Practical 4

- Configure IP ACLs to mitigate attacks.

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 F0/5
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
	Lo0	192.168.2.1	255.255.255.0	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Part 1 - Verify Basic Network Connectivity

Step 1 - From PC-A, verify connectivity to PC-C

PC> ping 192.168.3.3

Step 2 - From PC-A, PC, verify SSH on R2 (Lo0)

PC-A > ssh -l SSHadmin 192.168.2.1
PC-C > ssh -l SSHadmin 192.168.2.1

Step 3 - From PC-A's web browser access 192.168.1.3 to display the web page.

Part 2 - Secure Access to Routers

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

R1(config)# access-list 10 permit host 192.168.3.3
R2(config)# access-list 10 permit host 192.168.3.3
R3(config)# access-list 10 permit host 192.168.3.3

Step 2 - Apply ACL 10 to ingress traffic on the vty lines.

R1(config)# line vty 0 4
R1(config-line)# access-class 10 in

R2(config)# line vty 0 4
R2(config-line)# access-class 10 in

R3(config)# line vty 0 4
R3(config-line)# access-class 10 in

Step 3 - Verify exclusive access from PC-C

PC> ssh -l SSHadmin 192.168.2.1
should be success

From PC-A
PC> ssh -l SSHadmin 192.168.2.1
should be fail.

Part 3 - Create a Numbered IP ACL 120 on R1

Step 1 - Enable HTTPS and Disable HTTP on PC-A

Step 2 - Configure ACL 120 to specifically permit & deny the specific traffic

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 domain
R1(config)# access list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)# access list 120 permit tcp any host 192.168.1.3 eq 443
R1(config)# access list 120 permit tcp host 192.168.1.3 host 10.1.1.1 eq 22

Step 3 - Apply the ACL to correct interface

R1(config)# interface s0/0/0
R1(config-if)# ip access-group 120 in

Step 4 - Verify that PC-C Command access PC-A via HTTPS using web browser.

Part 4 - Verify that PC-A cannot successfully ping the loopback interface on R2

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

PC > ping 192.168.2.1

Step 2 - Make necessary changes to ACL 120 to permit and deny 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 permit 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

PC > ping 192.168.2.1

Part 5- Create a numbered IP ACL 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 G0/1

R3(config)# interface g 0/1
R3(config)# ip access-group 110 in

Part 6 - Create a numbered IP ACL 100 on 23.

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

23(config)# access-list 100 permit tcp 10.0.0.0 0.255.255.255 eq 22 host 192.168.3.3
23(config)# access list 100 deny ip 10.00.0 0.255.255.255 eq any
23(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any eq any
23(config)# access-list 100 deny ip 192.168.0.0 0.255.255.255 any.
23(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any
23(config)# access list 100 deny ip 224.0.0.0 15.255.255.255 any
23(config)# access-list 100 permit ip any any

Step 2 - Apply the ACL to interface S0/0/1

23(config)# interface S0/0/1
23(config-if)# ip access-group 100 in

Step 3 - Verify the ACL implementation From PC-C
PC> ping 192.168.1.3 # should be fail
PC> ping 192.168.3.1 # Should be success.

Step 4 - Establish SSH to 192.168.2.1 from PC-C
PC> ssh -l sshadmin 192.168.2.1 # should be success.