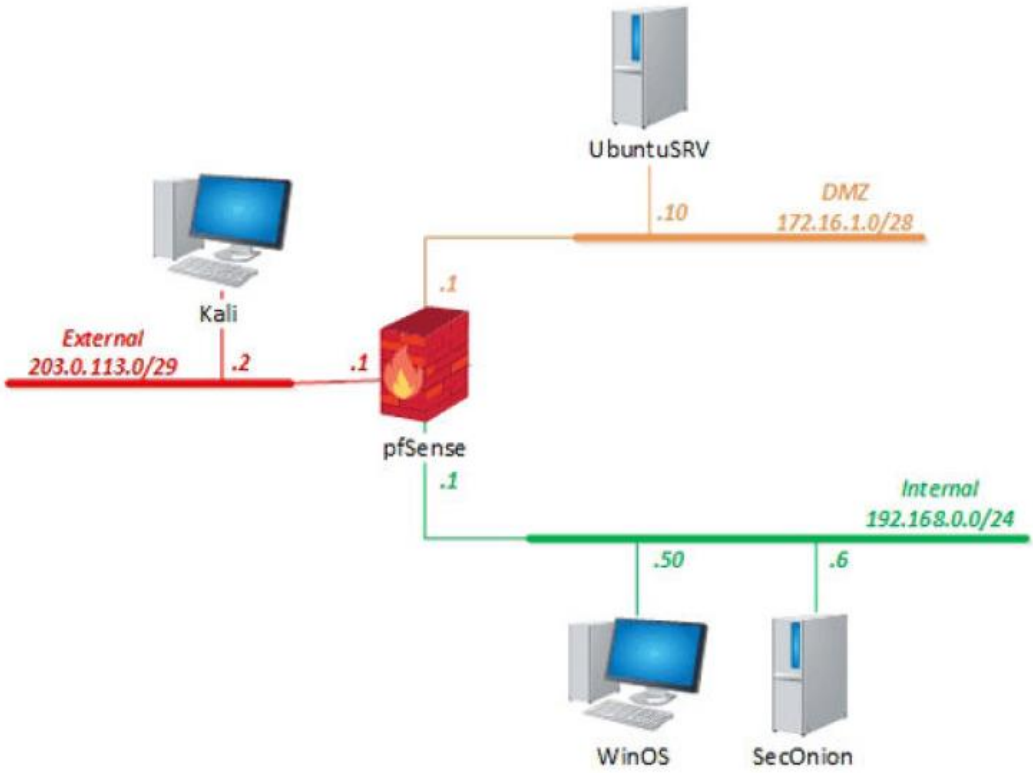
Use the lab reservation for LAB 22.

Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Kali	203.0.113.2	kali	kali
pfSense	192.168.0.1	sysadmin	NDGlabpass123!
SecOnion	192.168.0.6	sysadmin	NDGlabpass123!
UbuntuSRV	172.16.1.10	sysadmin	NDGlabpass123!
WinOS	192.168.0.50	Administrator	NDGlabpass123!

Use the lab reservation for LAB 22

Part One:

1. Log into the Kali Linux machine and use the appropriate command to scan for and identify all live hosts on the 172.16.1/28 network. Provide a screenshot of this command and its output, and label this as Screenshot-01. (5%)
2. Again, while on Kali, initiate a **ping scan** while spoofing the source *MAC* address at the same time. Provide a screenshot of this command and its output, and label this as Screenshot-02. (5%)
3. Initiate an operating system scan from Kali against the pfSense system to help identify what version of Linux it is running on. Provide a screenshot of this command and its output, and label this as Screenshot-03. (5%)
4. While still on Kali, open a browser window and navigate to the pfsense firewall. Sign in and navigate to the Rules page. Provide a full-screen screenshot of this screen, and label this as Screenshot-04. (5%)
5. Disable internal network access and apply the change. Provide a full-screen screenshot of the screen containing the confirmation message and label this as Screenshot-05. (5%)
6. Initial a terminal session on the Kali system, and start up Wireshark with the & option. Capture the primary Ethernet Interface and position the Wireshark window and the terminal window side-by-side on your screen. Start the capture. Provide a full-screen screenshot of the screen containing the confirmation message and label this as Screenshot-06. (5%)
7. In the terminal window, issue the following nmap command**: nmap -T5 203.0.113.1 192.168.0.0/24 172.16.1.0/28**. After it completes, issue the command **nmap -T4 -A -v 172.16.1.10**. This make take several minutes. Once this is finished, switch to the Wireshark window and stop the scan.

