (20 packets per second)	
SW1# show ip dhcp snooping binding	
SW1# show ip dhcp snooping	
SW1# show ip dhcp snooping statistics	

SW1#show ip dhcp snooping binding					
MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
AA:AA:AA:AA:11:11	192.168.1.102	86382	dhcp-snooping	1	GigabitEthernet0/0
Total number of bindings: 1					

```
SW1#show ip dhcp snooping
```

```
Switch DHCP snooping is enabled
```

```
Switch DHCP gleaning is disabled
```

```
DHCP snooping is configured on following VLANs:
```

```
1
```

```
DHCP snooping is operational on following VLANs:
```

```
1
```

```
DHCP snooping is configured on the following L3 Interfaces:
```

```
Insertion of option 82 is disabled
```

```
circuit-id default format: vlan-mod-port
```

```
remote-id: 0c05.d1cb.9f00 (MAC)
```

```
Option 82 on untrusted port is not allowed
```

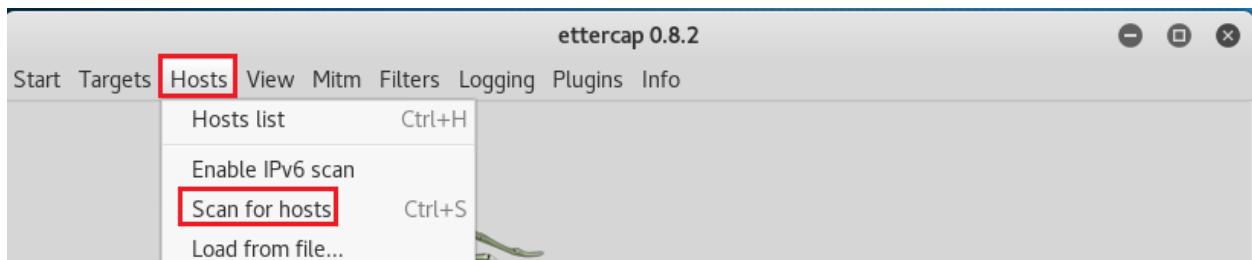
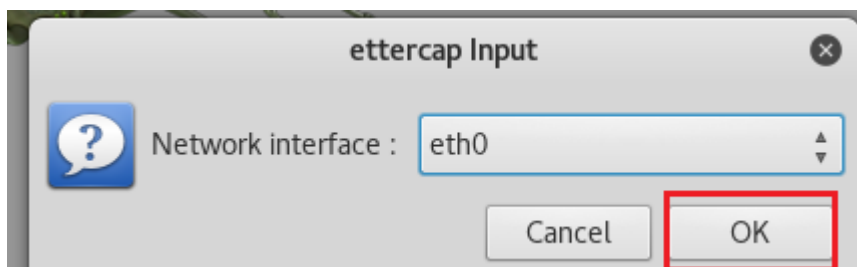
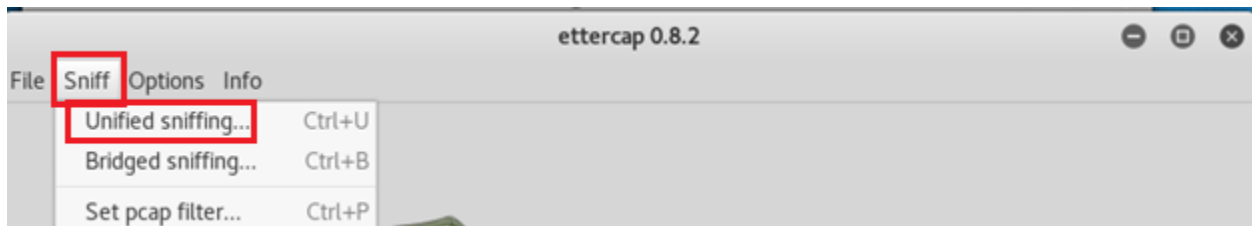
```
Verification of hwaddr field is enabled
```

