Experiment -10

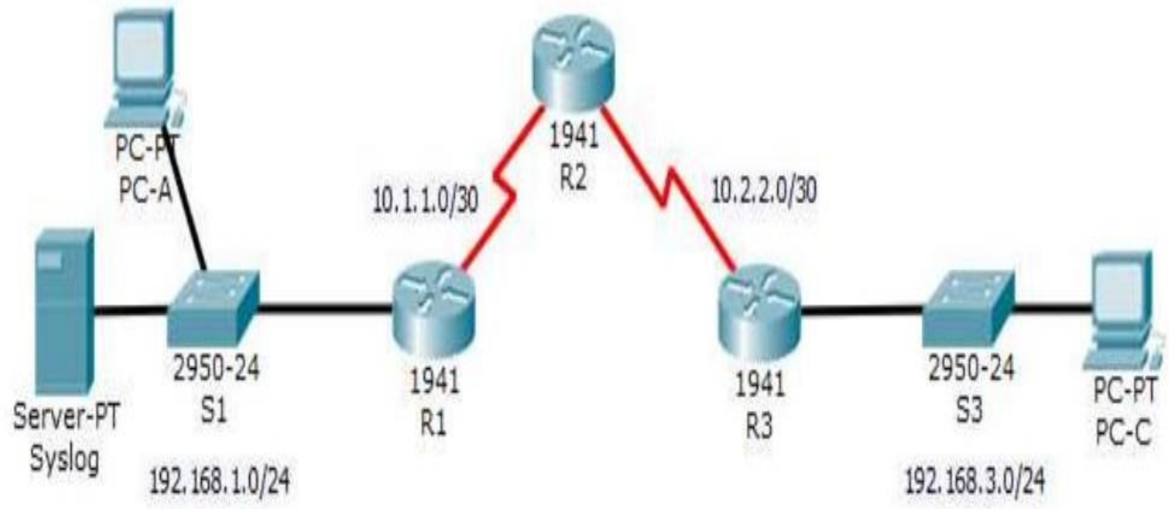
Demonstrate the intrusion detection system using any tool

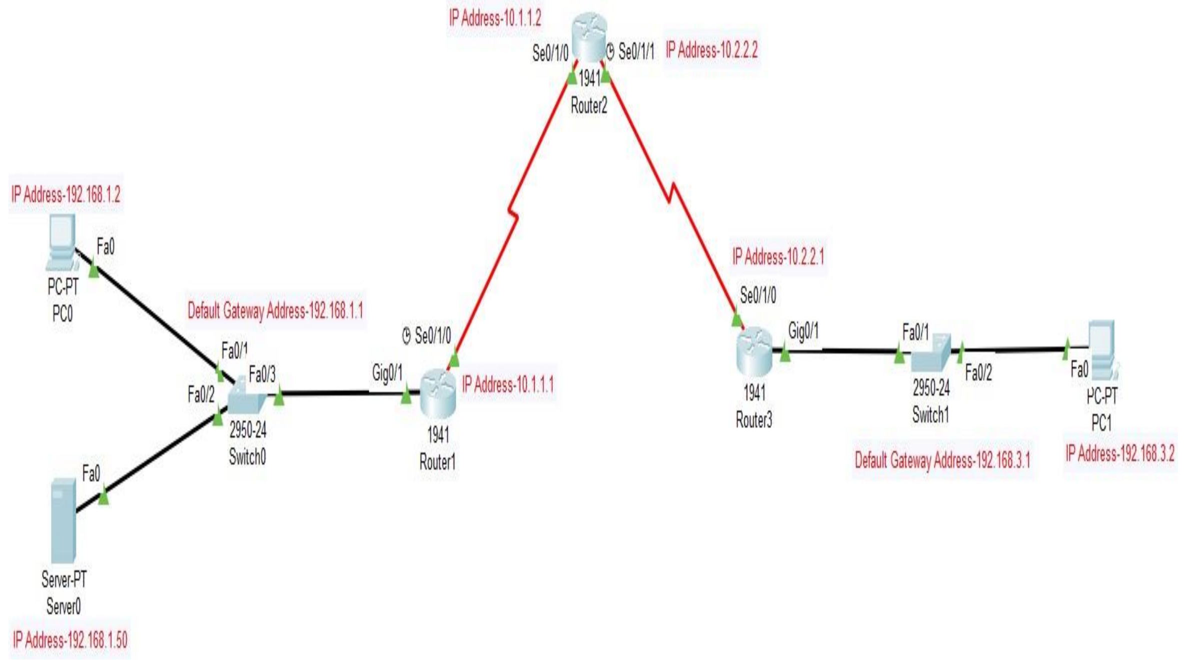
Aim:

To Configure the intrusion detection system using Cisco Packet Tracer.

