**Aim:** **Configure IP ACLs to Mitigate Attacks.**

**Part 1: Configure Router:**

1. **Step 1: Configure secret on router**

R(config) # **enable secret enpa55**

1. **Step 2: Configure console password on router**

R(config) # **line console 0**

R(config-line) #**password conpa55**

R(config-line) #l**ogin**

1. **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**

1. **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**

1. **Step 5: Configure static routing on routers Execute command on all routers**

R1(config)#**ip route 192.168.3.0 255.255.255.0 10.1.1.2**

R1(config)#**ip route 10.2.2.0 255.255.255.252 10.1.1.2**

R1(config)#**ip route 192.168.2.0 255.255.255.0 10.1.1.2**

R2(config)#**ip route 192.168.1.0 255.255.255.0 10.1.1.1**

R2(config)#**ip route 192.168.3.0 255.255.255.0 10.2.2.1**

R3(config)#**ip route 192.168.1.0 255.255.255.0 10.2.2.2**

R3(config)#**ip route 192.168.2.0 255.255.255.0 10.2.2.2**

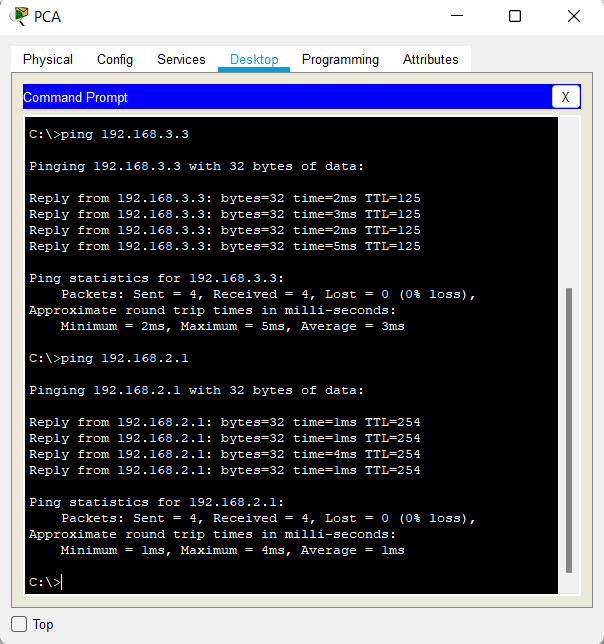
R3(config)#**ip route 10.1.1.0 255.255.255.0 10.2.2.2**

**Part 2: Verify Basic Network Connectivity:**

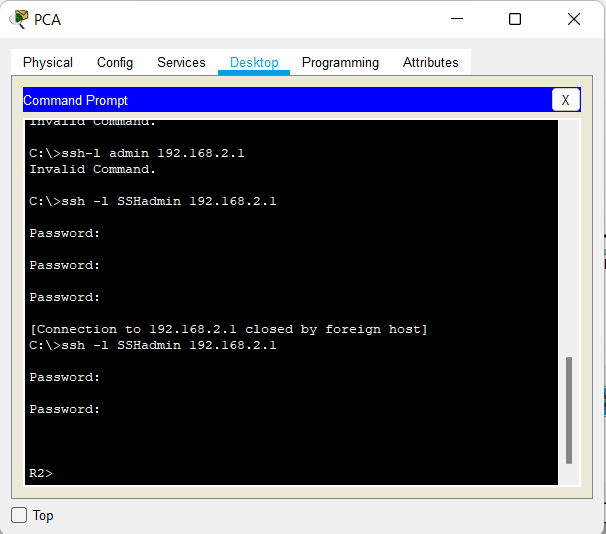
1. **Step 1: From PC-A, verify connectivity to PC-C and R2**

