

Module 07

NETWORK SECURITY CONTROLS - TECHNICAL CONTROLS

CERTIFIED CYBERSECURITY TECHNICIAN

INDEX

Module 07: Network Security Controls - Technical Controls

Exercise 1: Implement Host-based Firewall Protection with iptables	06
Exercise 2: Implement Host-based Firewall Functionality using Windows Firewall	16
Exercise 3: Implement Network-Based Firewall Functionality: Block Unwanted Website Access using pfSense Firewall	53
Exercise 4: Implement Network-Based Firewall Functionality: Block Insecure Ports using pfSense Firewall	76
Exercise 5: Implement Host-based IDS Functionality using Wazuh HIDS	115

Exercise 6:

Implement Network-based IDS Functionality using Suricata IDS

143**Exercise 7:**

Detect Malicious Network Traffic using HoneyBOT

206**Exercise 8:**

Establish Virtual Private Network Connection using SoftEther VPN

220**Exercise 9:**

Scan System for Viruses using Kaspersky Internet Security

251

LAB SCENARIO

The most important aspect of security controls is the protection of organizational assets such as people, property, and data. By establishing security controls, an organization can either reduce or completely mitigate risks to their assets.

The labs in this module will provide you with a real-time experience in using various methods and techniques used to implement technical controls in the network, thereby, preventing the network from unauthorized access to critical assets and resources.

LAB OBJECTIVE

The objective of this lab is to provide expert knowledge in implementing technical controls. This knowledge is gained through the following tasks:

- Implementation of Host-based firewall protection and Host-based firewall functionality
- Blocking access to unwanted website and insecure ports using pfSense firewall
- Implementation of Host-based IDS functionality and Network-based IDS functionality
- Detecting malicious traffic in the network using HoneyBOT
- Configuring VPN connection using tools such as SoftEther VPN
- Scanning the System for Viruses using Kaspersky Internet Security

OVERVIEW OF TECHNICAL CONTROL

Technical control is referred to as logical controls. It makes use of technology to control access to the physical assets or the facility of the organization. It is generally incorporated in the computer hardware, software, operations, or applications to control access to sensitive areas.

LAB TASKS

A cyber security professional or a security professional use numerous tools and techniques to implement technical controls in the network. Recommended labs that will assist you in learning various aspects of technical controls include the following:

- 01** Implement Host-based Firewall Protection with iptables
- 02** Implement Host-based Firewall Functionality using Windows Firewall
- 03** Implement Network-Based Firewall Functionality: Block Unwanted Website Access using pfSense Firewall
- 04** Implement Network-Based Firewall Functionality: Block Insecure Ports using pfSense Firewall
- 05** Implement Host-based IDS Functionality using Wazuh HIDS
- 06** Implement Network-based IDS Functionality using Suricata IDS
- 07** Detect Malicious Network Traffic using HoneyBOT
- 08** Establish Virtual Private Network Connection using SoftEther VPN
- 09** Scan System for Viruses using Kaspersky Internet Security

Note: Turn on **PfSense Firewall** virtual machine and keep it running throughout the lab exercises.

EXERCISE 1: IMPLEMENT HOST-BASED FIREWALL PROTECTION WITH IPTABLES

iptables is a command-line firewall utility that uses policy chains to allow or block traffic.

LAB SCENARIO

A security professional must know how to configure an iptables host-based firewall to allow or block traffic to or from a Linux system. iptables allows us to enter firewall rules into the existing tables using the command line.

LAB OBJECTIVE

This lab will demonstrate how to configure an iptables host-based firewall in an Ubuntu machine.

OVERVIEW OF IPTABLES

iptables is a standard firewall included in most Linux distributions. With the default chain policies configured, you can start adding rules to iptables, so that it knows what to do when it encounters a connection from or to a particular IP address or port.

LAB TASKS

Note: Ensure that **PfSense Firewall** virtual machine is running.

1. Turn on the **Attacker Machine-1** virtual machine.

2. Select User **Bob** and type password **user@123** press the **Enter** button.

3. Open the **Firefox** web browser, type **www.google.com** in the URL, and press **Enter**.

Note: If a notification appears at the top section of a browser window, click **Okay, Got it** and in **Before you continue to Google Search** wizard, click **I agree** button.

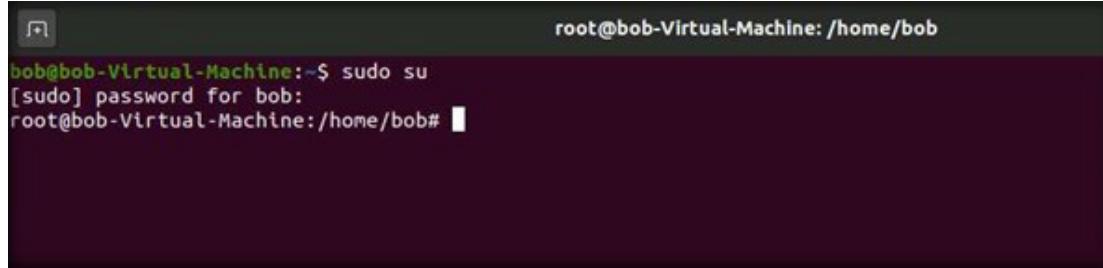
Note: If a **Software Updater** pop-up appears, click on **Remind Me Later**.

4. Bob is able to access the website, which implies that Bob has internet access. A security professional can block internet access on the user machine using iptables.

5. Press **ALT + CTL + T** to open the terminal, type the **sudo su** command for the root user, and press Enter.

6. When prompted for the password, type the password for the **root** user (here the root user password is **user@123**), and press **Enter**.

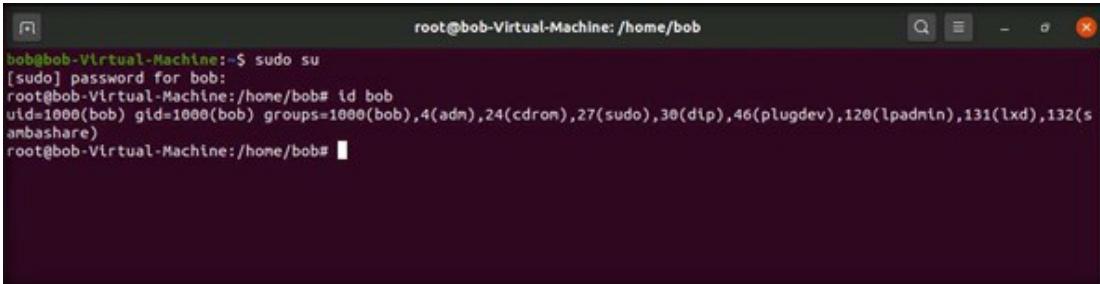
Note: The password that you type will not be visible.



A terminal window titled "root@bob-Virtual-Machine: /home/bob" displays the command "bob@bob-Virtual-Machine:~\$ sudo su". It prompts for a password with "[sudo] password for bob:" and shows the root prompt "root@bob-Virtual-Machine:/home/bob#".

EXERCISE 1:
IMPLEMENT HOST-BASED
FIREWALL PROTECTION
WITH IPTABLES

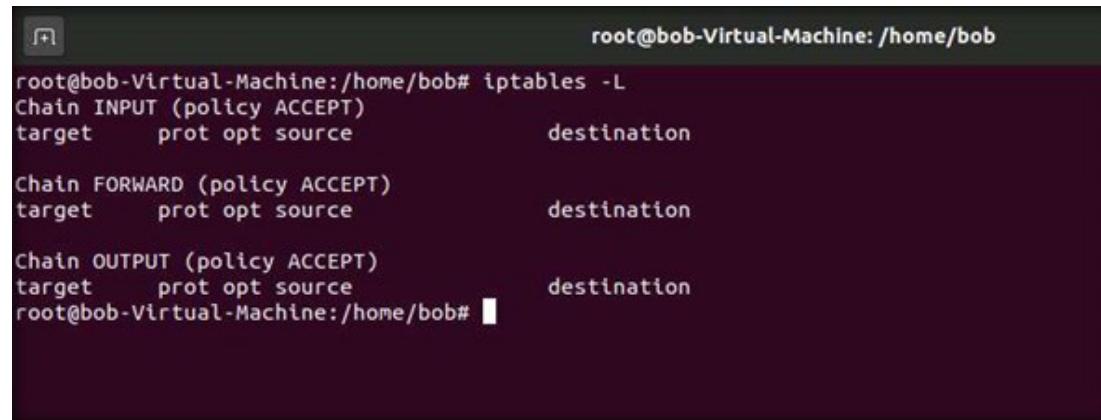
7. Next, to identify the user ID for **Bob**, type **id bob** in the terminal and press the **Enter** button. The user id displays as shown in the screenshot



```
root@bob-Virtual-Machine:~$ sudo su
[sudo] password for bob:
root@bob-Virtual-Machine:/home/bob# id bob
uid=1000(bob) gid=1000(bob) groups=1000(bob),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare)
root@bob-Virtual-Machine:/home/bob#
```

EXERCISE 1:
**IMPLEMENT HOST-BASED
FIREWALL PROTECTION
WITH IPTABLES**

8. Note down the user id (uid) for Bob (here 1000).
9. Further, we use the **iptables** command for network management activity.
10. Type **iptables -L** and press **Enter** to check the existing rules for users.



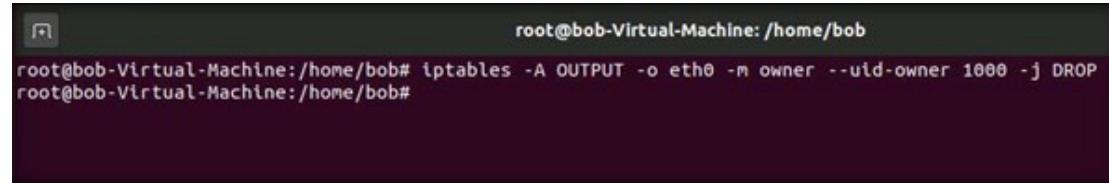
```
root@bob-Virtual-Machine:/home/bob
root@bob-Virtual-Machine:/home/bob# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@bob-Virtual-Machine:/home/bob#
```

EXERCISE 10

IMPLEMENT HOST-BASED FIREWALL PROTECTION WITH IPTABLES

11. No rules exist currently. Next, we will create a new rule with the following command for the user **Bob**.

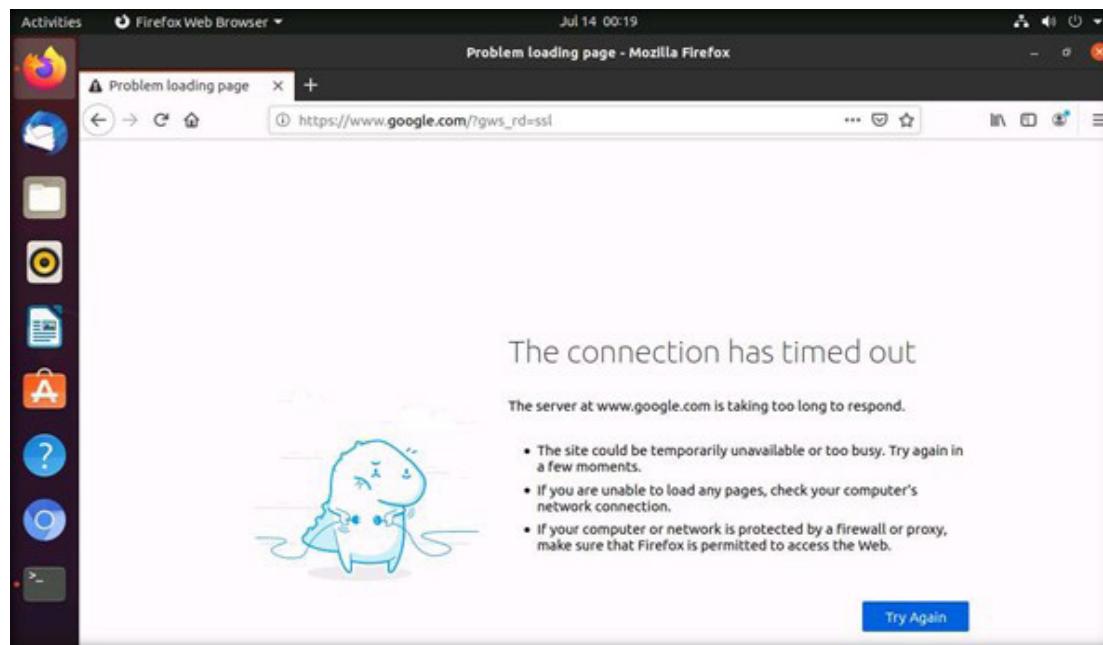
12. Type **iptables -A OUTPUT -o eth0 -m owner --uid-owner 1000 -j DROP** as shown in the screenshot below, and press **Enter**.



```
root@bob-Virtual-Machine:/home/bob
root@bob-Virtual-Machine:/home/bob# iptables -A OUTPUT -o eth0 -m owner --uid-owner 1000 -j DROP
root@bob-Virtual-Machine:/home/bob#
```

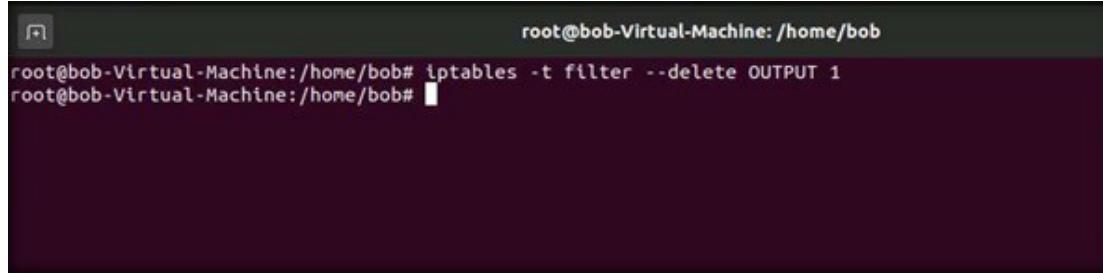
EXERCISE 1:
IMPLEMENT HOST-BASED
FIREWALL PROTECTION
WITH IPTABLES

13. The rule will be applicable only for the user Bob who has 1000 as the UID, as we have already noted.
14. Test the Internet connection to check whether or not the iptables rule is applied.
15. Open the browser, type **www.google.com**, and press the **Enter** button.
16. As the screenshot below shows, the website is not accessible to the user.



EXERCISE 10
IMPLEMENT HOST-BASED
FIREWALL PROTECTION
WITH IPTABLES

17. Now switch back to the terminal window, type **iptables -t filter --delete OUTPUT 1** in the terminal window and press **Enter**.

