Mini-Project 16: Small Lab Design

Mini-Project Overview
## Time Estimate: 1 hour

You have been chatting with fellow cybersecurity students on their efforts to learn cybersecurity by getting hands-on training. You have discovered that some students have built their own home labs and you want to try your hand at doing this as well. You have a budget of $500, an eBay account, and an Amazon account. Your goal for your lab is to have two servers, a switch, and a firewall. You also need software, some of which is free outright (like Linux), and some of which is free for evaluation purposes. Remember, virtualization technology will help you run more than one OS on a given hardware platform.

Project Submission Steps

Based on the above requirements, use 2-4 paragraphs to design and document the lab you will build, complete with the following details:

- **Hardware used, along with details like RAM and hard drive space**

- **Software downloaded and installed**

- **VMs created ● IP addressing scheme**

- **Attack machine details (e.g. Kali, Parrot, Black Arch)**

- **Firewall type**

- **Network traffic monitoring setup**

- **Log traffic setup**

- **Switch configuration, including any VLANs**

- **Wireless access**

Home Lab Network
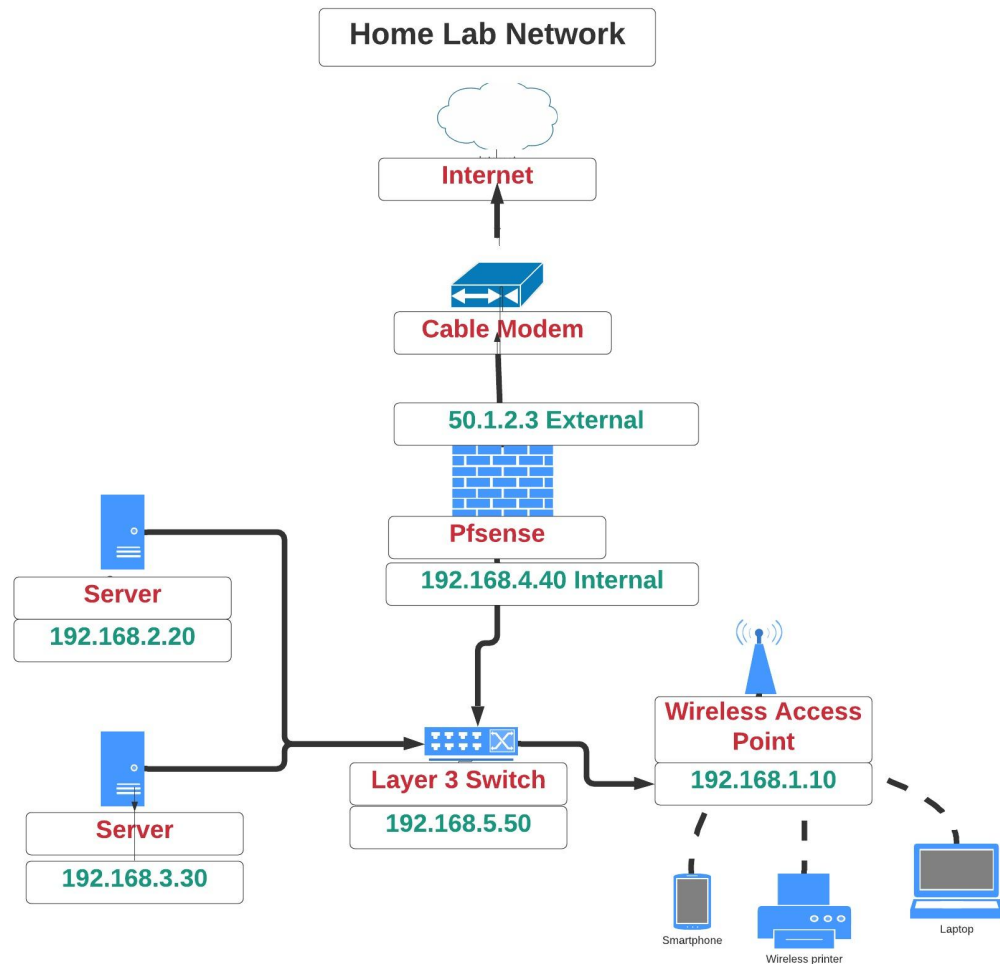
The following devices were bought from amazon to set up the home network lab :

- The cable modem is provided by the ISP (Verizon, AT&T, etc.)

- Cisco catalyst Layer 3 Switch
https://www.amazon.com/Cisco-Catalyst-WS-C3560X-24T-S-Layer-Switch/dp/B085LRP
PCZ/ref=sr_1_11?dchild=1&keywords=cisco+catalyst+layer+3+switch&qid=162173292
0&sr=8-11

- Dell Optiplex Desktop PC with Window 10 Professional used as server.
https://www.amazon.com/Dell-Optiplex-3020-SFF-Desktop/dp/B075WYN1JL/ref=sr_1_
3?crid=230XVR1FAYB05&dchild=1&keywords=dell+optiplex+3020+sff+desktop+compu
ter+refurbished&qid=1621733609&sprefix=DELL+optiplex+3020+SFF+%2Caps%2C15
7&sr=8-3
  The server consists of the following:
  - ❏ Hard drive 500 GB HDD 7200 rpm

❏ RAM 3 GB
❏ Hypervisor which comes with WIN 10 PRO

● Netgate SG-1100 security gateway appliance with pfSense Plus software. It consists of a WAN and LAN port.

