Self-Study

Intrusion Detection System

By: Farhan Akhter (1RV19EI017)

Branch: Electronics and Instrumentation

Submitted to: Prof. Veena Divya. K (Assistant Professor, Department of EIE)

Course: Data Networks [18EI52]

ABSTRACT

Intrusion Detection System is a software or a device that can monitor all the suspicious activities in the network or that activities that violates its policy.

IDS is very popular system to protect the networks from different types of attacks. Any intrusion activity or violation is reported or informed either to administrator or this information can be centrally collected in a system called SIEM (Security Information and Event Management).

It collects and combine information from different sources, and it uses alarm filtering techniques. There are two most common types of IDS.

(NIDS) Network based Intrusion detection system and (HIDS) Host based Intrusion detection system. HIDS is used for monitoring important operating system files and NIDS are used to analyze incoming network traffic. Here's how IDS work, IDS when placed at a strategic point or points within a network to monitor traffic to and from all devices on the network, an IDS will perform an analysis of passing traffic, and match the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator.

Modern networked business environments require a high level of security to ensure safe and trusted communication of information between various organizations.

An intrusion detection system acts as an adaptable safeguard technology for system security after traditional technologies fail. Cyber-attacks will only become more sophisticated, so it is important that protection technologies adapt along with their threats.

Introduction

An IDS is basically a software or device that is categorized into two common parts one is NID i.e., Network Intrusion Detection and second is HID i.e., Host Intrusion Detection. The work of both the NID & HID is same but their level is different. But IDS are categorized into 5 types – NIDS, HIDS, PIDS, Hybrid IDS & APIDS. Work is same to detect intrusions, but they are used at different levels.

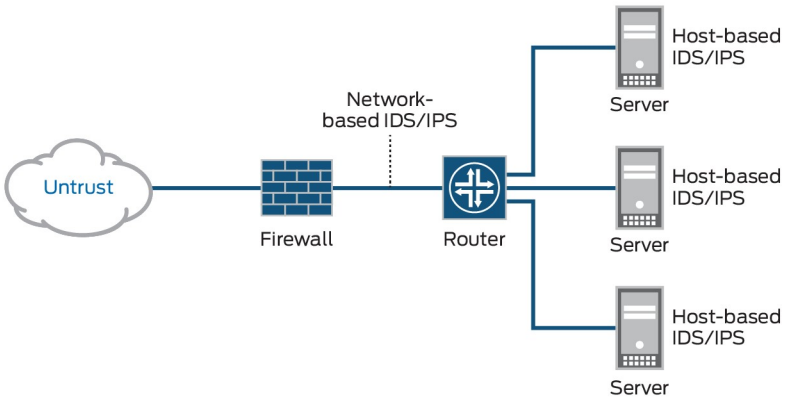


Fig 1.1

In Fig 1.1 you are now clear that where HIDSs are used and where NIDSs are used.

This project implements Intrusion Detection System by creating 3 different networks as in Fig 1.2. Implementing the IDS is very challenging task as it needs the implementor to have proper knowledge with prior knowledge with some common and special network devices and ethernet cables. One must know how to deal with CLI i.e., Command Line Interface

A layout of the network should be made prior to the implementation of IDS for implementing NIDS. There are various parameters which are to be kept in mind while designing network and configuring IDS. Here are some cans and can nots about the IDS.

- CAN recognize and report alterations to data.
- CAN detect when your system is under attack.
- CAN detect errors in your system configuration.
- CAN NOT analyze all the traffic on a busy network.
- CAN NOT prevent system from that attack which it detects.
- CAN NOT deal with some of the modern network hardware and features.