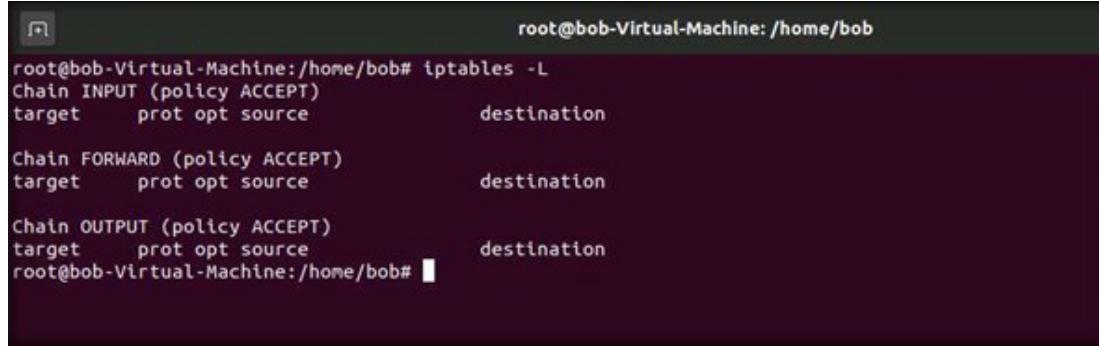


```
root@bob-Virtual-Machine:/home/bob
root@bob-Virtual-Machine:/home/bob# iptables -t filter --delete OUTPUT 1
root@bob-Virtual-Machine:/home/bob#
```

A screenshot of a terminal window titled "root@bob-Virtual-Machine:/home/bob". The window contains a single command: "root@bob-Virtual-Machine:/home/bob# iptables -t filter --delete OUTPUT 1". The cursor is positioned at the end of the command line.

EXERCISE 1:
IMPLEMENT HOST-BASED
FIREWALL PROTECTION
WITH IPTABLES

18. This will delete the rule that was created in **step 12** and to enable Internet connection to user **Bob**, to check the rule type **iptables -L** and press **Enter**.



```
root@bob-Virtual-Machine:/home/bob# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@bob-Virtual-Machine:/home/bob#
```

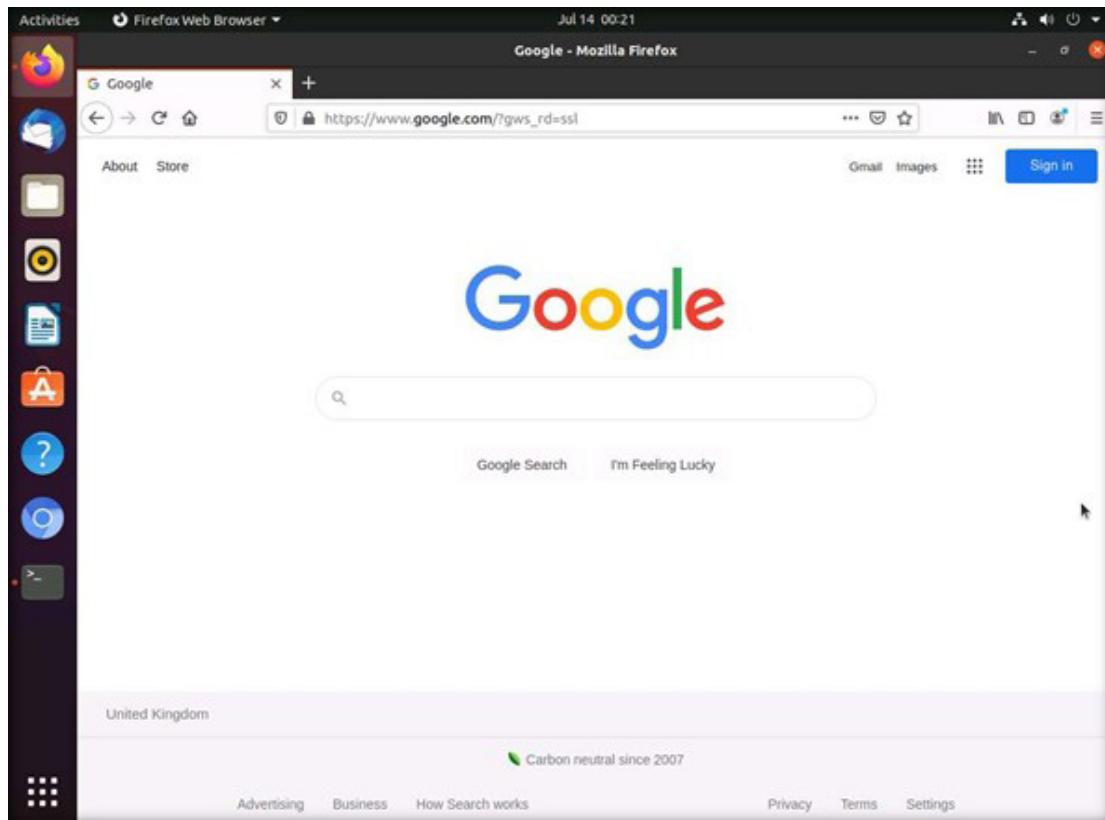
EXERCISE 1:
**IMPLEMENT HOST-BASED
FIREWALL PROTECTION
WITH IPTABLES**

19. No rules exist currently, we have successfully deleted the rule, now we will check for connectivity.

20. Open the browser, type **www.google.com**, and press the **Enter** button.

EXERCISE 10

IMPLEMENT HOST-BASED FIREWALL PROTECTION WITH IPTABLES



EXERCISE 2: IMPLEMENT HOST-BASED FIREWALL FUNCTIONALITY USING WINDOWS FIREWALL

A host-based firewall protects the system from various threats.

LAB SCENARIO

A security professional must have the required knowledge to implement various security layers in the organization; a single breach in security can allow the attacker to leave malicious code or transfer the malicious file over the network. Host-based firewall implementation is another security layer where the administrator can allow or restrict specific individual endpoints. In this lab, you will learn how to configure a host-based firewall to protect the individual system connected to the network.

LAB OBJECTIVE

This lab will demonstrate how to secure an individual endpoint within the network. In this lab, you will learn how to do the following:

- Hardening the host within the network
- Applying rules in a host-based firewall

OVERVIEW OF A HOST-BASED FIREWALL

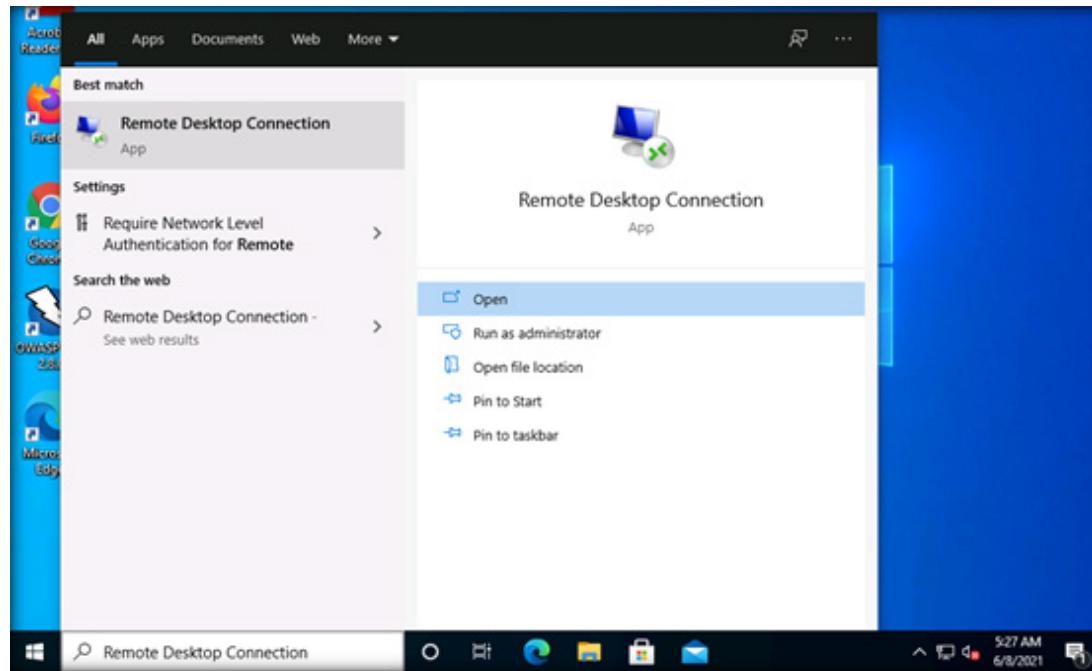
A host-based firewall is a software that makes the system or device secure. Configuring a host-based firewall will help achieve real security implementation and defense in depth within an organization. The normal strategy of a host-based firewall is to provide defense-in-depth and use a combination of layers of protection within the organization.

An example is the Windows firewall, which is inbuilt in the Windows platform. The Windows firewall developed by Microsoft Windows is an application that filters the incoming and outgoing Internet traffic and blocks the malicious program communicating to the individual endpoint. The Windows firewall (host-based) protects the individual endpoint over the network from various threats, viruses, and malware.

LAB TASKS

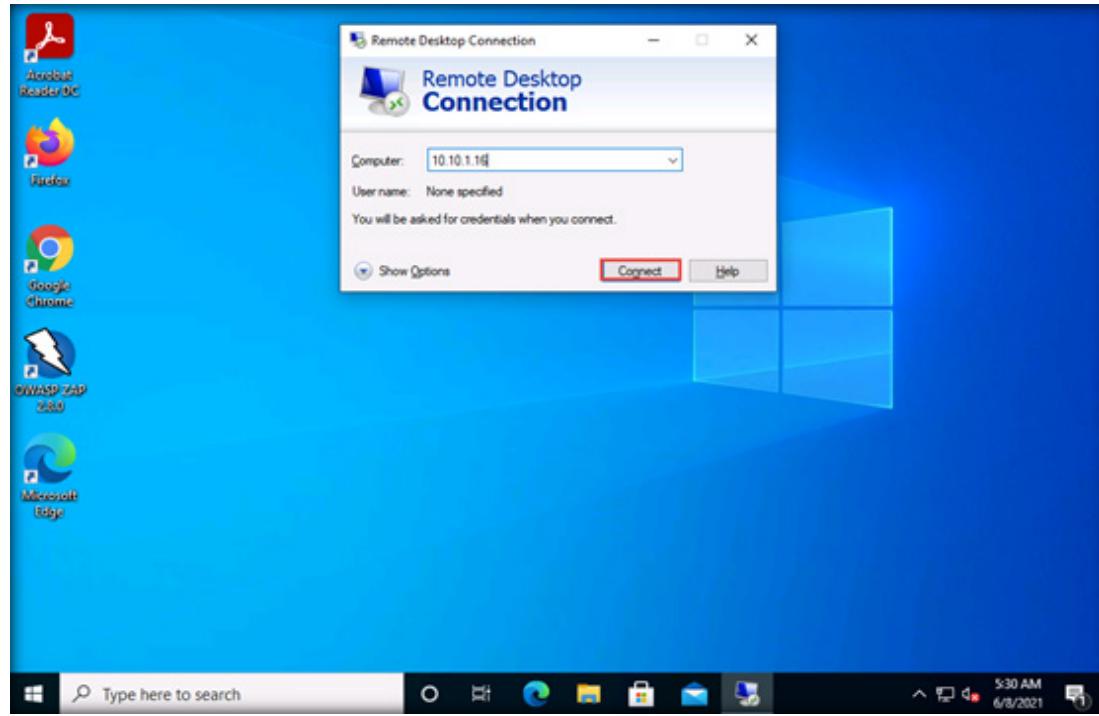
Note: Ensure that PfSense Firewall virtual machine is running.

- EXERCISE 2:
IMPLEMENT HOST-BASED
FIREWALL FUNCTIONALITY
USING WINDOWS
FIREWALL
1. Turn on **Admin Machine-1** and **Web Server** virtual machines.
 2. In the **Admin Machine-1** virtual machine, log in with the credentials **Admin** and **admin@123**.
Note: If the network screen appears, click **Yes**.
 3. Navigate to the **Windows Start** menu, type **Remote Desktop Connection**, and press **Enter**.

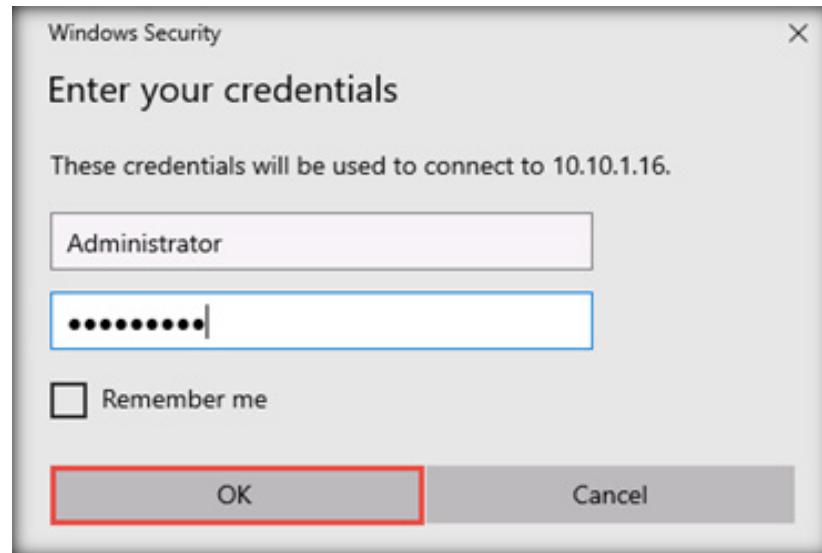


EXERCISE 2:
IMPLEMENT HOST-BASED
FIREWALL FUNCTIONALITY
USING WINDOWS
FIREWALL

4. The **Remote Desktop Connection** window will appear as shown in the screenshot below. Type the **10.10.1.16** IP address of the **Web Server** machine and click **Connect**.



