

Lab 4 – Network Security Introduction

1 Packet Filters

1.1 Standard Access Lists

Setup the Windows Host, Switch, Router1, Router2, and Linux Host (10.10X.2.2) in one of the Scenarios (RIP,OSPF,BGP) from Lab2 that allows the Windows Host to PING the Linux Host. Create a standard access list that denies and logs the 10.10X.0.0, 0.0.0.255 network from using the “outside” (Ethernet0/0) interface of Router2. In most of the examples in the lab, “X” denotes your station number, “W” denotes your Windows Vista subnet, “L” denotes your Linux subnet, and “R” denotes your Router-Router subnet. (Remember that access lists have an implicit deny match at the end). Activate the access list on the Ethernet0/0 interface. Watch the Console of Router2 while trying to PING or SSH or Telnet to the Server from the Host.

```
Router# conf term
Router(config)# access-list 1 deny 10.10X.W.0 0.0.0.255 log
Router(config)# access-list 1 permit any log
Router(config)# interface Ethernet 0/0
Router(config-if)# ip access-group 1 in
Router(config-if)# end
```

1.2 Extended Access Lists

Create an extended access list that will deny and log the Telnet protocol, while permitting and logging the SSH protocol from 10.10X.0.0, 0.0.0.255. Activate the access list (remove any previous lists) on the Ethernet0/0 interface of Router2. Watch the Console of Router2 while trying to Telnet to the Linux Host and to the FastEthernet interface of Router2, from the Windows Host. Verify that you can still SSH and PING between the Windows Host and Linux Host. (Remember that access lists have an implicit deny match at the end).

```
Router# conf term
Router(config)# access-list 100 deny tcp 10.10X.W.0 0.0.0.255
10.10X.L.0 0.0.0.255 eq 23 log
Router(config)# access-list 100 permit tcp 10.10X.W.0 0.0.0.255
10.10X.L.0 0.0.0.255 eq 22 log
Router(config)# access-list 100 permit icmp 10.10X.W.0 0.0.0.255
10.10X.L.0 0.0.0.255 log
Router(config)# access-list 100 permit ip 10.10X.R.0 0.0.0.255 any
Router(config)# interface Ethernet 0/0
Router(config-if)# no ip access-group 1 in
Router(config-if)# ip access-group 100 in
Router(config-if)# end
```

1.3 Named Access Lists

Duplicate the extended access list of section 1.2 as a named access list. Remove the unnamed Access list and duplicate the testing to make sure this new list works. Then add **another** entry to allow and log Telnet packets from only your Windows Host system through the list. You should test by trying to Telnet to the Linux Host and to the FastEthernet interface of Router2 and monitoring the console logging of Router2. **(Verify the list is doing what you want after adding the host entry, then remove all lists before going on to next part.)** You may have unexpected results until removing and re-adding lines to the access list that preserve the “stop-on-firstmatch” order that you desire. This is true when you’ve made a mistake and need to correct it also. Always “show” the configuration to make sure the list is as intended before testing.

1.3.1

```
Router# conf term
Router(config)# ip access-list extended ACL1
Router(config-ext-nacl)# deny tcp 10.10X.W.0 0.0.0.255 10.10X.L.0
0.0.0.255 eq 23 log
Router(config-ext-nacl)# permit tcp 10.10X.W.0 0.0.0.255 10.10X.L.0
0.0.0.255 eq 22 log
Router(config-ext-nacl)# permit icmp 10.10X.W.0 0.0.0.255 10.10X.L.0
0.0.0.255 log
Router(config-ext-nacl)# permit ip 10.10X.R.0 0.0.0.255 any
Router(config-ext-nacl)# exit
Router(config)# interface Ethernet 0/0
Router(config-if)# no ip access-group 100 in
Router(config-if)# ip access-group ACL1 in
Router(config-if)# end
```

1.3.2

```
Router# conf term
Router(config)# ip access-list extended ACL1
Router(config-ext-nacl)# no deny tcp 10.10X.W.0 0.0.0.255 10.10X.L.0
0.0.0.255 eq 23 log
Router(config-ext-nacl)# permit tcp 10.10X.W.0 0.0.0.255 10.10X.L.0
0.0.0.255 eq 23 log
Router(config-ext-nacl)# end
```

Remove all the access lists after successful testing, and before continuing on to the next portions of the lab.

2 NAT

2.1 Inside Source Translation

Setup Router1 to outside an address on 10.10X.1/24 (Ethernet 0/0). Unconfigure the 10.10X.0.1 address on the FastEthernet 0/0 VLAN, and use an inside network address of 192.168.0.1 for the NAT to translate. Setup your Windows Host to use an address on the 192.168.0.x and set the Default Gateway

on the host to the 192.168.0.1 address of the router. Verify you can transparently access the Linux Host (via SSH) or Router2 (via Telnet), and monitor what address the Linux Host sees the Windows Host as. (The Linux Host should have “netstat -na” run in a terminal shell, to watch ESTABLISHED connections).

```
Router# conf term
Router(config)# ip nat inside source static 192.168.0.x 10.10X.1.3
Router(config)# interface Ethernet 0/0
Router(config-int)# ip nat outside
Router(config-int)# interface FastEthernet 0/0
Router(config-int)# ip nat inside
Router(config)# end
```

2.2 Dynamic Translation

Change the static translation NAT to a dynamic translation. Using the same hardware configuration as above, repeat the test.

```
Router# conf term
Router# access-list 2 permit 192.168.0.0 0.0.0.255
Router(config)# ip nat pool NAT1 10.10X.1.50 10.10X.1.59 netmask
255.255.255.0
Router(config)# ip nat inside source list 2 pool NAT1
```

2.3 Overloading Addresses

For extra credit, convert the NAT translation to use overloaded addresses and repeat the tests. (requires independent reading of the Router Documentation)

2.4 Extension

Discuss which protocol layer ACL's operate on, and comment on some security threats that these types of protections can and can not protect against.