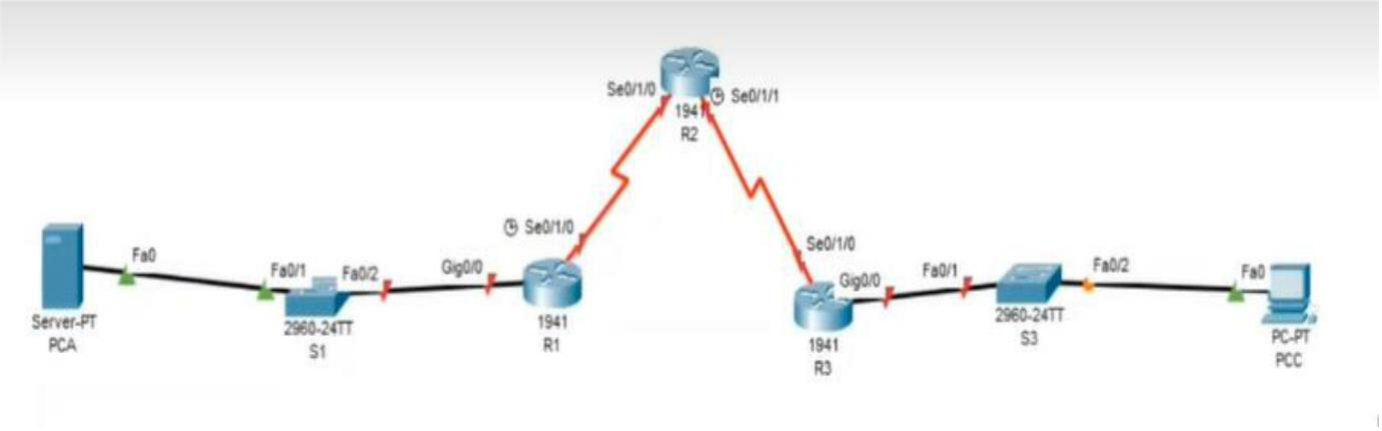
Security In Computing Practical

Practical 4: Configure IP ACLs to Mitigate Attacks

A]

Topology:



Addressing Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	gig0/0	192.168.1.1	255.255.255.0	N/A
	Se0/1/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	Se0/1/0	10.1.1.2	255.255.255.252	N/A
	Se0/1/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo0	192.168.2.1	255.255.255.0	N/A
R3	gig0/0	192.168.3.1	255.255.255.0	N/A
	Se0/1/0	10.2.2.1	255.255.255.252	N/A
PC-A	Fa0	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	Fa0	192.168.3.3	255.255.255.0	192.168.3.1

Objectives:

- Verify connectivity among devices before firewall configuration.
- Use ACLs to ensure remote access to the routers is available only from management station PC-C.
- Configure ACLs on R1 and R3 to mitigate attacks.
- Verify ACL functionality.

Configure Router:

Step 1: Configure secret on router

R(config) # enable secret enpa55

Step 2: Configure console password on router

R(config) # line console 0

R(config-line) #password conpa55

R(config-line) #login

Step 3: Configure SSH login on router

Execute command on all routers

R(config)# ip domain-name ccnasecurity.com

R(config)# username admin secret adminpa55

R(config)# line vty 0 4

R(config-line)# login local

R(config-line)# crypto key generate rsa

How many bits in the modulus [512]: 1024

Step 4: Configure loop back address on Router 2

R2(config)#int loopback 0

R2(config-if)#ip address 192.168.2.1 255.255.255.0

R2(config-if)# no shut

Step 5: Configure OSPF routing on routers

Part 2: Verify Basic Network Connectivity

Step 1: From PC-A, verify connectivity to PC-C and R2.

PCA> ping 192.168.3.3

(Successful)

PCA> ping 192.168.2.1

(Successful)

PCA> ssh –l admin 192.168.2.1

Password: adminpa55

R2>exit

Step 2: From PC-C, verify connectivity to PC-A and R2.

PCC> ping 192.168.1.3

(Successful)

PCC> ping 192.168.2.1

(Successful)

PCC> ssh –l admin 192.168.2.1

Password: adminpa55

R2>exit

Open a web browser to the PC-A server (192.168.1.3) to display the web page.

Close the browser when done.

Desktop->Web Browser->192.168.1.3

(Successful)

Part 3: Secure Access to Routers

Step 1: Configure ACL 10 to block all remote access to the routers except from PC-C

Execute command on all routers

R(config)# access-list 10 permit host 192.168.3.3

Step 2: Apply ACL 10 to ingress traffic on the VTY lines.

Execute command on all routers

R(config)# line vty 0 4

R(config-line)# access-class 10 in

Step 3: Verify exclusive access from management station PC-C.

PCC> ssh –l admin 192.168.2.1

Password: adminpa55

R2>exit

Step 4: Verify denial from PC-A.

PCA> ssh –l admin 192.168.2.1

Connection refused by remote host

Part 4: Create a Numbered IP ACL 120 on R1

Step 1: Verify that PC-C can access the PC-A via HTTPS using the web browser.

