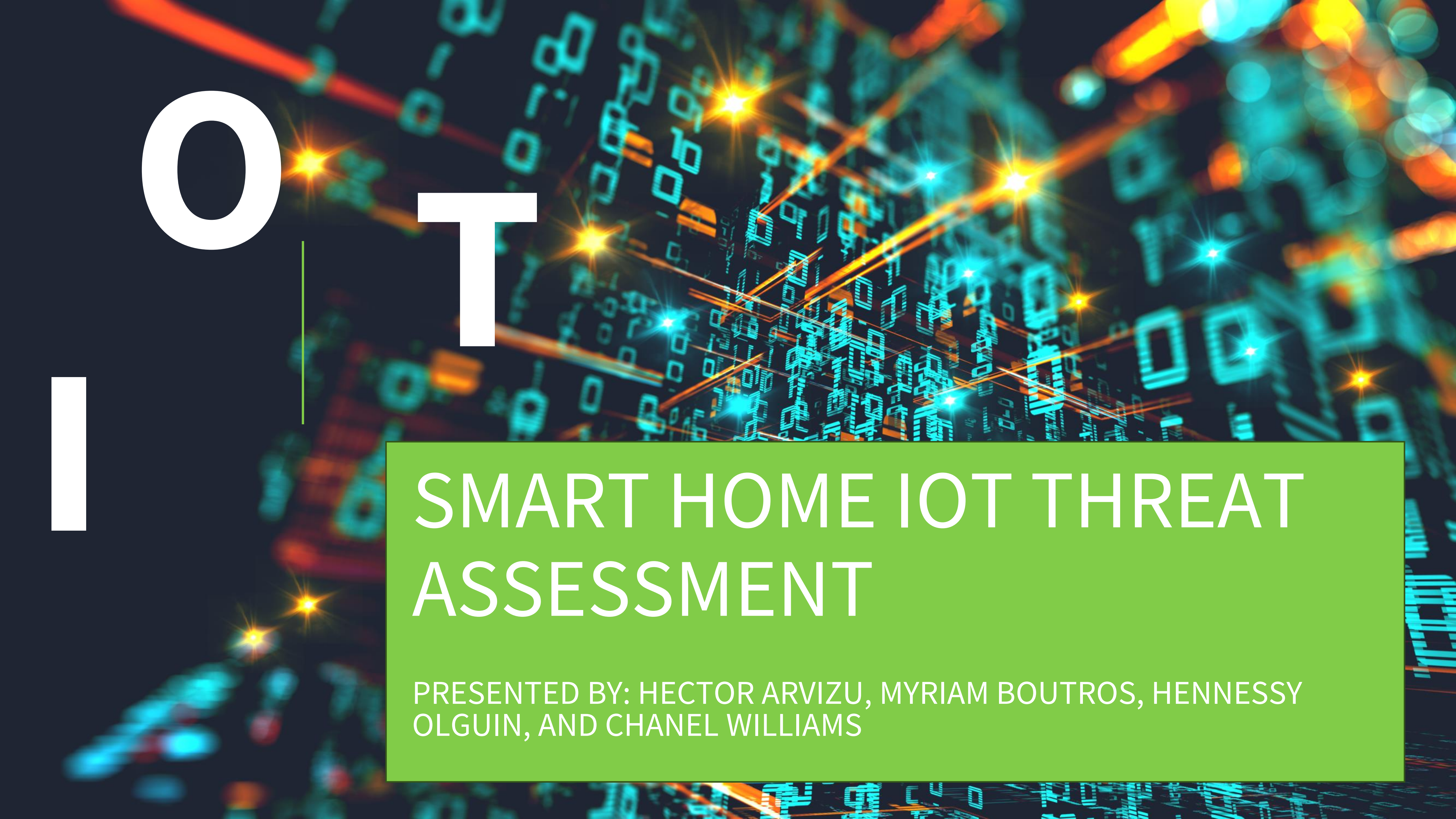


IOT

SMART HOME IOT THREAT ASSESSMENT

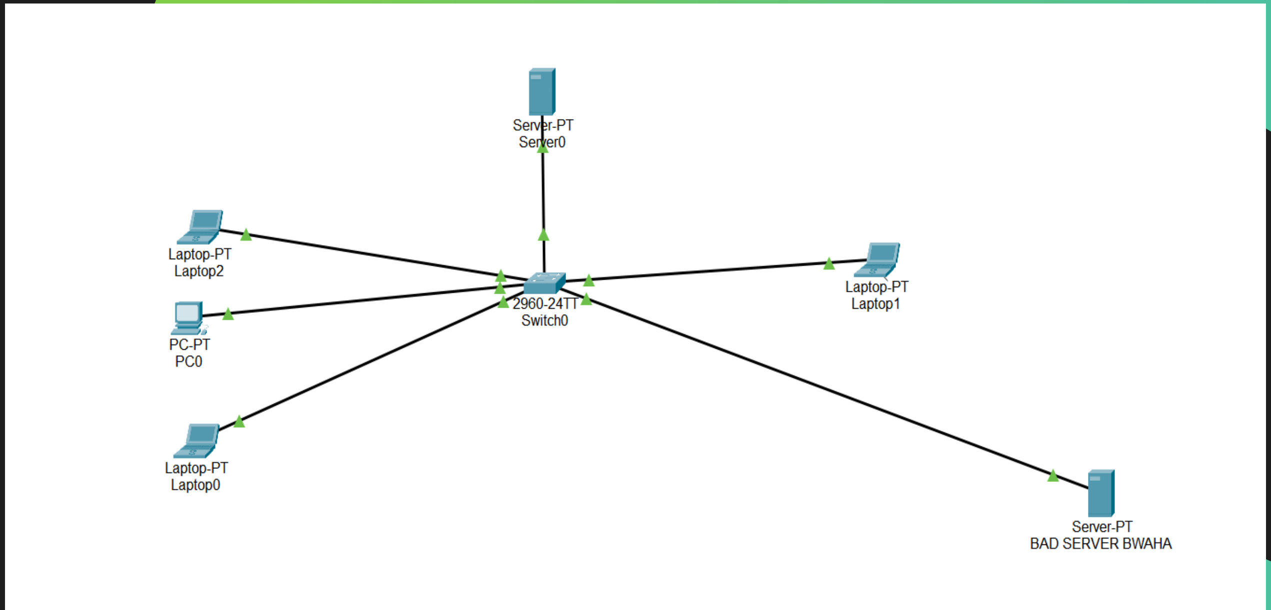
PRESENTED BY: HECTOR ARVIZU, MYRIAM BOUTROS, HENNESSY OLGUIN, AND CHANEL WILLIAMS

INTRODUCTION (PROJECT OBJECTIVES)

- Students showcase understanding of course through applying a network forensics with a real-life application
- Assess the security risks and vulnerabilities of IoT devices commonly found in a smart home environment and propose countermeasures to mitigate potential threats.

PROGRAM

DHCP STARVATION



A DHCP starvation attack is a type of cyber attack that aims to deplete the available IP addresses in a DHCP server's address pool. This attack floods the DHCP server with a large number of fake or unauthorized DHCP requests, causing it to run out of available IP addresses to assign to legitimate devices

DCHP STARVATION

HOW IT WORKS

An attacker wants to perform a DHCP starvation attack on this network. The attacker uses a tool that can generate many DHCP requests, each with a different MAC address. The tool sends these requests to the DHCP server in the home’s router.