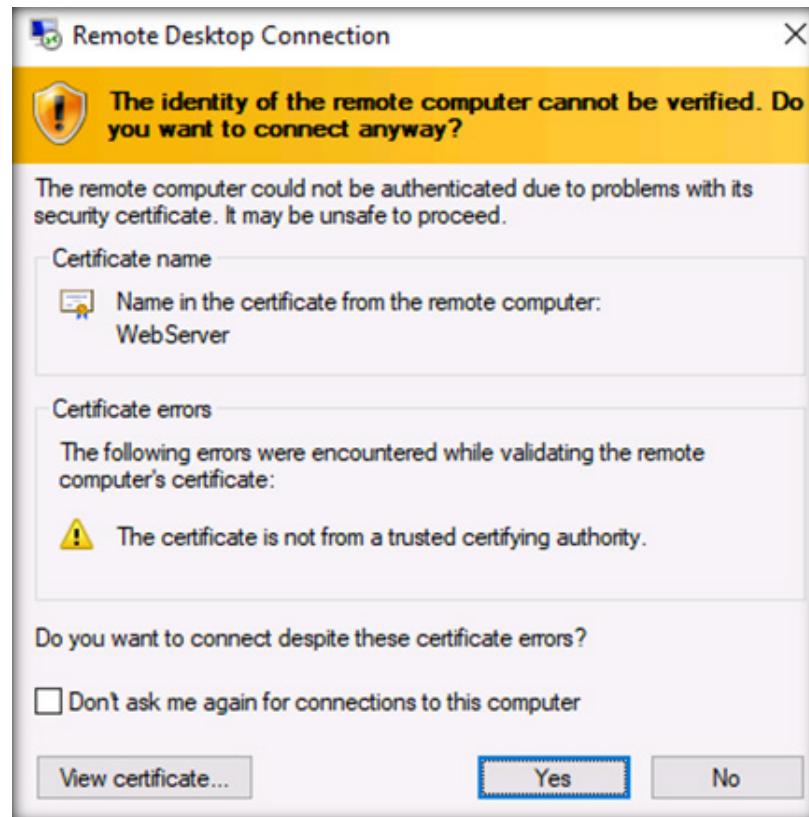
5. The **Windows Security** pop-up window will appear. Type the username **Administrator** and password **admin@123**, and click **OK**



**EXERCISE 2:
IMPLEMENT HOST-BASED
FIREWALL FUNCTIONALITY
USING WINDOWS
FIREWALL**

6. The **Security Certificate** pop-up will appear as shown in the screenshot below. Click **Yes**.

EXERCISE 2:
**IMPLEMENT HOST-BASED
FIREWALL FUNCTIONALITY
USING WINDOWS
FIREWALL**



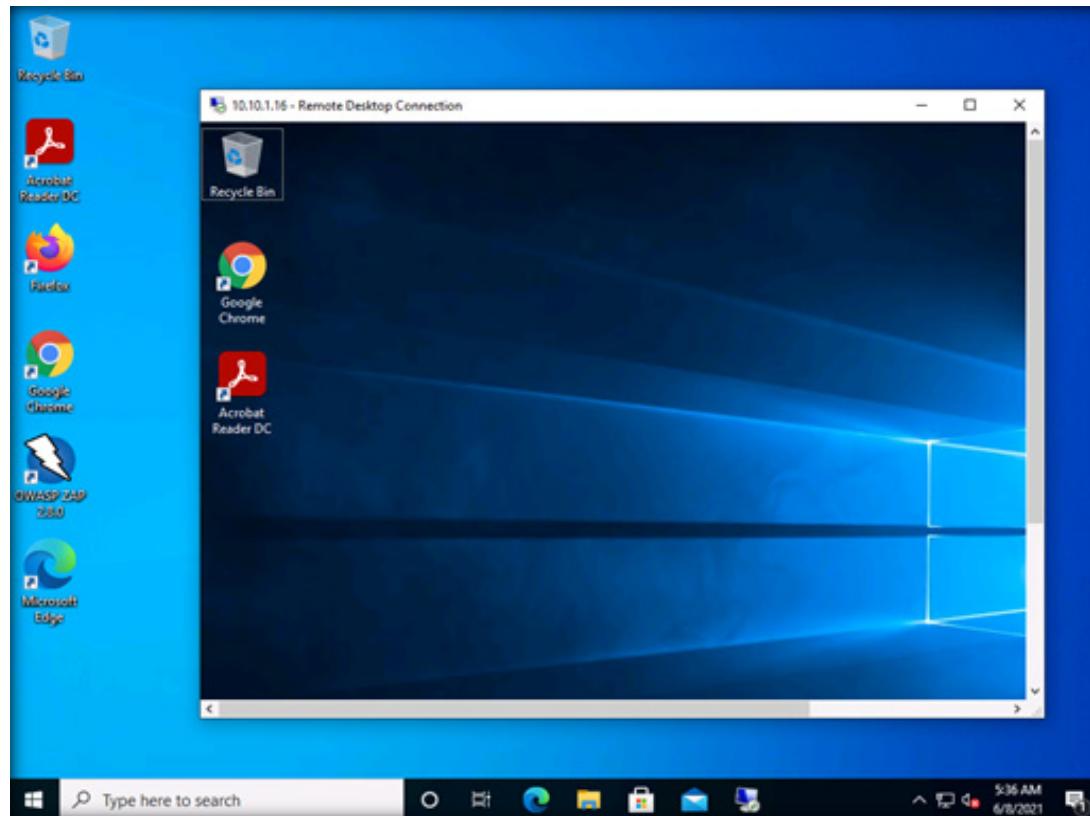
7. After clicking Yes, the **Web Server** virtual machine will appear as **10.10.1.16 – Remote Desktop Connection** in the **Admin Machine-1**.

EXERCISE 2:
IMPLEMENT HOST-BASED
FIREWALL FUNCTIONALITY
USING WINDOWS
FIREWALL



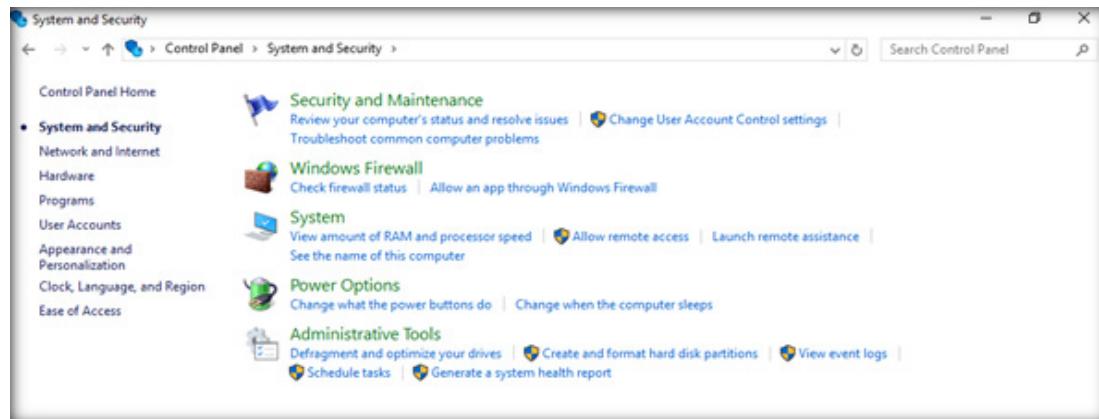
8. Click **Restore down** button of Remote Desktop window, to view connected desktop properly.

EXERCISE 2:
**IMPLEMENT HOST-BASED
FIREWALL FUNCTIONALITY
USING WINDOWS
FIREWALL**



9. In the previous task, we were able to access the Windows machine remotely because there was no restriction for the individual system; therefore, another machine can access this machine remotely. A security professional needs to apply a host-based firewall on an individual machine to prevent the machine from being accessed remotely.
10. Switch to the **Web Server** virtual machine.
11. Login with the credentials **Administrator** and **admin@123**.
12. Open **Control Panel**.
13. Click the **System and Security** option.

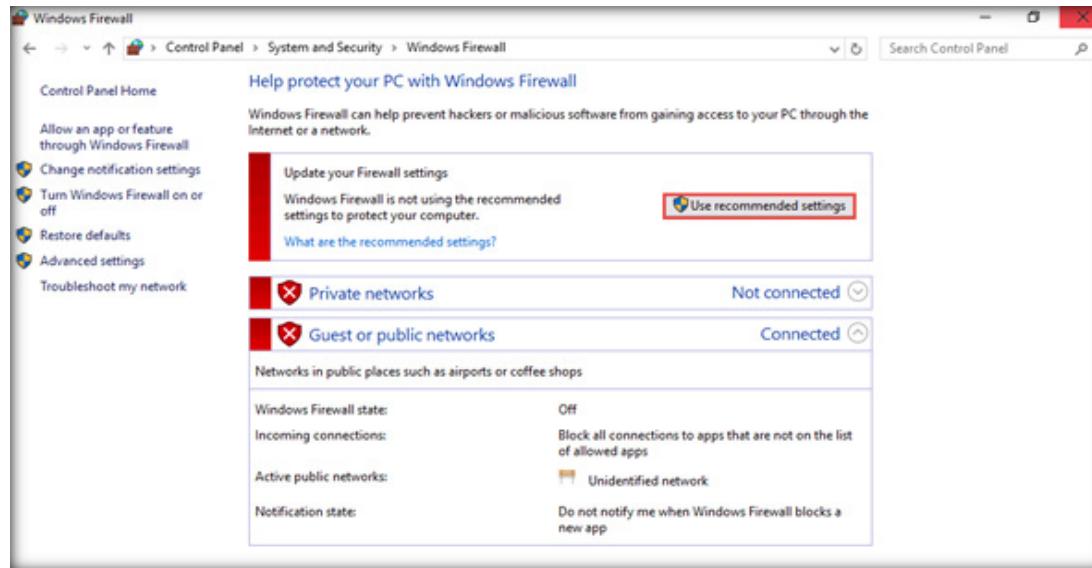
14. The **System and Security** windows will appear. Click **Windows Firewall**.



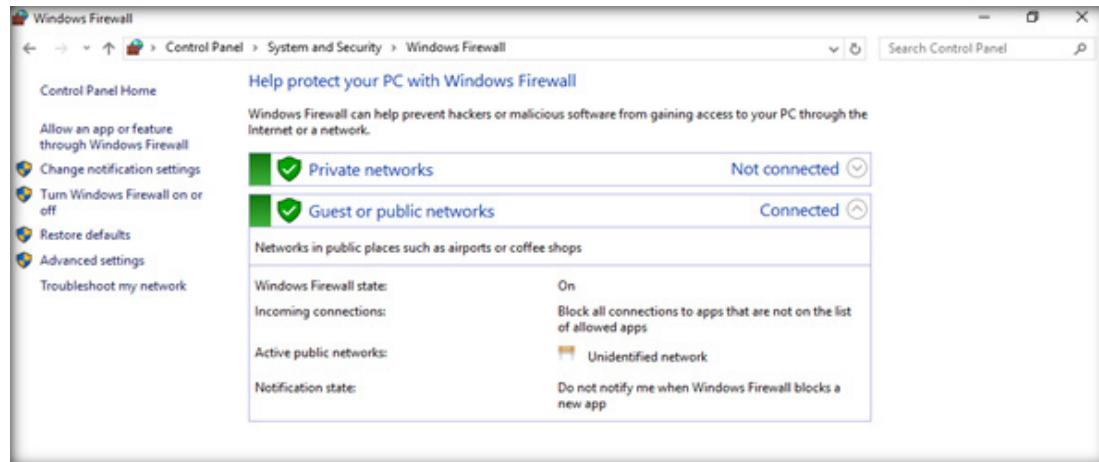
EXERCISE 2: IMPLEMENT HOST-BASED FIREWALL FUNCTIONALITY USING WINDOWS FIREWALL

15. The Windows Firewall window opens. Click **Use recommended settings**.

**EXERCISE 2:
IMPLEMENT HOST-BASED
FIREWALL FUNCTIONALITY
USING WINDOWS
FIREWALL**



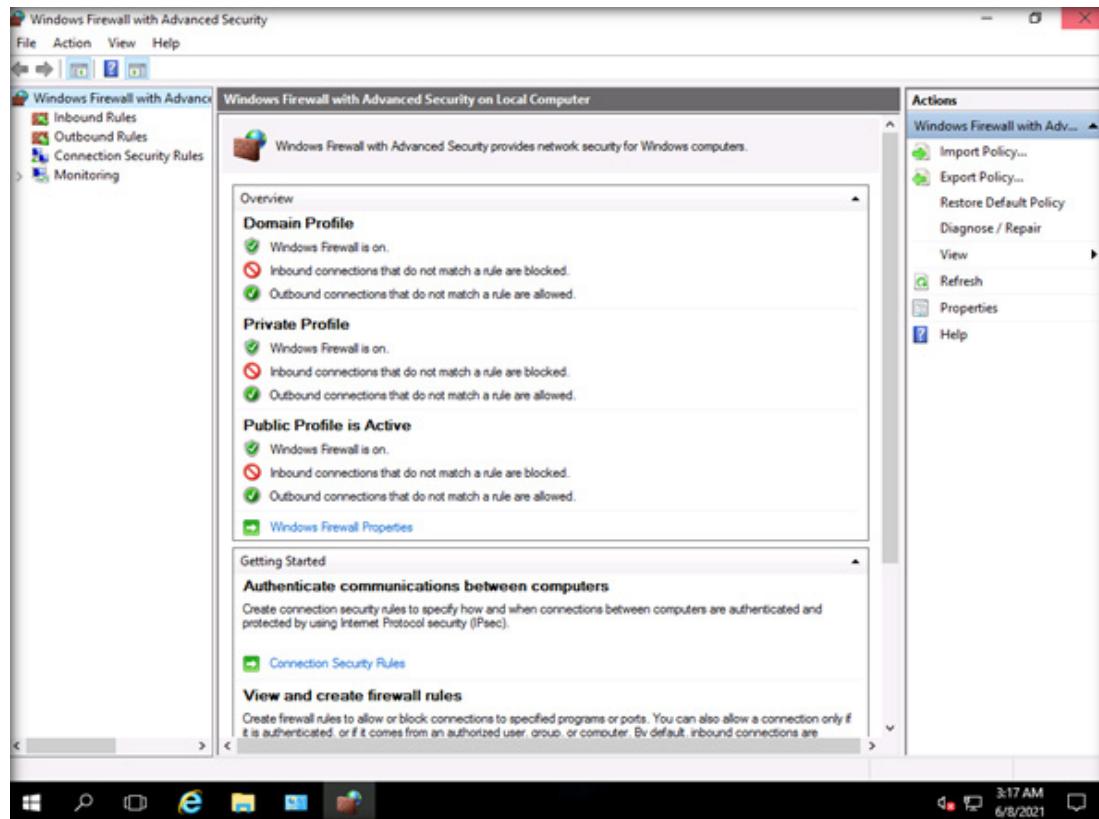
16. The **Windows Defender Firewall** is turned on for **Domain**, **Private**, and **Guest or Public** network settings as shown in the screenshot below.



