Intrusion Detection System

MINI PROJECT

Submitted by

Jacob Kevin P
[RA2111030010161]
Gowtham G [RA2111030010150]
Ethan RM Asher
[RA2111030010163]

Under the Guidance of

Dr. A. Arun

Assistant Professor, Networking and Communications

In partial satisfaction of the requirements for the degree of

BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE ENGINEERING
with specialization in Cyber security

SCHOOL OF COMPUTING

COLLEGE OF ENGINEERING AND TECHNOLOGY SRM

INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR - 603203

MAY 2023

SRM INSTITUTION OF SCIENCE AND TECHNOLOGY KATTANKULATHUR-603203

BONAFIDE CERTIFICATE

Certified that this project titled **“Intrusion Detection System”** is the bonafide work done by **Jacob Kevin P [RA2111030010161], Gowtham G [RA2111030010150] & Ethan RM Asher [RA2111030010163]** who carried out the lab exercises under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form part of any other work.

SIGNATURE

LAB INCHARGE

Dr. A. Arun

Assistant Professor

Department of Networking and Communications

SRMIST – KTR.

SIGNATURE

HEAD OF THE DEPARTMENT

Dr.Annapurani Panaiyappan.K

Professor & Head

Department of Networking and Communications

SRMIST – KTR

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 behaviour 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.

TABLE OF CONTENTS

CHAPTER NO.	**TITLE**	**PAGE NO.**
	ABSTRACT	
1	INTRODUCTION	3
2	SYSTEM DESIGN	4
3	SOFTWARE AND HARDWARE REQUIREMENTS	8
4	IMPLEMENTATION	10
5	TESTING THE NETWORK	12
6	CONCUSION	16
7	REFERENCES	17

Introduction

An IDS is basically a software or device that is categorised 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 categorised into 5 types – NIDS, HIDS, PIDS, Hybrid IDS & APIDS. Work is same to detect intrusions but they are used at different levels.

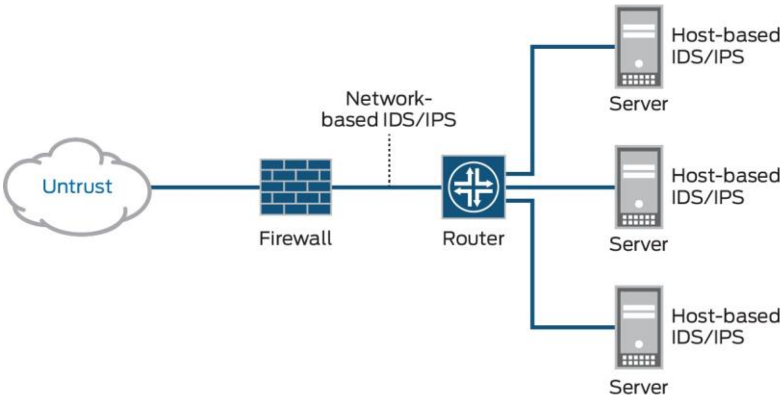


Fig 1.1

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

In this project I have implemented Intrusion Detection System by creating 3 different networks. Implementing the IDS is very challenging task as it needs the implementor to have proper knowledge with prior knowledge with some common andspecial network devices and ethernet cables. One have to know that how to deal with the CLI i.e. Command Line Interface. As I am performing this project on Cisco PacketTracer – A best available simulation tool which allows users to see the working of network in real time.

A layout of the network should be made prior to the implementation of IDS as I'm implementing NIDS. There are various parameters which are to be kept in mind while I designed network and configure IDS. Here are some 'can's and 'can not's 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 analyse 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