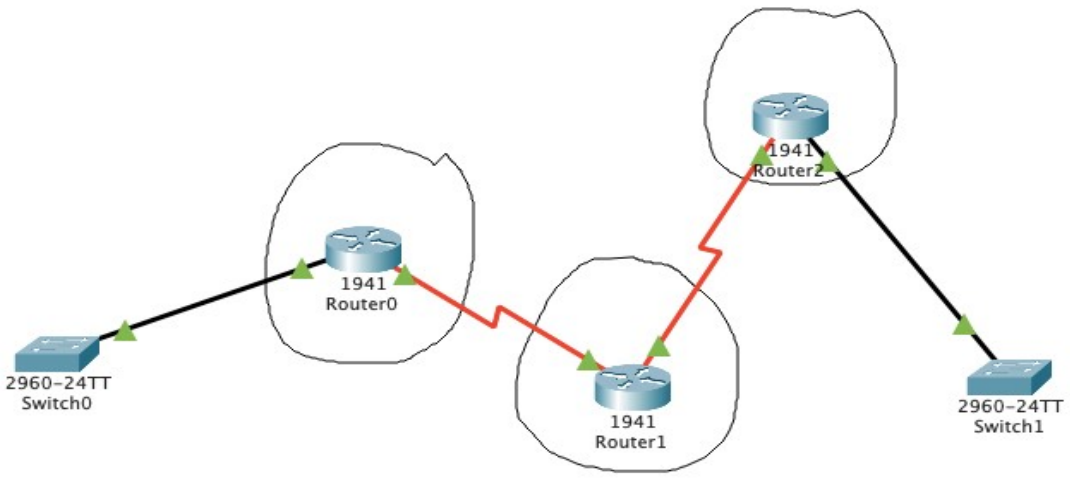


Fig 1.2

Goals and Specifications

The goal of this project is to design, implement and test a stable and secure IDS that can be used to secure any type of network. It also can immediately inform the administration about the intrusion or any suspicious activity. It collects all the different protocols and traffic information directly to the admin of the network and after informing the admin the work of the IDS is completed, next admin decides what to do with this traffic, whether to continue the traffic or block.

The final IDS design after all the configurations it should meet the following specifications:

1. The IDS must be capable of detecting the type of traffic which admin assigned to it.

2. The IDS must be capable of informing admin about any suspicious activity related to the signatures assigned by the admin.

3. The IDS should create a log report in the server which is specifically meant for logging these activities.

4. The IDS must be capable of scanning the traffic which is entering inside the network.

System Design

Project Layout :

The network layout stage includes the whole network blueprint that on which type of network our IDS will be implemented. We are using 3 different types of networks which has some hosts and servers inside it.

The First Network is made of IPv4 Addressing having the IP addresses in the range of

192.168.1.2 – 192.168.1.7

Default Gateway for this Network is 192.168.1.1

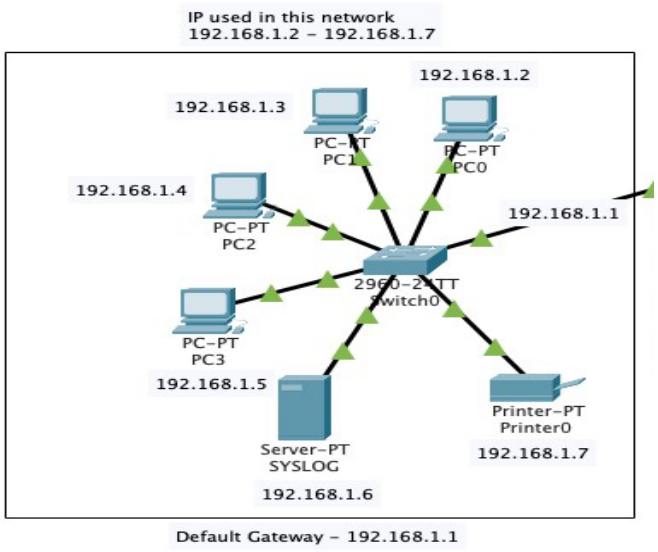


Fig 3.1 Network 1

Devices in this network :

- 4 Different PCs
- 1 SYSLOG Server
- 1 Printer
- 1 Switch as shown in Fig 3.1

The First Network is made of IPv4 Addressing having the IP addresses in the range of

192.168.10.2 – 192.168.10.8

Default Gateway for this Network is 192.168.10.1

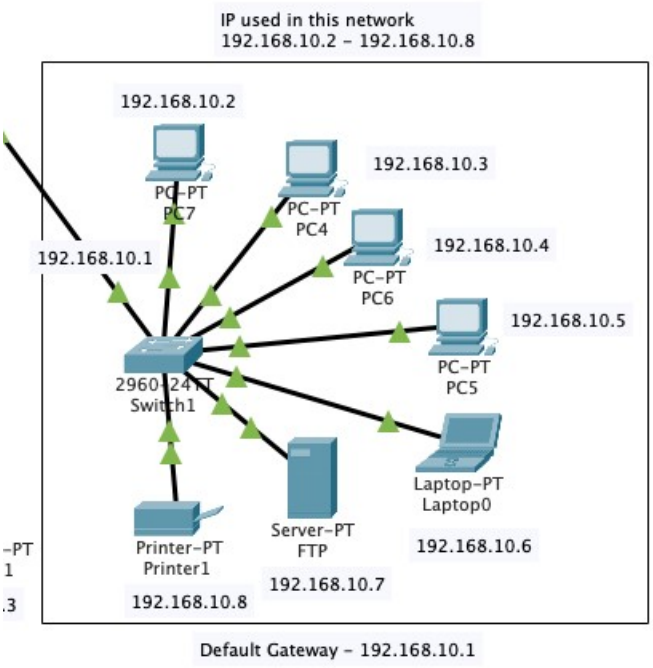


Fig 3.2 Network 2

Devices in this network :