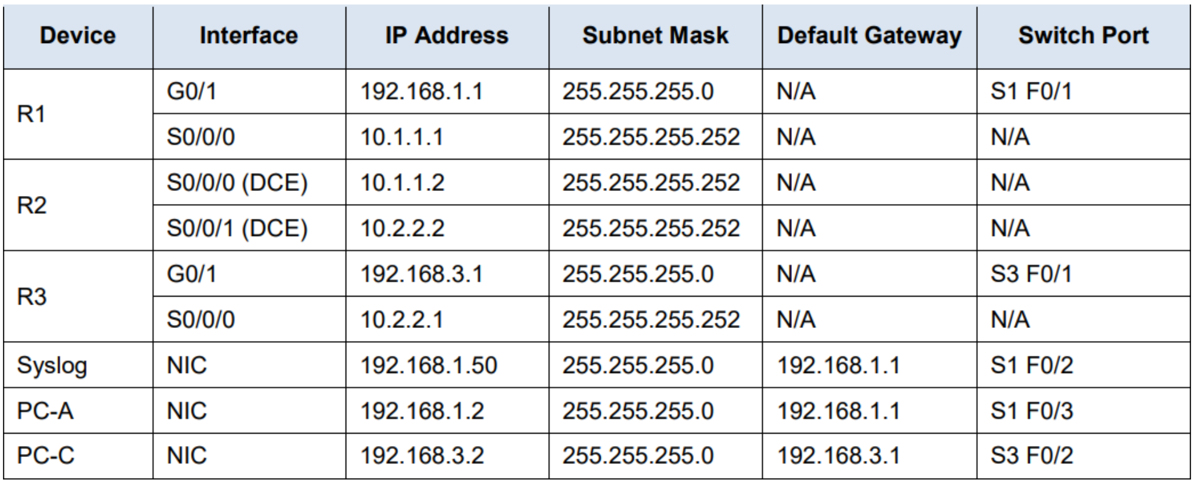
Procedure:

Network Topology





Addressing Table:



Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/1
	S0/0/0	10.2.2.1	255.255.255.252	N/A	N/A
Syslog	NIC	192.168.1.50	255.255.255.0	192.168.1.1	S1 F0/2
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1	S1 F0/3
PC-C	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 F0/2

Objectives:

- Enable IOS IPS.
- Configure logging.
- Modify an IPS signature.
- Verify IPS.

Background / Scenario

Your task is to enable IPS on R1 to scan traffic entering the 192.168.1.0 network.

The server labeled Syslog is used to log IPS messages. You must configure the router to identify the syslog

server to receive logging messages. Displaying the correct time and date in syslog messages is vital when

using syslog to monitor the network. Set the clock and configure the timestamp service for logging on the