EXERCISE 2:
IMPLEMENT HOST-BASED FIREWALL FUNCTIONALITY USING WINDOWS FIREWALL

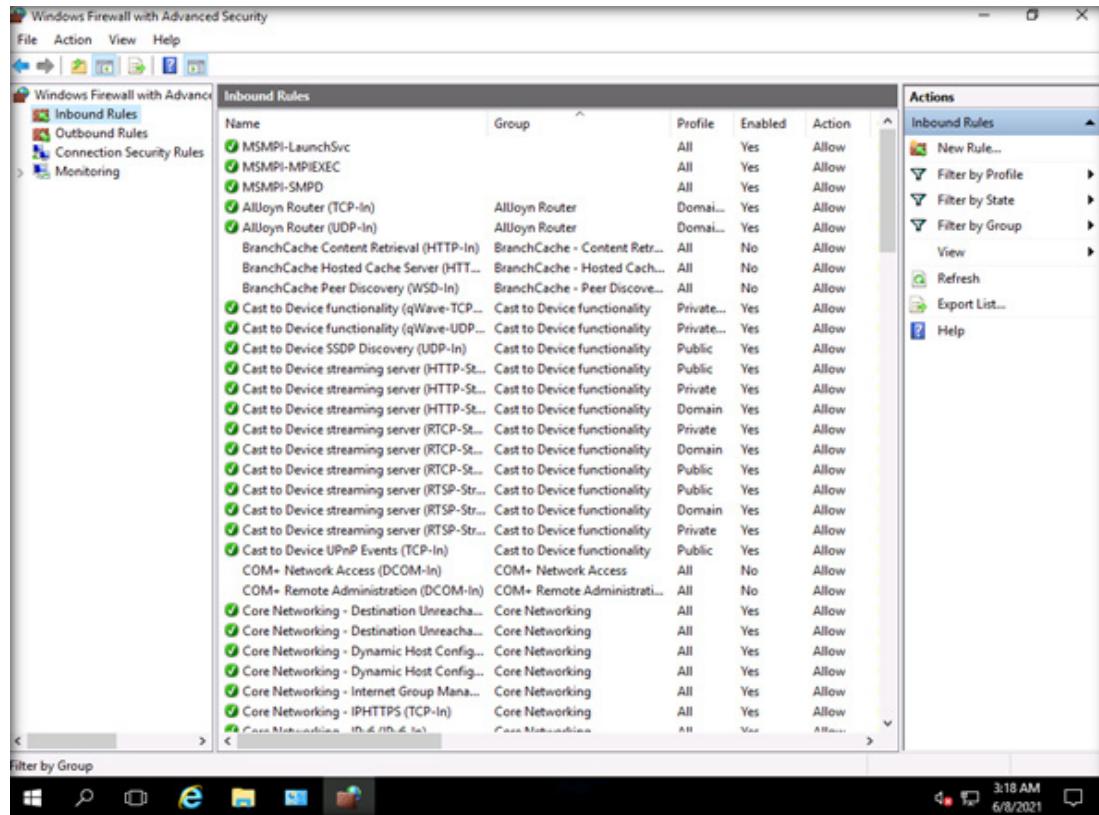
17. Click Advanced Settings in the left pane. The Windows Firewall with Advanced Security window opens.

EXERCISE 2: IMPLEMENT HOST-BASED FIREWALL FUNCTIONALITY USING WINDOWS FIREWALL



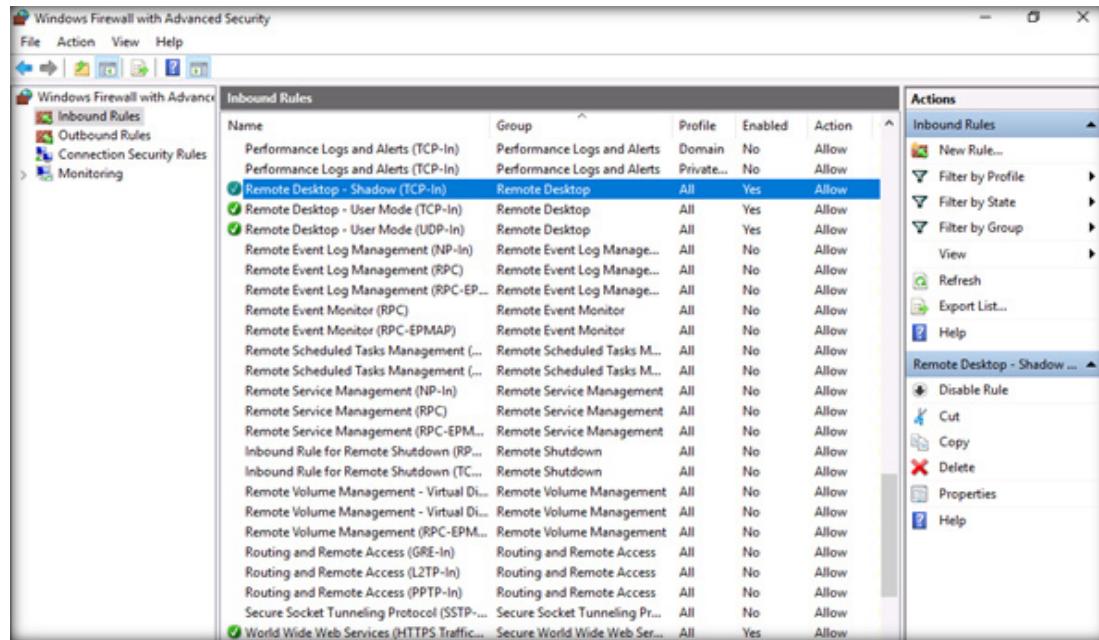
18. Click **Inbound Rules** option in the left side pane. The list of rules appears.

EXERCISE 2: IMPLEMENT HOST-BASED FIREWALL FUNCTIONALITY USING WINDOWS FIREWALL



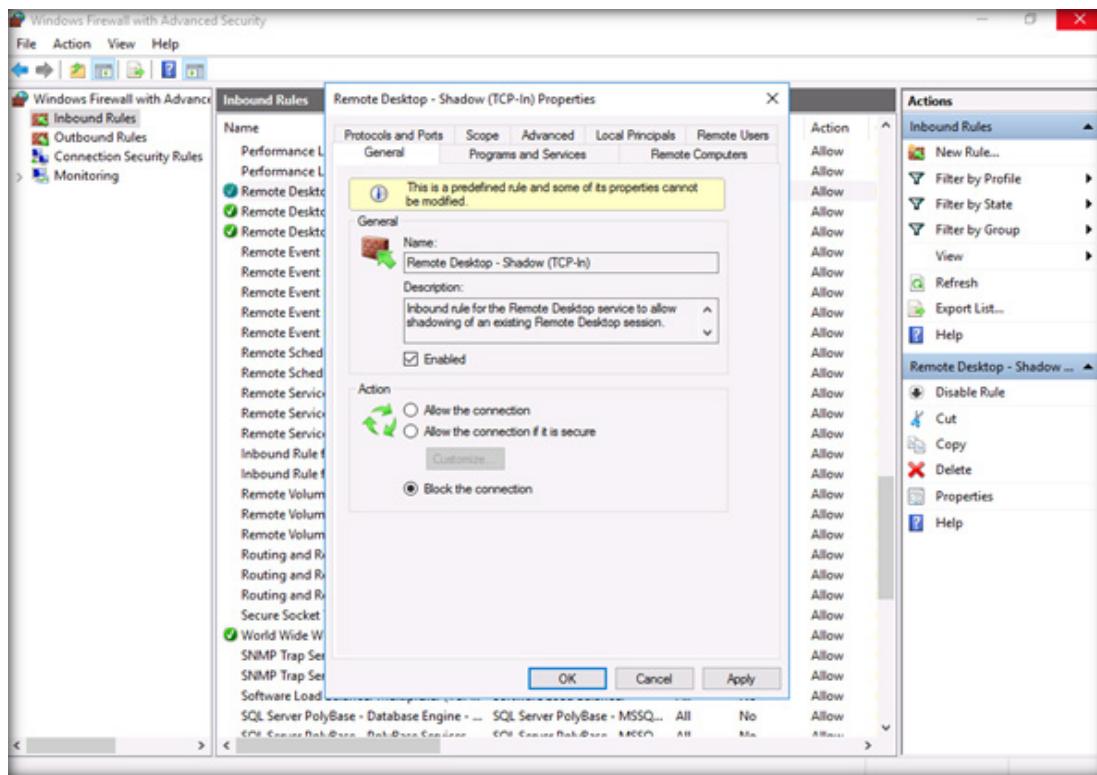
19. Search for **Remote Desktop- Shadow (TCP-In)** and double-click.

EXERCISE 2:
IMPLEMENT HOST-BASED FIREWALL FUNCTIONALITY USING WINDOWS FIREWALL



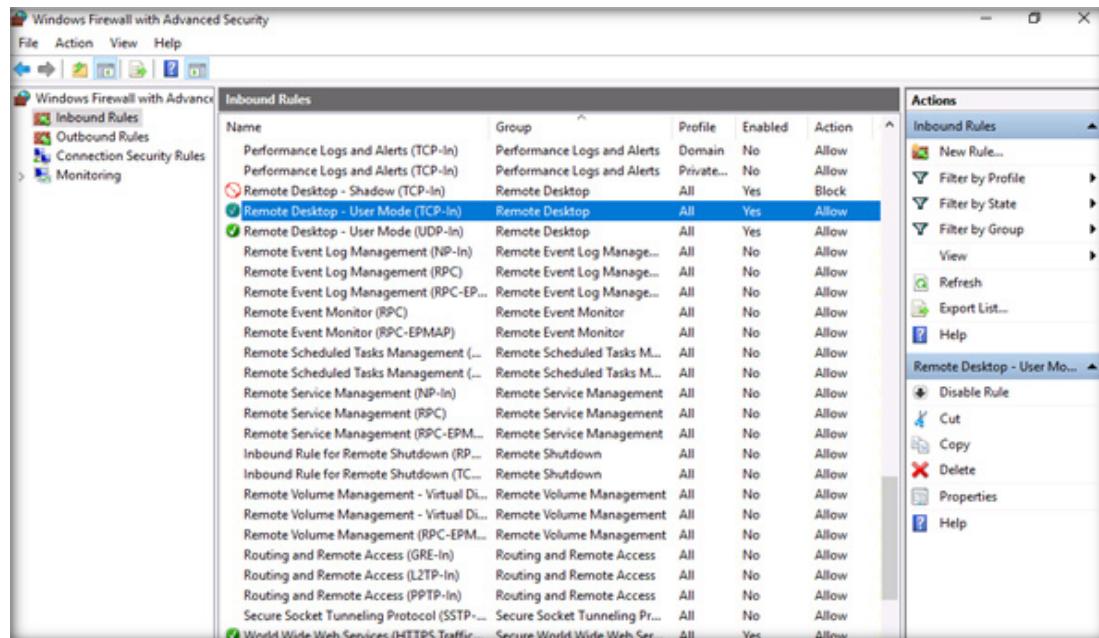
20. The **Remote Desktop- Shadow (TCP-in) Properties** window opens. Check radio button **Block the connection** and click **OK**.

EXERCISE 2:
IMPLEMENT HOST-BASED FIREWALL FUNCTIONALITY USING WINDOWS FIREWALL



EXERCISE 2: IMPLEMENT HOST-BASED FIREWALL FUNCTIONALITY USING WINDOWS FIREWALL

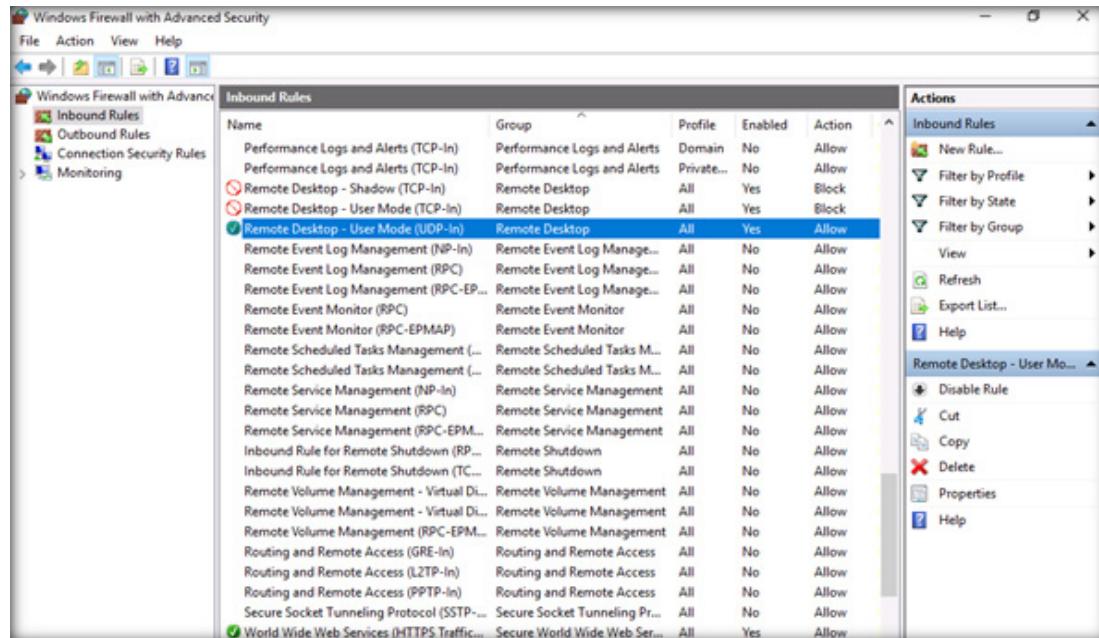
21. Next, search for **Remote Desktop- User Mode (TCP-In)** and double-click.



22. The **Remote Desktop- User Mode (TCP-in)** Properties window opens. Check radio button **Block the connection** and click **OK**.

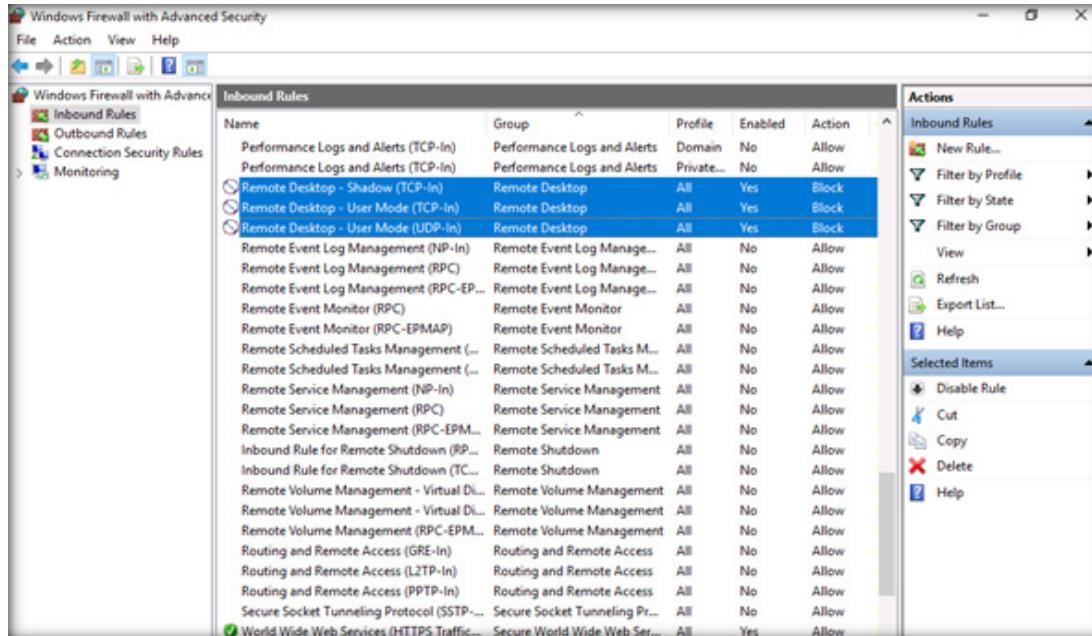
23. Next, search for **Remote Desktop- User Mode (UDP-In)** and double-click.