- 4 Different PCs
- 1 FTP Server
- 1 Printer
- 1 Laptop
- 1 Switch as shown in Fig 3.2

The Third Network is made of IPv4 Addressing having the IP addresses in the range of

192.168.30.2 – 192.168.30.4

Default Gateway for this Network is 192.168.30.1

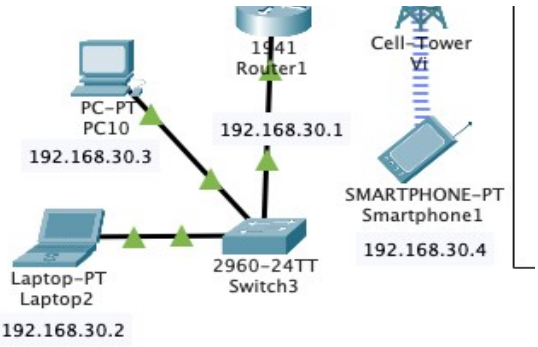


Fig 3.3 Network 3

Devices in this network – - 1 PC

- 1 Laptop
- 1 Switch as shown in Fig 3.3

3 (1941) Routers are used to connect all these 3 LANs together. Dynamic routing is used to route traffic across 3 networks.

Networks Connected with Router 1 (router0)

- 192.168.1.0
- 100.0.0.0
- 10.0.0.0

Networks Connected with Router 2 (router1)

- 10.0.0.0
- 20.0.0.0
- 192.168.30.0

Networks Connected with Router 3 (router2)

- 20.0.0.0
- 192.168.10.0

Network Devices and Connection Stage

Network Devices used in this Network :

- 1941 Router with 2 Gigabit Ethernets and 4 Serial Connection Ports
- HTTP Server
- FTP Server
- 2960 Switch with 24 Fast Ethernets and 2 Gigabit Ethernet Ports
- PT Printer
- Personal Computer
- SYSLOG Server
- Laptop
- Mobile Tower with 3G/4G Service
- 4G Compatible Smart Phone

Cabling used in this Network :

- Copper Straight-through Cable
- Serial DCE Cable

Straight-Through Cable is used between :

- PC to Switch
- Switch to Router
- Laptop to Switch

- Server to Switch

Serial Cable is used between :

- Router to Router

2 Different Servers are put across the networks to perform some more functions like Web Access, File transfer.

These Servers are HTTP and FTP.

HTTP is used for Web traffic like if we want to access any website HTTP protocol or server comes into play.

FTP is used for file transfer like if we want to store some files on the server or download some files from a server FTP protocol or server comes into play.

In proper connection IP addresses are very important to communicate across the network.

IP used in this network is Class A and Class C

From Class A IPs used are –

100.50.0.1 @ router interface gigabit ethernet 0/1

100.50.0.2 @ HTTP Server Port fast ethernet 0

10.10.10.1 @ router interface Serial 0/0/0

10.10.10.2 @ router interface Serial 0/0/0 20.20.20.1 @ router interface Serial 0/0/1

20.20.20.2 @ router interface Serial 0/0/0

As large number of IPs are from Class C because it has the greatest number of hosts from other classes such as A and B.

Command Line Interface

To configure any device in packet tracer you are required to open or access its CLI. You can do it by clicking any device and then navigating to CLI tab. Once you are at CLI you can perform all Cisco Commands here. A Cisco IOS router command line interface can be accessed through a console or connection, modem connection, or a telnet/ssh session.

Regardless of which connection method is used, access to the IOS command-line interface is generally referred to as an EXEC session as shown in Fig 3.4