As the DHCP server receives these requests, it assigns an IP address to each one, thinking they are legitimate devices. Eventually, the DHCP server runs out of IP addresses to assign because all available addresses have been taken by the attacker’s fake requests.

RELATING TO IOT THREAT ON A SMART HOME

In a smart home scenario, this could prevent legitimate devices like computers and smart home devices from connecting to the network, as they can’t be assigned an IP address. This effectively causes a denial of service, disrupting the functionality of the smart home. To prevent such attacks, security measures like DHCP snooping and port security can be implemented

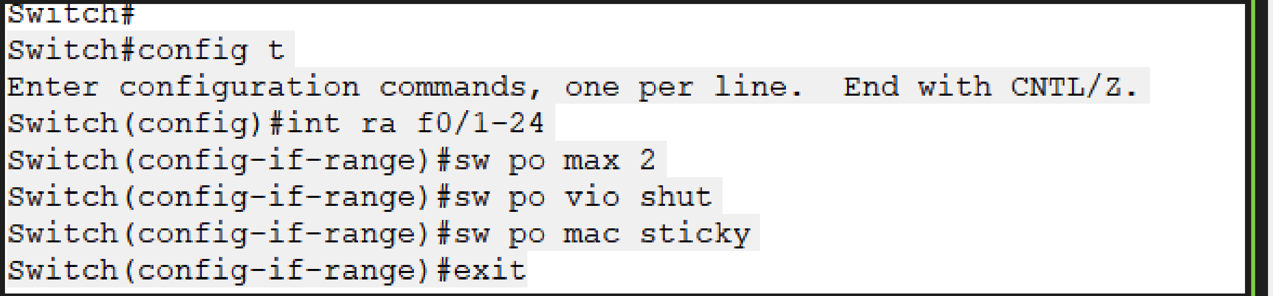
DHCP STARVATION: HOW TO ATTACK

- DoS Attack: The attacker sends a flood of bogus DHCP Discover messages with spoofed MAC addresses. As a result, the DHCP server tries to respond to all these bogus messages, and the pool of IP addresses used by the DHCP server is depleted. A legitimate user won’t be able to get an IP address via DHCP.

- MITM Attack: The attacker can set up a rogue DHCP server to assign IP addresses to legitimate users. This rogue server can also provide the gateway router and DNS server to users. Now, all the network traffic can be routed via the attacker’s machine. This is nothing but the MITM attack. The benefit of that to the attacker is that if a bogus DHCP server is handing out IP addresses, including default DNS and gateway information, clients who use those IP addresses and start to use that default gateway can now be routed through the attacker’s machine

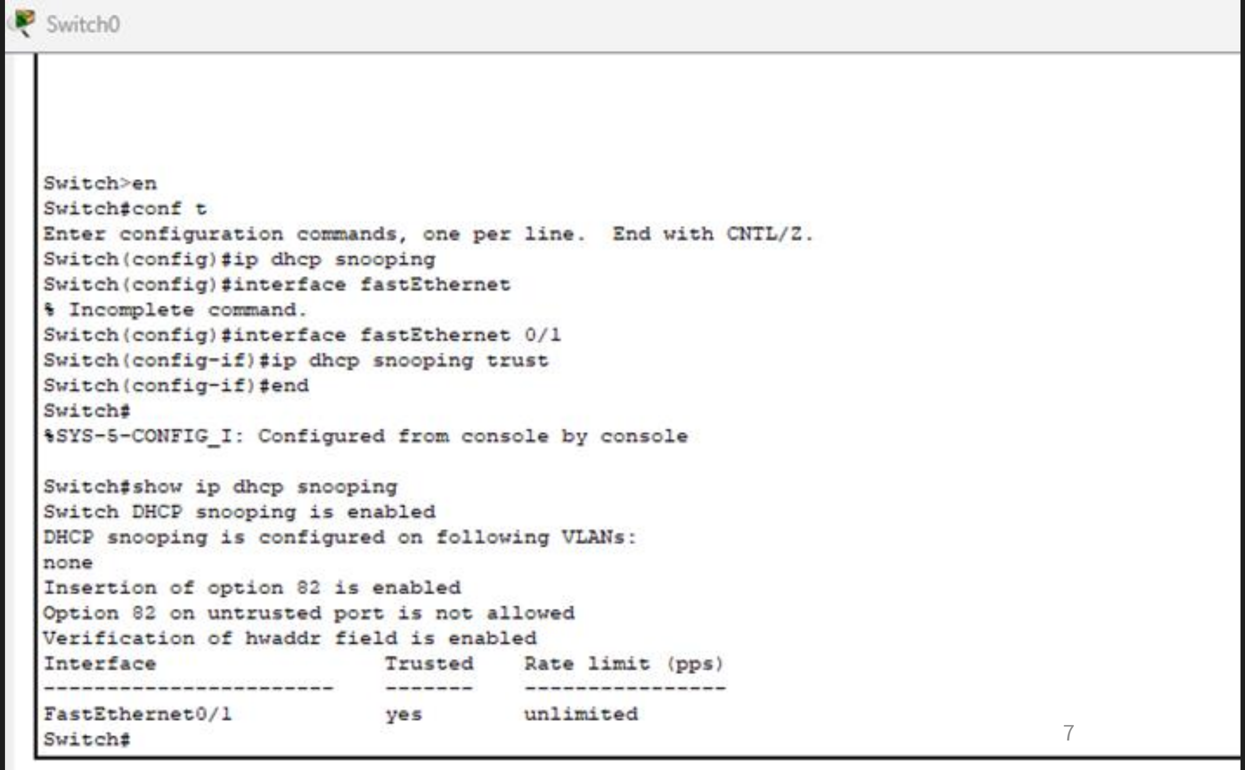
DHCP STARVATION CODE

ENABLING SECURITY PORT



```
Switch#
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int ra f0/1-24
Switch(config-if-range)#sw po max 2
Switch(config-if-range)#sw po vio shut
Switch(config-if-range)#sw po mac sticky
Switch(config-if-range)#exit
```

ENABLING DHCP SNOOPING



```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip dhcp snooping
Switch(config)#interface fastEthernet
% Incomplete command.
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
none
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted     Rate limit (pps)
-----------------------    -------     ----------------
FastEthernet0/1            yes         unlimited
Switch#
```

