BUILDING A SIMPLE NETWORK USING

CISCO PACKET TRACER

Introduction

Networking is a fundamental aspect of cybersecurity, and understanding how to build and configure a network is essential. As part of my cybersecurity course with 10Alytics, I am learning how to design, configure, and troubleshoot basic networks using Cisco Packet Tracer. This report details my experience, step-by-step implementation, and key takeaways from the project.

Objectives

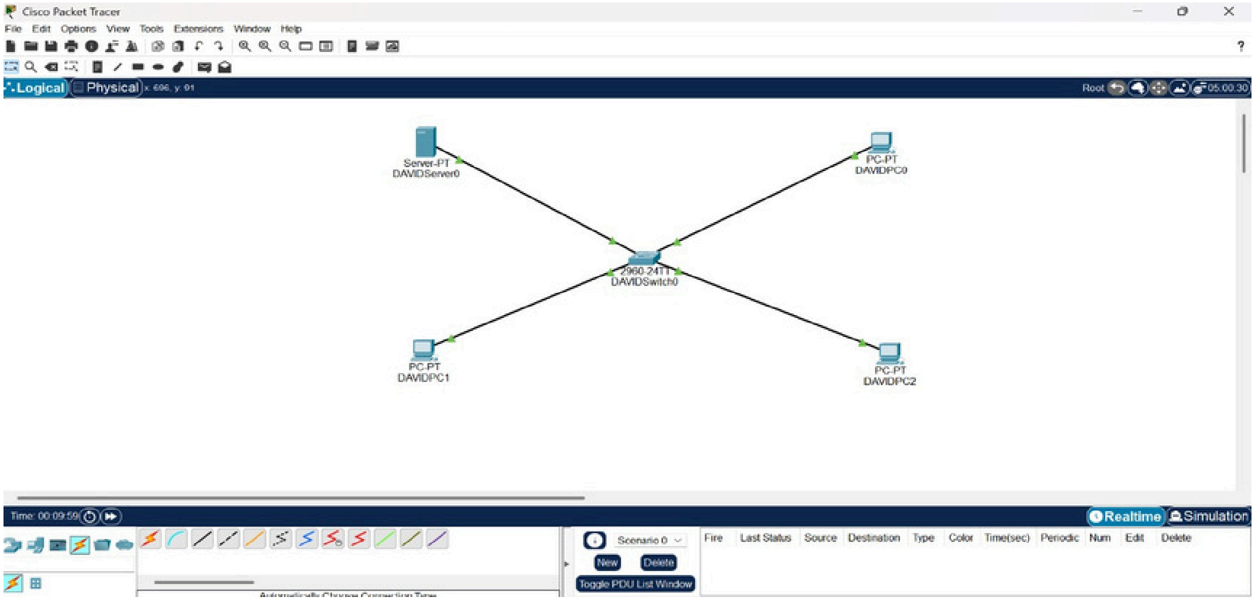
The goal of this project is to:

- Build a Complete Network Topology.
- Configure IP addresses and connectivity testing on all End Devices like PC's, Laptop and Server
- Configure Firewall on a Server and Block ICMP traffic
- Use Packet Tracer commands to Verify Network Configuration, to verify that ICMP traffic is blocked.

1. BUILD A COMPLETE NETWORK TOPOLOGY

to build a complete network topology, I will be using the following devices;

- One server
- One switch
- Three PC's
- Copper straight-through cable to connect the devices.