https://www.amazon.com/SG-1100-pfSense-Security-Gateway-Appliance/dp/B07MTMP XKG/ref=sr_1_1?crid=7QDD9ALHIDAJ&dchild=1&keywords=netgate+sg-1100&qid=16 21734169&sprefix=netgate+sg%2Caps%2C158&sr=8-1

● D-Link Wifi router used as Wireless Access Point

https://www.amazon.com/D-Link-Internet-Network-Assistant-DIR-1750-US/dp/B084H58 WN2/ref=sr_1_1_sspa?dchild=1&keywords=d-link+wireless+access+point&qid=162173 4255&sr=8-1-spons&psc=1&spLa=ZW5jcnlwdGVkUXVhbGlmaWVyPUEzNVc3Szc0V1 ZMOUtBJmVuY3J5cHRlZElkPUEwMzk5NTYxTzkzQUdWRFVLUlFDJmVuY3J5cHRlZE FkSWQ9QTA5ODA5ODcyNFhYR004VzBNU1ZXJndpZGdldE5hbWU9c3BfYXRmJmFj dGlvbj1jbGlja1JlZGlyZWN0JmRvTm90TG9nQ2xpY2s9dHJ1ZQ==

The following steps should be completed to configure the home network lab as shown in the diagram above :

● **Configure the ethernet adapters with the ip addresses shown in the diagram above.**

The two host servers come with Windows 10 Pro. On one of the servers, configure the ethernet adapter with ip address 192.168.2.20, subnet mask of 255.255.255.0 and default gateway of 198.168.2.1. For easier access to the server, add the entry "server1 192.168.2.1" to the hosts file in Windows (C:\Windows\System32\drivers\etc\hosts). On the other server, configure the ethernet adapter with ip address 192.168.3.30, subnet mask of 255.255.255.0 and default gateway of 198.168.3.1. For easier access to the server, add the entry "server2 192.168.3.30" to the hosts file in Windows (C:\Windows\System32\drivers\etc\hosts).

● **Using the Hypervisor that comes with windows (Hyper-V) install two virtual machines (VM) on sever1.**

Install the Linux Ubuntu operating system on the on VM. Next, install Apache on it and configure the VM to be used as a web server. On the second VM, install the free trial version of the Windows Server 2016 VM. This can be downloaded from the Microsoft website (https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019). Create an external virtual switch in Hyper-V manager to have the two VM's access the internet. In this case, the ethernet adapter will be represented as a virtual ethernet adapter. Configure the Windows Server VM as a file server.

● **Using the Hypervisor that comes with windows (Hyper-V) install two virtual machines (VM) on server2.**

Create a VM and install Kali Linux on it. Create another VM and install Linux Ubuntu on it. Install the free version of Nagios.Nagios is a monitoring tool whose functionality includes individual node status, server and network device monitoring and email/mobile phone notification. Another flavor of Nagios, Nagios Log Server provides an easy way to search log data by setting up alerts or querying log data to quickly audit a system. Nagios log server comes at a cost but there is a free trial period.

- **Configure the Cisco catalyst 24 port layer 3 switch for routing.**

Configure the switch with static ip address 192.168.5.50 and subnet mask 255.255.255.0. With regard to VLAN's the layer 3 switch is configured the same way as a regular L2 switch. Complete the following to assign VLANs to the devices on the private LAN :

- ❏ Assign the eth2/0 port to VLAN 20 and connect the cable to server1 . Next, assign the eth3/0 port to VLAN 30 which will connect to server2.
- ❏ Next for each VLAN, configure an IP address known as Switched Virtual Interface (SVI). The configuration for an SVI involves first enabling IP routing and then applying an IP address to the VLAN. The SVI will be configured as 192.168.2.1 for VLAN 20 and 192.168.3.1 for VLAN 30. The two configurations will allow routing between VLAN 20 and VLAN 30.
- ❏ Server1 and Server2 will use IP addresses 192.168.2.1 and 192.168.3.1 as their default gateway (respectively). The subnet mask for all IP addresses is 255.255.255.0.
- ❏ Configure eth0/4 with VLAN 40 and IP address 192.168.4.1. Connect a cable from this port to the LAN port on the pfsense router. Assign the pfsense router the default gateway of 192.168.4.1.
- ❏ Configure eth0/1 with VLAN 10 and IP address 192.168.1.1. Connect a cable from this port to the LAN port on the Wireless Access Point (WAP). Assign the WAP the default gateway of 192.168.1.1.

- **Configure the pfsense router to be used as a firewall.**

Assign the pfsense assign the static ip address 192.168.4.40/24 to the LAN port. This is the private IP address. The WAN port on the router will be connected to the cable modem. For security reasons and IP address shortage, the public address of 50.1.2.3.4 needs to be translated to the private IP address using NAT (Network Address Translation).This is done automatically.
Use pfsense to disable FTP (port 21), HTTP (port 80) and Telnet (port 23). Enable the secure versions of FTP, HTTP, and Telnet by enabling SCP (port 22), SSH (port 22) and HTTPS (443) respectively. These applications send encrypted data.

- **Connect the Wifi Router/Wireless Access Point to the layer 3 switch.**

Configure the Wifi router with IP address 192.168.1.10, subnet mask of 255.255.255.0 and gateway 192.168.1.1. Enable the DHCP IP address range from 192.168.1.11 to 192.168.1.50.