SOLUTION

DHCP STARVATION

PORT SECURITY

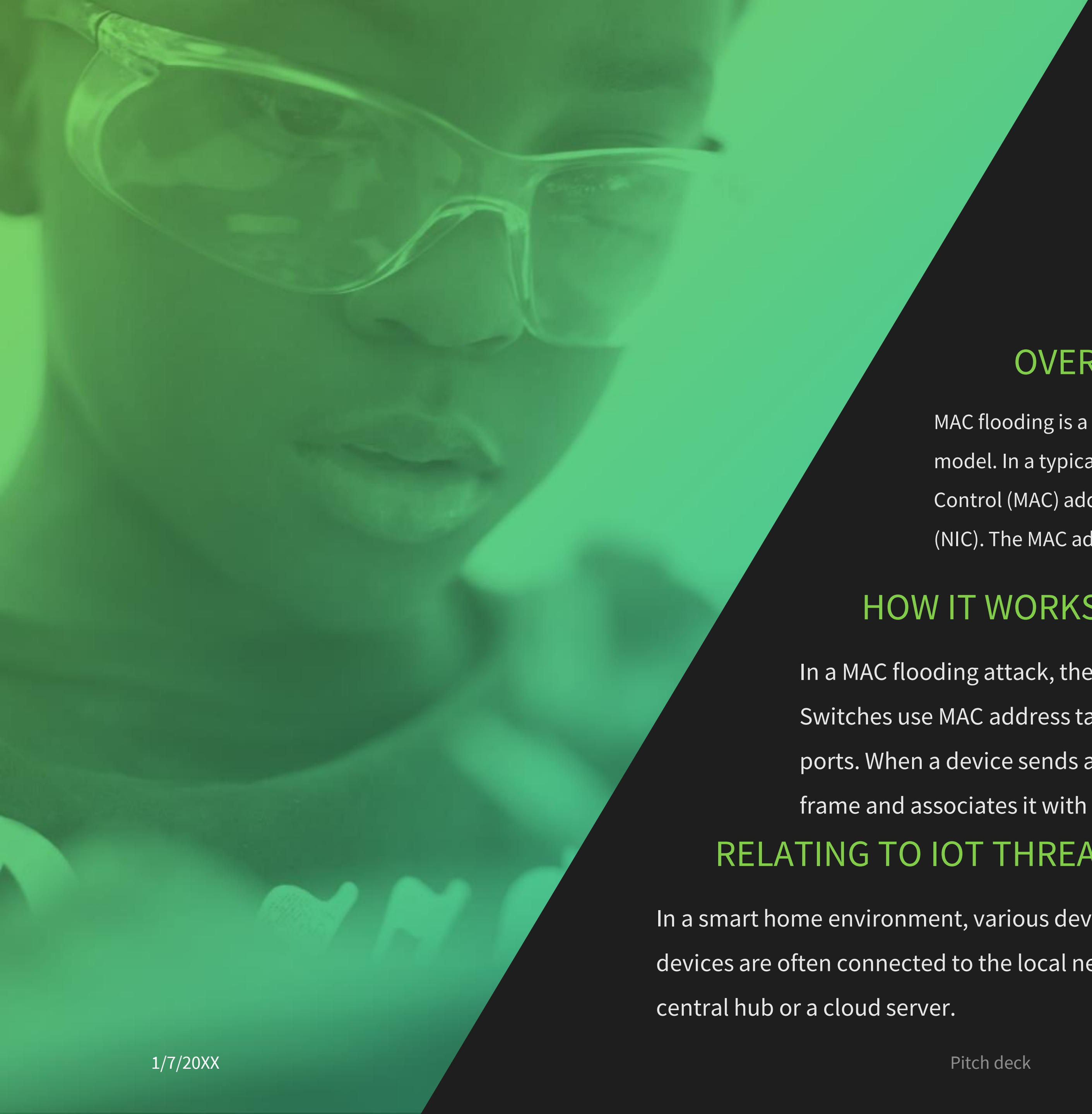
This can be configured in a switch. With port security, you can limit the number of MAC addresses learned by the port. The switch would forward packets with known MAC addresses, and discard others

IMPLEMENT DHCP SNOOPING

This feature verifies that the source MAC address and the Client Hardware Address inside the DHCP payload are the same. It can also set a “maximum threshold“, or number of packets per second that the switch can receive in a given port

MANUAL IP CONFIGURATION

This involves configuring IP information manually on all endpoints in the network.



MAC FLOODING

OVERVIEW

MAC flooding is a type of network attack that targets the layer 2 (Data Link layer) of the OSI model. In a typical Ethernet network, each device on the network has a unique Media Access Control (MAC) address, which is a hardware address assigned to the network interface card (NIC). The MAC address is used to identify devices on a local network.

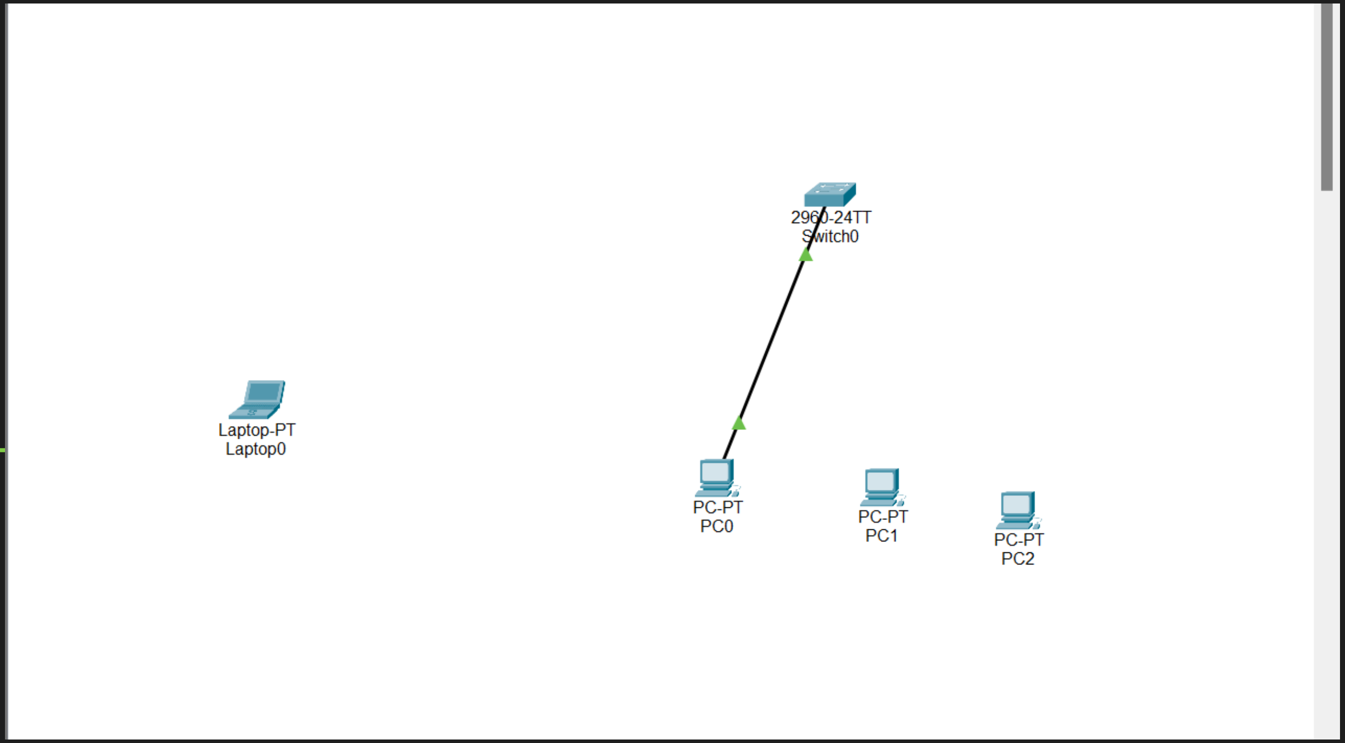
HOW IT WORKS

In a MAC flooding attack, the attacker attempts to overload the switch's MAC address table. Switches use MAC address tables to keep track of which devices are connected to each of their ports. When a device sends a frame to the switch, the switch learns the source MAC address of the frame and associates it with the port through which the frame arrived.