   Save the captured Wireshark capture using **myscan** as the file name, and a using the dropdown box to the right of Save As, select the option "**Wireshark/tcpdump/… -pcap"**. Before saving, ensure the path is **/home/kali/Desktop**, and provide a full-screen screenshot of the screen containing the confirmation message and label this as Screenshot-07. (5%)
8. Switch back to the terminal window. Press the Enter key a few times, and start the http.server using the **python3** command with the option to search sys.path for the named module. Provide a full-screen screenshot of the terminal screen, showing the http server running on port 8000 and label this as Screenshot-08. (5%)

9. Log into the SecOnion machine. Start the Chromium web browser and navigate to the web server at 203.0.113.2 using port 8000. Provide a full-screen screenshot of the browser screen, showing the http server running on port 8000 and label this as Screenshot-09. (5%)

10. Download the myscan.pcap file. After the download is finished (usually 5-30 seconds) close the browser, and open a terminal window. Run the status command as a root user to ensure all services are at a status of ok. (If not, wait a few minutes and try the status command again. When all status indicators are "OK" import the scan file using the command **sudo so-import-pcap** command. Import the file to the to the location **~/Downloads/myscan.pcap**. Provide a full-screen screenshot of the terminal screen, label this as Screenshot-10. (5%)

11. On the Kali machine, in the terminal window, stop the http server. On the browser window, start a new tab and access the Security Onion main page. If the warning page shows up, click the advanced button, and accept the risk. On the Login page, enter the username as **sysadmin@netlab.local** and the password as **NDGlabpass123!** and click LOGIN. Provide a full-screen screenshot of the screen, label this as Screenshot-11. (5%)

12. Navigate to the Alerts menu. The alerts screen will appear. Click on the first **ET-SCAN** rule name and select **Drilldown**. Click the Arrow on the left to expand to a detailed information screen. Provide a full-screen screenshot of the details screen, label this as Screenshot-12. (5%)

Part Two:

13. On Kali, in the terminal window, create an empty text file named **secretinfo.txt**. Launch the **veracrypt** application in the terminal window. Click the **Create Volume** option. The VeraCrypt Volume Creation Wizard screen should appear. Provide a full-screen screenshot of the screen, label this as Screenshot-13. (4%)

14. Select Create an encrypted container, click Next, select Standard VeraCrypt container, click Next. For **Volume Location**, click **Select File** and select the file name you created in step 13 from the display screen. A screen asking if you want to replace this file will appear. Select **Replace.** This should return you to the Volume Location Screen. Provide a full-screen screenshot of the screen, label this as Screenshot-14. (4%)

15. Select encryption options of **AES**, **SHA-512**, volume of **40 MB**, password of **PassWord**. If warned about a short password, say '**Yes**'. Use FAT filesystem, format the volume, and replace the file with a VeraCrypt container. Provide a full-screen screenshot of the **Volume Created** screen, label this as Screenshot-15. (4%)

16. Select the VeraCrypt container, select your text file, and place it into Slot 1 of the VeraCrypt, ad mount the device, using the password from the previous step. The drive should now be successfully mounted. Provide a full-screen screenshot of the VeraCrypt screen showing the mounted drive and slot**.** Label this as Screenshot-16. (4%)

Part Three:

17. In the Windows OS Server, add a server role for **Certification Authority Management Tools,** under **Active Directory Certificate Services Tools.** For **Role Services**, be sure to check Certification Authority. Install the role, using the defaults. This will take 2-4 minutes. When this is complete, prior to clicking on the Close button, provide a full-screen screenshot of the **Feature Installation** screen, label this as Screenshot-17. (4%)
18. From the Server Manager window, Customize the Certificate services by clicking on the **AD CS** function in the left pane. Configure **Active Directory Certificate Services** on the destination server link. Select "**More…**" and **Configure Active Directory Certificate.** Setup the **Certificate Authority** as a **Standalone CA, Root CA**, and **create a new private key**, using **SHA256**. Name the common name for the CA as "**FINAL CA**", with expiration of **30 days**, and use the default database locations. On the Confirmation step, **BEFORE** clicking on **Configure,** provide a full-screen screenshot of the **Confirmation** screen, label this as Screenshot-18. (5%)

Part Four:

19. Using a Firefox browser, log into the pfsense firewall from the UbuntuSRV machine. Navigate to the Firewall, Rules screen. Provide a full-screen screenshot of the WAN rules. Label this as Screenshot-19. (5%)
20. Add a new WAN rule to block ICMP, all subtypes from the DMZ network. Save and apply the rule. Provide a current full-screen screenshot of the WAN rules. Label this as Screenshot-20. (5%)
21. From the Firewall, add a NAT rule for Port Forwarding to redirect all SSH traffic to the Ubuntu server, also using SSH. Save and apply the changes. Provide a current full-screen screenshot of the Port Forwarding rules. Label this as Screenshot-21. (5%)