System Design

Project Overview

Project Layout Stage

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

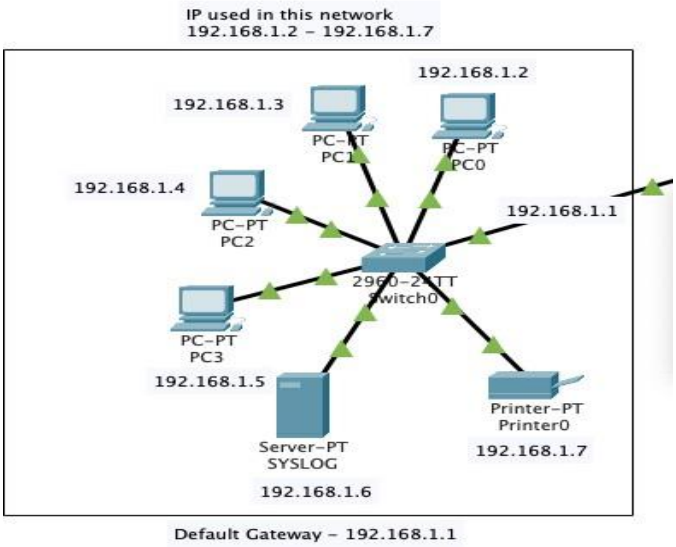


Fig 3.1 Network 1

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

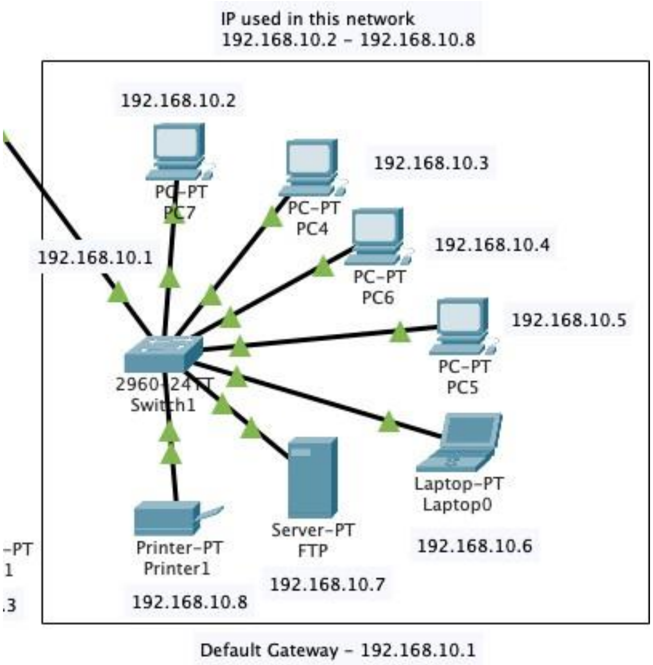


Fig 3.2 Network 2

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

Devices in this network –

- 1 PC
- 1 Laptop
- 1 Switch as shown in Fig 3.3

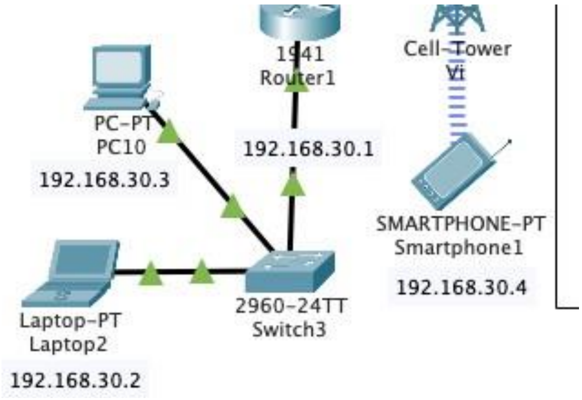


Fig 3.3 Network 3

3 (1941) Routers are used to connect all these 3 LANs together. Dynamic routing is used to route traffic all 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 most number of hosts from other classes such as A and B.

Software and Hardware Requirements

To implement this project we have to meet some software and hardware requirements.

For Software Requirement it is required to have (CISCO PACKET TRACER) installed on the System. Every implementation is done on this tool.

For Hardware Requirement it is required to have the followings

- Intel Pentium 4, 2.53GHz or equivalent Processor
- 2GB Ram
- 1GB of free storage space
- Display of resolution 1024*768
- Language fonts supporting Unicode encoding
- Latest video card and OS updates

Cisco Packet Tracer

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts. Previously students enrolled in a CCNA Academy program could freely download and use the tool free of charge for educational use.

Packet Tracer can be run on Linux, Microsoft Windows, and macOS. Similar Android and iOS apps are also available. Packet Tracer allows users to create simulated network topologies by dragging and dropping routers, switches and various other types of network devices. A physical connection between devices is represented by a 'cable' item. Packet Tracer supports an array of simulated Application Layer protocols, as well as basic routing with RIP, OSPF, EIGRP, BGP, to the extents required by the current CCNA curriculum. As of version 5.3, Packet Tracer also supports the Border Gateway Protocol.

