Practical 4: Configure IP ACLs to Mitigate Attacks and IPV6 ACLs.

1. Go to R1>CLI>Write following command.

Commands:

1. en
2. conf t
3. ip route 192.168.0.0 255.255.255.0 10.10.10.2

PCA And PC C 🡪cmd 🡪ping 10.10.10.2

1. R1 CLI>

type do show run command

Commands:

1. enable secret enpa55
2. line console 0
3. password conpa55
4. login
5. exit
6. ip domain-name ccnasecurity.com
7. username admin secret adminpa55
8. line vty 0 4
9. login local
10. exit
11. crypto key generate rsa
12. access-list 1 permit 192.168.0.2 0.0.0.0
13. access-list 1 deny any

3. Go to PCC > Command Prompt > ssh -1 admin 192.168.0.1 and write password as adminpa55. Do the same from PCA.

4. Go to R1>CLI

Commands:

1. line vty 0 4
2. access-class 1 in
3. access-list 120 permit tcp host 192.168.0.3 host 10.10.10.2 eq ftp
4. access-list 120 permit tcp host 192.168.0.3 host 10.10.10.2 eq www
5. access-list 120 permit tcp host 192.168.0.2 host 10.10.10.2 eq 22
6. int gi 0/0/0
7. ip access-group 120 in
8. Go to PCA>Command prompt> ftp 10.10.10.2 uname $pass cisco
9. Go to PCA>Web Browser> <https://10.10.10.2>
10. Go to R1

access-list 120 permit icmp any any

access-list 120 permit tcp host 192.168.0.2 host 192.168.0.1 eq 22

1. Go to R1>CLI>write command do show run and access-list 120 permit tcp host 192.168.0.2 host 192.168.0.1 eq 22.
2. Go to PCC> ftp 10.10.10.2
3. Go to PCA> ssh -l admin 192.168.0.1 and after that write ftp 10.10.10.2.
4. Go to R1>CLI

Commands:

1. en
2. conf t
3. interface gigabitEthernet 0/0/0
4. ipv6 address 2001:DB8:1:10::1/64
5. ipv6 address FE80::1 link-local
6. ex
7. interface gigabitEthernet 0/0/1
8. ipv6 address 2001:DB8:1:30::1/64
9. ipv6 address FE80::30 link-local
10. ipv6 unicast-routing
11. ipv6 route 2001:DB8:1:10::1/64 2001:DB8:1:30::30
12. Go to PCC>Web browser>https:// 2001:DB8:1:30::30 ipv6 address. Do the same with PCA and it should open in both
13. Go to R1>CLI>Write following commands.

Commands:

1. ipv6 access-list HTTP
2. permit tcp host 2001:DB8:1:10::9 host 2001:DB8:1:30::30 eq www
3. permit tcp host 2001:DB8:1:10::9 host 2001:DB8:1:30::30 eq 443
4. ex
5. interface G0/0/0
6. ipv6 traffic-filter HTTP in
7. Go to PC-A>Web browser> https://2001:DB8:1:30::30

15. Now Go to PC-C>Web browser>Enter 2001:DB8:1:30::30> It should not open.