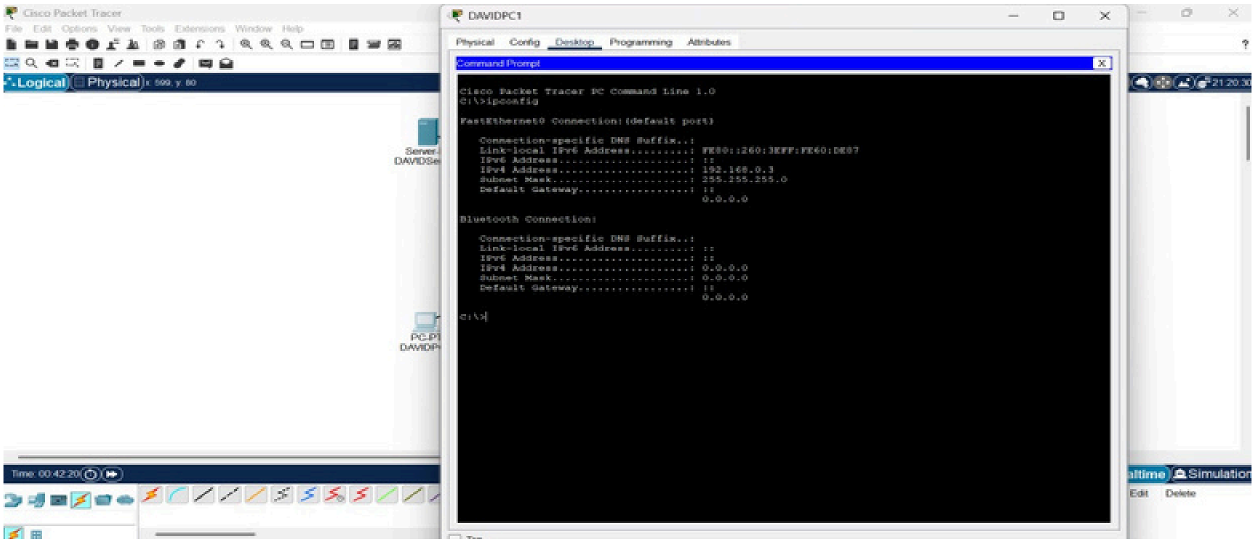


2. ASSIGNING IP ADDRESSES

Each End Device was assigned a unique IP address within the same subnet. Below is the configuration:

DEVICES	IP ADDRESS	SUBNET MASK
DAVIDSERVER0	192.168.0.1	255.255.255.0
DAVIDPC0	192.168.0.2	255.255.255.0
DAVIDPC1	192.168.0.3	255.255.255.0
DAVIDPC3	192.168.0.4	255.255.255.0

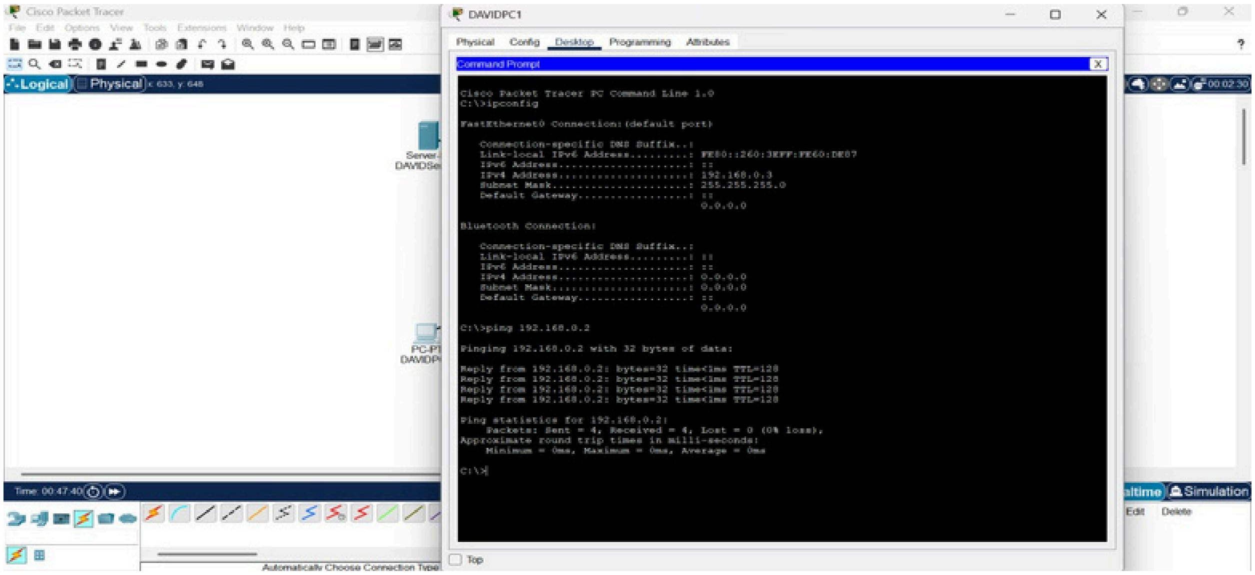
To verify IP Assigning was done properly, I used the ipconfig command from one Device to check. This can be seen in the screenshot below;