In addition to simulating certain aspects of computer networks, Packet Tracer can also be used for collaboration. As of Packet Tracer 5.0, Packet Tracer supports a multi-user system that enables multiple users to connect multiple topologies together over a computer network. Packet Tracer also allows instructors to create activities that students have to complete. Packet Tracer is often used in educational settings as a learning aid. Cisco Systems claims that Packet Tracer is useful for network experimentation.

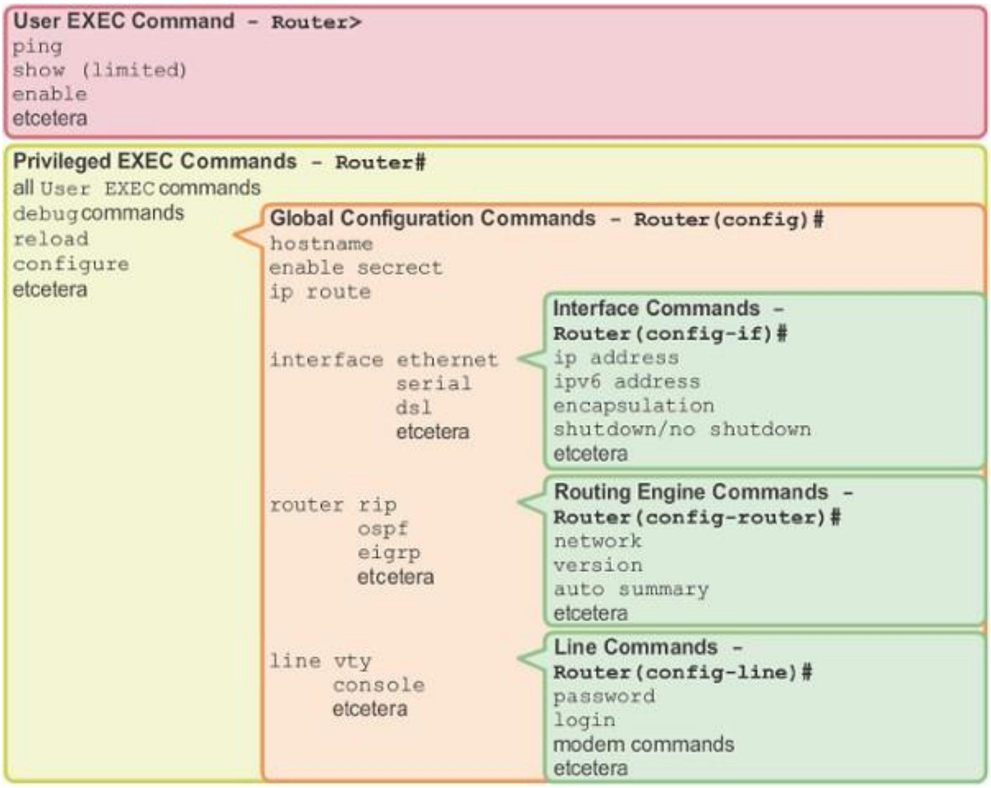
Packet Tracer allows students to design complex and large networks, which is often not feasible with physical hardware, due to costs. Packet Tracer is commonly used by CCNA Academy students, since it is available to them for free. However, due to functional limitations, it is intended by CISCO to be used only as a learning aid, not a replacement for Cisco routers and switches. The application itself only has a small number of features found within the actual hardware running a current Cisco IOS version. Thus, Packet Tracer is unsuitable for modelling production networks. It has a limited command set, meaning it is not possible to practice all of the IOS commands that might be required. Packet Tracer can be useful for understanding abstract networking concepts, such as the Enhanced Interior Gateway Routing Protocol by animating these elements in a visual form. Packet Tracer is also useful in education by providing additional components, including an authoring system, network protocol simulation and improving knowledge an assessment system.

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 of 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. In order to be able to configure the router, it is important to understand this hierarchy.

