CSEC 744 Network Security

Name : Shriram Karpoora Sundara Pandian Course

Title : Infrastructure Security

Lab : 6

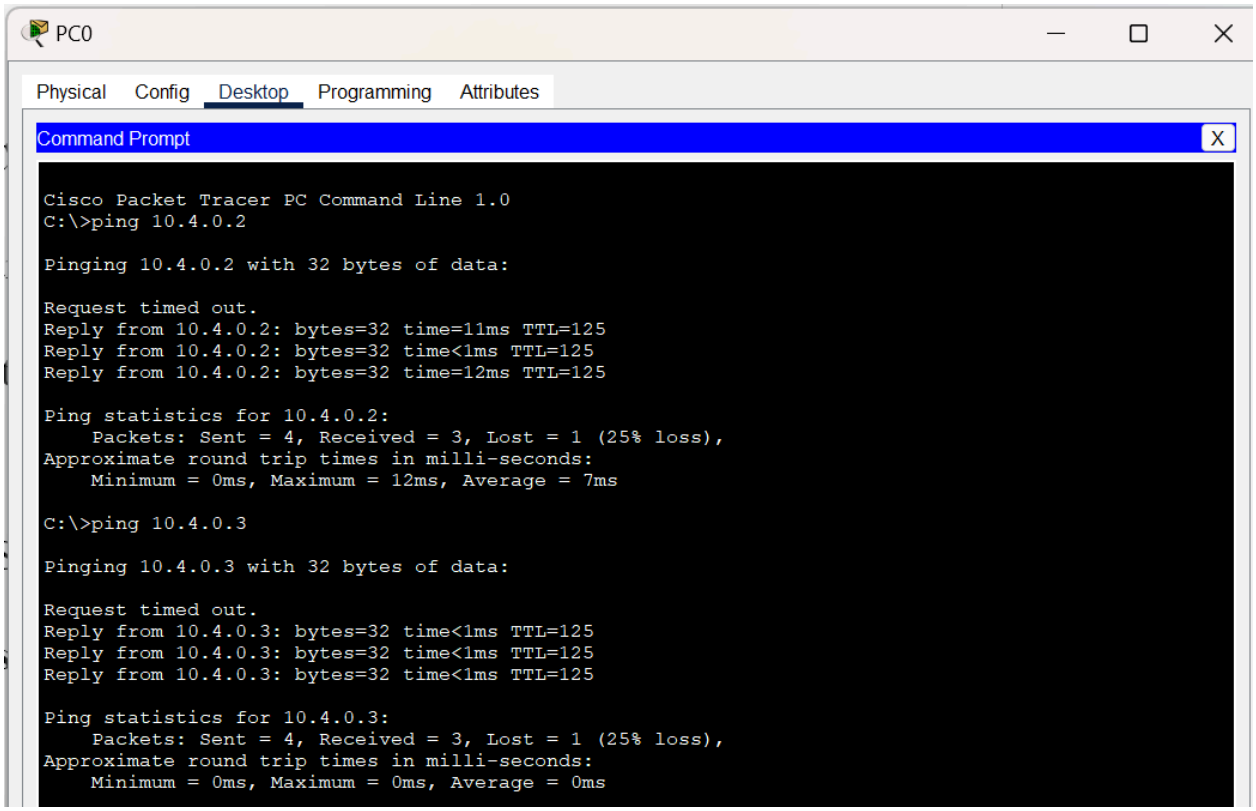
Chapter : 10 (Security Plus)

(I am using Cisco Packet tracer for my lab and not using physical device)

Exercise 10. 02

Step 1 :

A.