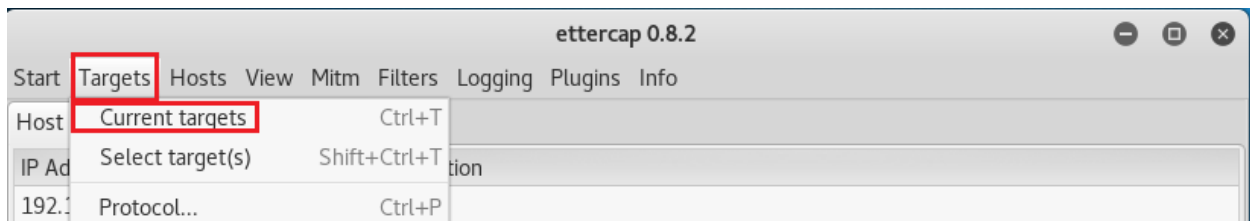
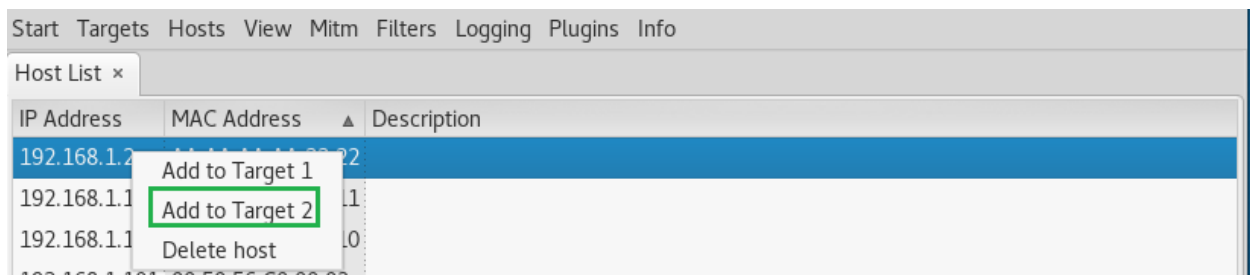
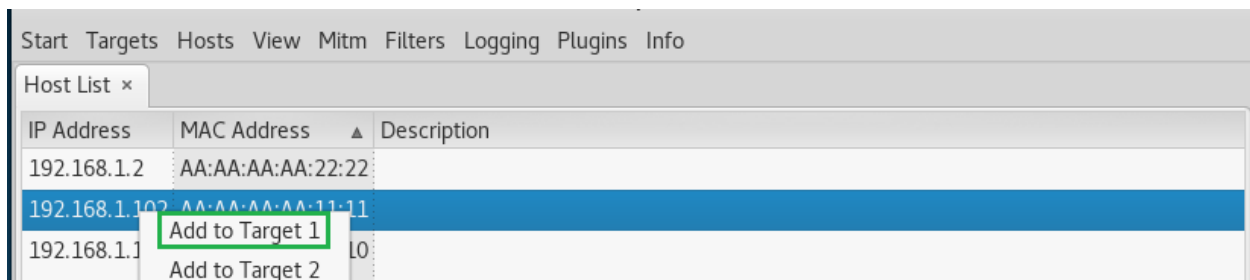
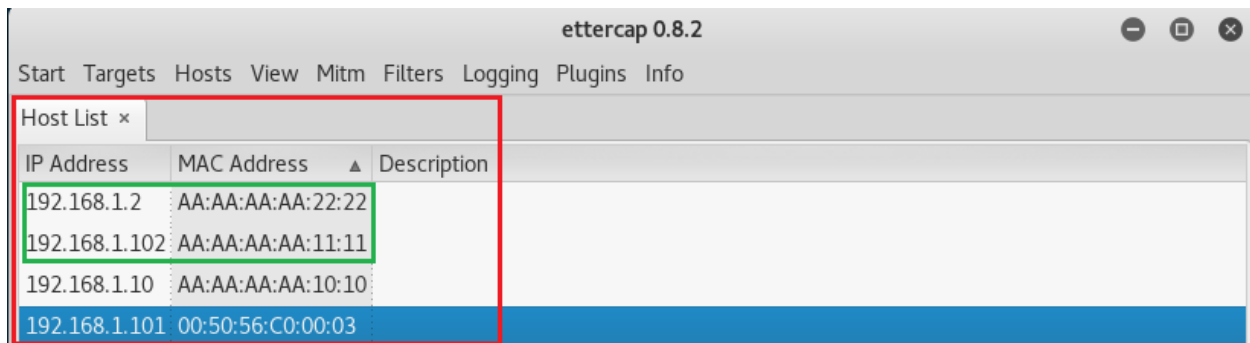
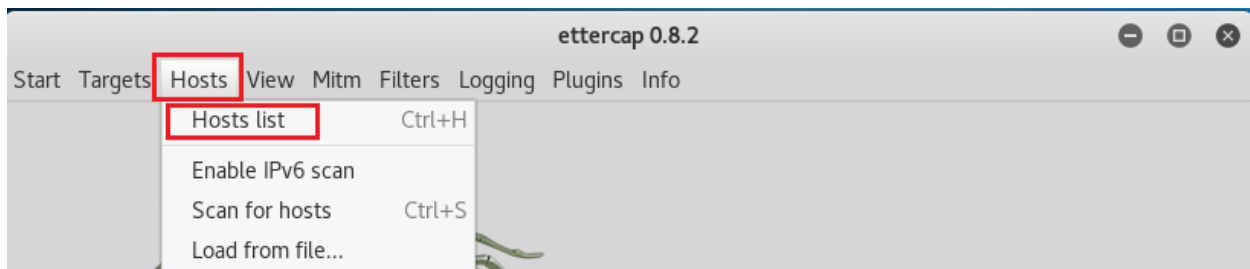
```
Verification of giaddr field is enabled
```