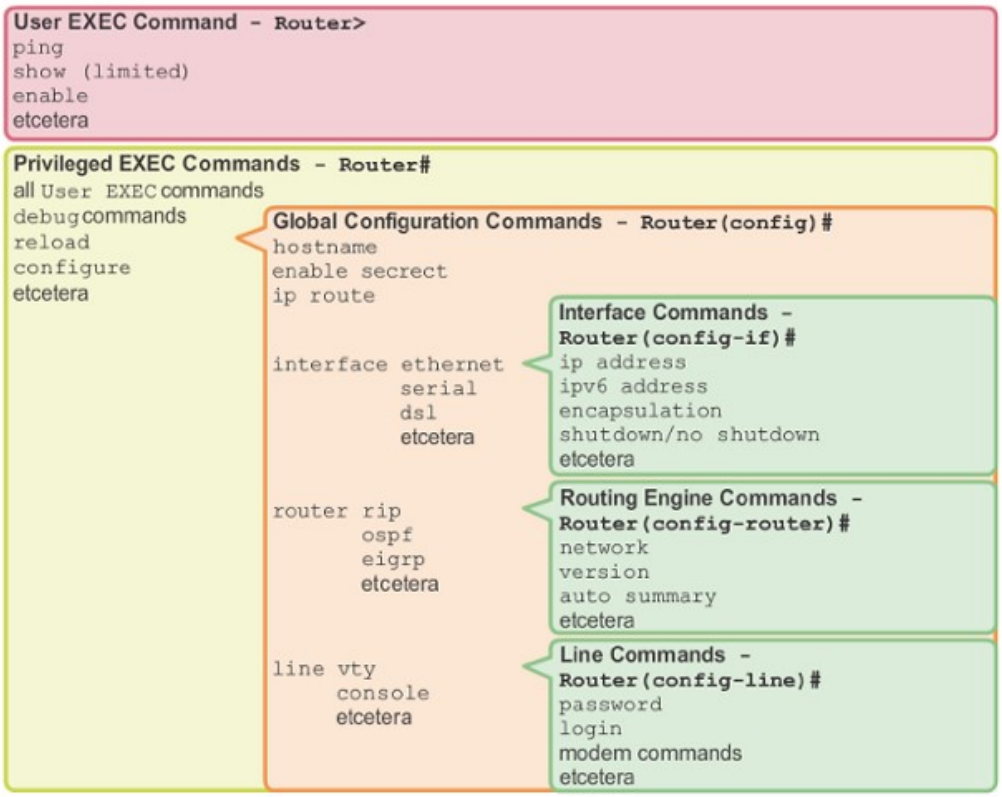
As a security feature, Cisco IOS separates EXEC sessions into two different access levels — the user level and the privileged EXEC level.

EXEC user level allows a person to access only a limited amount of basic monitoring commands.

Privileged EXEC level allows a person to access all the router's commands (e.g. configuration and management) and can be password protected to allow only authorized users the ability to configure or maintain the router.

Once an EXEC session is established, commands within Cisco IOS are hierarchically structured. To be able to configure the router, it is important to understand this hierarchy.

Fig 3.4 IOS Mode Hierarchical Structure



Configuring the Network

Placing the devices and connecting it with cables is not enough! We must do far more than this. After connecting with cables first task is to assign them IP addresses. As discussed above Class A and C IPv4 are used. After assigning IP to each interface in the network. Next step is to check connectivity from one PC to another. But here connectivity only works inside the network, our network is still not capable of communicating with outside PCs as you can see in Fig 3.5, 3.6 & 3.7