Fig 3.4 IOS Mode Hierarchical Structure



User EXEC Command - Router>
ping
show (limited)
enable
etcetera

Privileged EXEC Commands - Router#
all User EXEC commands
debug commands
reload
configure
etcetera

Global Configuration Commands - Router(config)#
hostname
enable secrect
ip route

interface ethernet
serial
dsl
etcetera

router rip
ospf
eigrp
etcetera

line vty
console
etcetera

Interface Commands - Router(config-if)#
ip address
ipv6 address
encapsulation
shutdown/no shutdown
etcetera

Routing Engine Commands - Router(config-router)#
network
version
auto summary
etcetera

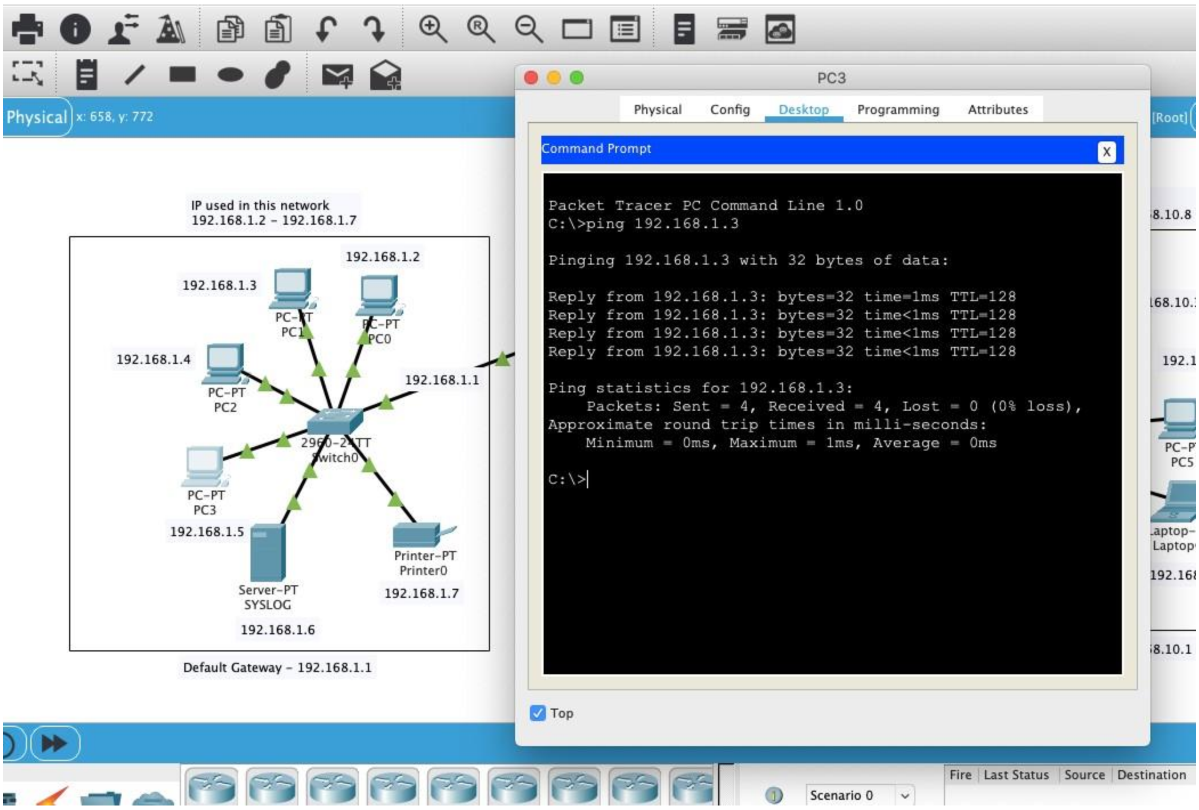
Line Commands - Router(config-line)#
password
login
modem commands
etcetera

Implementation

In this section we have gone through all the processes done in implementing the IDS successfully.