RELATING TO IOT THREAT ON A SMART HOME

In a smart home environment, various devices like smart thermostats, cameras, door locks, and other IoT devices are often connected to the local network. These devices communicate with each other and with a central hub or a cloud server.

MAC FLOODING



MAC FLOODING: HOW TO ATTACK

1. **Sending a Flood of Frames:** The attacker floods the switch with a large number of frames, each containing different source MAC addresses. These MAC addresses may be randomly generated or taken from legitimate devices on the network.
2. **Overloading the MAC Address Table:** Since switches have a limited size for their MAC address tables, the flood of frames causes the table to fill up quickly. As the table becomes full, the switch starts behaving like a hub rather than a switch. In a hub-like mode, the switch forwards incoming frames to all of its ports, regardless of the destination MAC address.
3. **Packet Sniffing or Man-in-the-Middle Attacks:** With the switch in this hub-like mode, the attacker can sniff or intercept the network traffic, potentially capturing sensitive information or launching further attacks.

MAC FLOODING

en

conf t

int f0/1

switchport mode access

switchport port-security

switchport port-security maximum 3

switchport port-security violation ?

switchport port-security violation shutdown

switchport port-security mac-address ?

switchport port-security mac-address sticky

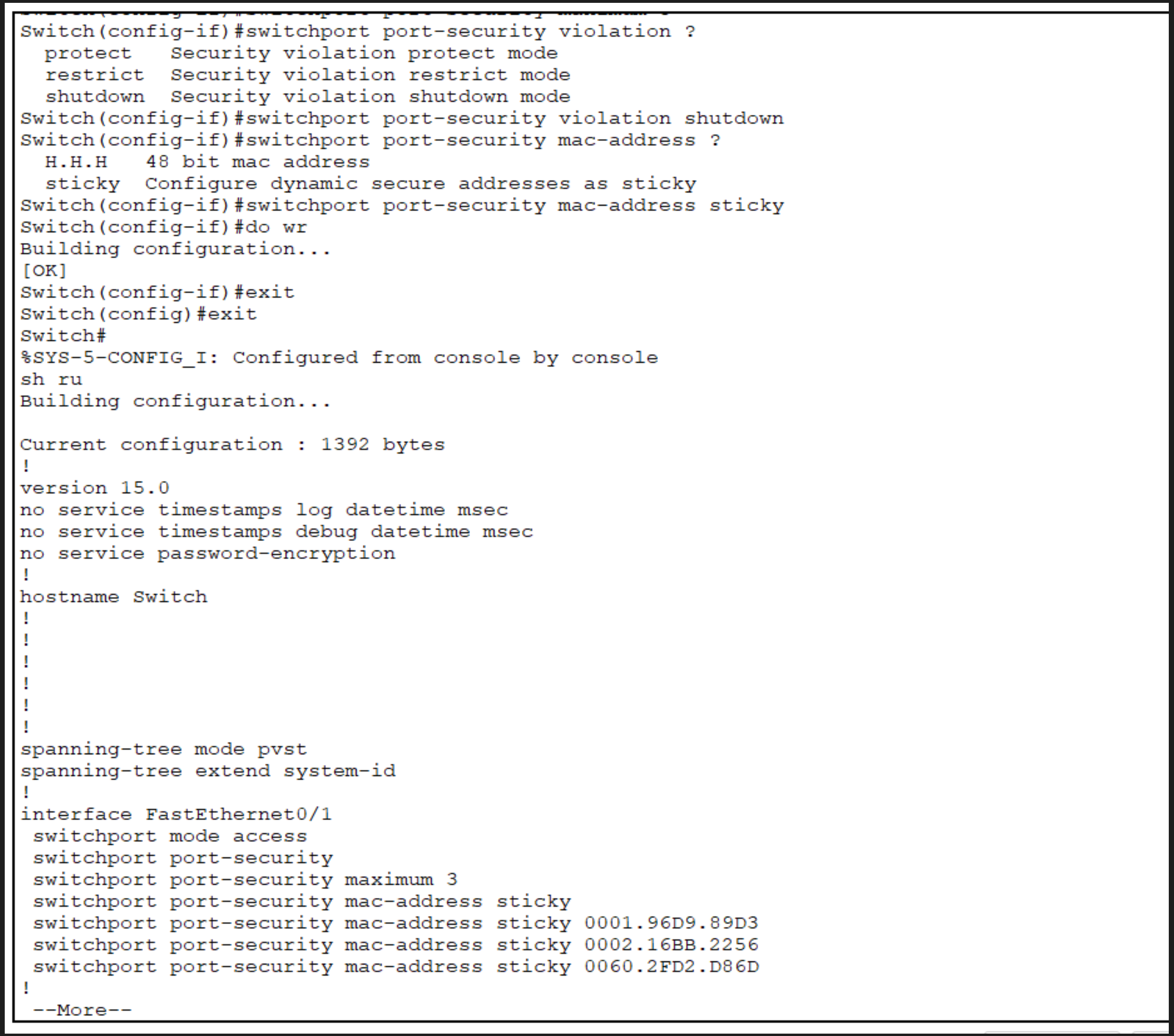
do wr

exit

exit

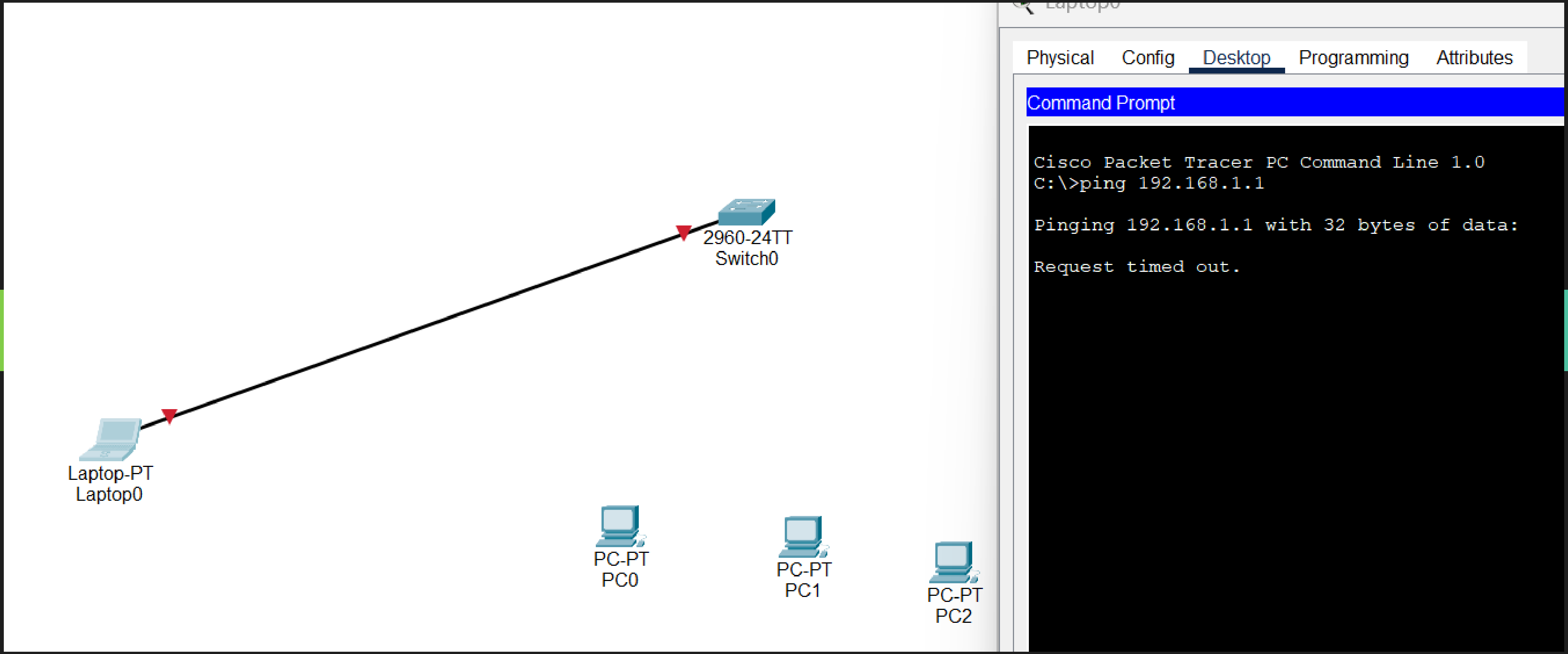
sh r

(enter to see the rest of the mac addresses)



```
Switch(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#switchport port-security mac-address ?
  H.H.H   48 bit mac address
  sticky  Configure dynamic secure addresses as sticky
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#do wr
Building configuration...
[OK]
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
sh ru
Building configuration...

Current configuration : 1392 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security maximum 3
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0001.96D9.89D3
 switchport port-security mac-address sticky 0002.16BB.2256
 switchport port-security mac-address sticky 0060.2FD2.D86D
!
 --More--
```

