COMPUTER COMMUNICATION NETWORK

MINI PROJECT

INTRUSION PREVENTION SYSTEM

BY

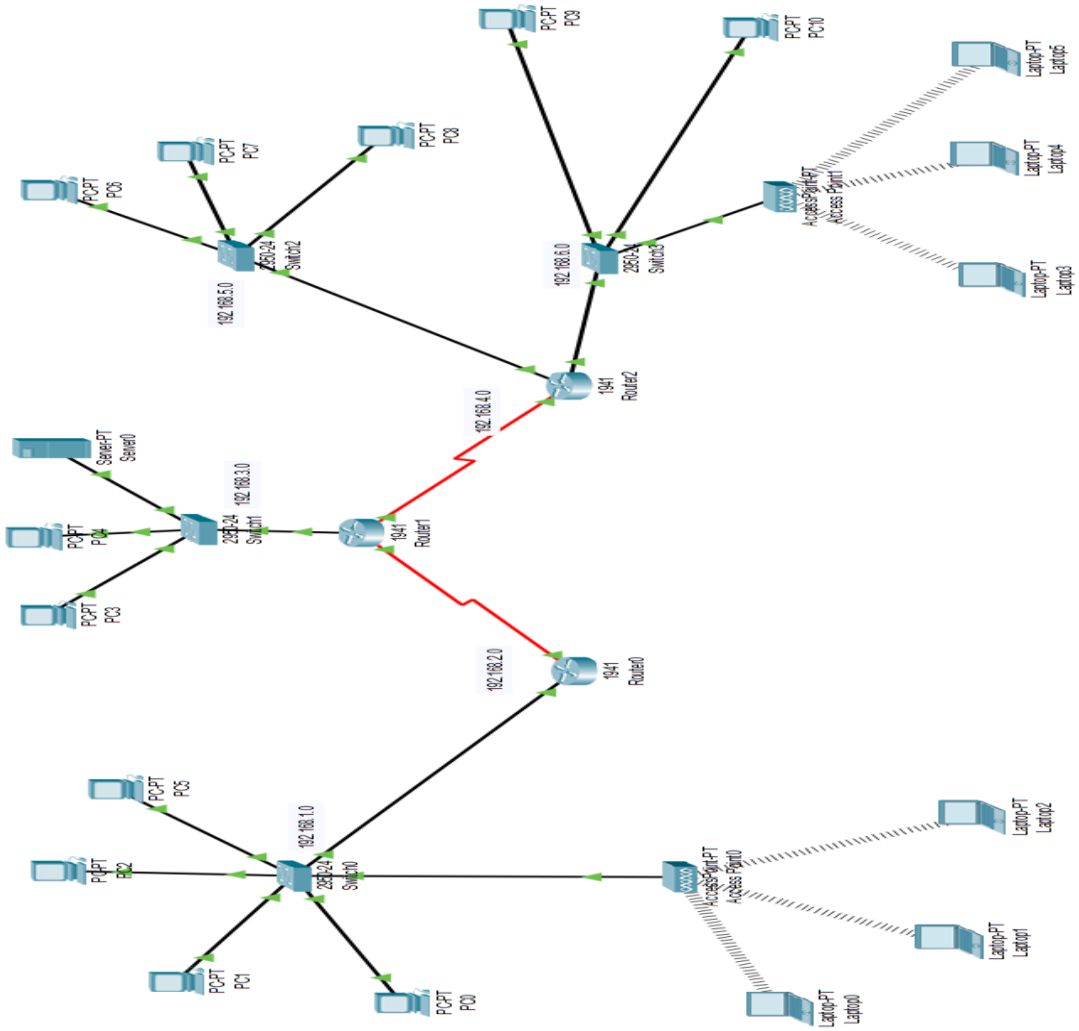
PARAMASIVAM S K (21BEC108)

VISHANTH S S (21BEC121)

AIM:

To create an intrusion prevention system (IPS) using cisco packet tracer to provide better security to the network by detecting and preventing potential Security breaches including intrusion attempts.