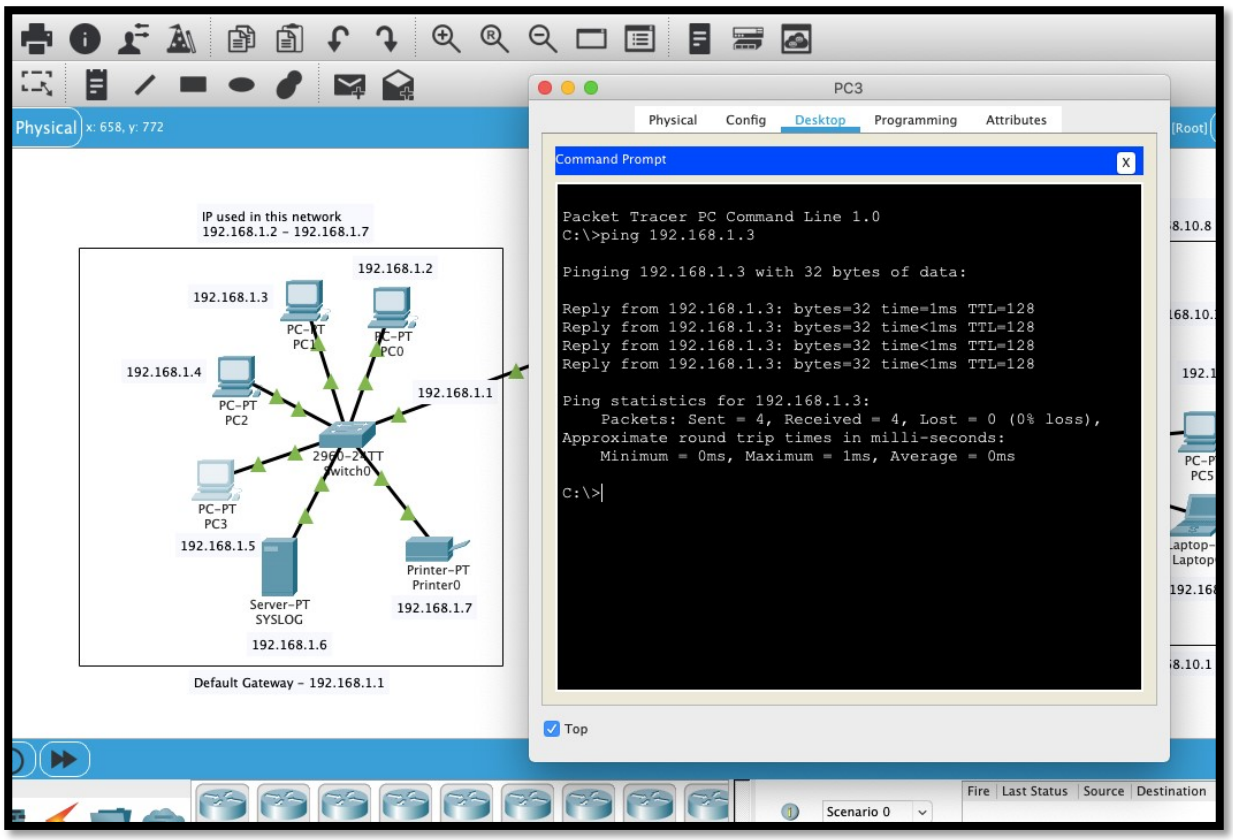


Fig 3.4 Ping test form PC3 to PC1

Ping is a command used to test connectivity between two hosts or devices.

Ping test from PC3 to PC1 is successful.

Let's take another test of sending a ICMP packet from PC 3 to PC7 (other network) and check whether it successfully reached or not.

As you can see in Fig 3.6, it didn't reach its destination.