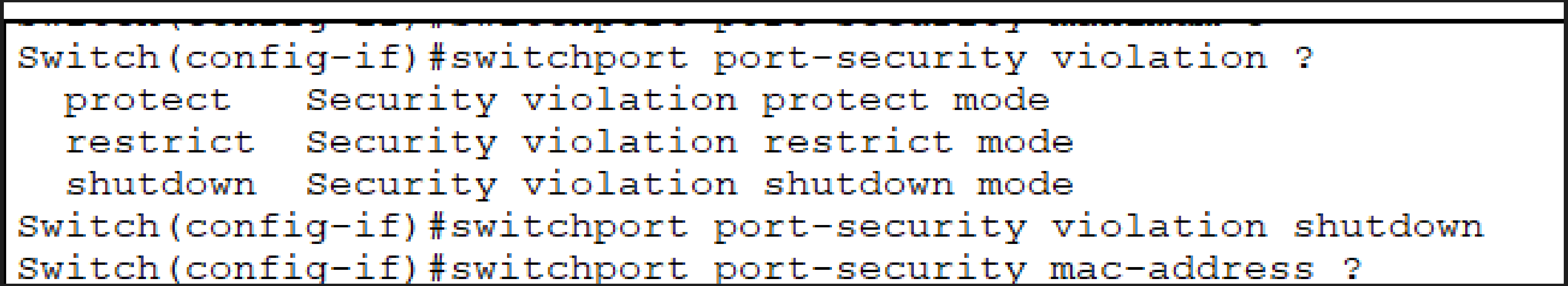
MAC FLOODING



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
```

MAC FLOODING: SOLUTION

- **Network Segmentation:** Implement network segmentation to isolate IoT devices from critical network infrastructure. This can help contain the impact of a potential attack on IoT devices.
- **Security Best Practices:** Follow security best practices for both the network infrastructure and individual IoT devices. This includes using strong passwords, regularly updating firmware/software, and enabling encryption where possible.
- **Intrusion Detection and Prevention Systems:** Deploy intrusion detection and prevention systems to monitor network traffic for unusual patterns or activities. This can help in detecting and responding to MAC flooding attacks or other malicious activities.
- **Regular Security Audits:** Conduct regular security audits to identify and address vulnerabilities in the smart home network. This includes reviewing the configuration of network devices and ensuring that security features are properly configured.



```
Switch(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#switchport port-security mac-address ?
```

IP SPOOFING

OVERVIEW

IP spoofing is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both. It is a technique often used by bad actors to invoke DDoS attacks against a target device or the surrounding infrastructure.

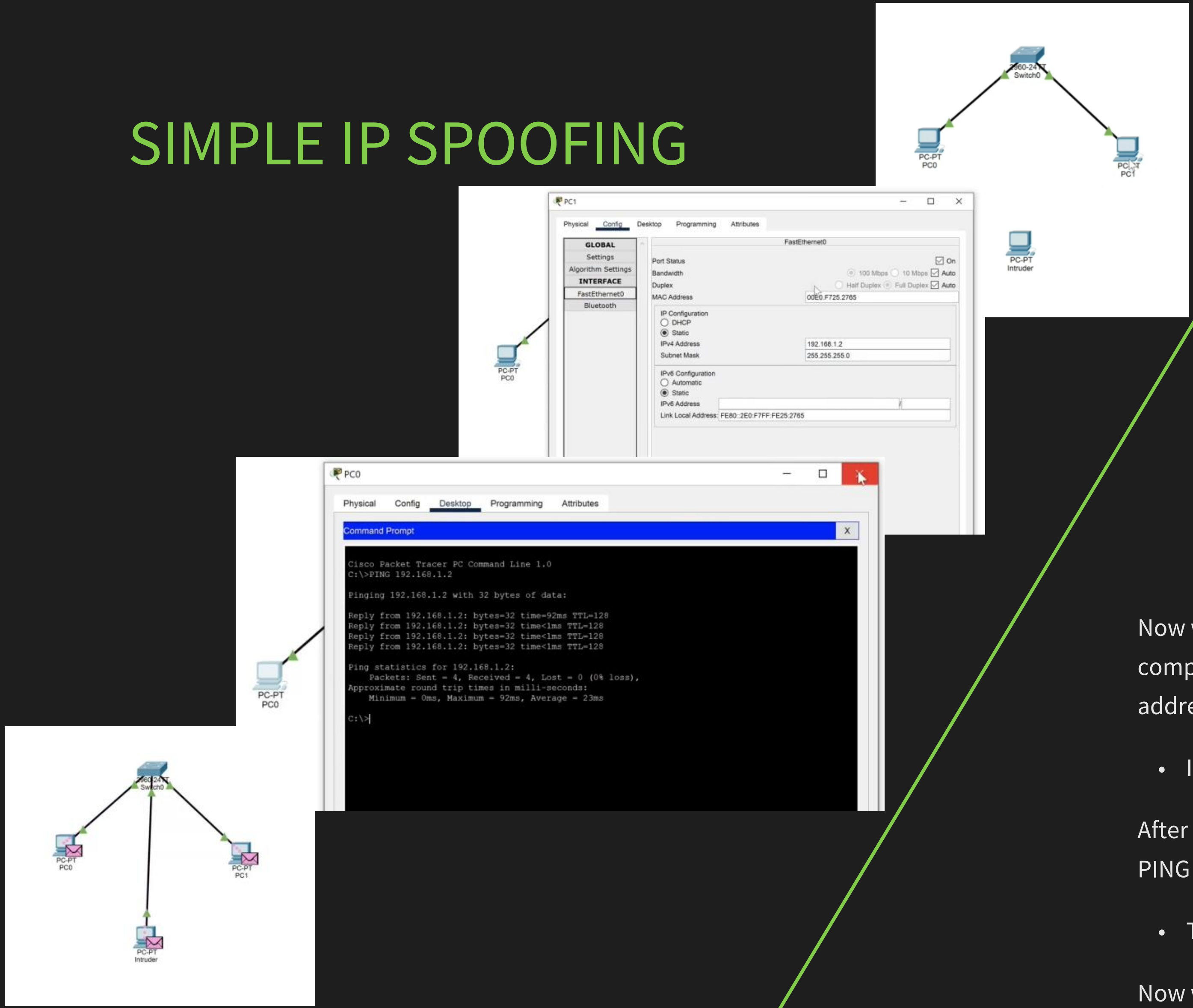
HOW IT WORKS

In IP spoofing, a hacker uses tools to modify the source address in the packet header to make the receiving computer system think the packet is from a trusted source, such as another computer on a legitimate network, and accept it. This occurs at the network level, so there are no external signs of tampering.

Relating to IoT Threat on a smart home

In a smart home environment, devices like laptops and office computers located inside a smart house are vulnerable towards this kind of attack.

SIMPLE IP SPOOFING



FastEthernet0

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 00E0.F725.2765

IP Configuration

○ DHCP

● Static

IPv4 Address 192.168.1.2

Subnet Mask 255.255.255.0

IPv6 Configuration

○ Automatic

● Static

IPv6 Address /

Link Local Address: FE80::2E0:F7FF:FE25:2765