NETWORK:

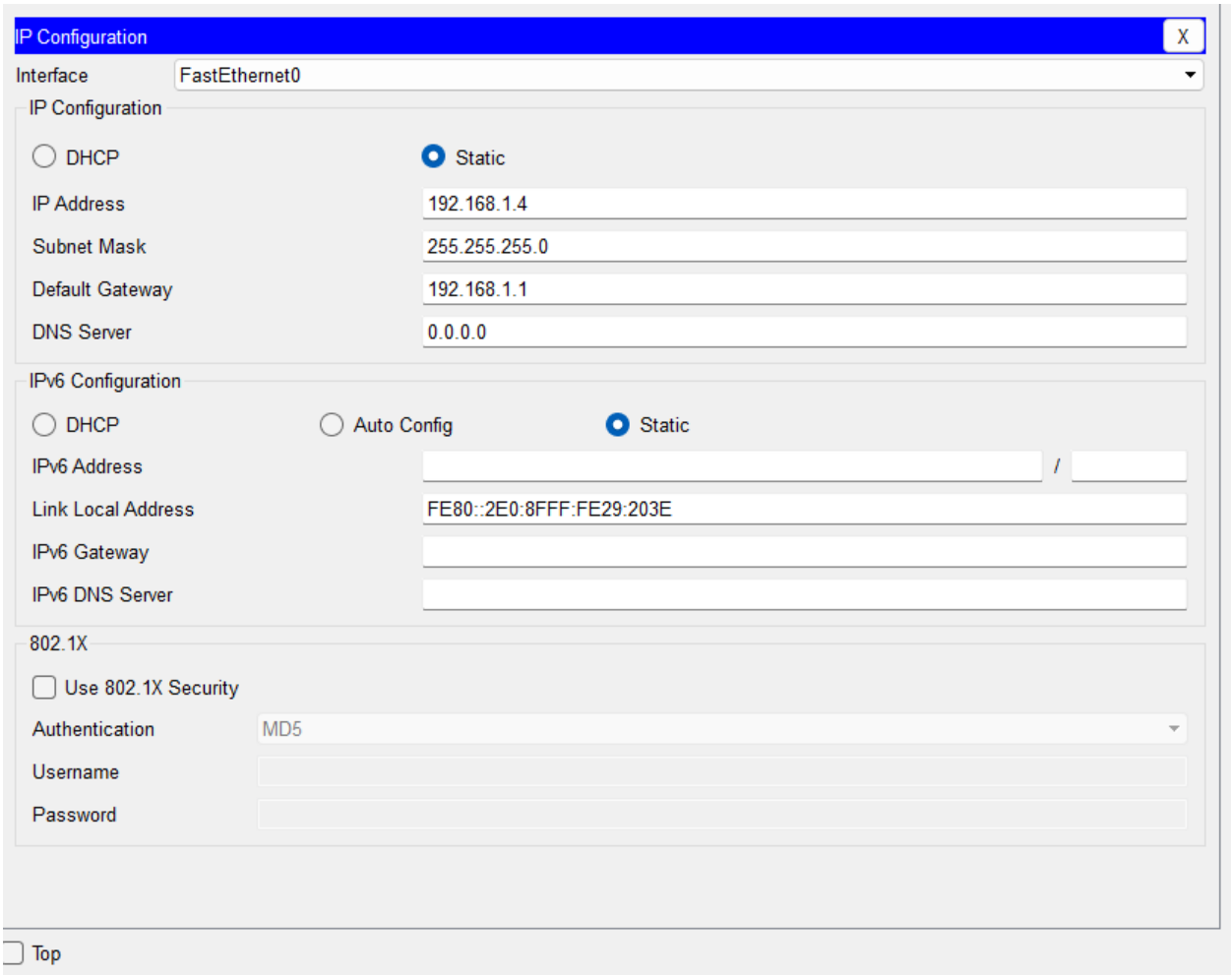


CONFIGURATION:

ROUTERS	NAMES	PC	IP ASSIGNED	NETMASK	DEFAULT GATEWAY
ROUTER1	SWITCH1	HOST-1	192.168.3.4	255.255.255.0	192.168.3.1
		HOST-2	192.168.3.5	255.255.255.0	192.168.3.1
		SERVER	192.168.3.50	255.255.255.0	192.168.3.1
ROUTER0	Switch0	client 1	192.168.1.7	255.255.255.0	192.168.1.1
		Client-2	192.168.1.6	255.255.255.0	192.168.1.1
		Client-3	192.168.1.5	255.255.255.0	192.168.1.1
		client 4	192.168.1.4	255.255.255.0	192.168.1.1
		client 5	192.168.1.8	255.255.255.0	192.168.1.1
		client 6	192.168.1.9	255.255.255.0	192.168.1.1
		client 7	192.168.1.10	255.255.255.0	192.168.1.1
ROUTER2	Switch3	client 8	192.168.6.8	255.255.255.0	192.168.6.1
		client 9	192.168.6.7	255.255.255.0	192.168.6.1
		client 10	192.168.6.6	255.255.255.0	192.168.6.1
		client 11	192.168.6.5	255.255.255.0	192.168.6.1
		client 12	192.168.6.4	255.255.255.0	192.168.6.1
	Switch2	client 13	192.168.5.6	255.255.255.0	192.168.5.1
		client 14	192.168.5.5	255.255.255.0	192.168.5.1
		client 15	192.168.5.4	255.255.255.0	192.168.5.1

