**Net 1061 Switching, Routing, and Wireless Essentials**

**Name: Andrew Koenig**

**Lab: #**

**Follow the instructions down below for the lab itself. For this lab, all answers need to be in blue font. For the questions right below, answer in complete sentences. If this is a self-grading packet tracer. Ensure you paste the screen shot of your score page at the bottom of the document. You will upload both this document and the pkt file regardless if it is self-grading or not. Let the instructor know if you have any questions.**

***Lab Analysis Report***

1. Using complete sentences summarize work you completed during the lab.

I implemented security on a few switches in a network

2. Using complete sentences describe what you learned from the lab. Hint; look at the lab objectives listed at the top of the lab section.

I learned further how to secure a network

***Problems Encountered***

1. Using complete sentences describe any problem(s) experienced during lab.

No problems

2. Using complete sentences describe how you solved your problem(s).

No problems

3. Using complete sentences explain if you needed any assistance with the lab; then list what you learned from that assistance. No problems

Packet Tracer - Switch Security Configuration

# VLAN Table

| Switch | VLAN Number | VLAN Name | Port Membership | Network |
| --- | --- | --- | --- | --- |
| SW-1 | 10 | Admin | F0/1, F0/2 | 192.168.10.0/24 |
| SW-1 | 20 | Sales | F0/10 | 192.168.20.0/24 |
| SW-1 | 99 | Management | F0/24 | 192.168.99.0/24 |
| SW-1 | 100 | Native | G0/1, G0/2 | None |
| SW-1 | 999 | BlackHole | All unused | None |
| SW-2 | 10 | Admin | F0/1, F0/22 | 192.168.10.0/24 |
| SW-2 | 20 | Sales | F0/10 | 192.168.20.0/24 |
| SW-2 | 99 | Management | F0/24 | 192.168.99.0/24 |
| SW-2 | 100 | Native | None | None |
| SW-2 | 999 | BlackHole | All unused | None |

# Objectives

Part 1: Create a Secure Trunk

Part 2: Secure Unused Switchports

Part 3: Implement Port Security

Part 4: Enable DHCP Snooping

Part 5: Configure Rapid PVST PortFast and BPDU Guard

# Background

You are enhancing security on two access switches in a partially configured network. You will implement the range of security measures that were covered in this module according to the requirements below. Note that routing has been configured on this network, so connectivity between hosts on different VLANs should function when completed.

# Instructions

## Create a Secure Trunk.

* + - 1. Connect the G0/2 ports of the two access layer switches.
      2. Configure ports G0/1 and G0/2 as static trunks on both switches.
      3. Disable DTP negotiation on both sides of the link.
      4. Create VLAN 100 and give it the name Native on both switches.
      5. Configure all trunk ports on both switches to use VLAN 100 as the native VLAN.

## Secure Unused Switchports.

* + - 1. Shutdown all unused switch ports on SW-1.
      2. On SW-1, create a VLAN 999 and name it BlackHole. The configured name must match the requirement exactly.
      3. Move all unused switch ports to the BlackHole VLAN.

## Implement Port Security.

* + - 1. Activate port security on all the active access ports on switch SW-1.
      2. Configure the active ports to allow a maximum of 4 MAC addresses to be learned on the ports.
      3. For ports F0/1 on SW-1, statically configure the MAC address of the PC using port security.
      4. Configure each active access port so that it will automatically add the MAC addresses learned on the port to the running configuration.
      5. Configure the port security violation mode to drop packets from MAC addresses that exceed the maximum, generate a Syslog entry, but not disable the ports.

## Configure DHCP Snooping.

* + - 1. Configure the trunk ports on SW-1 as trusted ports.
      2. Limit the untrusted ports on SW-1 to five DHCP packets per second.
      3. On SW-2, enable DHCP snooping globally and for VLANs 10, 20 and 99.

**Note:** The DHCP snooping configuration may not score properly in Packet Tracer.

## Configure PortFast, and BPDU Guard.

* + - 1. Enable PortFast on all the access ports that are in use on SW-1.
      2. Enable BPDU Guard on all the access ports that are in use on SW-1.
      3. Configure SW-2 so that all access ports will use PortFast by default.

End of document

Graphical user interface, application

Description automatically generated