EXERCISE 2:
IMPLEMENT HOST-BASED FIREWALL FUNCTIONALITY USING WINDOWS FIREWALL



24. The **Remote Desktop- User Mode (UDP-in)** Properties window opens. Check radio button **Block the connection** and click **OK**.

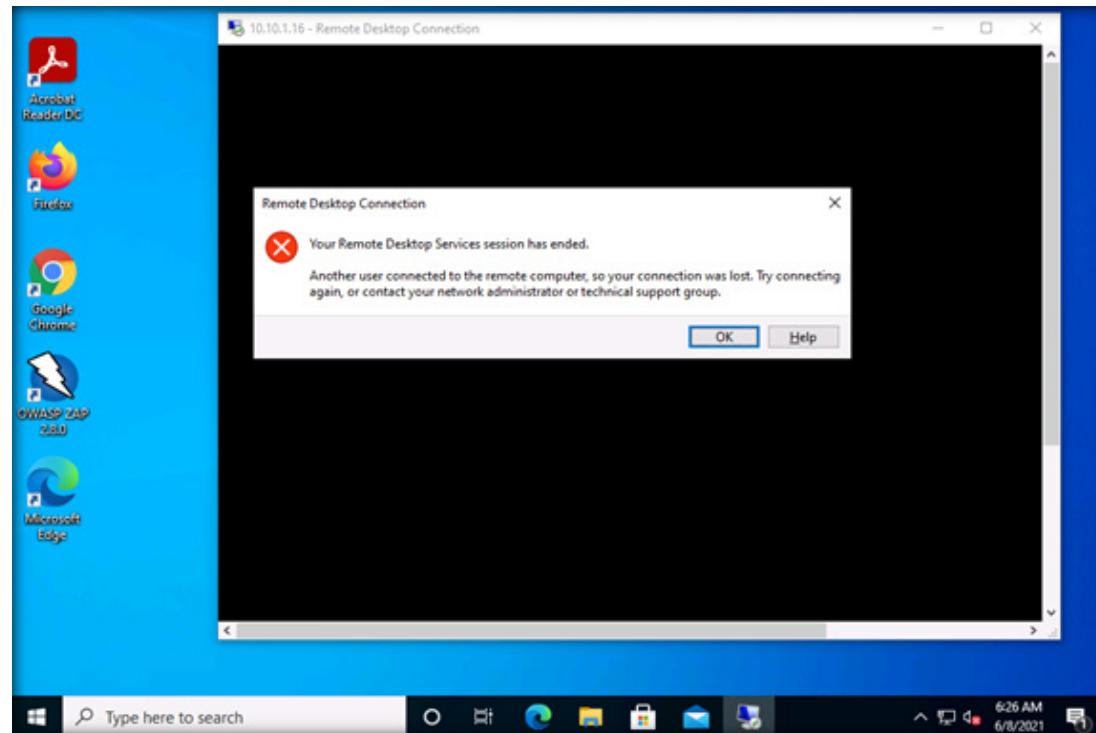
25. Now, we have blocked Remote Desktop inbound connections. Let us verify this.



EXERCISE 2: IMPLEMENT HOST-BASED FIREWALL FUNCTIONALITY USING WINDOWS FIREWALL

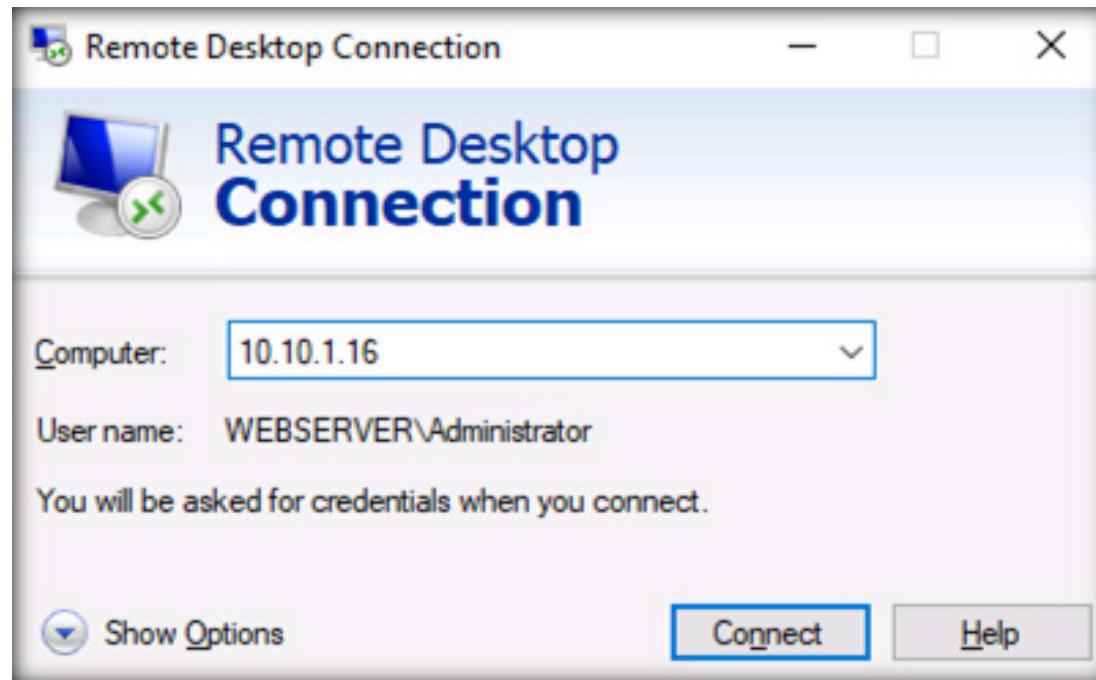
26. Close all open windows.
27. Switch back to the **Admin Machine-1** virtual machine.
28. The previous session will end. Click **OK**.

EXERCISE 2:
**IMPLEMENT HOST-BASED
FIREWALL FUNCTIONALITY
USING WINDOWS
FIREWALL**



29. Next, try to access **Web Server** machine remotely. Type the **10.10.1.16** IP address of the **Web Server** machine in opened Remote Desktop connection window and click **Connect**.

EXERCISE 2:
IMPLEMENT HOST-BASED FIREWALL FUNCTIONALITY USING WINDOWS FIREWALL

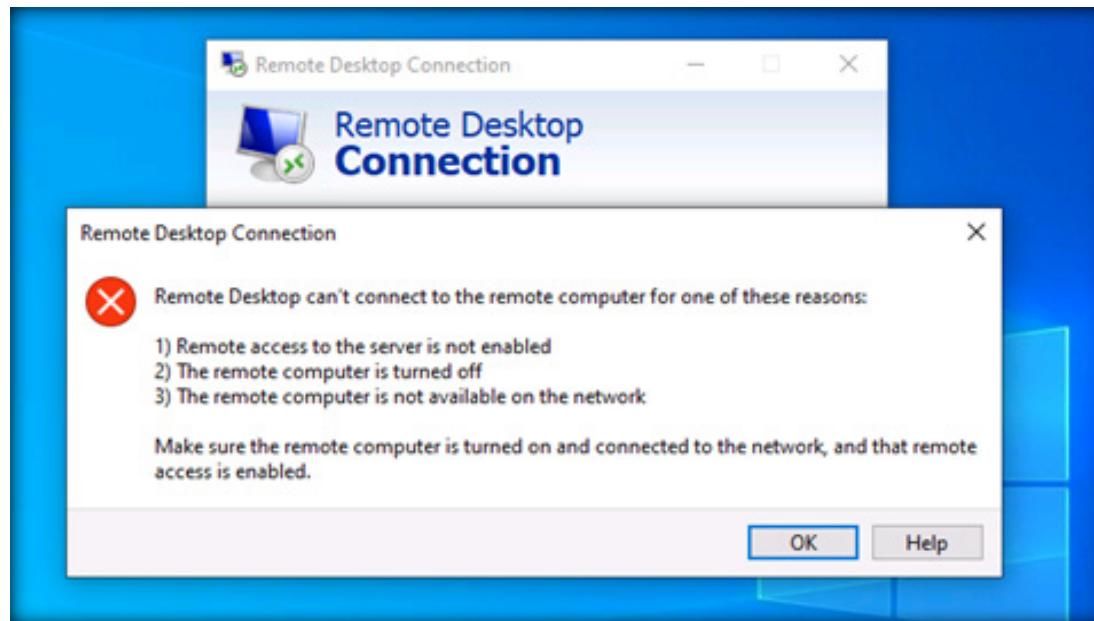


30. This time, you will not be able to connect the Remote Desktop for **10.10.1.16**.

31. The host-based Windows firewall on host **10.10.1.16** will not allow the other host (Admin Machine-1) to communicate with unchecked programs listed in the allowed app of the firewall in Web Server host (**10.10.1.16**).

32. You will get the error message shown in the screenshot below.

EXERCISE 2:
**IMPLEMENT HOST-BASED
FIREWALL FUNCTIONALITY
USING WINDOWS
FIREWALL**



33. Close the **Remote Desktop Connection** window. Now we will try to connect to Web Server using FTP connection.

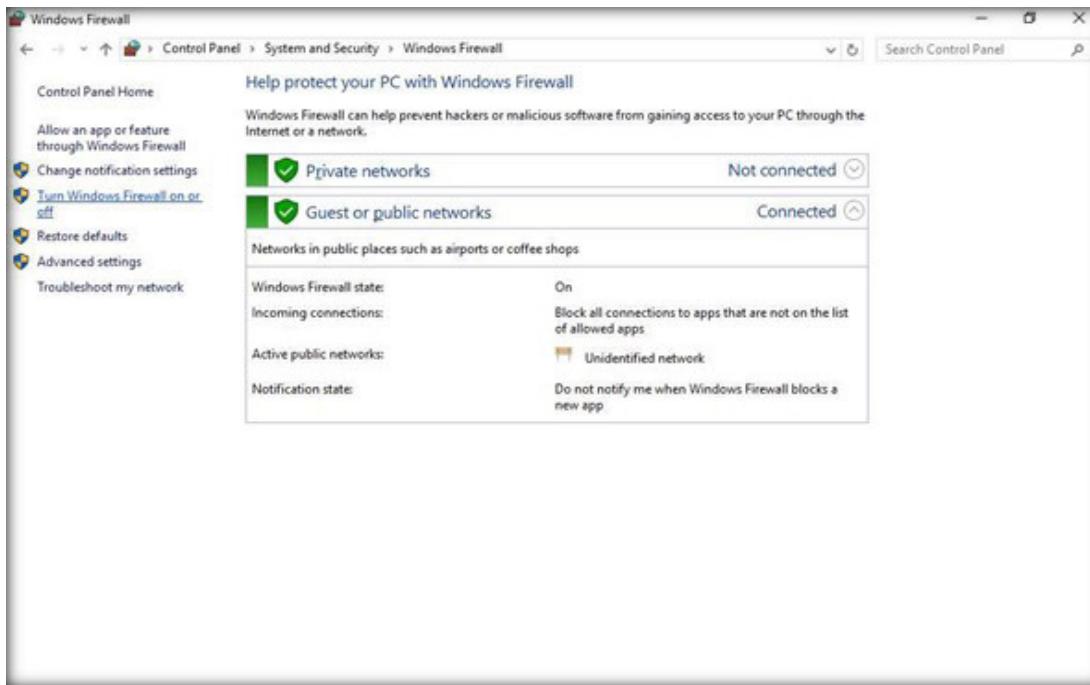
34. Switch to the **Web Server** virtual machine.

35. Open **Control Panel**.

36. Click the **System and Security** option.

37. The **System and Security** windows will appear. Click **Windows Firewall**.

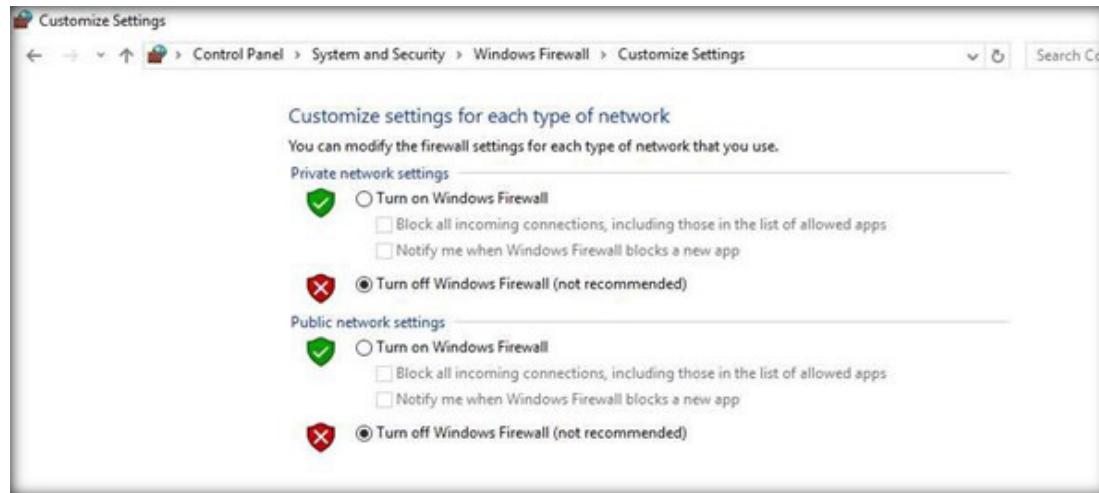
38. The Windows Firewall window opens. Click Turn Windows Firewall on or off.