Be sure to disable HTTP and enable HTTPS on server PC-A in Services tab.

Step 2: Configure ACL 120 to specifically permit and deny the specified traffic.

R1(config)# access-list 120 permit udp any host 192.168.1.3 eq domain

R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq smtp

R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq ftp

R1(config)# access-list 120 deny tcp any host 192.168.1.3 eq 443

R1(config)# access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22

Step 3: Apply the ACL to interface

R1(config)# int se0/1/0

R1(config-if)# ip access-group 120 in

Step 4: Verify that PC-C cannot access PC-A via HTTPS using the web browse.

Desktop->Web Browser->192.168.1.3

(Unsuccessful) Request timed out

Part 5: Modify an Existing ACL on R1

Step 1: Verify that PC-A cannot successfully ping the loopback interface on R2.

PCA> ping 192.168.2.1

(Unsuccessful) Request timed out

Step 2: Make any necessary changes to ACL 120 to permit and deny the specified traffic.

R1(config)# access-list 120 permit icmp any any echo-reply

R1(config)# access-list 120 permit icmp any any unreachable

R1(config)# access-list 120 deny icmp any any

R1(config)# access-list 120 permit ip any any

Step 3: Verify that PC-A can successfully ping the loopback interface on R2.

PCA> ping 192.168.2.1 (Successful)

Part 6: Create a Numbered IP ACL 110 on R3

Step 1: Configure ACL 110 to permit only traffic from the inside network.

R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 any

Step 2: Apply the ACL to interface

R3(config)# int gig0/1

R3(config-if)# ip access-group 110 in

Part 7: Create a Numbered IP ACL 100 on R3

Step 1: Configure ACL 100 to block all specified traffic from the outside network.

R3(config)# access-list 100 permit tcp 10.0.0.0 0.255.255.255 host 192.168.3.3 eq 22

R3(config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any

R3(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any

R3(config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any

R3(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any

R3(config)# access-list 100 deny ip 224.0.0.0 15.255.255.255 any

R3(config)# access-list 100 permit ip any any

Step 2: Apply the ACL to interface

R3(config)# interface se0/1/0

R3(config-if)# ip access-group 100 in

Step 3: Confirm that the specified traffic entering interface Serial is handled correctly.

PCC> ping 192.168.1.3

(Unsuccessful)

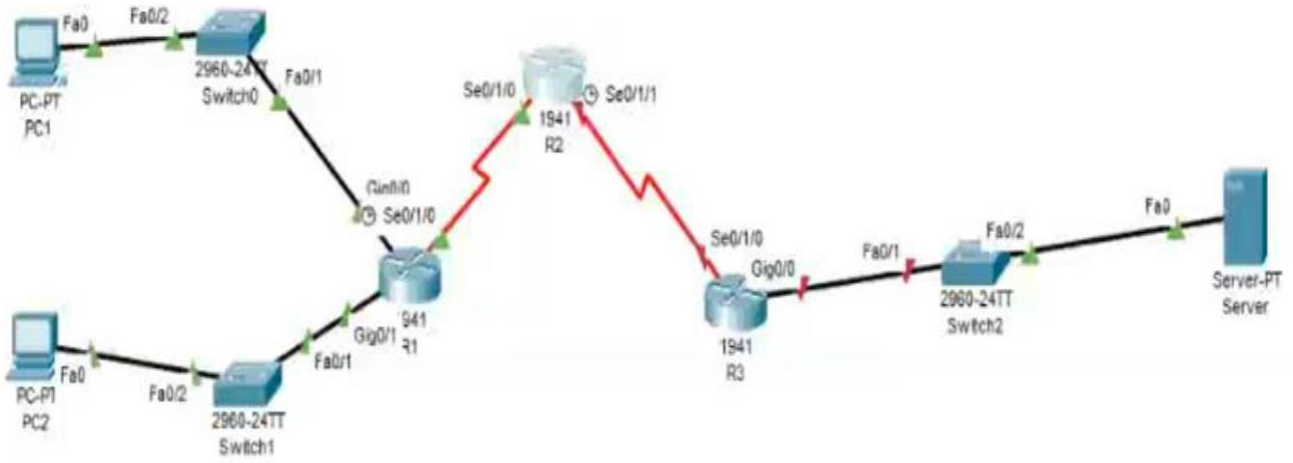
PCC> ssh –l admin 192.168.2.1

Password: adminpa55

R2>exit

B]

Topology:



Addressing Table:

Device	Interface	IPv6 Address/Prefix	Default Gateway
PC1	NIC	2001:DB8:1:10::10/64	FE80::1
PC2	NIC	2001:DB8:1:11:11/64	FE80::1
R1	gig0/0	2001:DB8:1:10::1/64	FE80::1
	se0/1/0	2001:DB8:1:1::1/64	FE80::1
	gig0/1	2001:DB8:1:11::1/64	FE80::1
R3	se0/1/0	2001:DB8:1:1::2/64	FE80::2
	se0/1/1	2001:DB8:1:2::2/64	FE80::2
R3	gig0/0	2001:DB8:1:30::1/64	FE80::3
	se0/1/0	2001:DB8:1:2::1/64	FE80::3
Server	NIC	2001:DB8:1:30::30/64	FE80::3