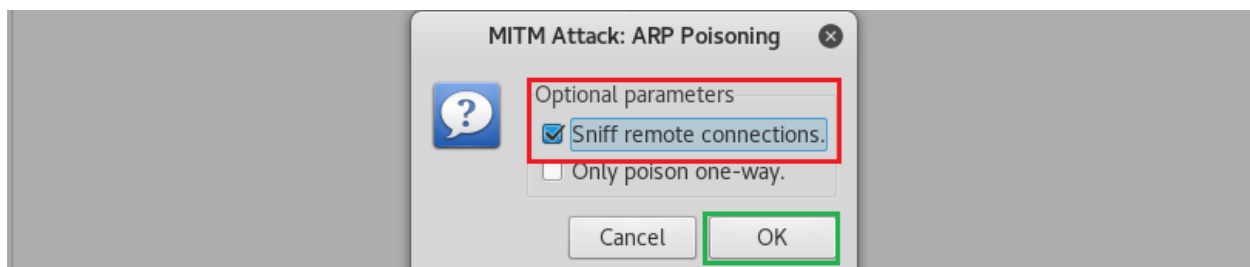
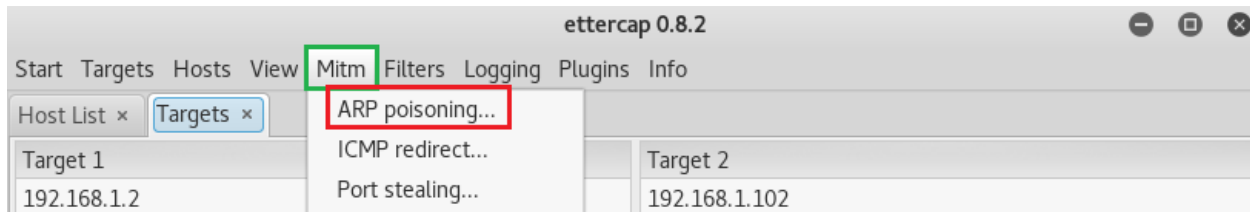
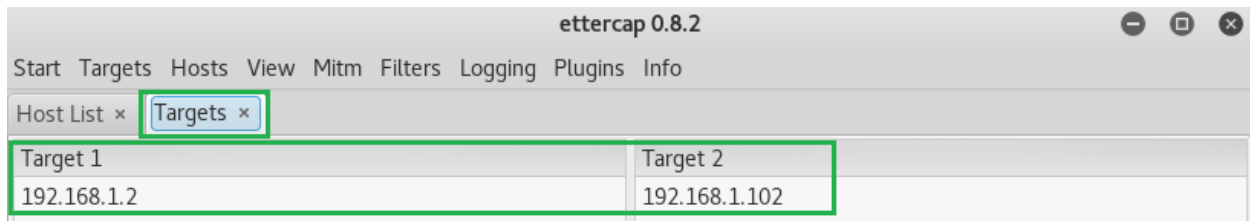
```
DHCP snooping trust/rate is configured on the following Interfaces:
```