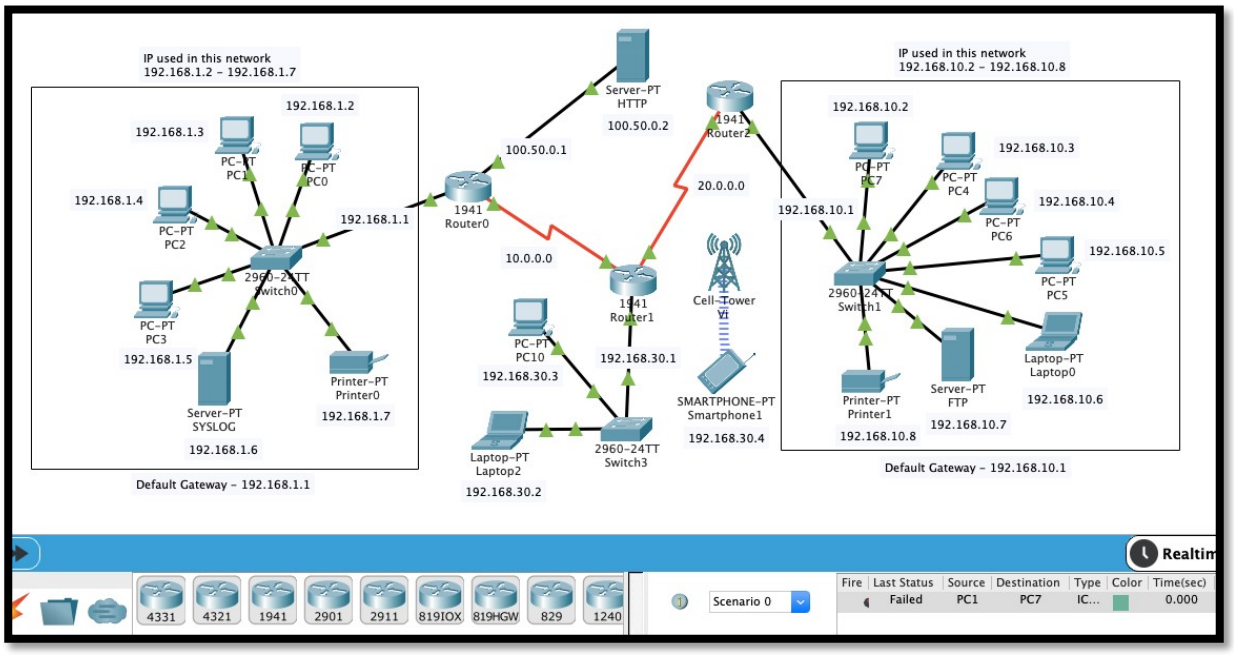


Fig 3.6 ICMP Packet Sent from PC3 to PC7

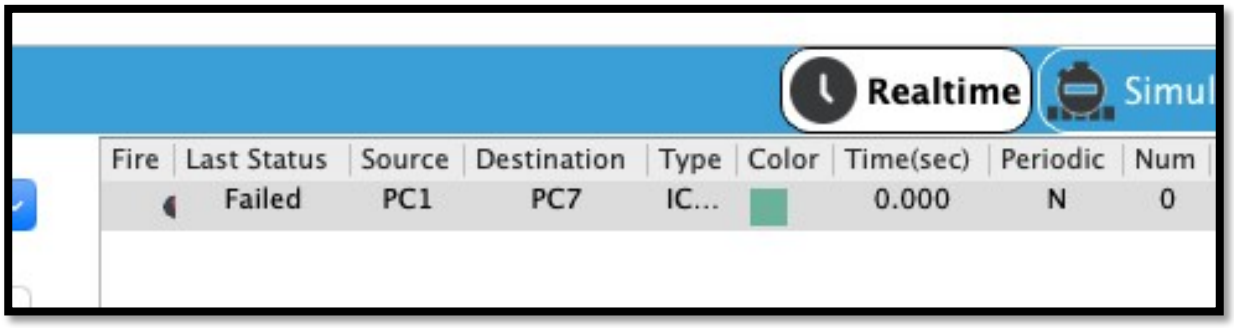


Fig 3.7 Failed ICMP packet history from PC3 to PC7

This failure occurs because we have not told router, where it should send the packet it comes to it.

The concept of Routing comes here. There are two types of routing.

- Static Routing
- Dynamic Routing

For our project we have used dynamic routing concept because it is easier to use.

Another task for configuring this network was configuration of Servers i.e., Syslog, HTTP, FTP. For Syslog server I have turned down all the service except logging service called 'SYSLOG' so that it can focus only to logging information come from IDS.

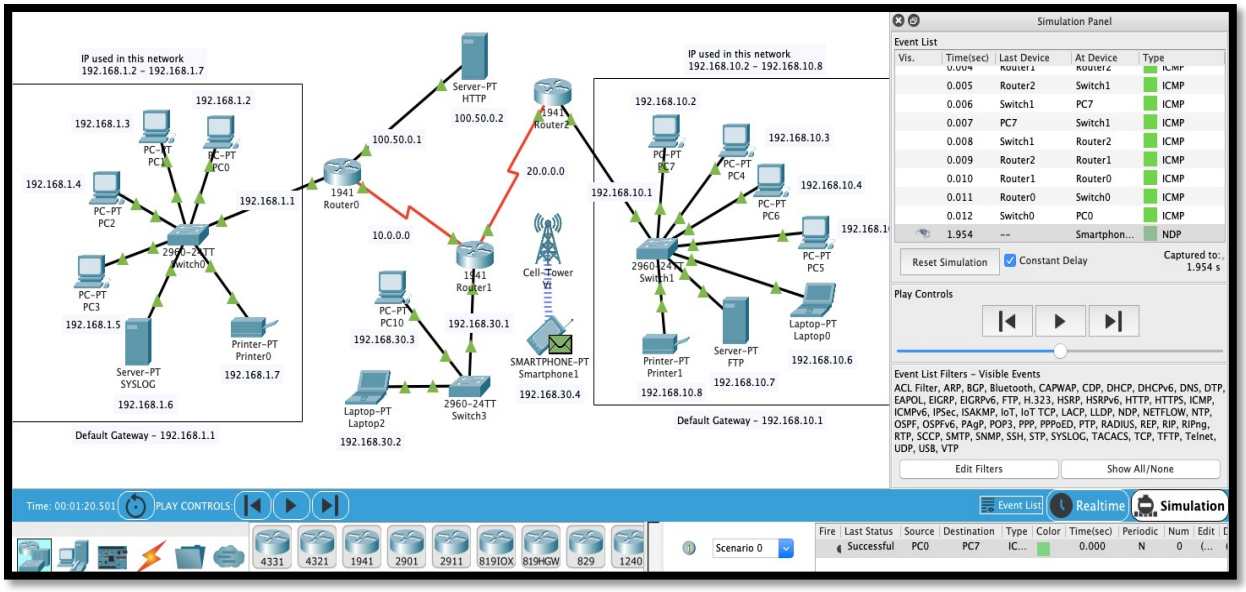
For configuring HTTP same concept as syslog. Here I made a custom webpage which can be accessed from any host in the any network by IP address called 100.50.0.2

For configuring FTP same concept. Here I made a user called 'farhan' and password '123'

So now our entire network is configured properly.

Testing the Network

Before moving towards the implementation of IDS. It is important to test the connectivity of the entire network. So here are the testing results.



In this a Packet is sent to PC7 from PC1 and acknowledgement of that packet is received back to the PC1 and the whole process is successfully completed.

Implementation of NIDS using CLI

Now the main task has reached. We must apply IDS into this network for securing it.