EXERCISE 2: IMPLEMENT HOST-BASED FIREWALL FUNCTIONALITY USING WINDOWS FIREWALL

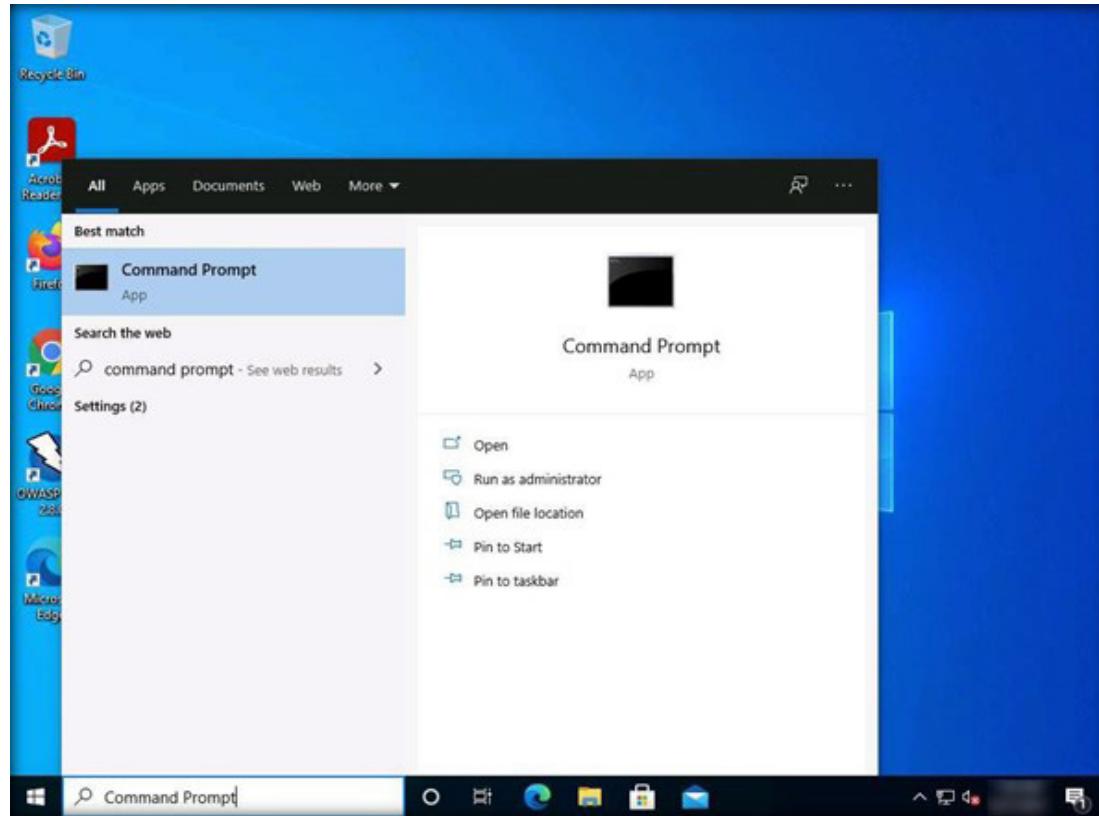
39. In the **Customize Settings** window select **Turn off Windows Firewall** under Private and Public networks and click **OK**.

EXERCISE 2:
IMPLEMENT HOST-BASED
FIREWALL FUNCTIONALITY
USING WINDOWS
FIREWALL

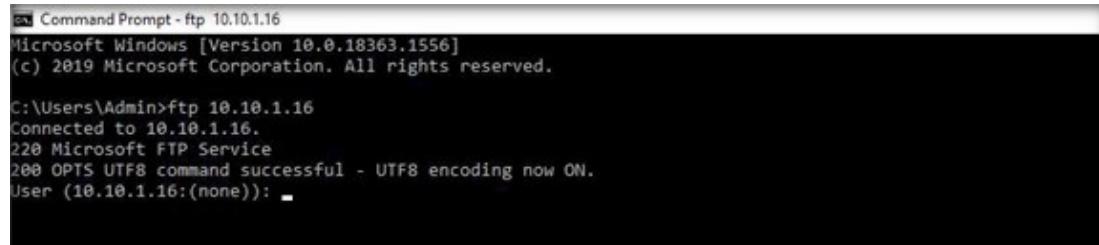


40. Close all open windows.
41. Switch to the **Admin Machine-1** virtual machine.
42. Navigate to the **Windows Start** menu, type **Command Prompt**, and press **Enter** to open a Command Prompt window.

EXERCISE 2:
**IMPLEMENT HOST-BASED
FIREWALL FUNCTIONALITY
USING WINDOWS
FIREWALL**



43. In the **Command Prompt** window type **ftp 10.10.1.16**. It will ask for Username and Password for Login.



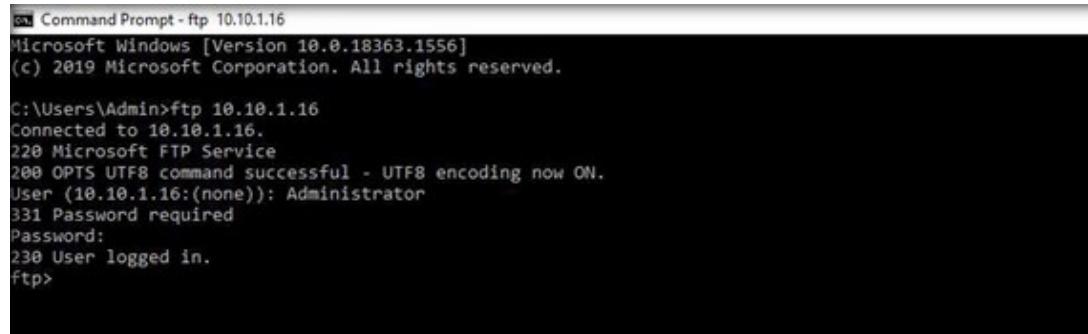
```
Command Prompt - ftp 10.10.1.16
Microsoft Windows [Version 10.0.18363.1556]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Admin>ftp 10.10.1.16
Connected to 10.10.1.16.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (10.10.1.16:(none)): -
```

EXERCISE 2:
IMPLEMENT HOST-BASED
FIREWALL FUNCTIONALITY
USING WINDOWS
FIREWALL

44. Enter **Administrator** in the User field and **admin@123** in the Password field to login to ftp. You will be successfully logged in to ftp.

EXERCISE 2:
IMPLEMENT HOST-BASED
FIREWALL FUNCTIONALITY
USING WINDOWS
FIREWALL

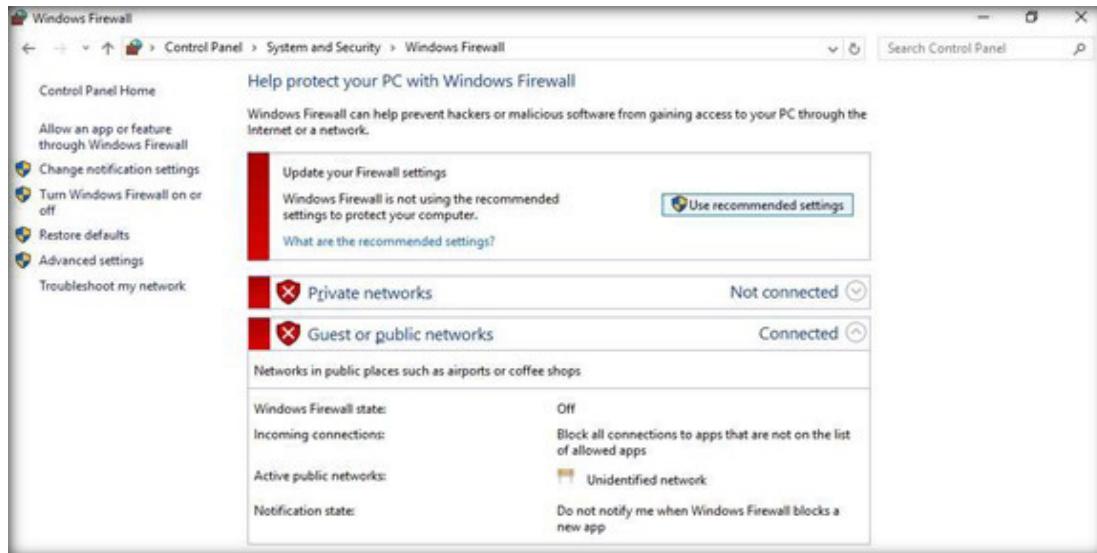


```
Command Prompt - ftp 10.10.1.16
Microsoft Windows [Version 10.0.18363.1556]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Admin>ftp 10.10.1.16
Connected to 10.10.1.16.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (10.10.1.16:(none)): Administrator
331 Password required
Password:
230 User logged in.
ftp>
```

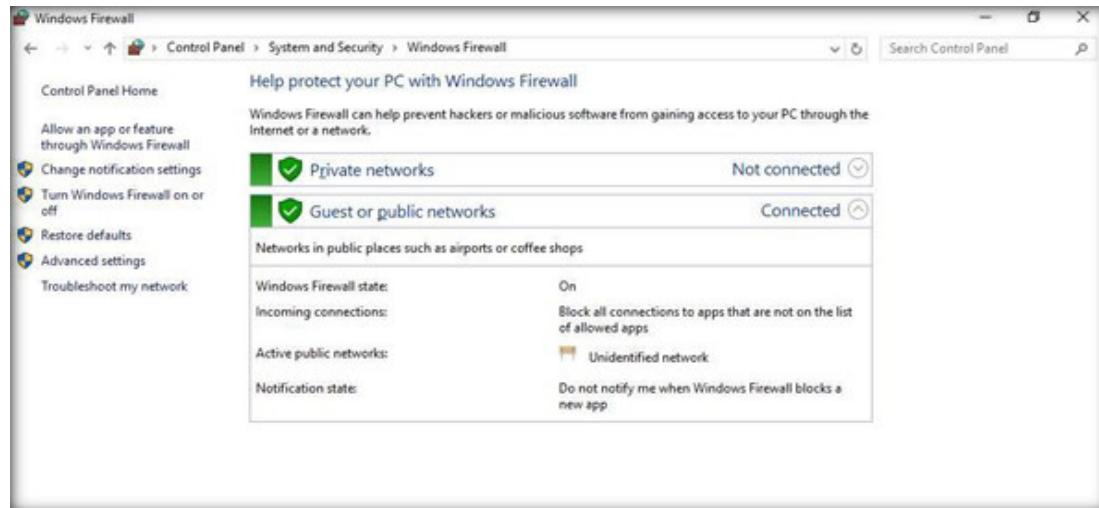
45. Close the **Command Prompt** window.
46. Switch to the **Web Server** virtual machine.
47. Open **Control Panel**.
48. Click the **System and Security** option.
49. The **System and Security** windows will appear. Click **Windows Firewall**.

50. The Windows Firewall window opens. Click **Use recommended settings**.



EXERCISE 2: IMPLEMENT HOST-BASED FIREWALL FUNCTIONALITY USING WINDOWS FIREWALL

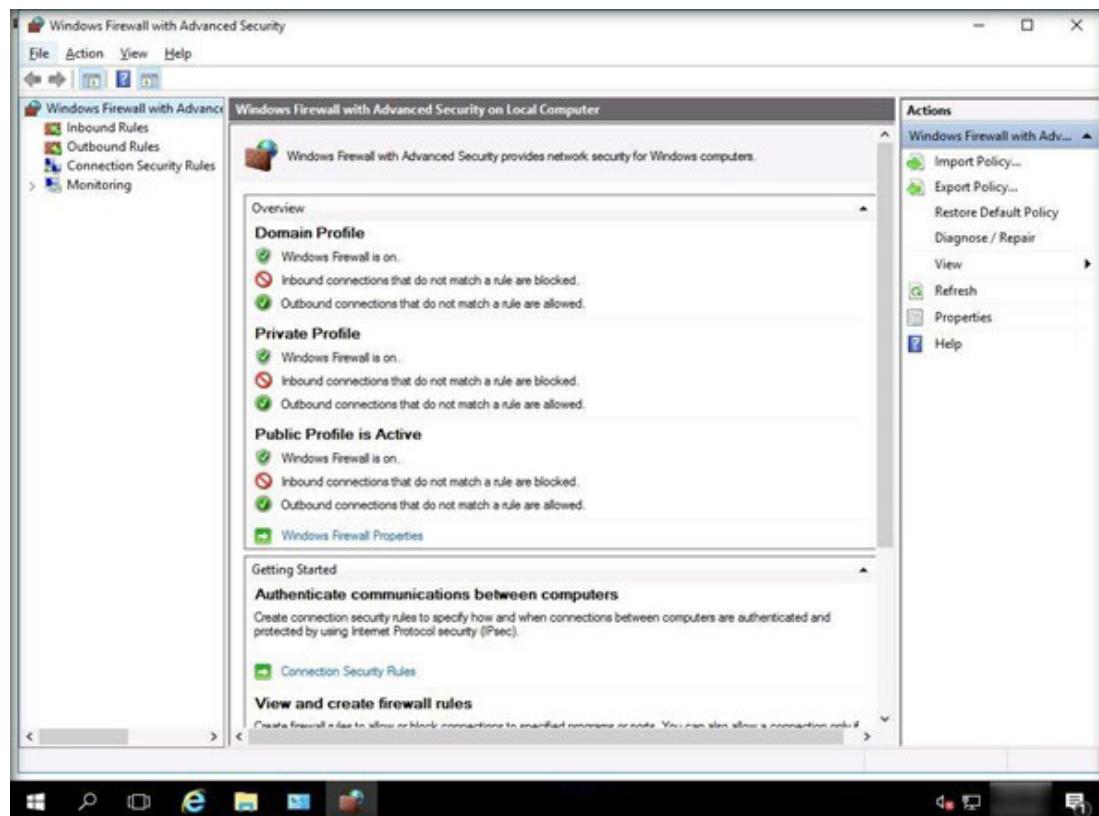
51. The Windows Defender Firewall is turned on for Domain, Private, and Guest or Public network settings as shown in the screenshot below.