Configuring the Network

Placing the devices and connecting it with cables is not enough! We have to 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



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

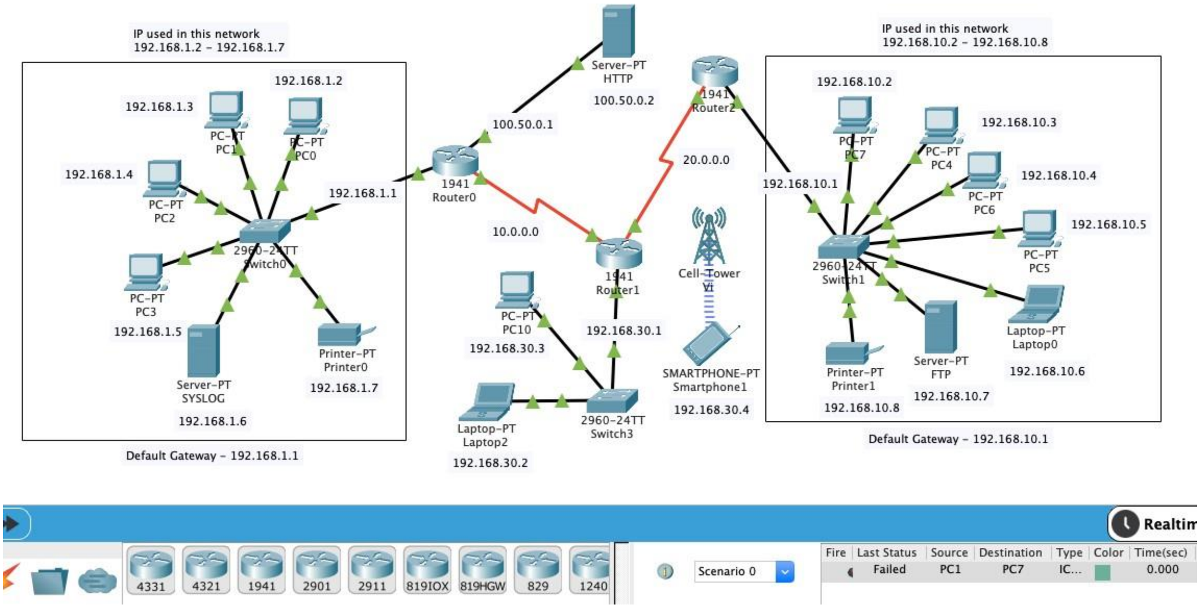
Fig 3.4 Ping test form PC3 to PC1

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

Ping test from PC3 to PC1 is successful.

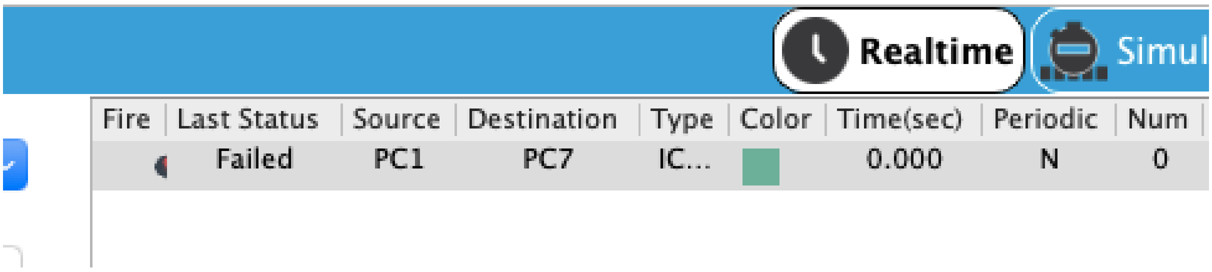
Let’s take another test of sending a ICMP packet from PC 3 to PC7 (other network) and check whether it successfully reached or not.

As you can see in Fig 3.5 & 3.6, it didn’t reached its destination.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)
	Failed	PC1	PC7	IC...	🟩	0.000

Fig 3.6 ICMP Packet Sent from PC3 to PC7



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Failed	PC1	PC7	IC...	🟩	0.000	N	0

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.

There are two types of routing.

- Static Routing
- Dynamic Routing

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 like 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