PC1

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.4.0.2

Pinging 10.4.0.2 with 32 bytes of data:

Reply from 10.4.0.2: bytes=32 time<1ms TTL=125
Reply from 10.4.0.2: bytes=32 time<1ms TTL=125
Reply from 10.4.0.2: bytes=32 time<1ms TTL=125
Reply from 10.4.0.2: bytes=32 time<1ms TTL=125

Ping statistics for 10.4.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.4.0.3

Pinging 10.4.0.3 with 32 bytes of data:

Reply from 10.4.0.3: bytes=32 time<1ms TTL=125
Reply from 10.4.0.3: bytes=32 time<1ms TTL=125
Reply from 10.4.0.3: bytes=32 time<1ms TTL=125
Reply from 10.4.0.3: bytes=32 time<1ms TTL=125

Ping statistics for 10.4.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

B - H.

```
R2>
R2>
R2>enable
R2#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 1 deny 10.1.0.0 0.0.255.255
R2(config)#access-list 1 permit any
R2(config)#int g0/0
R2(config-if)#ip access-group 1 out
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show access-lists
Standard IP access list 1
    10 deny 10.1.0.0 0.0.255.255
    20 permit any
```

```
R2#show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 10.4.0.99/16
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is 1
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: MCI Check
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
```

J.

```
ip classless
!
ip flow-export version 9
!
!
access-list 1 deny 10.1.0.0 0.0.255.255
access-list 1 permit any
!
!
```

K.

```
C:\>ping 10.4.0.2

Pinging 10.4.0.2 with 32 bytes of data:

Reply from 10.3.0.99: Destination host unreachable.
Reply from 10.3.0.99: Destination host unreachable.
Reply from 10.3.0.99: Destination host unreachable.
Reply from 10.3.0.99: Destination host unreachable.

Ping statistics for 10.4.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.4.0.3

Pinging 10.4.0.3 with 32 bytes of data:

Reply from 10.3.0.99: Destination host unreachable.
Reply from 10.3.0.99: Destination host unreachable.
Reply from 10.3.0.99: Destination host unreachable.
Reply from 10.3.0.99: Destination host unreachable.

Ping statistics for 10.4.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```


```
C:\>ping 10.4.0.2

Pinging 10.4.0.2 with 32 bytes of data:

Reply from 10.3.0.99: Destination host unreachable.
Reply from 10.3.0.99: Destination host unreachable.
Reply from 10.3.0.99: Destination host unreachable.
Reply from 10.3.0.99: Destination host unreachable.

Ping statistics for 10.4.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.4.0.3

Pinging 10.4.0.3 with 32 bytes of data:

Reply from 10.3.0.99: Destination host unreachable.
Reply from 10.3.0.99: Destination host unreachable.
Reply from 10.3.0.99: Destination host unreachable.
Reply from 10.3.0.99: Destination host unreachable.

Ping statistics for 10.4.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```


L.

```
R2#
R2#show access-lists
Standard IP access list 1
    10 deny 10.1.0.0 0.0.255.255 (16 match(es))
    20 permit any
```

M.

```
R1#ping 10.4.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

R1#ping 10.4.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

N.

After clearing the access-lists, the 10 matches got cleared.

```
R2#show access-lists
Standard IP access list 1
    10 deny 10.1.0.0 0.0.255.255
    20 permit any (10 match(es))

R2#clear access-list counters
R2#show access-lists
Standard IP access list 1
    10 deny 10.1.0.0 0.0.255.255
    20 permit any
```

Step 2 :

A.

```
R2#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#no access-list 1
R2(config)#
```

B, C, D.

```
R2>
R2>enable
R2#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 1 deny 10.1.0.1
R2(config)#access-list 1 permit any
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
sh
% Incomplete command.
R2#
R2#show access-lists
Standard IP access list 1
    10 deny host 10.1.0.1
    20 permit any
```

E.

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.4.0.2

Pinging 10.4.0.2 with 32 bytes of data:

Request timed out.
Reply from 10.4.0.2: bytes=32 time<1ms TTL=125
Reply from 10.4.0.2: bytes=32 time<1ms TTL=125
Reply from 10.4.0.2: bytes=32 time<1ms TTL=125

Ping statistics for 10.4.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.4.0.3

Pinging 10.4.0.3 with 32 bytes of data:

Request timed out.
Reply from 10.4.0.3: bytes=32 time<1ms TTL=125
Reply from 10.4.0.3: bytes=32 time<1ms TTL=125
Reply from 10.4.0.3: bytes=32 time<1ms TTL=125

Ping statistics for 10.4.0.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

F.