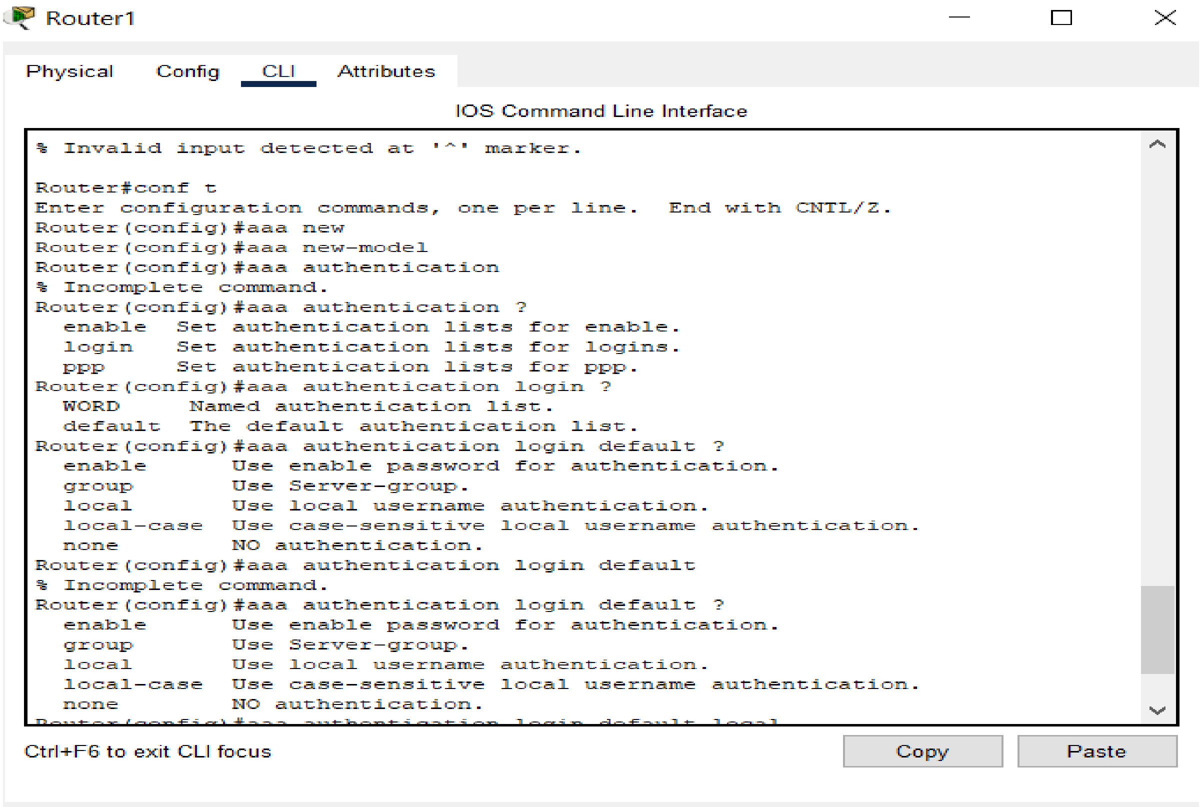
routers. Finally, enable IPS to produce an alert and drop ICMP echo reply packets inline.

The server and PCs have been preconfigured.