Interface	Trusted	Allow option	Rate limit (pps)
GigabitEthernet0/0	no	no	10
Custom circuit-ids:			
GigabitEthernet0/1	yes	yes	100
Custom circuit-ids:			
GigabitEthernet0/2	no	no	10
Interface	Trusted	Allow option	Rate limit (pps)

ARP Poisoning or Spoofing Attack:







```
Client#show arp
Protocol Address      Age (min)  Hardware Addr  Type   Interface
Internet 192.168.1.102      -          aaaa.aaaa.1111 ARPA    FastEthernet0/0
Internet 192.168.1.3        10         000c.2968.9f3b ARPA    FastEthernet0/0
Internet 192.168.1.2        0          000c.2968.9f3b ARPA    FastEthernet0/0
```

```
SERVER#show arp
Protocol Address      Age (min)  Hardware Addr  Type   Interface
Internet 192.168.1.102      0          000c.2968.9f3b ARPA    FastEthernet0/0
Internet 192.168.1.3        12         000c.2968.9f3b ARPA    FastEthernet0/0
Internet 192.168.1.2        -          aaaa.aaaa.2222 ARPA    FastEthernet0/0
```

Dynamic ARP Inspection:

- o DAI stands for Dynamic Address Resolution Protocol Inspection.
- o DAI is a security feature that rejects invalid and malicious ARP packets.
- o DAI feature prevent man-in-the-middle attacks such as ARP poisoning.
- o DIA feature prevent man-in-the-middle attack such as ARP Spoofing.
- o DAI relies on Dynamic Host Control Protocol snooping.
- o DHCP snooping builds bindings' database of valid MAC address, IP & VLAN interface.
- o DAI uses the DHCP snooping binding database to validate bindings.
- o Dynamic ARP Inspection (DAI) verifies IPv4 address to MAC address bindings.
- o If mismatch happened on untrusted port, DAI will discard spoofed ARP packets.
- o Dynamic ARP Inspection (DAI) only inspects ARP packets from untrusted ports.
- o Dynamic ARP Inspection (DAI) can be enabled globally per VLAN.

Dynamic ARP Inspection Configuration SW1

```
SW1(config)#ip dhcp snooping
SW1(config)#ip dhcp snooping vlan 1
SW1(config)#interface GigabitEthernet 0/1
SW1(config-if)#ip dhcp snooping trust
SW1(config-if)# no ip dhcp snooping information option
SW1(config)#interface GigabitEthernet 0/1
SW1(config-if)# ip dhcp snooping limit rate 100
```

```
SW1(config)#ip arp inspection vlan 1
```

```
SW1(config)# interface GigabitEthernet 0/1
SW1(config-if)# ip arp inspection trust
```

```
SW1# show ip arp inspection
```