```
C:\>ping 10.4.0.2

Pinging 10.4.0.2 with 32 bytes of data:

Reply from 10.3.0.99: Destination host unreachable.
Reply from 10.3.0.99: Destination host unreachable.
Reply from 10.3.0.99: Destination host unreachable.
Reply from 10.3.0.99: Destination host unreachable.

Ping statistics for 10.4.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.4.0.3

Pinging 10.4.0.3 with 32 bytes of data:

Reply from 10.3.0.99: Destination host unreachable.
Reply from 10.3.0.99: Destination host unreachable.
Reply from 10.3.0.99: Destination host unreachable.
Reply from 10.3.0.99: Destination host unreachable.

Ping statistics for 10.4.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

G, H, I :

```
R2#show access-lists
Standard IP access list 1
    10 deny host 10.1.0.1 (8 match(es))
    20 permit any

R2#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#no access-list 1
R2(config)#int g0/0
R2(config-if)#no ip access-group 1 out
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

Exercise : 10. 03

Extended ACLs can filter by three or four criteria: source IP, destination IP, protocol, and port, with port being the only optional parameter. This gives you more granular control over the rules.

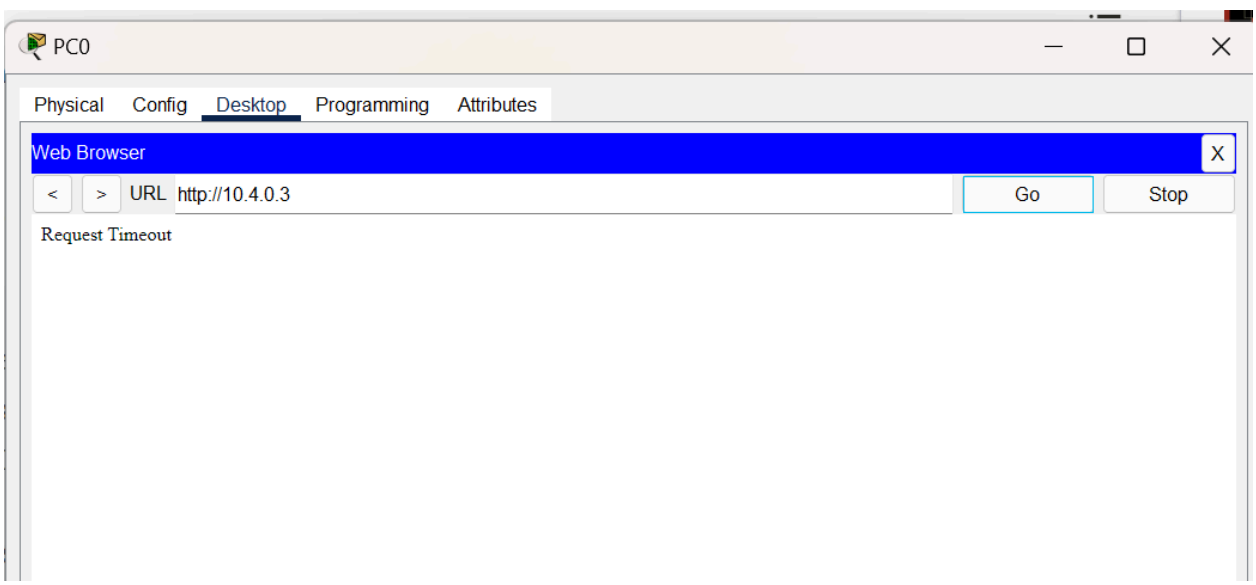
Step 1 :

A - E :