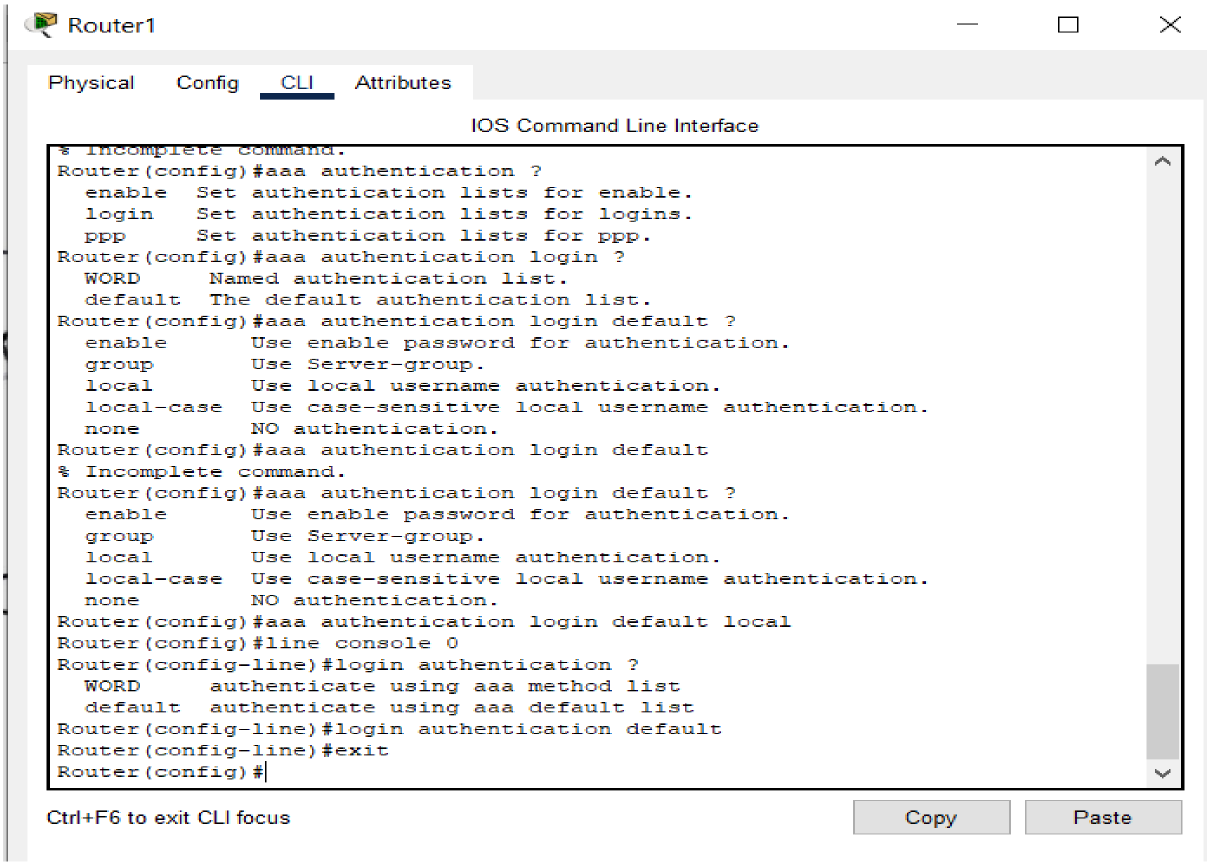
User Access Authentication

Step-1 Click on Router1

```
#enable

#conf t

#username xxxx secret yyyy

#aaa new

#aaa  new-model

#aaa authentication ?

#aaa authentication login ?

#aaa authentication login default ?

#aaa authentication login default local

#line console 0

#login authentication ?

#login authentication default

#exit
```



```
% Invalid input detected at '^' marker.

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#aaa new
Router(config)#aaa new-model
Router(config)#aaa authentication
% Incomplete command.
Router(config)#aaa authentication ?
  enable  Set authentication lists for enable.
  login   Set authentication lists for logins.
  ppp     Set authentication lists for ppp.
Router(config)#aaa authentication login ?
  WORD     Named authentication list.
  default  The default authentication list.
Router(config)#aaa authentication login default ?
  enable      Use enable password for authentication.
  group       Use Server-group.
  local       Use local username authentication.
  local-case  Use case-sensitive local username authentication.
  none        NO authentication.
Router(config)#aaa authentication login default
% Incomplete command.
Router(config)#aaa authentication login default ?
  enable      Use enable password for authentication.
  group       Use Server-group.
  local       Use local username authentication.
  local-case  Use case-sensitive local username authentication.
  none        NO authentication.
Router(config)#aaa authentication login default local
```



```
% Incomplete command.
Router(config)#aaa authentication ?
  enable  Set authentication lists for enable.
  login   Set authentication lists for logins.
  ppp     Set authentication lists for ppp.
Router(config)#aaa authentication login ?
  WORD     Named authentication list.
  default  The default authentication list.
Router(config)#aaa authentication login default ?
  enable      Use enable password for authentication.
  group       Use Server-group.
  local       Use local username authentication.
  local-case  Use case-sensitive local username authentication.
  none        NO authentication.
Router(config)#aaa authentication login default
% Incomplete command.
Router(config)#aaa authentication login default ?
  enable      Use enable password for authentication.
  group       Use Server-group.
  local       Use local username authentication.
  local-case  Use case-sensitive local username authentication.
  none        NO authentication.
Router(config)#aaa authentication login default local
Router(config)#line console 0
Router(config-line)#login authentication ?
  WORD     authenticate using aaa method list
  default  authenticate using aaa default list
Router(config-line)#login authentication default
Router(config-line)#exit
Router(config)#
```

****

Step-2 Click on Router1

```
#enable

#show version

#conf t

#license boot module c1900 technology-package securityk9

#yes

#end

#copy running startup

#reload
```

****

```
#enable

#show version
```

****

Step-3 Click on PC0 Ping PC1 IP address

Step-4 Click on PC1 ping PC0 IP address

****

Step-5 Click on R1

```
#mkdir ipsdir

(create directory filename() ?)

(create directory flash:ipsdir)

#conf t

#ip ips config location flash:ipsdir
```

```
#ip ips name iosips
#ip ips notify log
#exit
#clock set 19:25:59 9 July 2023
#conf t
#service timestamps log datetime msec
#logging host 192.168.1.50
#ip ips signature-category
#category all
#retired true
#exit
#category ios_ips basic
#retired false
#exit
#exit
Do you want to accept these changes? [Confirm]
#int g0/1
#ip ips iosips out
#ip ips signature-definition
#signature 2004 0
#status
#retired false
```

```
#enabled true
#exit
#engine
#event-action produce-alert
#event-action deny-packet-inline
#exit
#exit
#exit
[Confirm]
#end
#show ip ips all
```