Change Client IP Address

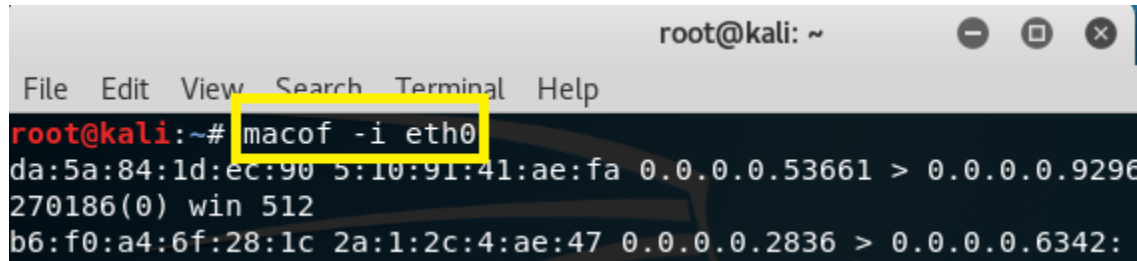
```
Client(config)#interface f0/0
Client(config-if)#ip address 192.168.1.103 255.255.255.0
```

```
Client# ping 192.168.1.2
```

```
Client(config)#interface f0/0
Client(config-if)#ip address dhcp
```


MAC Flooding Attack:

Now **Macof** can flood a switch with random MAC addresses. **macof -i eth0**



The screenshot shows a terminal window titled 'root@kali: ~'. The menu bar includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The command 'macof -i eth0' is entered and highlighted with a yellow box. The output shows a stream of random MAC addresses and IP addresses being generated, such as 'da:5a:84:1d:ec:90 5:10:91:41:ae:fa 0.0.0.0.53661 > 0.0.0.0.9296' and '270186(0) win 512'.

Port Security:

- o Port Security feature protect the switch from MAC flooding attacks.
- o Port security feature protect the switch from DHCP starvation attacks.
- o Attacker start flooding the switch with very large number of DHCP requests.
- o Port Security prevent unauthorized access & limit access, based on MAC address.
- o Port Security is disabled by default on every interface of switch.
- o If Port Security is enabled by default only one MAC address is, allow per interface.
- o If Port Security is enabled by default, violation is shutdown.
- o If Port Security is enabled by default, no aging is configured for recovery.
- o Port Security can be configure Static, Dynamic and Sticky.
- o There are three different types of violation Shutdown, Protect and Restrict.
- o Port Security limit (1-8192) MAC address to attach on particular port.

Port Security Violation Types:

- o There are three different types of violation Shutdown, Protect and Restrict.

Shutdown:

- o Default action after violation.
- o Port send to err-disabled mode.
- o For re-enable err-disabled recover, shutdown/no shutdown.
- o MAC counter keeps history.

Protect:

- o Need to configure for violation action.
- o Traffic not send to network from violator.
- o Interface will be working even after violation.
- o No MAC counter keeps history.

Restrict:

- o Need to configure for violation action.
- o Traffic not send to network from violator.
- o Generate log (SNMP/Syslog).
- o No MAC counter keeps history.

Violation Action	Description
Protect	Discards the bogus or extra MAC address without notifying the administrator.
Restrict	Discards the bogus or extra MAC address and generates Syslog message or SNMP trap. Alert generation feature of this action makes it preferable over the aforementioned action.
Shutdown	Puts the port in err-disable state and everything is discarded. Syslog/SNMP based alert is also generated. shutdown is default violation action defined in Cisco IOS

Static:

- o Static secure MAC addresses are statically configured on each switchport.
- o Static secure MAC addresses are stored in the address table.
- o Configuration of static secure MAC address is stored in the running configuration.
- o Can be made permanent by saving them to the startup configuration.
- o SW1(config-if) # switchport port-security mac-address mac-address

Dynamic:

- o Dynamic secure MAC addresses are learned from device connected to switchport.
- o Dynamic secure MAC addresses are stored in the address table only.
- o Dynamic secure MAC addresses lost when the switchport state goes down.
- o Dynamic secure MAC addresses also lost when the switch reboots.
- o SW1(config-if) # switchport port-security
- o By default, MAC addresses are learned on a switchport dynamically.