**EXERCISE 2:
IMPLEMENT HOST-BASED
FIREWALL FUNCTIONALITY
USING WINDOWS
FIREWALL**

52. Click Advanced Settings in the left pane. The Windows Firewall with Advanced Security window opens.

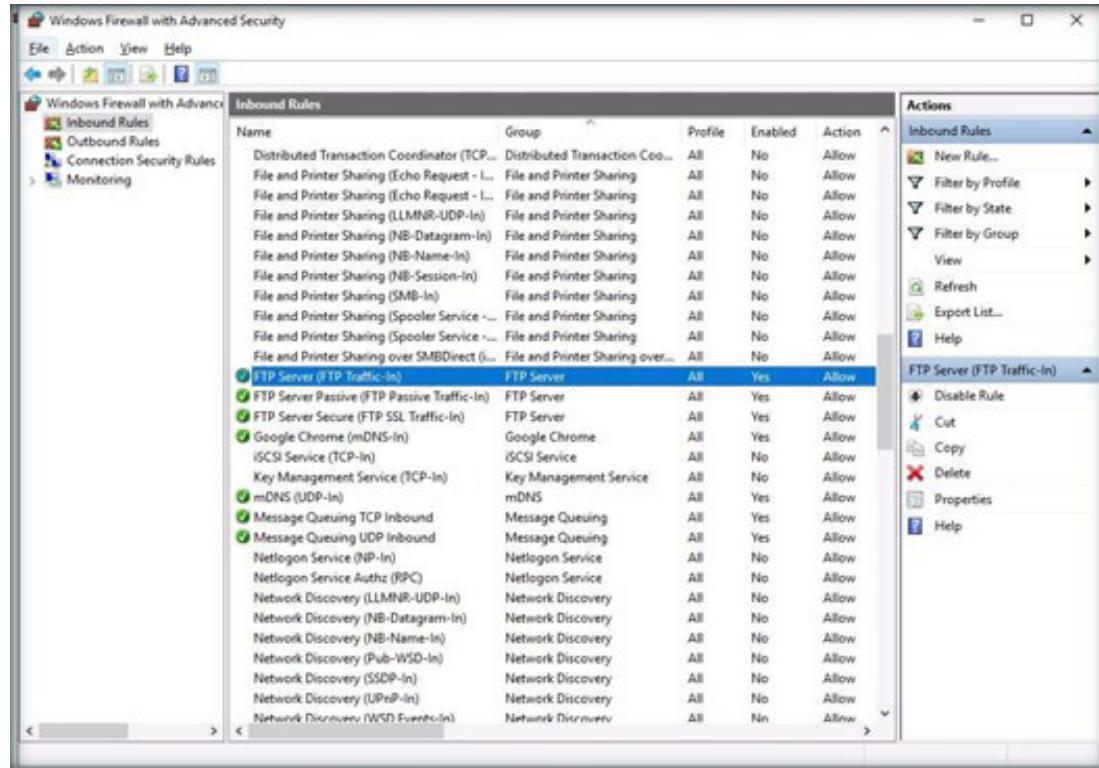
EXERCISE 2: IMPLEMENT HOST-BASED FIREWALL FUNCTIONALITY USING WINDOWS FIREWALL



53. Click **Inbound Rules** option in the left side pane. The list of rules appears.

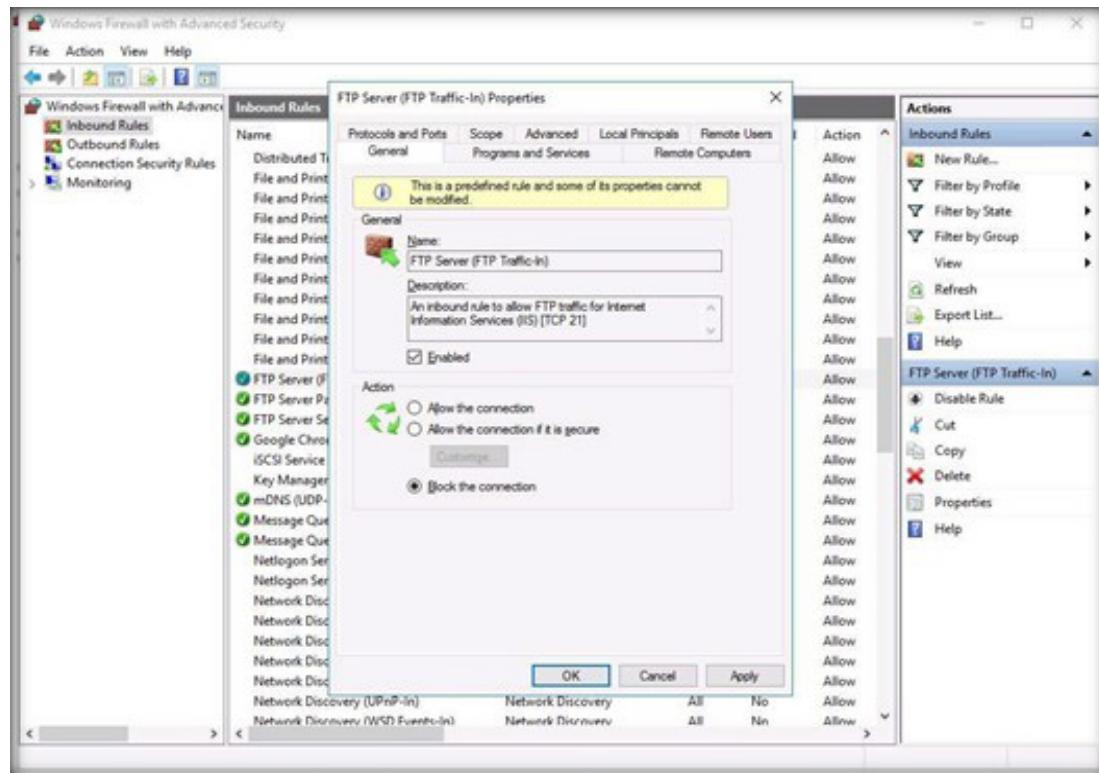
54. Search for **FTP Server (FTP Traffic-In)** and double-click.

EXERCISE 2: IMPLEMENT HOST-BASED FIREWALL FUNCTIONALITY USING WINDOWS FIREWALL



EXERCISE 2:
**IMPLEMENT HOST-BASED
FIREWALL FUNCTIONALITY
USING WINDOWS
FIREWALL**

55. The **FTP Server (FTP Traffic-In)** Properties window opens. Check radio button **Block the connection** and click **OK**.



56. Next, search for **FTP Server Passive (FTP Passive Traffic-In)** and double-click.

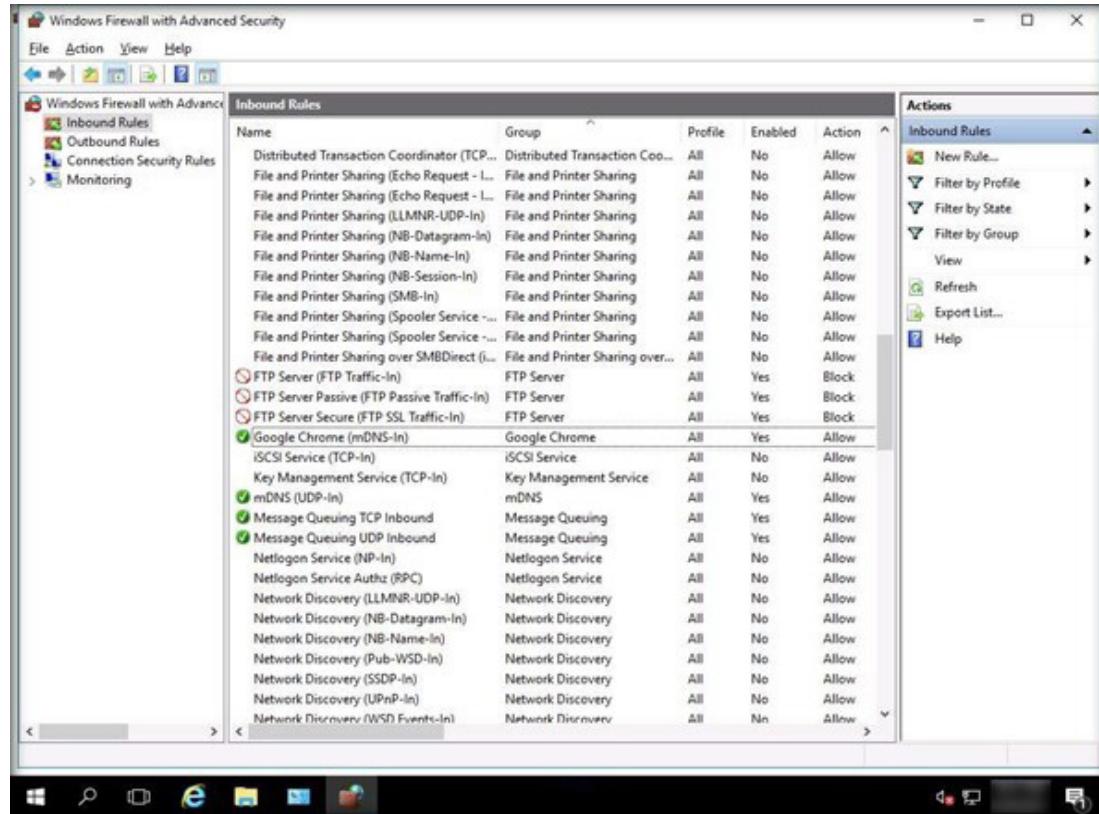
57. The **FTP Server Passive (FTP Passive Traffic-In) Properties** window opens. Check radio button **Block the connection** and click **OK**.

58. Next, search for **FTP Server Secure (FTP SSL Traffic-In)** and double-click.

59. The **FTP Server Secure (FTP SSL Traffic-In) Properties** window opens. Check radio button **Block the connection** and click **OK**.

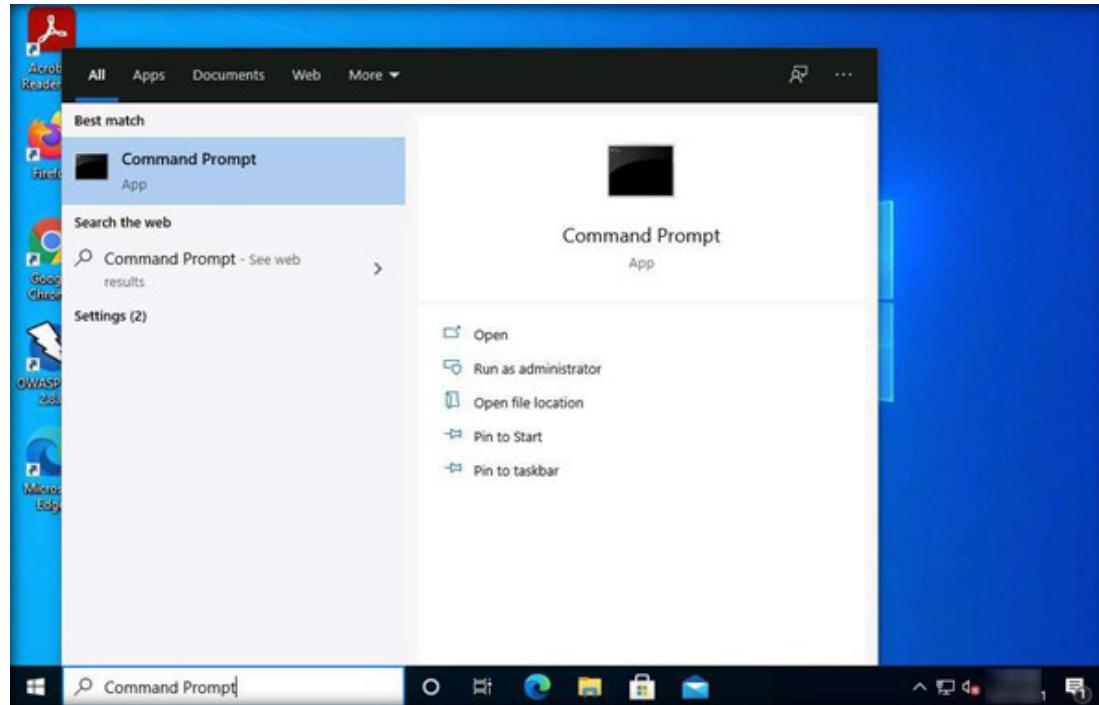
60. Now, we have blocked FTP inbound connection. Let us verify this.

EXERCISE 2:
IMPLEMENT HOST-BASED FIREWALL FUNCTIONALITY USING WINDOWS FIREWALL



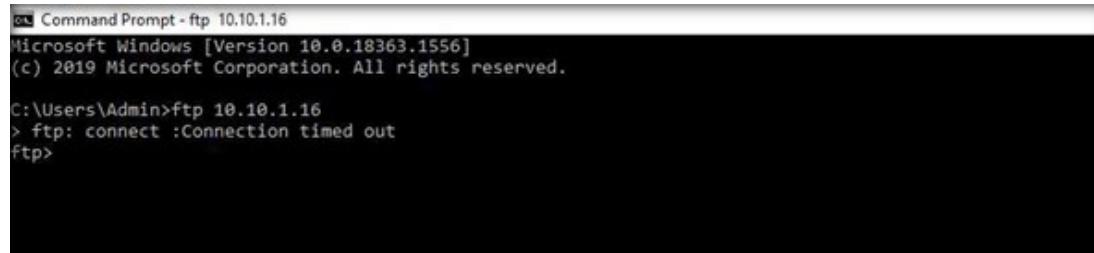
61. Close all open windows.
62. Switch to the **Admin Machine-1** virtual machine.
63. Navigate to the **Windows Start** menu, type **Command Prompt**, and press **Enter** to open a Command Prompt window.

EXERCISE 2:
**IMPLEMENT HOST-BASED
FIREWALL FUNCTIONALITY
USING WINDOWS
FIREWALL**



64. In the **Command Prompt** window type **ftp 10.10.1.16**, We will get **Connection timed out** error message.

Note: It might take a while for the error message to appear.



```
Command Prompt - ftp 10.10.1.16
Microsoft Windows [Version 10.0.18363.1556]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Admin>ftp 10.10.1.16
> ftp: connect :Connection timed out
Ftp>
```

EXERCISE 2:

IMPLEMENT HOST-BASED FIREWALL FUNCTIONALITY USING WINDOWS FIREWALL

65. We have successfully blocked the FTP connection to **Web Server**.

66. Switch to the Web Server virtual machine. Navigate to **Control Panel > System and Security > Windows Firewall** and follow **step 53 to step 60** and click on **Allow the connection** in the **FTP Server (FTP Traffic-In) Properties**, **FTP Server Passive (FTP Passive Traffic-IN) Properties** and **FTP Server Secure (FTP SSL Traffic-In)** Properties windows.

67. Follow **steps 35 to step 40** to turn off the firewall in **Web Server** virtual machine.

68. Close all open windows.

EXERCISE 3: IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK UNWANTED WEBSITE ACCESS USING PFSENSE FIREWALL

The pfSense firewall/router is the world's most trusted open-source network security solution software.

LAB SCENARIO

To prevent users from visiting malicious websites and to secure against phishing attacks, security professionals must block known malicious websites and protect the network from various viruses and malware. As a security measure organizations need to prevent employees from accessing unwanted websites for employees.

LAB OBJECTIVE

The lab will demonstrate how to use the pfSense firewall alias to block access to unwanted websites. If we implement one rule per host, the number of rules will be greater and more difficult to manage. Using an alias for multiple hosts requires the use of only one rule.