PCA> **ping 192.168.3.3 (Successful)**

PCA> **ping 192.168.2.1 (Successful)**



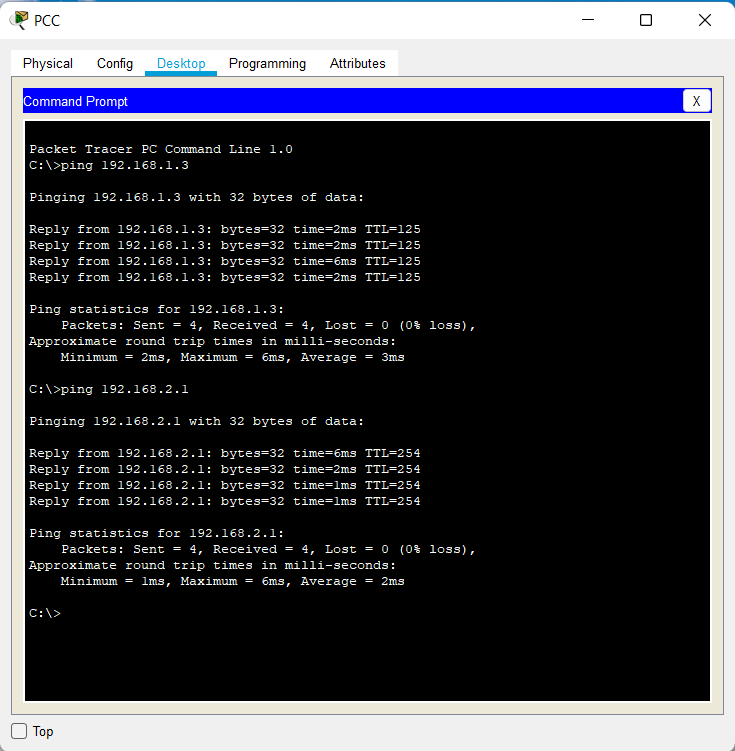
PCA> **ssh –l admin 192.168.2.1** (Password: adminpa55)



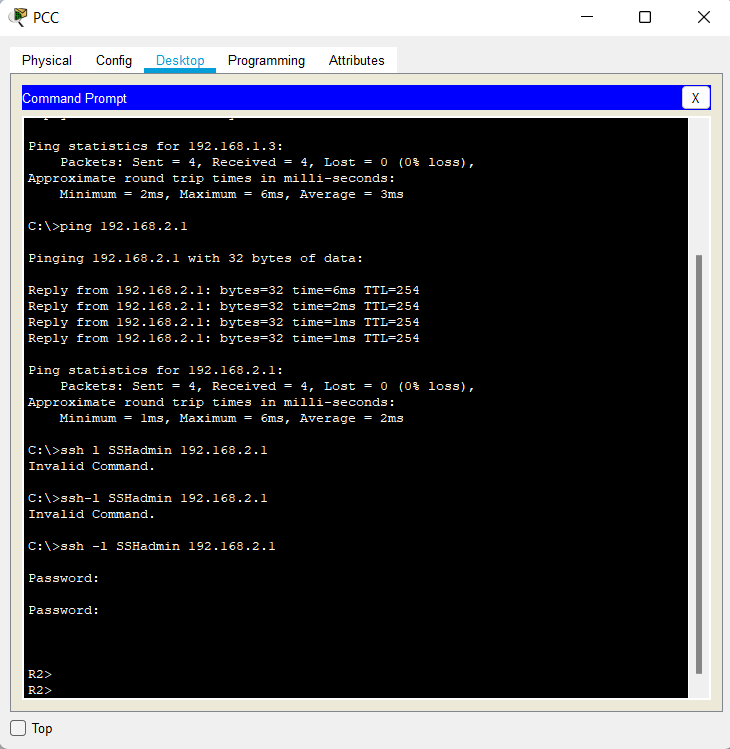
1. **Step 2: From PC-C, verify connectivity to PC-A and R2.**