Our IDS will be implemented on Router0 on interface (gigabit ethernet 0/0). Our IDS will scan all the ICMP traffic which is coming into the Network 1 from this interface. For that we have used IPS Signature 2004

2004 ICMP Echo Request (Info, Atomic)

Triggers when an IP datagram is received with the “protocol” field in the IP header set to 1 (ICMP) and the “type” field in the ICMP header set to 8 (Echo Request).

Although we have a list of different Signatures which made for different types of data traffic. Some signatures are –

- 2001 ICMP Host Unreachable (Info, Atomic)
- 1101 Unknown IP Protocol (Attack, Atomic)
- 2007 ICMP Timestamp Request (Info, Atomic)
- 3040 TCP - no bits set in flags (Attack, Atomic)

- 3100 Smail Attack (Attack, Compound)

For implementing IDS on router0 we must firstly activate security package of that router. We have activated 'securityk9' package as shown in Fig 3.8

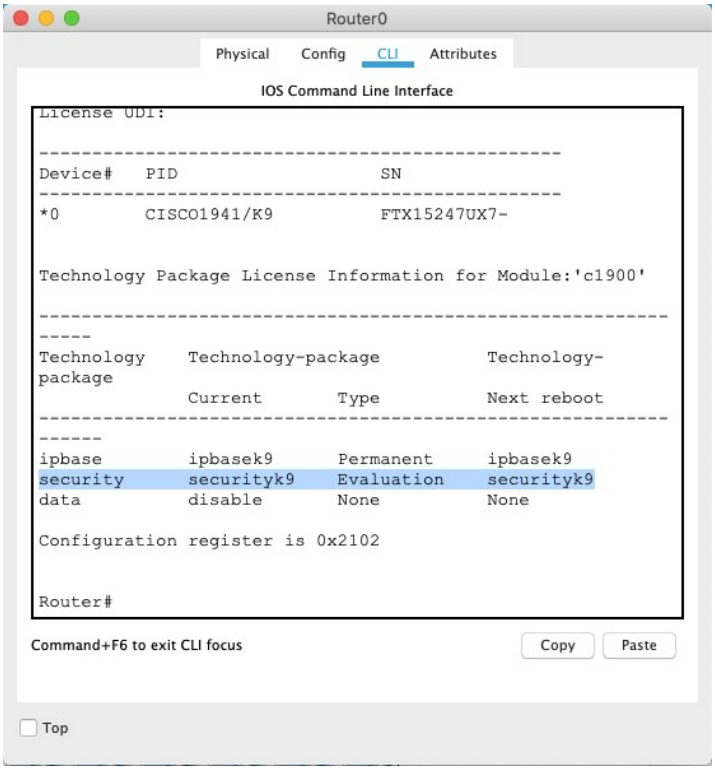


Fig 3.8 Security Package

Commands for Implementing IDS

There are different commands used for implementing and enabling IDS on that specific interface.

Commands	Description
enable	It is used to enable the networking device.
config t	It will enter the device into configuration mode.
show version	It is used to show version of router with some other details and security & data packages.
license boot module c1900 technology package securityk9	It is used to activate the securityk9 package in the router for IDS implementation.
do reload	For reloading the router.
mkdir (directory_name)	Used for making a directory in router
ip ips config location (directory_name)	Assigning the location to store IPS signatures.
ip ips (name)	For creating a IPS rule