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

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::260:3EFF:FE60:DE87
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.0.3
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>
```

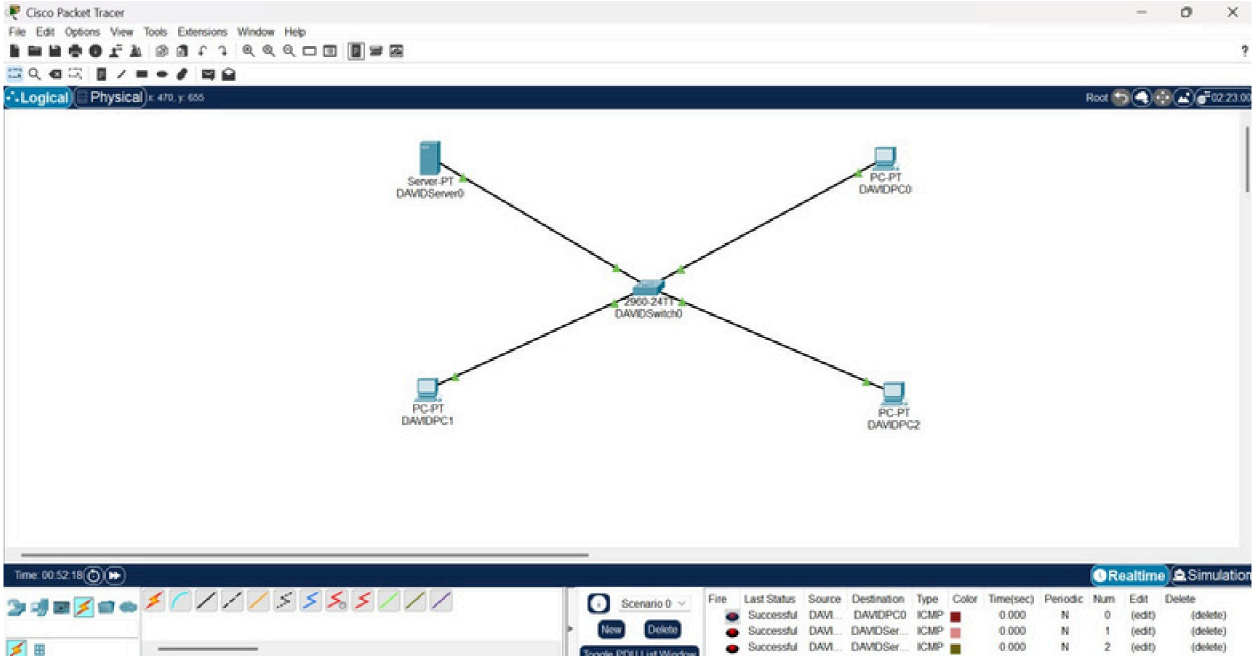
2B. TESTING NETWORK CONNECTIVITY

To verify network connectivity, I used the ping command from one Device to another. Successful responses confirmed proper network configuration as shown below;



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

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::260:3EFF:FE60:DE87
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.0.3
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

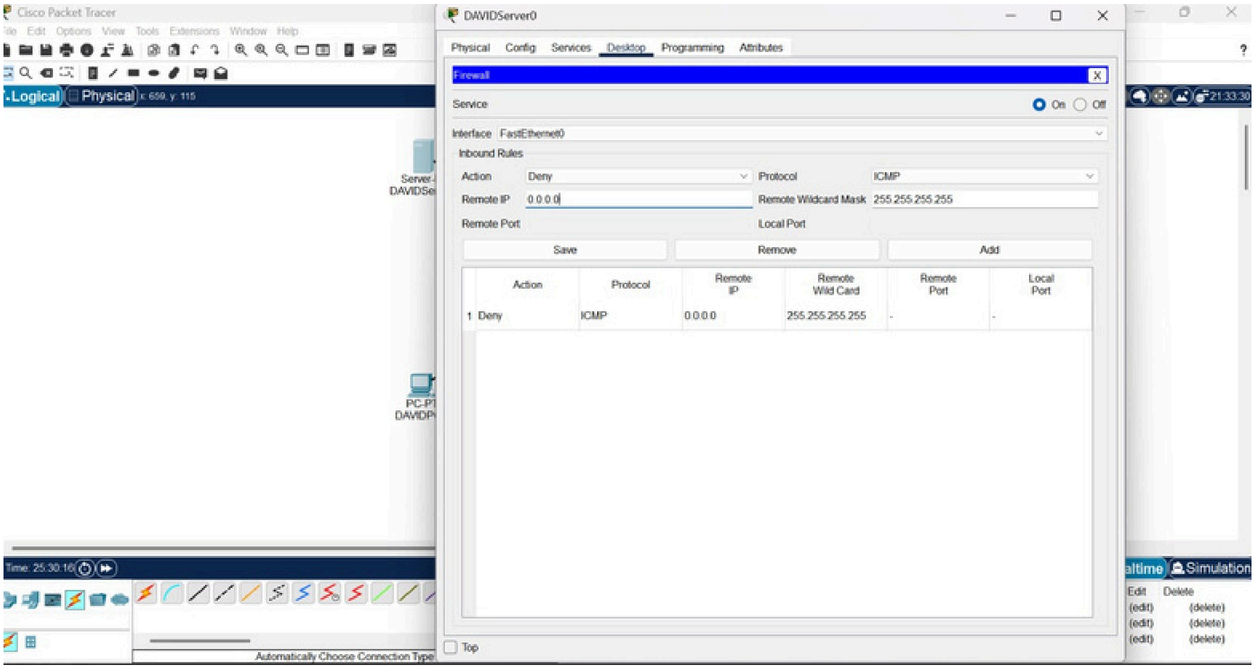