```
Cisco Packet Tracer PC Command Line 1.0
C:\>PING 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=92ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 92ms, Average = 23ms

C:\>
```

IP spoofing basically consists of replacing the source IP address of a TCP packet with another IP address which was said to be spoofed. This is generally achieved thanks to programs designed for it and can be used for any protocol within TCP like icmp, udp, or tcp.

In order to perform IP spoofing in TCP sessions, the behavior of said protocol with packet sending must be taken into account. For this example, we will need a victim computer, a switch, a server, and a third computer that we will call the intruder. From there we will create the IPs for each computer and make the corresponding network links.

Now we will take the information from the victim computer, which will be mainly the Mac address and the IP address, we will copy it and replace it on the intruder PC.

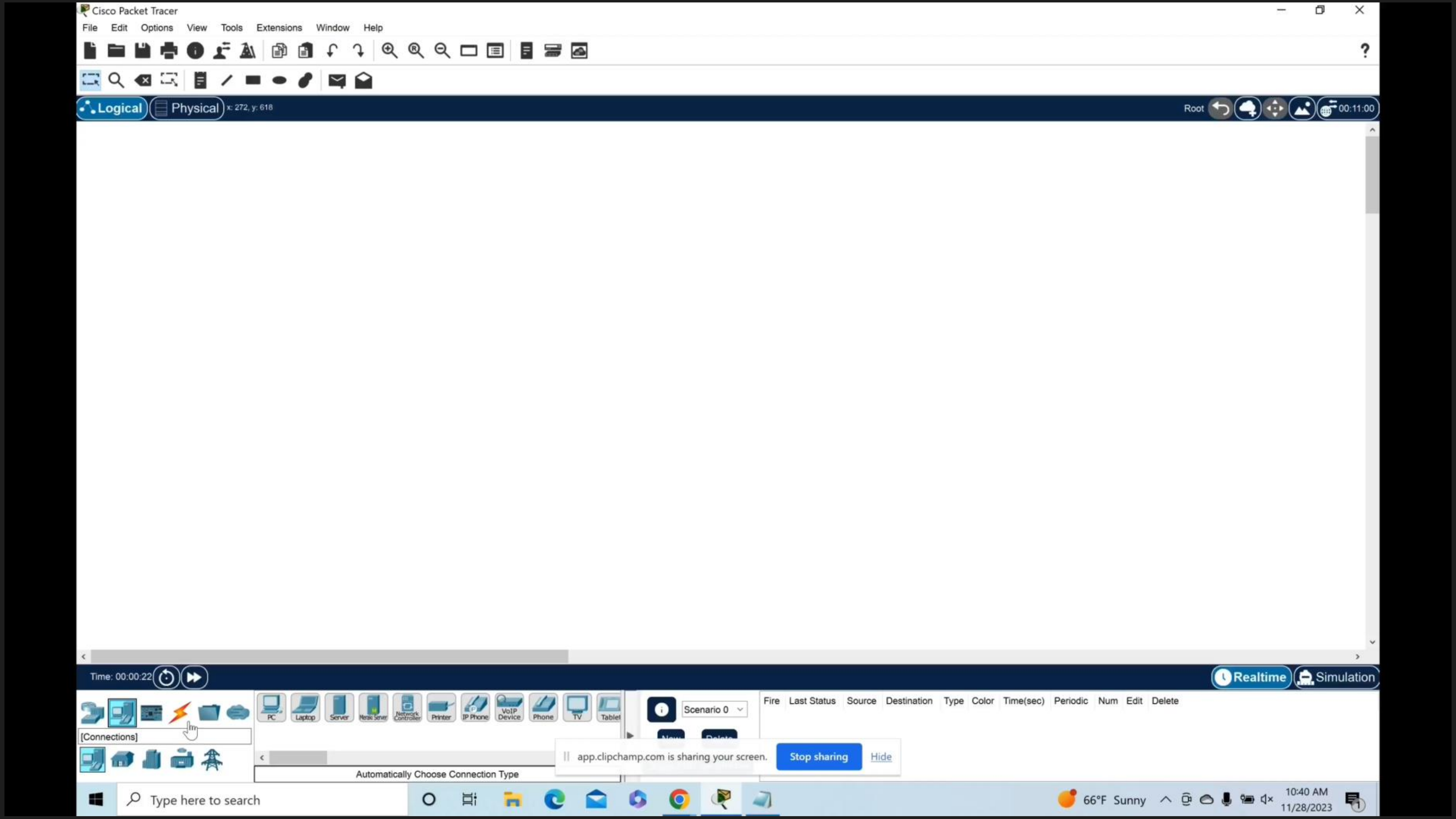
- In this we copy the IP and the same MAC address

After we make the network connection, we will create a PING in order to create the ARP table.

- The same process is repeated.

Now we proceed to send the packages to the victim team.

SIMPLE IP SPOOFING


Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical
Physical
x: 272, y: 618
Root
00:11:00
Time: 00:00:22
Realtime
Simulation
[Connections]
PC Laptop Server Meraki Server Network Controller Printer IP Phone VoIP Device Phone TV Tablet
Scenario 0
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
Automatically Choose Connection Type
app.clipchamp.com is sharing your screen.
Stop sharing
Hide
Type here to search
66°F Sunny
10:40 AM
11/28/2023

HOW TO PREVENT IP SPOOFING

FIREWALLS

Firewalls can be used to help detect suspicious IP packets, fake IP addresses, and suspicious traffic.

NEW VERIFICATION METHODS

Using strong methods can help your device to not allow devices to connect to your network based on IP addresses. Other tools can also verify websites that are trying to connect to your network.

HTTPS WEBSITES

Some websites offer secure encryption protocols. Using HTTPS websites are safer as they help users detect dangerous websites while they browse the internet.

ANTIVIRUS PROTECTION

Using reliable and affordable security software can help verify and detect any suspicious activity.

ARP SPOOFING

WHAT IS ARP SPOOFING?

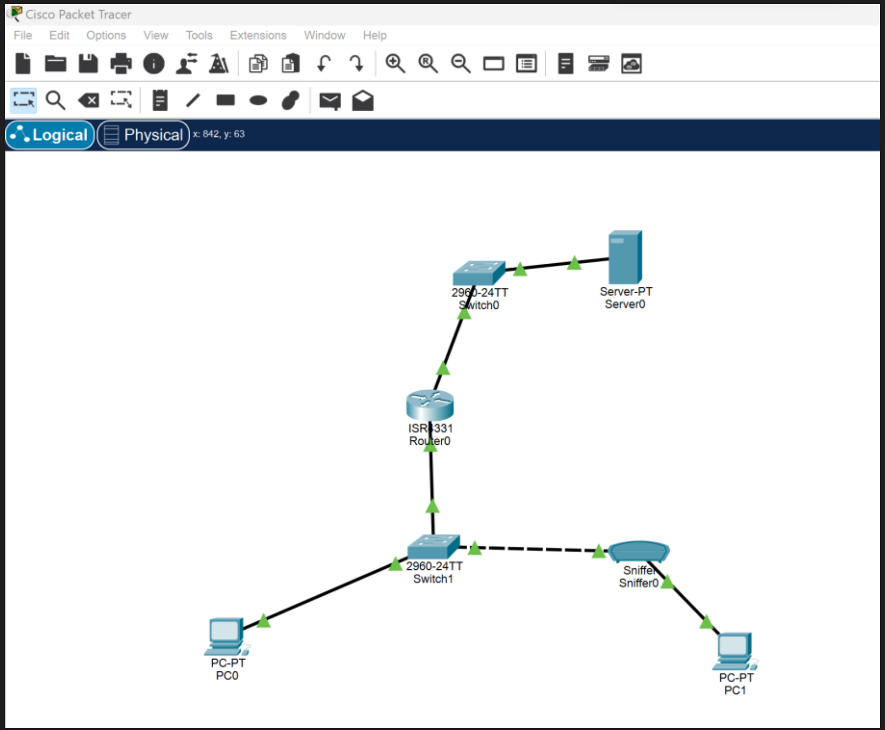