COMMANDS:

- **Assigning IP address, Subnet Mask and Default Gateway for all the Client and Host PC'S.**



- Now we have enabled RIP (Routing Information Protocol) for automatic logging for all Routers.

```
Router(config)#router rip
Router(config-router)#netw 192.168.1.0

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Serial0/1/0
L 192.168.2.2/32 is directly connected, Serial0/1/0
R 192.168.3.0/24 [120/1] via 192.168.2.1, 00:00:18, Serial0/1/0
R 192.168.4.0/24 [120/1] via 192.168.2.1, 00:00:18, Serial0/1/0
```

R 192.168.5.0/24 [120/2] via 192.168.2.1, 00:00:18, Serial0/1/0
R 192.168.6.0/24 [120/2] via 192.168.2.1, 00:00:18, Serial0/1/0

- We have to install a server to monitor the login.
- Now, all the PC's can connect to other PC's.
- Now we have to install IPS in the host network router (router1)
- First we have to check the security status of the router1.

Technology Package License Information for Module:'c1900'

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

Configuration register is 0x2102

- We see that there is no security type assigned.
- We have to enable the security.

liscence boot module c1900 technology-package securityk9

do reload

- To install IPS in the router we have to create a Folder

Router#mkdir ipsdir
Create directory filename [ipsdir]?
Created dir flash:ipsdir

- Now we are going to configure the IPS signature location and ipsdir

Router(config)#ip ips config location ipsdir!

- Now we are going to create a ips rule.

Router(config)#ip ips name iosips

- Now we are going to retire all the ips signature.

Router#ip ips signature-category

- Retiring all unassigned categories in ips signature.

```
Router(config)#ip ips name ios
Router(config)#ip ips name iosips
Router(config)#ip ips signature-category
Router(config-ips-category)#?
  category  Category keyword
  exit      Exit from Category Mode
  no        Negate or set default values of a
command
Router(config-ips-category)#category all
Router(config-ips-category-action)#retired true
```

- Now we select our category ios_ips

```
Router(config-ips-category)#category ?
  all      All Categories
  ios_ips  IOS IPS (more sub-categories
Router(config-ips-category)#category ios_ips ?
  basic  Basic
Router(config-ips-category)#category ios_ips basic
Router(config-ips-category-action)#retired false
```

- Now all the rules is configured in our ips.
- We need to block the Out bound traffic on gigabitEthernet 0/0 in that we connected the switch.

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip ips iosips ?
  in   Inbound IPS
  out  Outbound IPS
Router(config-if)#ip ips iosips out
```

- Now we have to Log our alerts in HOST server

Router(config)#logging host 192.168.1.50
Router(config)#service timestamps log datatime msec

- Now let’s see ips signature definition.

```
Router(config)#ip ips signature-definition
Router(config-sigdef)#signature ?
  <1-65535>  Signature ID value
Router(config-sigdef)#signature 2004 ?
  <0-65535>  Signature SubID value
  <cr>
Router(config-sigdef)#signature 2004 0
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#?
  enabled  Enable Category Signatures
  exit     Exit from status submode
  no       Negate or set default values of a
command
  retired  Retire Category Signatures
Router(config-sigdef-sig-status)#retired fals
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#enable
Router(config-sigdef-sig-status)#enabled true
```

- Now let's enter into the engine to change the signature alert in the packet drop.