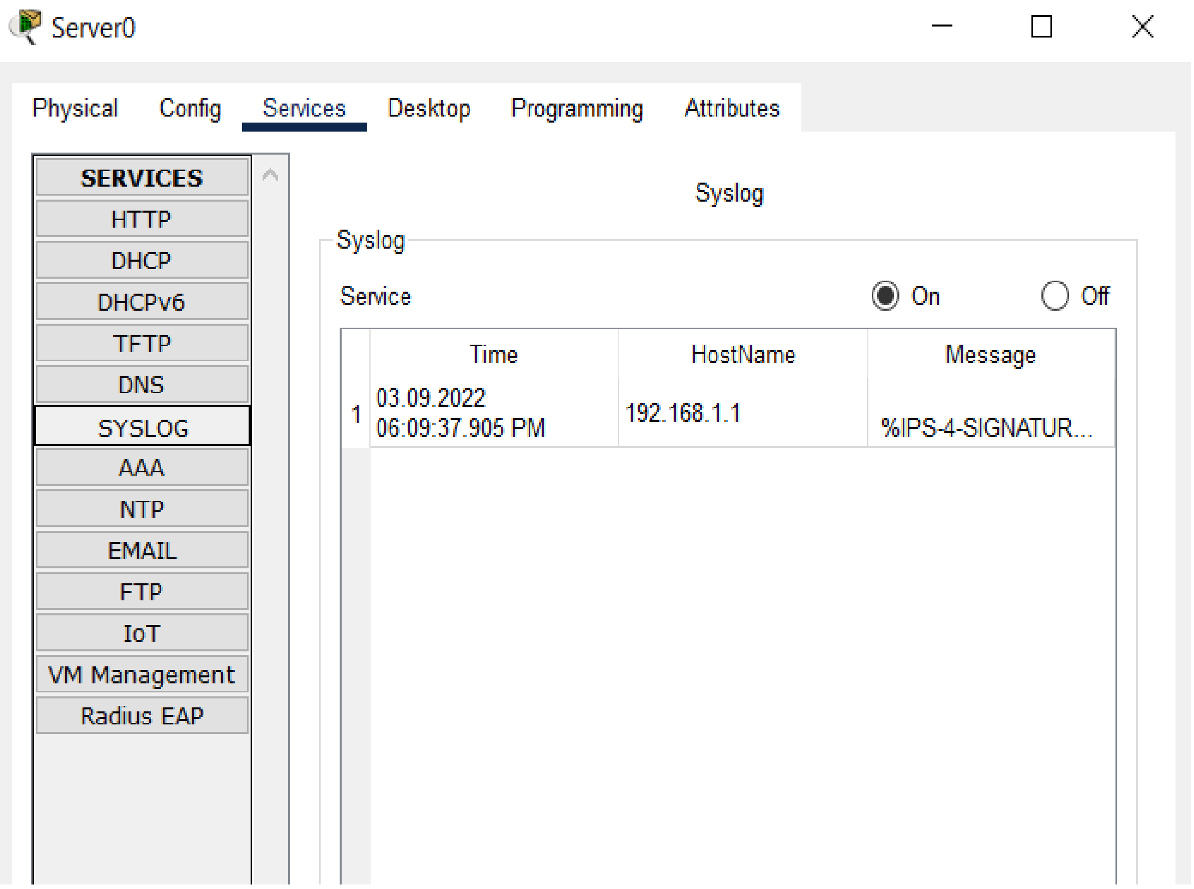
Step-6 Ping PC1

(Now, the request connection should be timeout the packets between the devices should deny the packets from the given IP address. This ping should fail. This PC2 the IPS rule for event-action of an echo request was set to deny-packet-inline.)

Step-7 Ping PC0

(Now, the request should be successful….)

Step-8 Check syslog (in server)



Syslog

Syslog

Service ● On ○ Off

	Time	HostName	Message
1	03.09.2022 06:09:37.905 PM	192.168.1.1	%IPS-4-SIGNATUR...

RESULT:

Thus intrusion detection system is configured using Cisco Packet Tracer has been successfully done and the output is verified.