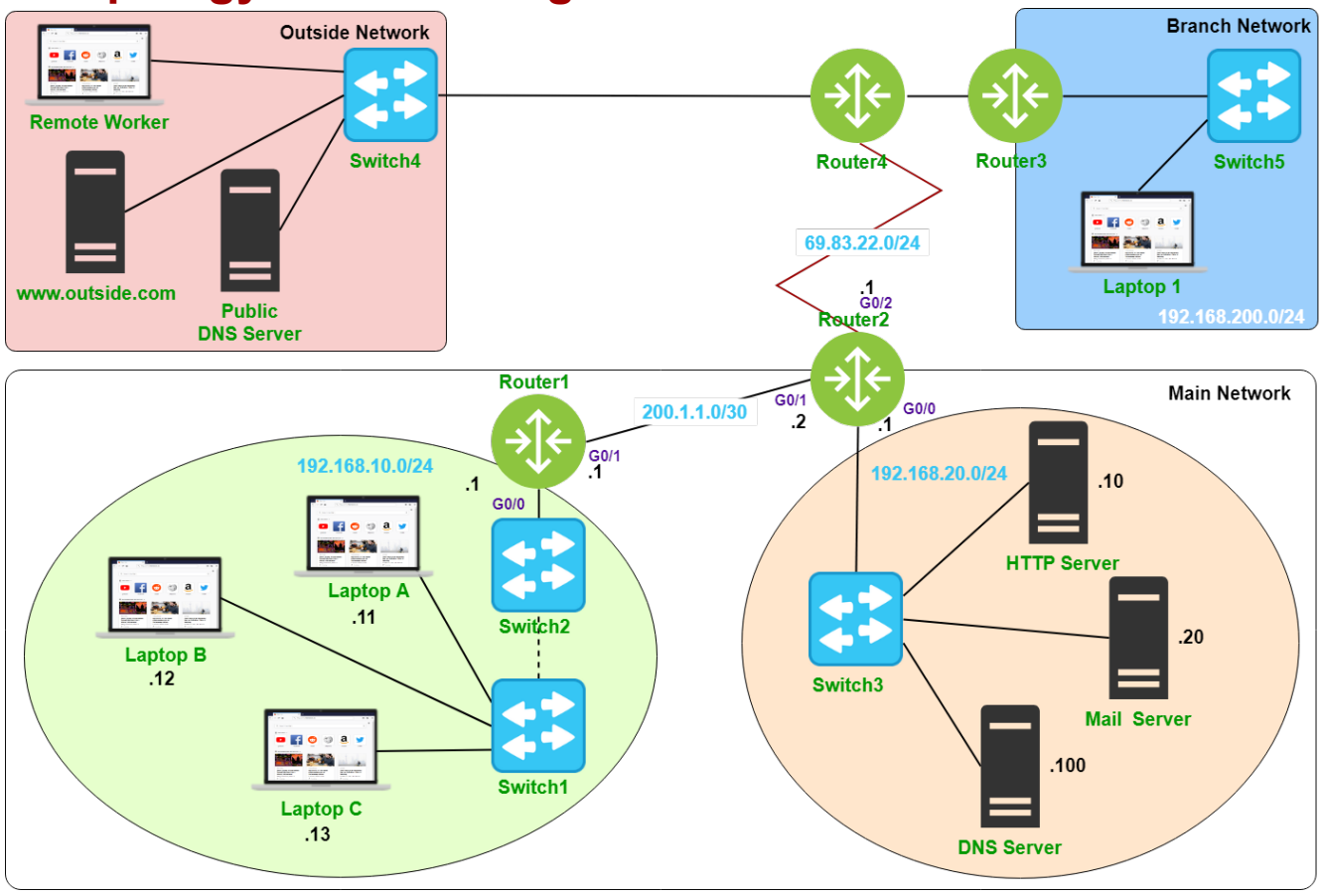
Lab 10 – Improving LAN Security

Lab Topology and Learning Goals



The LAN is often considered to be a "safe" zone of the network; however, some protocols that operate in the lower layers of the OSI model contain little to no safeguards and as such are vulnerable to attack. In this lab, we will configure mitigation steps to reduce the risk of LAN attacks.

Lab Instructions and Required Resources

- Complete this lab in the Packer Tracer file: **INFO-6078 – Lab 10 – Improving LAN Security.pkz**
- Take Lab Quiz: **Lab 10 - Requires Respondus LockDown Browser**

Lab 10 – Improving LAN Security

Secure Access and Trunk Ports

Attackers that gain physical access to network resources can be extremely dangerous. Proper measures should be put in place to ensure that anyone with physical access to the network does not gain logical access.