```
Router(config-sigdef-sig)#engine
Router(config-sigdef-sig-engine)#?
  event-action  Action
  exit          Exit from engine submode
  no            Negate or set default values of a
command
Router(config-sigdef-sig-engine)#event-act
Router(config-sigdef-sig-engine)#event-action ?
  deny-packet-inline  Deny Packet
  produce-alert       Produce Alert
Router(config-sigdef-sig-engine)#event-action
produc
Router(config-sigdef-sig-engine)#event-action
produce-alert
Router(config-sigdef-sig-engine)#event-action
deny-pac
Router(config-sigdef-sig-engine)#event-action
deny-packet-inline
```

- Now we have seen the signature is assigned.

do show ip ips all

```
IPS Signature Status
    Total Active Signatures: 1
    Total Inactive Signatures: 0
```

- It's over. Now we can ping OUTSIDE from inside but no one can connect from outside.

From HOST to Client:

Pinging 192.168.1.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.10: bytes=32 time=11ms TTL=126
Reply from 192.168.1.10: bytes=32 time=23ms TTL=126
Reply from 192.168.1.10: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.1.10:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),

Approximate round trip times in milli-seconds:
Minimum = 11ms, Maximum = 23ms, Average = 15ms

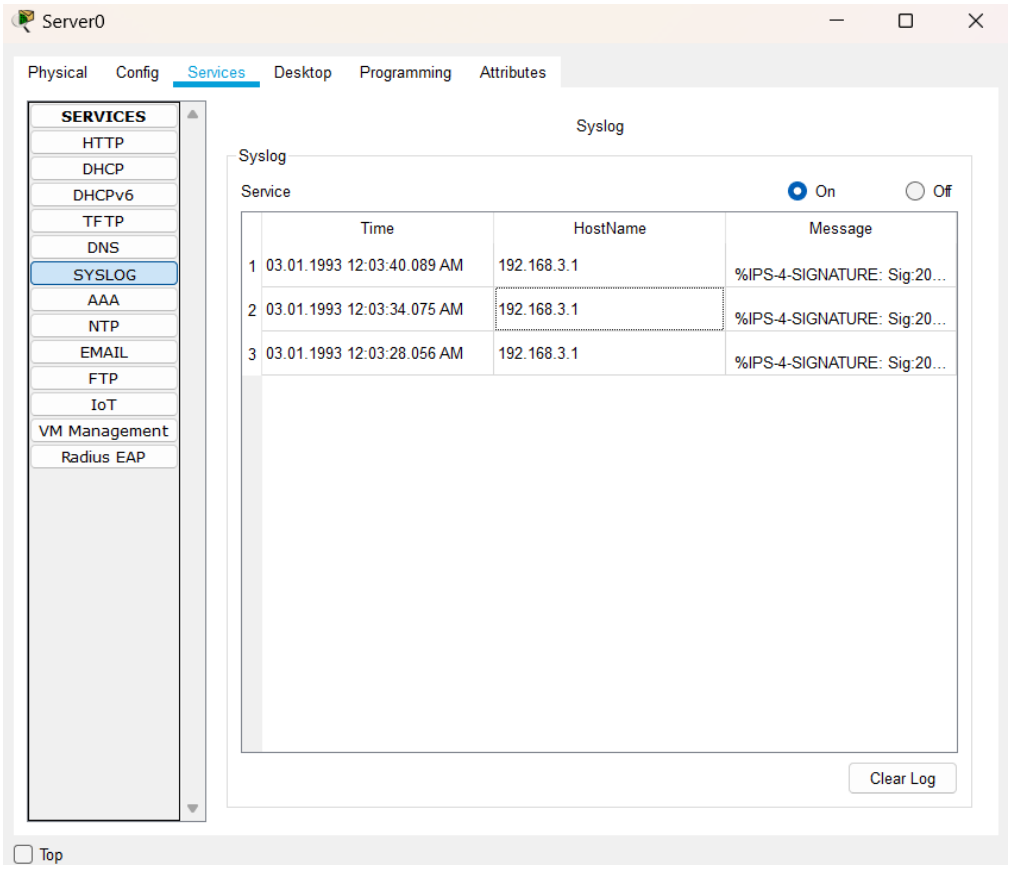
From Client to HOST:

Pinging 192.168.3.5 with 32 bytes of data:

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

Ping statistics for 192.168.3.5:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Alert from SYSLOG



OBJECTIVES:

- Implement an effective IPS solution using Cisco Packet Tracer.
- Monitor network traffic for suspicious patterns and behaviors.
- Detect and prevent potential security breaches, including intrusion attempts and malware infections.
- Enhance the overall security posture of the network infrastructure.

CONCLUSION:

- The Intrusion Prevention System (IPS) implemented using Cisco Packet Tracer represents a critical layer of defense in safeguarding the network against cyber threats. By continuously monitoring and analyzing network traffic, the IPS helps detect and prevent security breaches, thereby enhancing the overall security posture of the organization.