Sticky:

- o A sticky MAC address is a hybrid between a static and dynamic MAC address.
- o Dynamically learned, MAC address is automatically entered into the running configuration.
- o The address is then kept in the running configuration until a reboot.
- o Once the switch is reboot, the MAC address will be lost.
- o To keep the MAC address across a reboot a configuration save is required.

Maximum MAC Addresses:

- o By default, each secure switchport is configured with a maximum of one MAC address.
- o If more than one MAC address is seen on any given port, a violation will occur.
- o Maximum MAC address can be modified.

Dynamic Port Security Configuration
SW1(config)#interface g0/0
SW1(config-if)#switchport mode access
SW1(config-if)#switchport port-security
SW1#show port-security
SW1#show port-security address
SW1#show port-security interface g0/0

```

SW1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)         (Count)         (Count)
-----
Gi0/0              1              1              0      Shutdown

Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 4096

SW1#show port-security address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
(mins)
-----
1       aaaa.aaaa.1111   SecureDynamic       Gi0/0    -

Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 4096

```

Static Port Security Configuration

```

SW1(config)#interface g0/0
SW1(config-if)#switchport mode access
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security mac-address aaaa.aaaa.1111

SW1#show port-security
SW1#show port-security address
SW1#show port-security interface g0/0

```

```

SW1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)         (Count)         (Count)
-----
Gi0/0              1              1              0      Shutdown

Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 4096

SW1#show port-security address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
(mins)
-----
1       aaaa.aaaa.1111   SecureConfigured    Gi0/0    -

Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 4096

```

Sticky Port Security Configuration

```
SW1(config)#interface g0/0
SW1(config-if)#switchport mode access
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security mac-address sticky
SW1#show port-security
SW1#show port-security address
SW1#show port-security interface g0/0
```

```
SW1#show port-security address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
(mins)
-----
1       aaaa.aaaa.1111   SecureSticky       Gi0/0    -
-----
Total Addresses in System (excluding one mac per port)  : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

```
Client(config)#interface f0/0
Client(config-if)#mac-address aaaa.aaaa.5555
SW1(config)# interface g0/0
SW1(config-if) #shutdown
SW1(config-if)# no shutdown
SW1(config)#errdisable recovery cause psecure-violation
SW1(config)#errdisable recovery interval 30
SW1# show interfaces status
SW1#show errdisable recovery
```

```
SW1(config)#
*Apr  5 17:23:19.702: %PM-4-ERR_DISABLE: psecure-violation error detected on Gi0/0, putting Gi0/0 in err-disable state
*Apr  5 17:23:19.705: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address aaaa.aaaa.5555 on port GigabitEthernet0/0.
```

```
SW1# show interfaces status
Port      Name      Status      Vlan    Duplex  Speed  Type
Gi0/0     Name      err-disabled 1       auto   auto   unknown
Gi0/1     Name      connected   1       auto   auto   unknown
Gi0/2     Name      connected   1       auto   auto   unknown
```

SW1(config)# interface g0/0
SW1(config-if)#switchport port-security violation restrict
SW1(config-if)#switchport port-security violation protect
SW1#show port-security address
SW1#show port-security
SW1#show port-security interface g0/0

```
SW1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
          (Count)          (Count)          (Count)
-----
Gi0/0              1              1              0              Protect
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

```
SW1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
          (Count)          (Count)          (Count)
-----
Gi0/0              1              1              0              Restrict
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

Port Security Drawbacks:

- o Modern hacking tools can be used to spoof MAC address & bypass this security check.
- o Similarly, port security does not work with dynamically configured ports.
- o Switch port needs to be in a static access or static trunk mode for port security to work.
- o 802.1x is better & secure way of mitigating attacks related to layer two MAC addresses.