ARP Spoofing, also known as ARP poisoning or ARP poisoning attack, is a technique used by attackers to manipulate the Address Resolution Protocol (ARP) on a local area network (LAN). ARP is a protocol used to map an IP address to a physical MAC address, which is essential for communication between devices on a network.

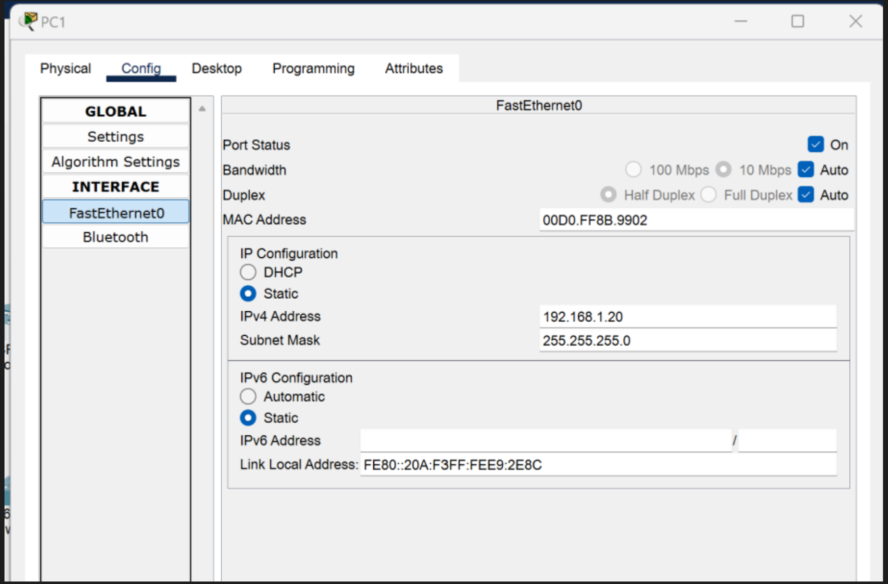
HOW TO ATTACK USING ARP SPOOFING

Man-in-the-Middle (MITM) Attacks: By manipulating ARP tables, an attacker can intercept, modify, or block the communication between two devices. This allows them to eavesdrop on the traffic or even inject malicious content.

Denial of Service (DoS): ARP spoofing can be used to flood the network with fake ARP replies, leading to confusion and disruption of network services.

Session Hijacking: By intercepting and manipulating communication between two parties, an attacker can hijack sessions, gaining unauthorized access to sensitive information.





FastEthernet0

Port Status ☑ On

Bandwidth ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ○ Full Duplex ☑ Auto

MAC Address 00D0.FF8B.9902

IP Configuration

○ DHCP

● Static

IPv4 Address 192.168.1.20

Subnet Mask 255.255.255.0

IPv6 Configuration

○ Automatic

● Static

IPv6 Address /

Link Local Address: FE80::20A:F3FF:FEE9:2E8C

ARP SPOOFING SIMULATION

IP ADDRESSES & MAC ADDRESSES

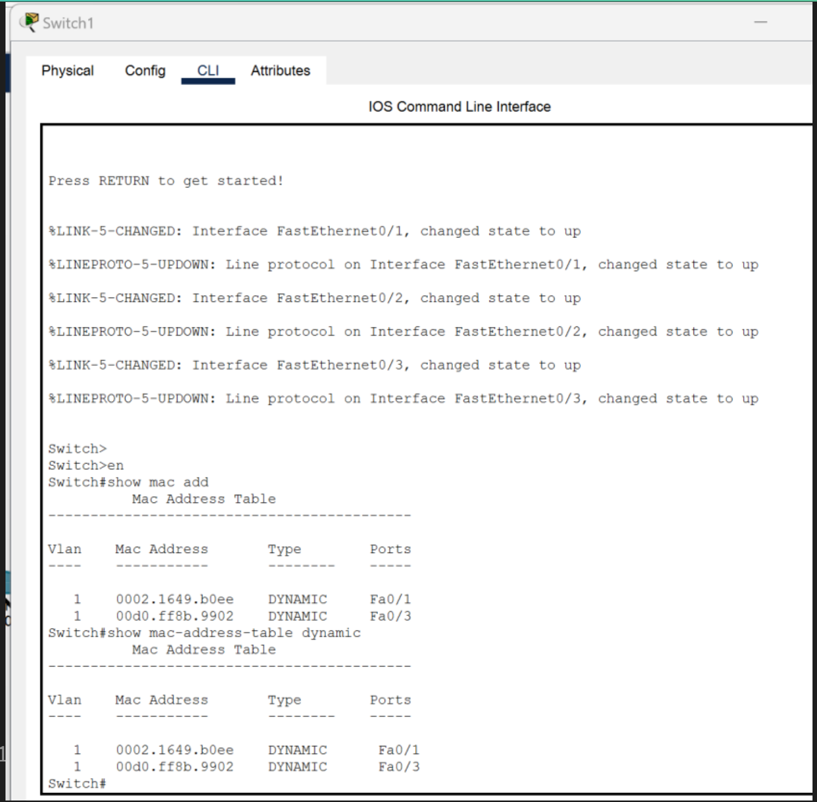
- PC0
  - 192.168.1.10
  - 00:02:16:49:B0:EE
- Router 1
  - 192.168.1.254
  - 00:D0:FF:8B:99:02
- Web Server
  - 192.168.2.100
- PC1 (Threat)
  - 192.168.1.20
  - 00:06:70:80:20:A8

MAN IN THE MIDDLE ATTACK USED

In order for PC0 to communicate with the router to get to the web server, PC0 needs to know the MAC address of the default gateway. Once we successfully, get PC0 to understand what the default gateway's IP and MAC address is, we have to make sure the threat PC (PC1) also knows what the default gateway is. Once that is successful, we manually change the threat PC's MAC address to the MAC address router 1 has, to spoof router 1. Then, we run a constant ping to talk to the IP address of PC0 with the source being the spoofed MAC address. The ARP cache for PC0 will now show the IP address for the original source (Router 1) and the spoofed source (Threat PC1) , indicating that the Man in the Middle attack was completed.

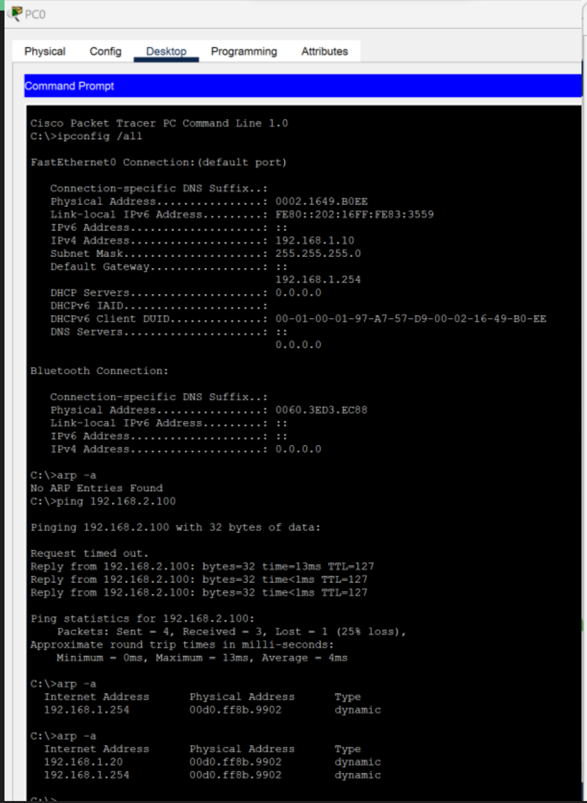
ARP SPOOFING

CODE

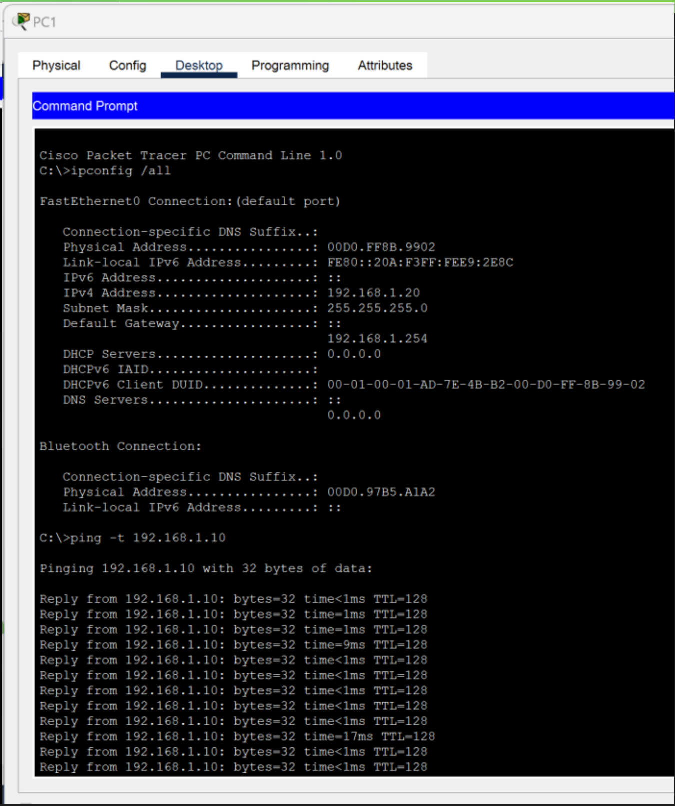