I also sent simple test messages in Realtime mode and Successful message received confirmed proper network configuration as shown below;



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	DAVI...	DAVIDPC0	ICMP	🟥	0.000	N	0	(edit)	(delete)
●	Successful	DAVI...	DAVIDSer...	ICMP	🟥	0.000	N	1	(edit)	(delete)
●	Successful	DAVI...	DAVIDSer...	ICMP	🟫	0.000	N	2	(edit)	(delete)

3. CONFIGURE FIREWALL ON A SERVER

To increase network security, I configured a firewall on the server to control incoming and outgoing traffic. The firewall was set up to: Block ICMP (ping) request traffic. The Firewall configuration is shown in the image below;



Service ● On ○ Off

Interface FastEthernet0

Inbound Rules

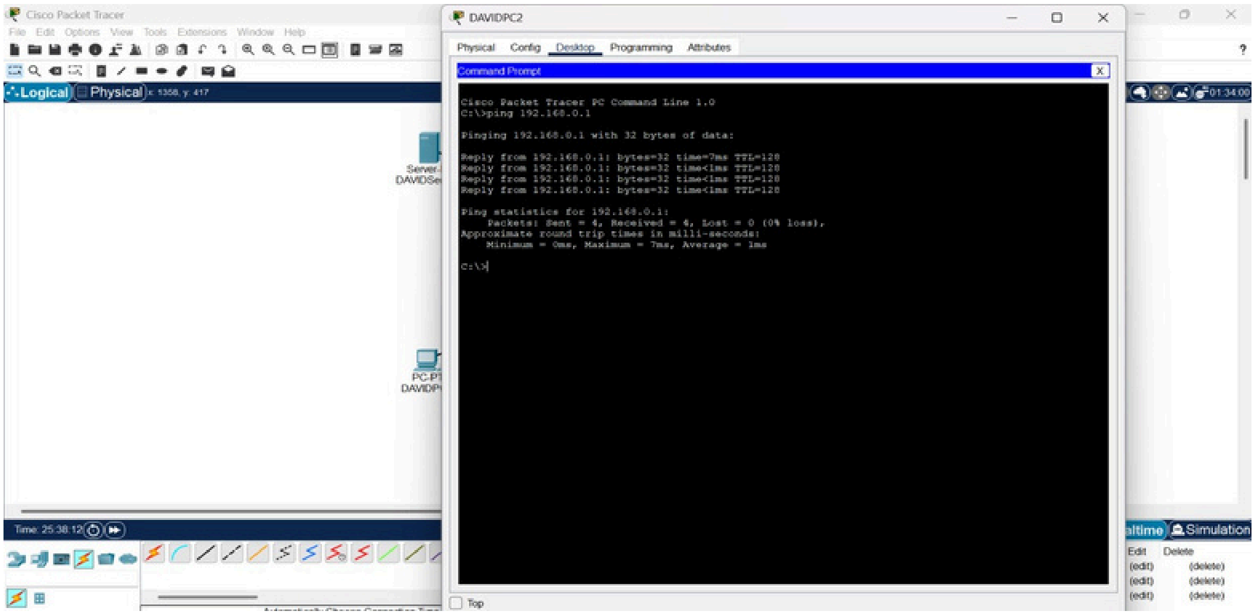
Action: Deny
Protocol: ICMP
Remote IP: 0.0.0.0
Remote Wildcard Mask: 255.255.255.255