PCC> **ping 192.168.1.3 (Successful)**

PCC> **ping 192.168.2.1 (Successful)**

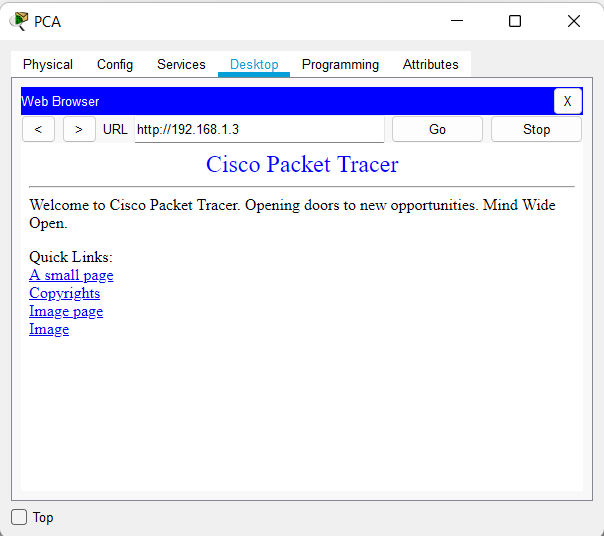


PCC> **ssh –l admin 192.168.2.1 (**Password: adminpa55)



1. 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**:

1. **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**

1. **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**

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

PCC> **ssh –l admin 192.168.2.1** (Password: adminpa55)

R2>**exit**

1. **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**:

1. **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.

1. **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**

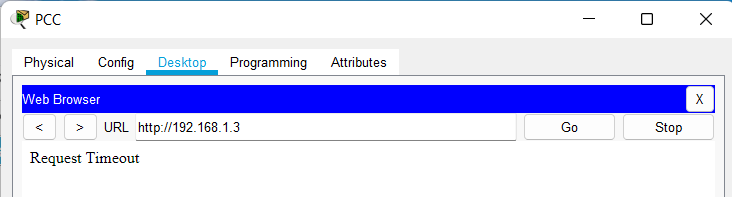
1. **Step 3: Apply the ACL to interface**

R1(config)# **int se0/1/0**

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

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

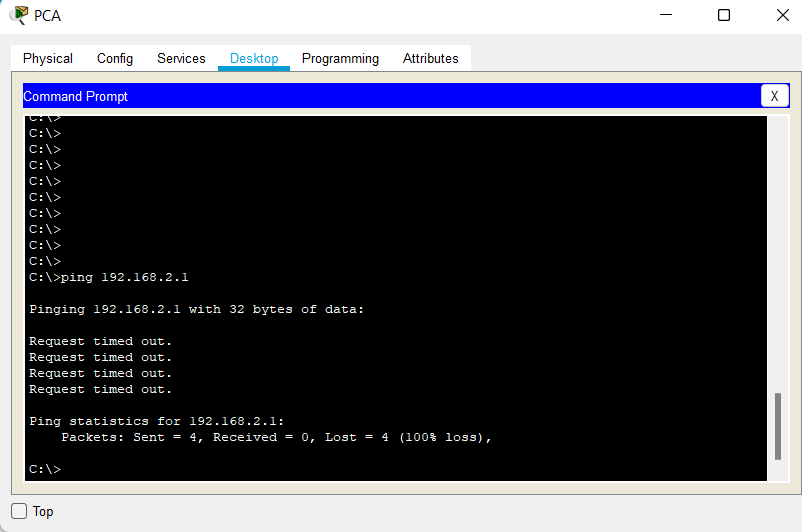
**Desktop->Web Browser->192.168.1.3** (Unsuccessful) Request timed out



**Part 5: Modify an Existing ACL on R1**:

1. **Step1: Verify that PC-A cannot successfully ping the loopback interface on R2.**