```
Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up


Switch>
Switch>en
Switch#show mac add
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0002.1649.b0ee    DYNAMIC     Fa0/1
   1    00d0.ff8b.9902    DYNAMIC     Fa0/3
Switch#show mac-address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0002.1649.b0ee    DYNAMIC      Fa0/1
   1    00d0.ff8b.9902    DYNAMIC      Fa0/3
Switch#
```

COMMAND PROMPT



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0002.1649.B0EE
   Link-local IPv6 Address.........: FE80::202:16FF:FE83:3559
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.10
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.1.254
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-97-A7-57-D9-00-02-16-49-B0-EE
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 0060.3ED3.EC88
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0

C:\>arp -a
No ARP Entries Found
C:\>ping 192.168.2.100

Pinging 192.168.2.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.100: bytes=32 time=13ms TTL=127
Reply from 192.168.2.100: bytes=32 time<1ms TTL=127
Reply from 192.168.2.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 4ms

C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.254         00d0.ff8b.9902        dynamic

C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.20          00d0.ff8b.9902        dynamic
  192.168.1.254         00d0.ff8b.9902        dynamic

C:\>
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 00D0.FF8B.9902
   Link-local IPv6 Address.........: FE80::20A:F3FF:FEE9:2E8C
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.20
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.1.254
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-AD-7E-4B-B2-00-D0-FF-8B-99-02
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 00D0.97B5.A1A2
   Link-local IPv6 Address.........: ::

C:\>ping -t 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time=1ms TTL=128
Reply from 192.168.1.10: bytes=32 time=1ms TTL=128
Reply from 192.168.1.10: bytes=32 time=9ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time=17ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
```

ARP SPOOFING

HOW TO PREVENT ARP SPOOFING ATTACKS

- **Use a Virtual Private Network (VPN)** — a VPN allows devices to connect to the Internet through an encrypted tunnel. This makes all communication encrypted, and worthless for an ARP spoofing attacker.
- **Use static ARP** — the ARP protocol lets you define a static ARP entry for an IP address and prevent devices from listening on ARP responses for that address. For example, if a workstation always connects to the same router, you can define a static ARP entry for that router, preventing an attack.
- **Use packet filtering** — packet filtering solutions can identify poisoned ARP packets by seeing that they contain conflicting source information and stop them before they reach devices on your network.
- **Run a spoofing attack** — check if your existing defenses are working by mounting a spoofing attack, in coordination with IT and security teams. If the attack succeeds, identify weak points in your defensive measures and remediate them.

THANK YOU