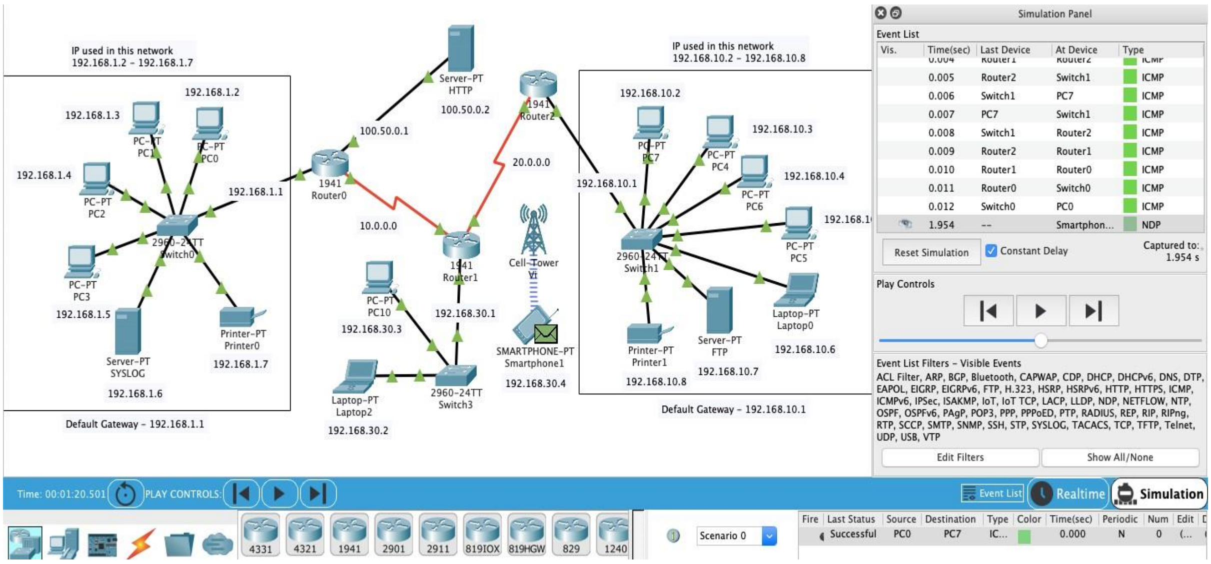
For configuring FTP same concept. Here I made a user called 'harsh' and password '123'

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.



Vis.	Time(sec)	Last Device	At Device	Type
	0.004	Router1	Router2	🟩 ICMP
	0.005	Router2	Switch1	🟩 ICMP
	0.006	Switch1	PC7	🟩 ICMP
	0.007	PC7	Switch1	🟩 ICMP
	0.008	Switch1	Router2	🟩 ICMP
	0.009	Router2	Router1	🟩 ICMP
	0.010	Router1	Router0	🟩 ICMP
	0.011	Router0	Switch0	🟩 ICMP
	0.012	Switch0	PC0	🟩 ICMP
	1.954	--	Smartphon...	NDP

Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	PC7	IC...	🟩	0.000	N	0	(...

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 have to apply IDS into this network for securing it.

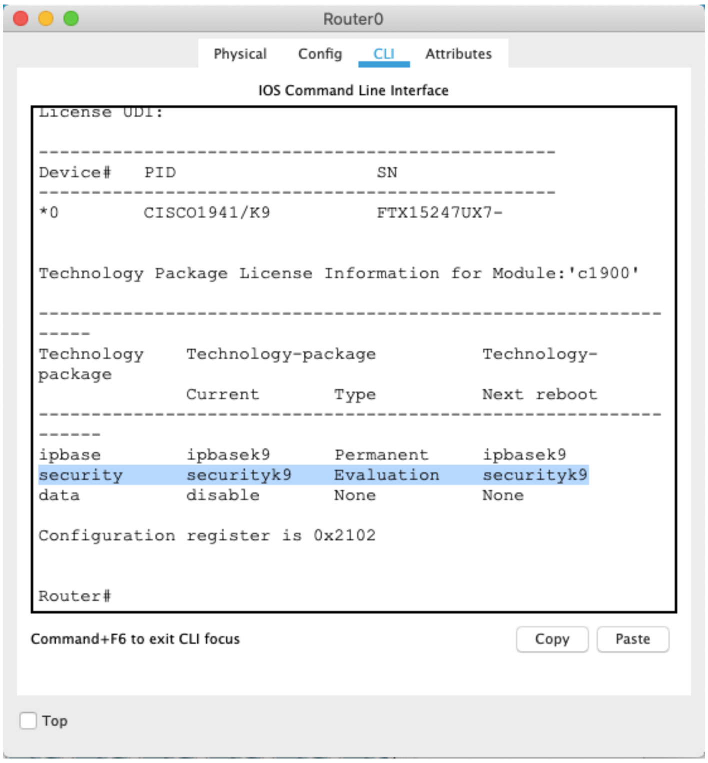
Our IDS will be implemented on Router0 on interface (gigabit ethernet 0/0). Our IDS will scan all the ICMP traffic which is coming into the Network 1 from this interface. For that we have used IPS Signature 2004