**PCA> ping 192.168.2.1** (Unsuccessful) Request timed out



1. **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**

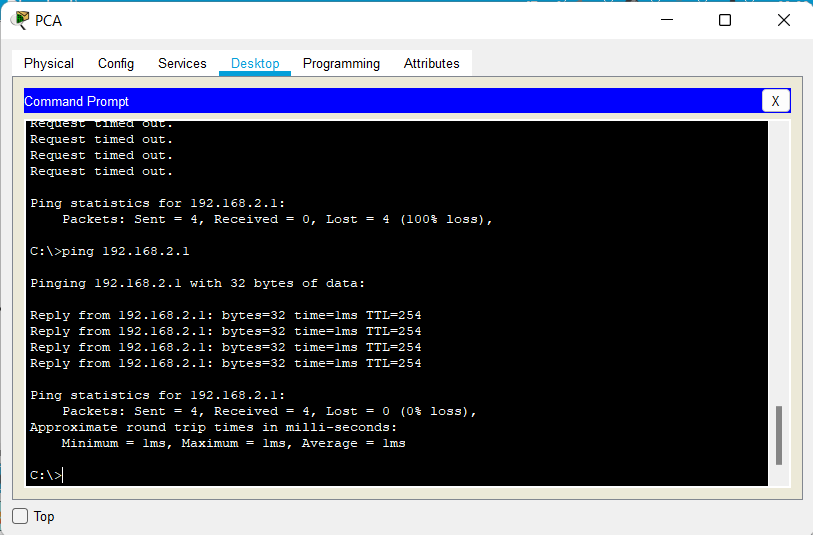
R1(config)# **access-list 120 permit icmp any any unreachable**

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

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

1. **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:**

1. **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**

1. **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:**

1. **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**

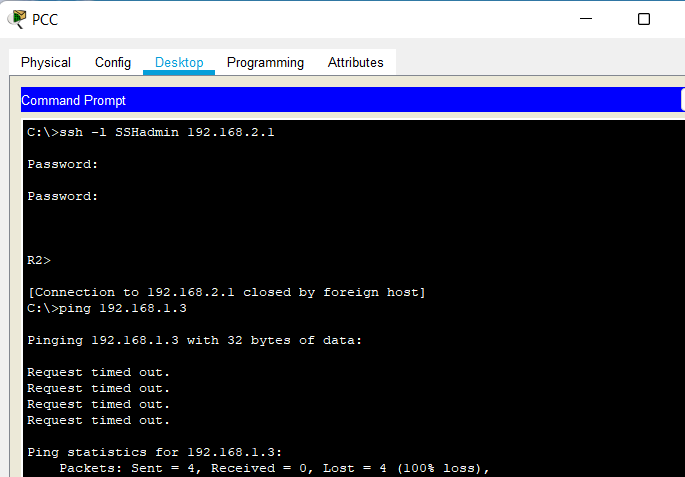
1. **Step 2: Apply the ACL to interface**

R3(config)# **interface se0/1/0**

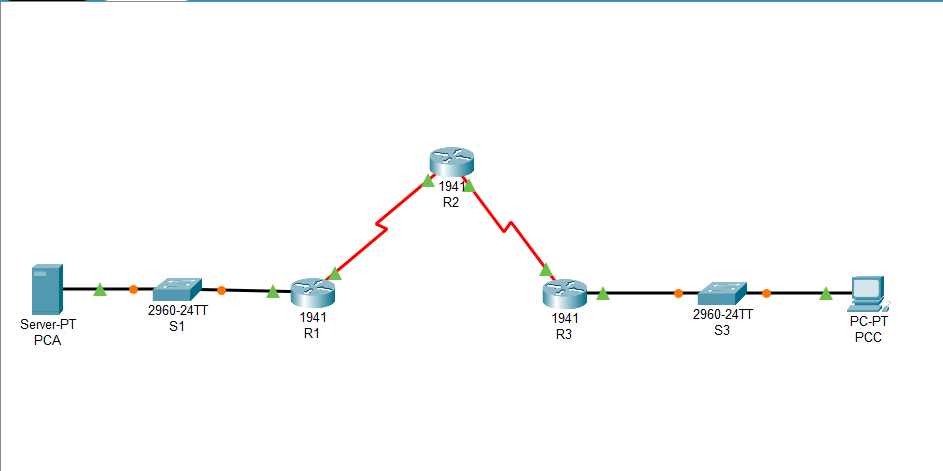
R3(config-if)# **ip access-group 100 in**

1. **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



**Output:**

****