Some simple steps can be taken to increase the security of the LAN. By default, Cisco switches dynamically configure trunk links when a switch in trunk mode is connected to an interface. An attacker could connect a switch or emulate a switches behavior with a laptop and exploit this behavior. To prevent this, all non-trunk ports should be statically configured as access ports, all trunk ports should be configured as such and dynamic trunking should be disabled. Additionally, all unused ports should be shut down and placed in a non-used VLAN.

Improve Port Security on Switch2

Statically configure GigabitEthernet0/2 as an access port
Switch2(config)# interface GigabitEthernet0/2
Switch2(config-if)# switchport mode access

Statically configure GigabitEthernet0/1 as an trunk port and disable dynamic trunking protocol (DTP)
Switch2(config)# interface GigabitEthernet0/1
Switch2(config-if)# switchport mode trunk
Switch2(config-if)# switchport nonegotiate

Create a VLAN for unused ports and disable ports
Switch2(config)# vlan 66
Switch2(config-vlan)# name UNUSED
Switch2(config-vlan)# exit
Switch2(config)# interface range fastEthernet0/1-24
Switch2(config-if-range)# switchport access vlan 66
Switch2(config-if)# shutdown

Create a separate VLAN to act as the native VLAN
Switch2(config)# vlan 77
Switch2(config-vlan)# name NATIVE
Switch2(config-vlan)# exit
Switch2(config)# interface GigabitEthernet0/1
Switch2(config-if)# switchport trunk native vlan 77
Notice the log messages presented by the console. You must modify the native VLAN on both sides of the link to resolve native VLAN mismatch errors. Configure GigabitEthernet0/1 on switch 1 with the appropriate settings.

Verify the configured VLANs
Switch2# show vlan

Notice that G0/1 is not listed
Switch2# show interface trunk

Verify the interface status
Switch2# show ip int brief

Lab 10 – Improving LAN Security

Configure Static and Sticky MAC Addresses

On **Switch 1**, configure interface **FastEthernet0/1** to communicate only with the MAC address of **Laptop A**, and learn the MAC address for **Laptop B** dynamically and communicate only with that
Switch1(config)# interface FastEthernet0/1
Switch1(config-if)# switchport mode access
Switch1(config-if)# shutdown

Enter the **switchport port-security** command to enable port security on **FastEthernet0/1**
Switch1(config-if)# switchport port-security
The default settings for port security limit the maximum MAC address to one and automatically shut down the port when a violation is detected

Locate the MAC address for **Laptop A** (**ipconfig**) and configure a static MAC address on **Fa0/1**
Switch1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx

Enable Fa0/1
Switch1(config-if)# no shutdown

Verify the configured settings
Switch1# show port-security
Switch1# show port-security interface FastEthernet0/1
From **Laptop A**, ping the default gateway to verify operation
Next, violate the security setting by connecting **Laptop C** to **Fa0/1**
Test the connection by pinging the default gateway again, is the ping successful?

Re-Verity the configuration
Switch1# show port-security
Switch1# show port-security interface FastEthernet0/1
Switch1# show port-security address

Remove **Laptop C** and reconnect **Laptop A**

Re-Enable **Fa0/1**
Switch1(config-if)# shutdown
Switch1(config-if)# no shutdown

Lab Challenge

Configure Switch 1 to dynamically learn the MAC address of Laptop B by subsisting the **switchport port-security mac-address xxxx.xxxx.xxxx** command with the **switchport port-security mac-address sticky** command. Research what port violation modes are available on Cisco devices and what actions they take. Set the port violation mode to restrict with the **switchport port-security violation restrict** command. Test and troubleshoot as necessary

When finished, return the Laptops to their default configuration

Lab 10 – Improving LAN Security

Configure DHCP Snooping

DHCP snooping monitors DHCP traffic and creates a database of learned values that is used to protect the network

Enable DHCP Snooping on Switch1

Client machines are configured on VLAN 10, enable DHCP snooping on this VLAN

Switch1(config)# ip dhcp snooping
Switch1(config)# ip dhcp snooping vlan 10

In order for DHCP snooping to work, at least one trusted port must be configured

Configure G0/1 as a trusted port

Switch1(config)# interface GigabitEthernet0/1
Switch1(config-if)# ip dhcp snooping trust

On all laptops, open the Command Prompt and renew the DHCP lease

C:\> ipconfig /renew

Verify DHCP Snooping operation

Switch1# show ip dhcp snooping
Switch1# show ip dhcp snooping binding