Remote Port
Local Port

	Action	Protocol	Remote IP	Remote Wild Card	Remote Port	Local Port
1	Deny	ICMP	0.0.0.0	255.255.255.255	-	-

3B. TESTING THE FIREWALL-BLOCKING ICMP TRAFFIC.

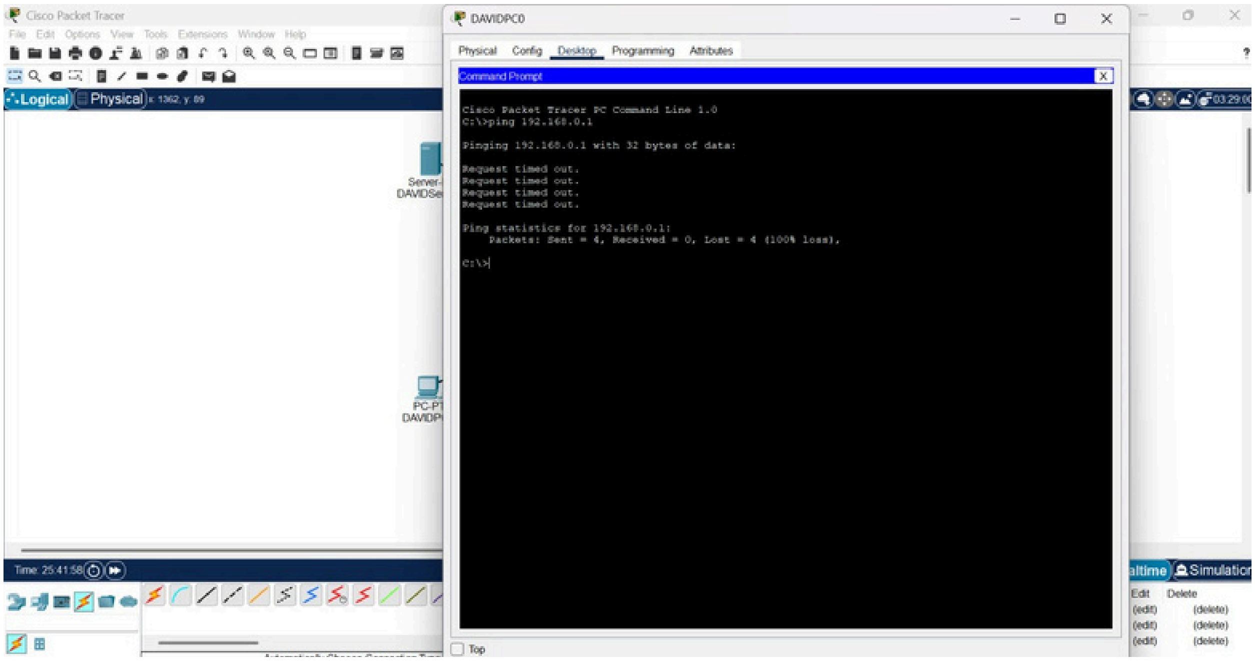
To verify that ICMP traffic is blocked, I performed a ping test from a PC to the Server.

Ping Test before blocking ICMP;



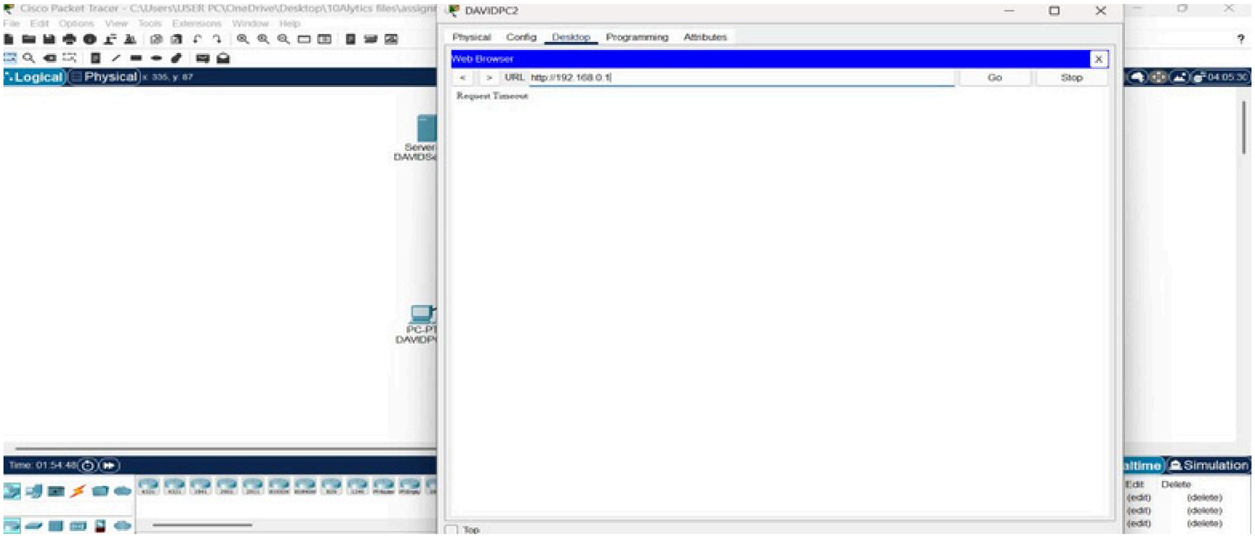
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=7ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 1ms

C:\>
```

Ping Test after blocking ICMP;



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

To verify that web traffic is allowed, I performed a test from one PC as shown in the image below;



URL http://192.168.0.1

Request Timeout

The image above shows a request timeout message, which indicates that the webpage cannot be reached.

KEY TAKEAWAYS:

- Learned how to configure end devices like server, switches, and PC in Packet Tracer.
- Understood IP addressing, subnetting, and network connectivity testing.
- Implemented firewall rules to control traffic and enhance security.

- Successfully blocked ICMP traffic to prevent reconnaissance attacks.

CHALLENGES FACED:

Issue: when trying to check web traffic, to see if server web page loads, demonstrating that HTTP traffic is permitted, server web page was not displayed. A request timeout messages displayed instead.

I also observed that when disabled the firewall, server webpage was displayed without any errors.

I will research on this issue to find out what I did wrong so as to improve on my learning.