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 have to firstly activate security package of that router. We have activated ‘securityk9’ package as shown in Fig 3.8



```
License UDI:

-------------------------------------------------
Device#   PID                    SN
-------------------------------------------------
*0        CISCO1941/K9           FTX15247UX7-

Technology Package License Information for Module:'c1900'

-----------------------------------------------------------
-----
Technology    Technology-package           Technology-
package
              Current       Type           Next reboot
-----------------------------------------------------------
------
ipbase        ipbasek9      Permanent      ipbasek9
security      securityk9    Evaluation     securityk9
data          disable       None           None

Configuration register is 0x2102


Router#
```

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 make 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 into all the categories of IPS.
retired true	For retiring a category.
retired false	For unretiring a category.

category (name) basic	For entering into a category which we made earlier as IPS rule. And unretiring all the basic categories of this rule.
int (interface_name)	To enter into 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.

IDS Enabled & Protected Network

Network-based intrusion detection systems (NIDS) are devices intelligently distributed within networks that passively inspect traffic traversing the devices on which they sit. NIDS can be hardware or software-based systems and, depending on the manufacturer of the system, can attach to various network mediums such as Ethernet, FDDI, and others. Oftentimes, NIDS have two network interfaces. One is used for listening to network conversations in promiscuous mode and the other is used for control and reporting.

With the advent of switching, which isolates unicast conversations to ingress and egress switch ports, network infrastructure vendors have devised port-mirroring techniques to replicate all network traffic to the NIDS. There are other means of supplying traffic to the IDS such as network taps. Cisco uses Switched Port Analyzer (SPAN) functionality to facilitate this capability on their network devices and, in some network equipment, includes NIDS components directly within the switch. We’ll discuss Cisco’s IDS products in the next chapter.

While there are many NIDS vendors, all systems tend to function in one of two ways; NIDS are either signature-based or anomaly-based systems. Both are mechanisms that separate benign traffic from its malicious brethren. Potential issues with NIDS include high-speed network data overload, tuning difficulties, encryption, and signature development lag time. We’ll cover how IDS work and the difficulties involved with them later in this section.

Summary

An IDS is basically a software or device that is categorised into two common parts one is NID i.e. Network Intrusion Detection and second is HID. In this project I have implemented 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
Here are some ‘can’s and ‘can not’s 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 analyse 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.

The aim of this project was to build a security technique to secure a network for malicious activity. This project was a great learning opportunity for all of us as we come to know some new things which we don’t. There were many difficulties for us during the whole process but we didn’t lose hope and tried to complete this as soon as possible.

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
Devices in this network –

- 4 Different PCs
- 1 SYSLOG Server
- 1 Printer

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.
Packet Tracer can be run on Linux, Microsoft Windows, and macOS. Similar Android and iOS apps are also available. Packet Tracer allows users to create simulated network topologies by dragging and dropping routers, switches and various other types of network devices. A physical connection between devices is represented by a 'cable' item. Packet Tracer supports an array of simulated Application Layer protocols, as well as basic routing with RIP, OSPF, EIGRP, BGP, to the extents required by the current CCNA curriculum. As of version 5.3, Packet Tracer also supports the Border Gateway Protocol.

Just like this using ping and synack DDoS attack.

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, IP’s 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.

References

1. https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/#
2. http://neuro.bstu.by/ai/To-dom/My_research/Paper-0-again/For-research/D-mining/Anomaly-D/Intrusion-detection/taxonomy.pdf
3. https://books.google.com/books?id=TnE85sckwMAC&q=IDS+network+host+signature&pg=PA64
4. https://books.google.com/books?id=_R5ndK-i3vkC&q=%22intrusion+prevention+system%22+AND+%28reaction+OR+reactive%29&pg=PA266
5. https://books.google.com/books?id=ebbwmOFWvR8C&q=%22intrusion+prevention+system%22+AND+%22application+layer+firewall%22&pg=PA46