**Step-by-Step Project Manual for Campus Network Analysis and Cyber Security Implementation**

**1. Introduction:**

Welcome to the Cisco Virtual Internship Program for Cyber Security! In this project, you will analyze and secure the network infrastructure of APSIT College. We will be using Cisco Packet Tracer to map the network, apply security controls, and propose countermeasures to mitigate potential risks.

**2. Install Cisco Packet Tracer:**

If you haven't installed Cisco Packet Tracer already, please download and install it from the Cisco Networking Academy website.

**3. Network Analysis:**

Start by gathering information about the APSIT College network, including its devices, connections, and layout. Make sure you have a clear understanding of the current network topology.

**4. Network Mapping in Packet Tracer:**

Now, let's use Cisco Packet Tracer to create a visual representation of the APSIT College network infrastructure. Follow these steps:

**a.** Open Cisco Packet Tracer.

**b.** Click "Add a Simple PDU" from the bottom-left menu and add "End Devices" to the workspace, representing computers and servers.

**c.** Click "Add a Switch" and place "Layer 2 Switches" in the topology.

**d.** Connect the devices using appropriate cables (e.g., copper straight-through cables for connecting PCs to switches).

**e.** Continue adding devices and connections based on the gathered information about the network layout.

**5. Creating Separate VLANs:**

We will configure separate VLANs to segment the network. This will improve security by isolating different departments. Follow these steps:

**a.** Select a Layer 2 switch in the topology and click on it to open its configuration.

**b.** Enter the following commands:

```

**config t**

**int range fa0/1-24**

**switchport mode access**

**switchport access vlan 10**

**do wr**

```

**c.** Repeat the above steps for other Layer 2 switches and assign them to different VLANs as needed.

**6. Multiswitch Access Point to All VLANs:**

To allow communication between VLANs, we need to configure an inter-VLAN routing mechanism. Follow these steps for VLAN 30:

**a.** Select the Multilayer switch connected to VLAN 30 and click on it to open its configuration.

**b.** Enter the following command:

```

**en**

**config t**

**int gig1/0/2**

**switchport access vlan 30**

```

**c.** Repeat the above steps for all other VLANs to enable access between them.

**7. Enabling Trunking on Links:**

To carry multiple VLAN traffic over a single physical link, configure trunking on the inter-switch links. Follow these steps:

**a.** Select the Multilayer switch and click on one of its ports connected to another switch.

**b.** Enter the following commands:

```

**int gig1/0/1**

**switchport trunk encapsulation dot1q**

**switchport mode trunk**

**ex**

**do wr**

```

**c.** Repeat the above steps for all inter-switch links.

**8. Configuring Main Campus Router for DHCP:**

We will configure the Main Campus Router to provide DHCP services to the PCs in different departments. Follow these steps for VLAN 10:

**a.** Select the Main Campus Router and enter the following commands:

```

**en**

**config t**

**int gig0/0.10**

**encapsulation dot1Q 10**

**ip address 192.168.1.1 255.255.255.0**

```

**b.** Repeat the above steps for other VLANs (e.g., VLAN 80).

**c.** Create DHCP pools for each department. Enter the following commands for VLAN 10:

```

**service dhcp**

**ip dhcp pool acc-pool**

**network 192.168.1.0 255.255.255.0**

**default-router 192.168.1.1**

**dns-server 192.168.1.1**

**ex**

```

**d.** Repeat the above steps for other VLANs' DHCP pools.

**9. Enabling RIP for Branch-to-Branch Communication:**

To enable communication between different branches, we will use the RIP routing protocol. Follow these steps for the Main Campus Router:

**a.** Enter the following commands:

```

**en**

**config t**

**router rip**

**version 2**

**network 10.10.10.0**

**network ...**

**ex**

**do wr**

```

b. Repeat the above steps for the Cloud Router, adding network 10.10.10.0 and other required networks to RIP.

**10. VPN Tunneling for Secure Communication:**

To establish secure communication between different campuses, we will configure a VPN tunnel. Follow these steps on both routers:

**a.** Enter the following commands on Main Campus Router:

```

**en**

**config t**

**interface tunnel 1**

**ip address 172.16.1.1 255.255.255.252**

**tunnel source Se/1/0**

**tunnel destination 10.10.10.6**

**no shut**

```

**b.** Repeat the above steps on the Cloud Router, using appropriate IP addresses.

**11. Firewall Configurations for FTP Server:**

To protect the FTP server, we will set up a firewall rule. Follow these steps:

**a.** Access the firewall configuration on the appropriate device.

**b.** Set up a rule to allow ICMP for only admin systems (e.g., 192.168.8.0 IP pattern) and deny ICMP for other systems.

**12. Security Assessment Report:**

Prepare a comprehensive security assessment report that highlights identified security risks, proposed solutions, and countermeasures to mitigate attack surface risks.

**13. Conclusion:**

Congratulations on completing the project! You have successfully analyzed and secured the network infrastructure of APSIT College. Your efforts in implementing various security controls will contribute to a safer network environment.