```
R0>
R0>enable
R0#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R0(config)#access-list 101 deny tcp 10.1.0.100 0.0.0.0 10.4.0.3 0.0.0.0 eq 80
R0(config)#access-list 101 permit ip any any
R0(config)#int g0/1
R0(config-if)#ip access-group 101
% Incomplete command.
R0(config-if)#ip access-group 101 in
R0(config-if)#end
R0#
%SYS-5-CONFIG_I: Configured from console by console
```

Step 2

A - B :

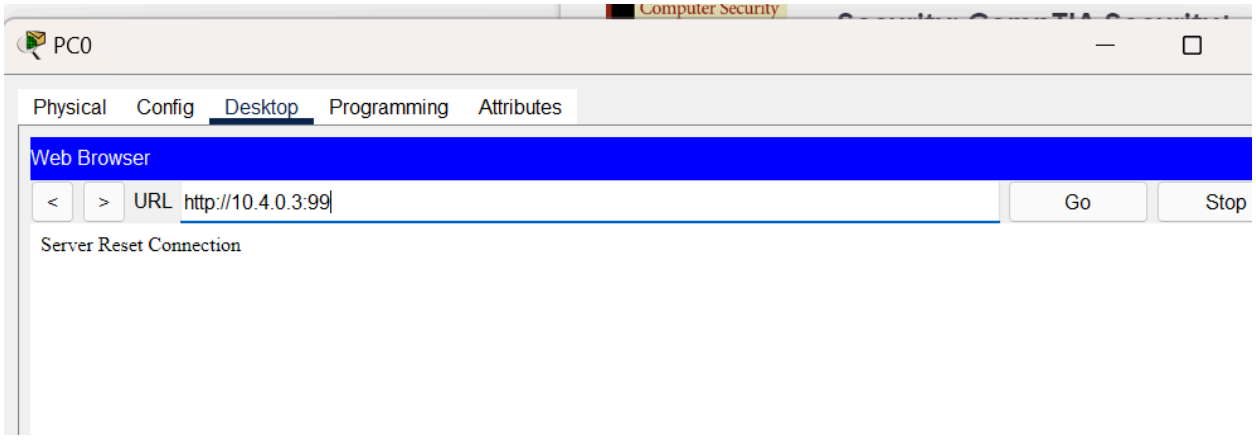


C.

```
R0#show access-lists
Extended IP access list 101
    10 deny tcp host 10.1.0.100 host 10.4.0.3 eq www (29 match(es))
    20 permit ip any any

R0#
```

D - E :



F.

```
R0#show access-lists
Extended IP access list 101
    10 deny tcp host 10.1.0.100 host 10.4.0.3 eq www (29 match(es))
    20 permit ip any any (2 match(es))
```

Lab Analysis :

1. * To Prevent CAM overflow attack
   * Limit the MAC address allowed per port to Prevent Cam Overflow
   * To Mitigate the MAC address spoofing and even ARP cache poisoning.

2. * Shutdown : Shuts the whole port and generates the log message
   * Restrict : Drops the Packet and generates the log message
   * Protect : Drops the packets until the problem resolves and doesn't generate any records.

3. The Standard ACL filter by sources IP address only and it is placed near the destination.
4. The Extended ACL filter by source IP address, Destination IP address and Protocol type with Port numbers
5. Standard ACL should be placed near the Destination and especially the interface outbound.
6. Extended ACL should be placed as inbound to the router closer to the source.
7. Wildcard Masks helps the ACL to understand about the host ID and Network ID. Also helps to filter the IP address.
8. Inbound ACL works when the Packet enters the interface and Outbound ACL works when the packet leaves the interface. This is different from their normal usage, where inbound refers to packets destined for the device, and outbound refers to packets originating from the device

Quiz :

1. MAC address
2. Source IP address
3. Port
4. Interface