Objective:

- Configure, Apply, and Verify an IPv6 ACL
- Configure, Apply, and Verify a Second IPv6 ACL

Configure Router:

Step 1: Configure secret on router

Execute command on all routers

R(config)# enable secret enpa55

Step 2: Assign static ipv6 address

R1(config)# int gig0/0

R1(config-if)# ipv6 address 2001:DB8:1:10::1/64

R1(config-if)# ipv6 address FE80::1 link-local

R1(config-if)# no shut

R1(config)# int gig0/1

R1(config-if)# ipv6 address 2001:DB8:1:11::1/64

R1(config-if)# ipv6 address FE80::1 link-local

R1(config-if)# no shut

R1(config)# int se0/1/0

R1(config-if)# ipv6 address 2001:DB8:1:1::1/64

R1(config-if)# ipv6 address FE80::1 link-local

R1(config-if)# no shut

R2(config)# int se0/1/0

R2(config-if)# ipv6 address 2001:DB8:1:1::2/64

R2(config-if)# ipv6 address FE80::2 link-local

R2(config-if)# no shut

R2(config)# int se0/1/1

R2(config-if)# ipv6 address 2001:DB8:1:2::2/64

R2(config-if)# ipv6 address FE80::2 link-local

R2(config-if)# no shut

R3(config)# int gig0/0

R3(config-if)# ipv6 address 2001:DB8:1:30::1/64

R3(config-if)# ipv6 address FE80::3 link-local

R3(config-if)# no shut

R3(config)# int se0/1/0

R3(config-if)# ipv6 address 2001:DB8:1:2::1/64

R3(config-if)# ipv6 address FE80::3 link-local

R3(config-if)# no shut

Step 3: Enable IPv6 routing

R1(config)# ipv6 unicast-routing

R1(config)# ipv6 route 2001:DB8:1:2::0/64 2001:DB8:1:1::2

R1(config)# ipv6 route 2001:DB8:1:30::0/64 2001:DB8:1:1::2

R2(config)# ipv6 unicast-routing

R2(config)# ipv6 route 2001:DB8:1:10::0/64 2001:DB8:1:1::1

R2(config)# ipv6 route 2001:DB8:1:11::0/64 2001:DB8:1:1::1

R2(config)# ipv6 route 2001:DB8:1:30::0/64 2001:DB8:1:2::1

R3(config)# ipv6 unicast-routing

R3(config)# ipv6 route 2001:DB8:1:10::0/64 2001:DB8:1:2::2

R3(config)# ipv6 route 2001:DB8:1:11::0/64 2001:DB8:1:2::2

R3(config)# ipv6 route 2001:DB8:1:1::0/64 2001:DB8:1:2::2

Step 4: Verify connectivity

PC1> ping 2001:DB8:1:30::30

(Successful)

PC2> ping 2001:DB8:1:30::30

(Successful)

Part 2: Configure, Apply, and Verify an IPv6 ACL

Step 1: Configure an ACL that will block HTTP and HTTPS access.

R1(config)# ipv6 access-list BLOCK_HTTP R1(config-ipv6-acl)# deny tcp any host 2001:DB8:1:30::30 eq www R1(config-ipv6-acl)# deny tcp any host 2001:DB8:1:30::30 eq 443 R1(config-ipv6-acl)# permit ipv6 any any R1(config-ipv6-acl)# exit

Step 2: Apply the ACL to the correct interface.

R1(config)# int gig0/1

R1(config-if)# ipv6 traffic-filter BLOCK_HTTP in

Step 3: Verify the ACL implementation

Open a web browser to the PC1 to display the web page.

Desktop->Web Browser->http://2001:DB8:1:30::30

(Successful)

Desktop->Web Browser->https://2001:DB8:1:30::30

(Successful)

Open a web browser to the PC2 to display the web page.

Desktop->Web Browser->http://2001:DB8:1:30::30

(Unsuccessful) – Request Timeout

Desktop->Web Browser->https://2001:DB8:1:30::30

(Unsuccessful) – Request Timeout PC2> ping

2001:DB8:1:30::30

(Successful)

Part 3: Configure, Apply, and Verify a Second IPv6 ACL

Step 1: Create an access list to block ICMP.

R3(config)# ipv6 access-list BLOCK_ICMP
R3(config-ipv6-acl)# deny icmp any any R3(config-
ipv6-acl)# permit ipv6 any any R3(config-ipv6-acl)#
exit

Step 2: Apply the ACL to the correct interface.

R3(config)# int gig0/0
R3(config-if)# ipv6 traffic-filter BLOCK_ICMP out

Step 3: Verify that the proper access list functions.

PC2> ping 2001:DB8:1:30::30 (Unsuccessful) -
Destination host unreachable PC1> ping
2001:DB8:1:30::30 (Unsuccessful) - Destination host
unreachable

Open a web browser to the PC1 to display the web page.
Desktop->Web Browser->http://2001:DB8:1:30::30
(Successful)
Desktop->Web Browser->https://2001:DB8:1:30::30
(Successful)