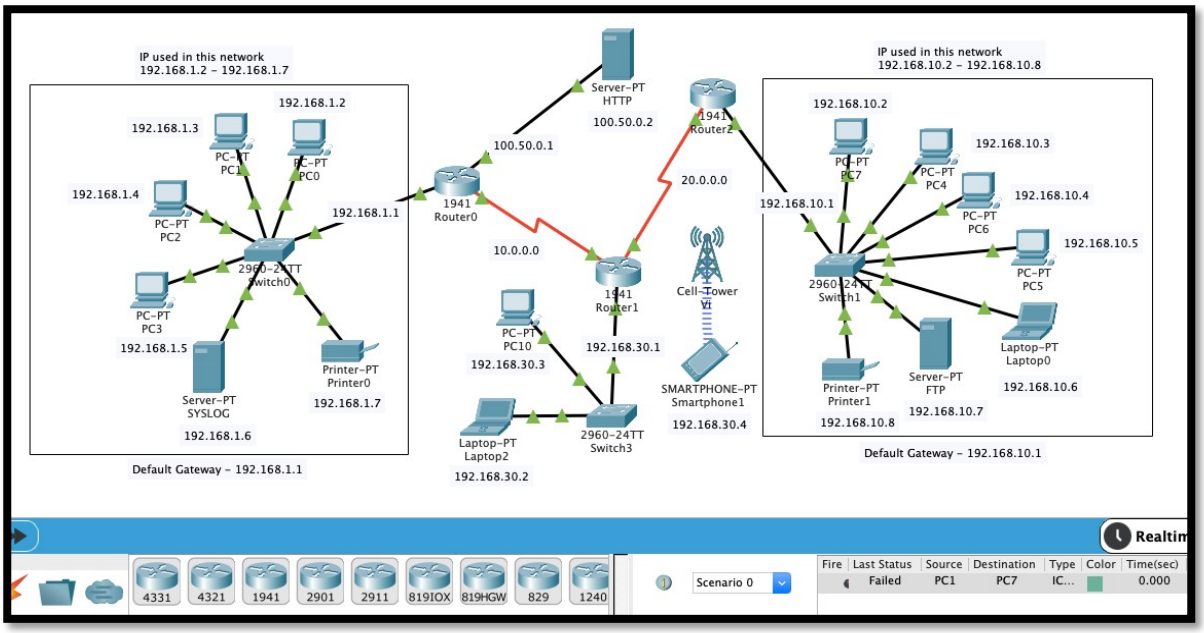
ip ips signature-category	For checking or entering the IPS signature categories.
category all	For entering all the categories of IPS.
retired true	For retiring a category.
retired false	For unretiring a category.
category (name) basic	For entering a category which we made earlier as IPS rule. And unretiring all the basic categories of this rule.
int (interface_name)	To enter an interface.
ip ips (rule_name) out	To apply the IPS signature inward at a interface.
logging on	Turning on the logging capability of the router.
logging host (ip_address)	Assigning the syslog server for logging
service timestamps log datetime msec	To synchronize clock between system clock and log message.
ip ips signature-definition	To enter a specific signature and change the definition of that signature
signature 2004 0	2004 is the signature ID and 0 is the SubID of the IPS signature we have used in our system.
status	To enter the status of this signature
enabled	To enable this category signature
engine	This command is used to change the action of that signature whether to inform or block.
event-action	Action of the signature is configured in the event-action section
produce-alert	This will alert the admin by logging into syslog server
deny-packet-inline	This will block all the packet if it matches with the signature we have configured. THIS IS NOT USED AS THIS IS ONLY IDS NOT IPS.
do show	This will show all the configuration of IDS implemented on that router interface.

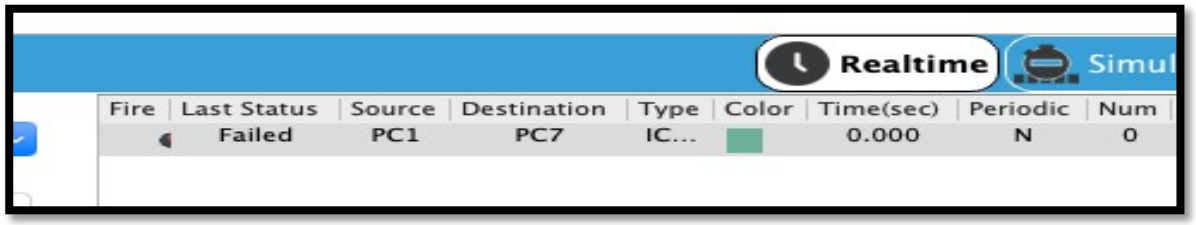
Experimental Results

Testing NIDS & SYSLOG

Dynamic routing concept is used because it is easier to use.

Another task for configuring this network was configuration of Servers i.e., Syslog, HTTP, FTP. For Syslog server all the services are turned down except logging service called 'SYSLOG' so that it can focus only to logging information come from IDS.
For configuring HTTP same concept as syslog. Here a custom webpage has been created which can be accessed from any host in the any network by IP address called 100.50.0.2
For configuring FTP same concept. Here a user called 'farhan' and password '123' has been created
So now our entire network is configured properly.





Difficulties

- Setting up the IP address of all the systems in the network
- Then we had Issue with Routing which was then tackled and solved using the concept of Dynamic routing which enabled us to transfer files and packet from one system to another.
- Setting the protocols for http and ftp servers.
- Having the command lines to work and prevent the intrusion with syslog.

Future Work

In future reference we need to work on the Honeypot System to implement and work the Intrusion Prevention System along with the Intrusion Detection System.

Conclusion

In this project of implementing an Intrusion detection System using Cisco Packet Tracer, we created a network using different components likes pc's, routers, switches, servers, connecting wires, hubs, etc.

After Connecting the network, we accessed the networks and allotted different protocols to different components like FTP, HTTP etc. to servers, IPs to all the devices in the network, And Shared ICMP packets through the network to ensure its flawless working.

Then we fed and flooded the network using Pings and monitored the ping, type of message and connection status. This was done to test the NIDS and implemented the IDS.