OVERVIEW OF PFSENSE FIREWALL

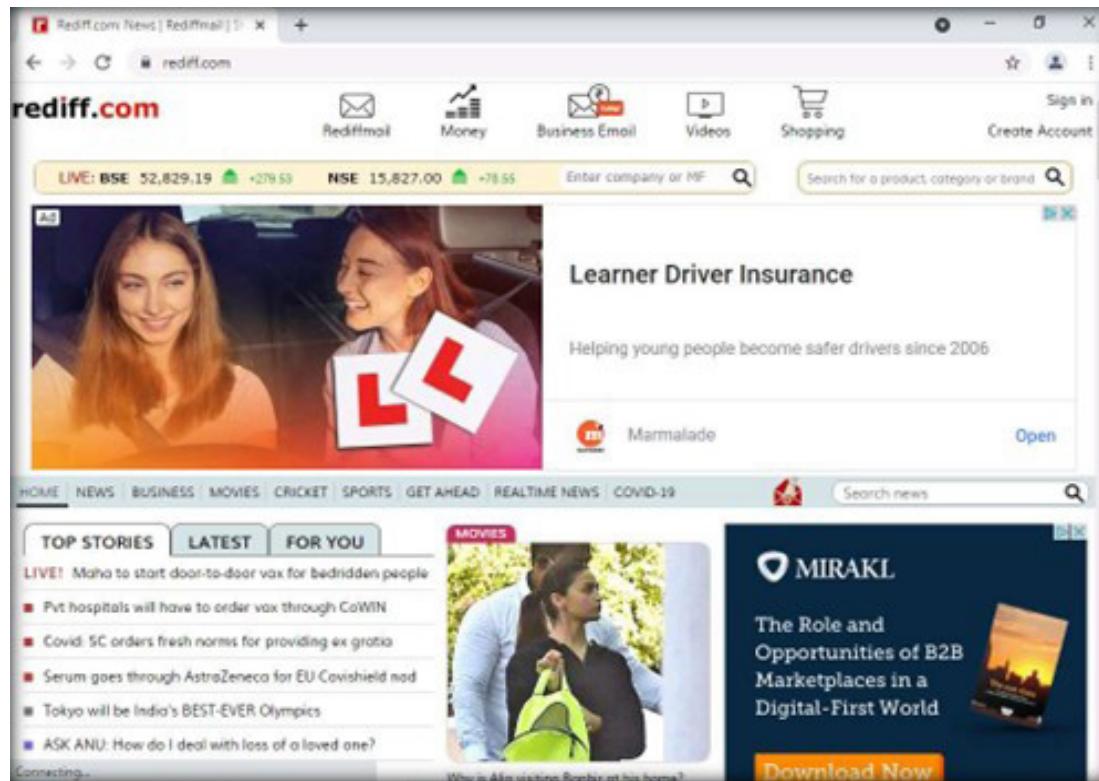
pfSense is a free, open-source Operating System that functions like a firewall, intrusion detection system, and router. Firewall features are integrated into pfSense, and it contains basic firewall rules and firewall logs. A security professional can use the pfSense firewall to manage network security easily.

Aliases act as placeholders for real hosts, networks, or ports and help in reducing the number of changes required when the host, network, or port changes. The name of an alias can be used instead of specifying the host, network, or port for defining firewall rules.

LAB TASKS

Note: Ensure that **Admin Machine-1**, **Web Server** and **PfSense Firewall** virtual machines are running.

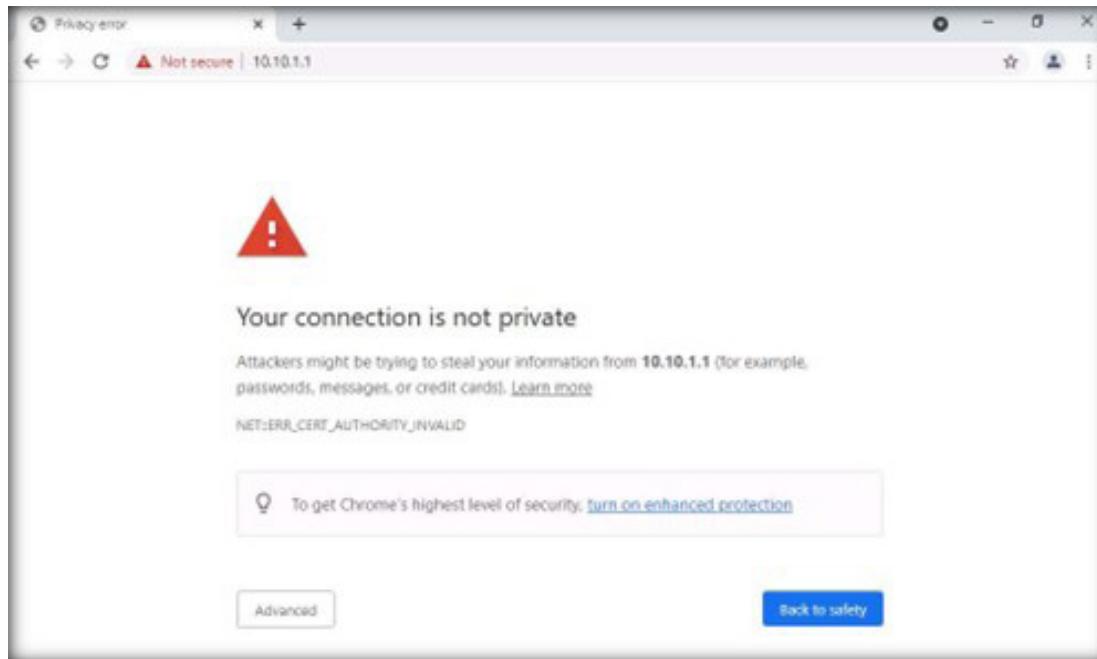
- EXERCISE 3:
IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK UNWANTED WEBSITE ACCESS USING PFSENSE FIREWALL
1. Turn on the **AD Domain Controller** virtual machine.
 2. Login with the credentials **CCT\Administrator** and **admin@123**.
Note: If the network screen appears, click **Yes**.
 3. Switch to the **Admin Machine-1** virtual machine.
 4. Open the **Google Chrome** browser, and type **www.rediff.com** and press **Enter**, the rediff.com website opens.



5. Close the browser. This infers that the www.rediff.com website is accessible to users. You can block access to this website using the pfSense firewall as follows.

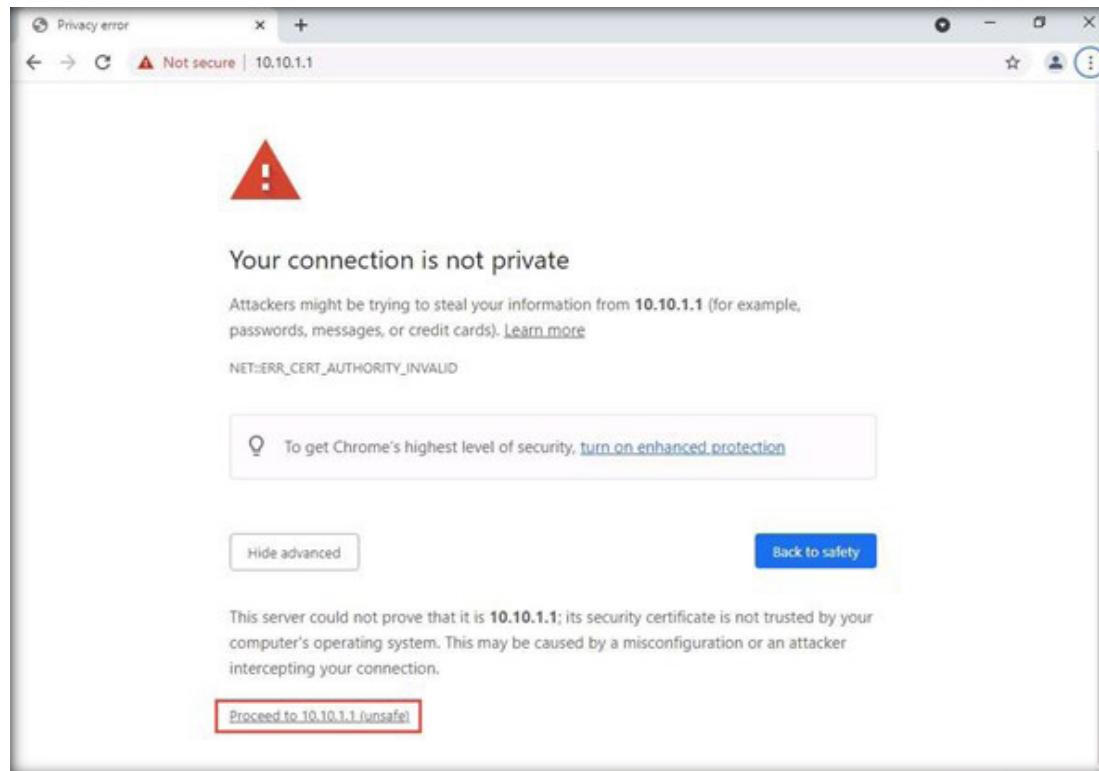
6. Open the **Google Chrome** browser, and type **https://10.10.1.1** and press **Enter** to access the web interface of pfSense.

EXERCISE 3: IMPLEMENT NETWORK- BASED FIREWALL FUNCTIONALITY: BLOCK UNWANTED WEBSITE ACCESS USING PFSENSE FIREWALL



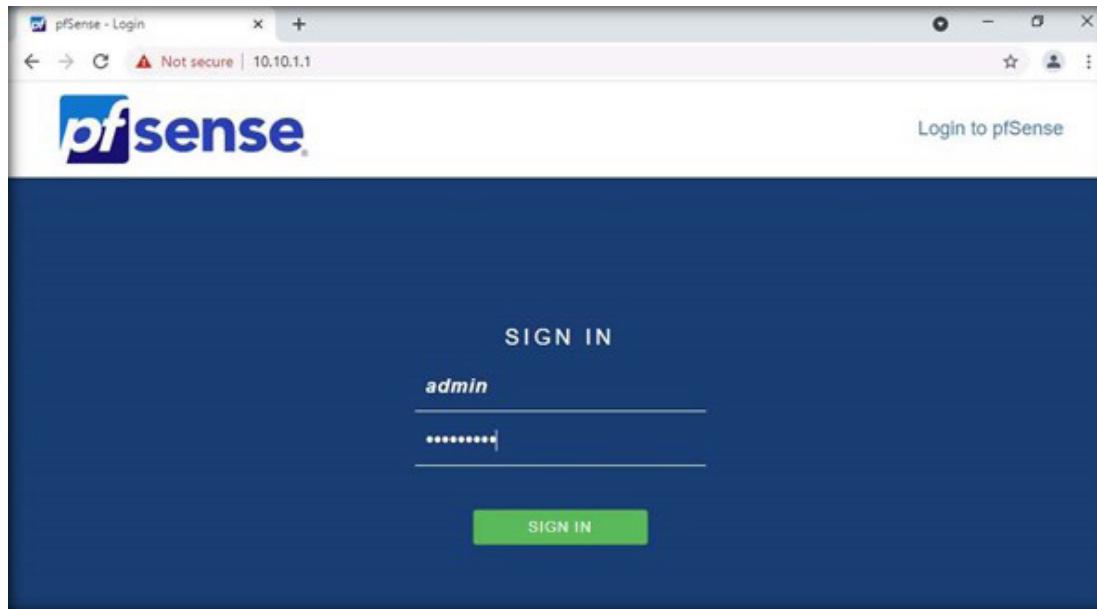
7. The privacy error shows. Click **Advanced** button and click on **Proceed to 10.10.1.1 (unsafe)** link.

EXERCISE 3: IMPLEMENT NETWORK- BASED FIREWALL FUNCTIONALITY: BLOCK UNWANTED WEBSITE ACCESS USING PFSENSE FIREWALL



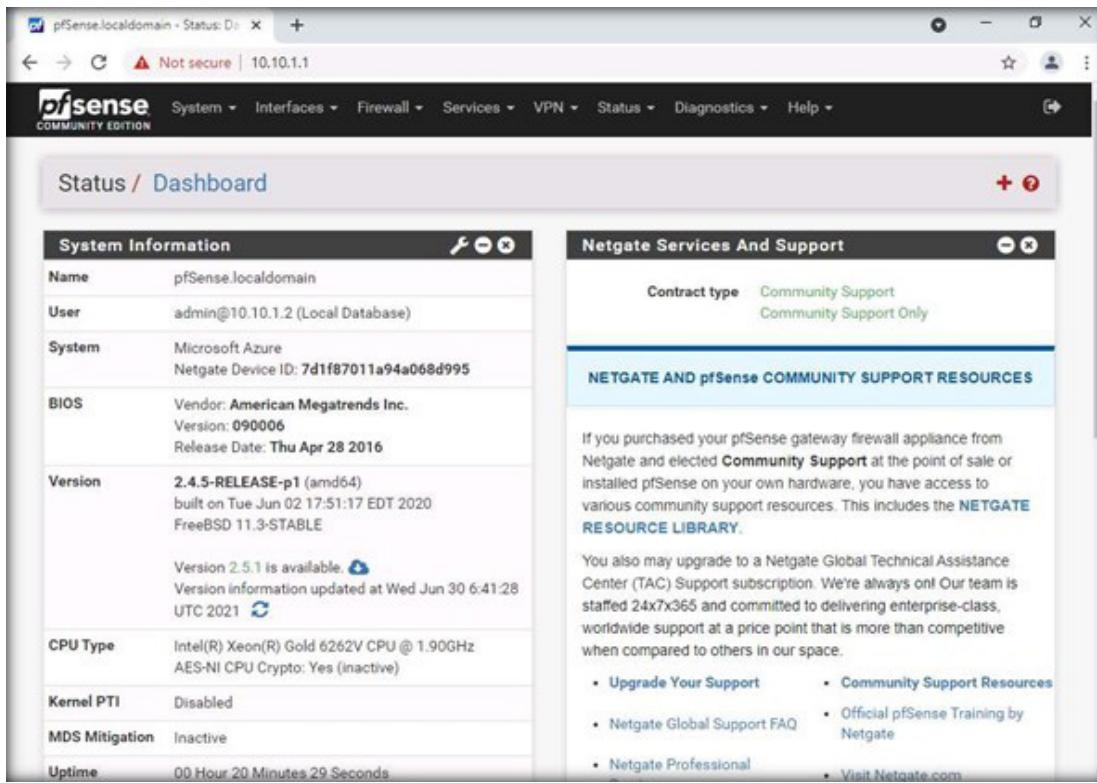
8. The login page appears, use the Username as **admin** and Password as **admin@123**. Click **SIGN IN**.

EXERCISE 3:
**IMPLEMENT NETWORK-
BASED FIREWALL
FUNCTIONALITY: BLOCK
UNWANTED WEBSITE ACCESS
USING PFSENSE FIREWALL**



9. The pfSense home page will appear, as shown in the screenshot below.

EXERCISE 3: IMPLEMENT NETWORK- BASED FIREWALL FUNCTIONALITY: BLOCK UNWANTED WEBSITE ACCESS USING PFSENSE FIREWALL



The screenshot shows the pfSense Status / Dashboard page. On the left, there is a System Information panel displaying the following details:

System Information	
Name	pfSense.localdomain
User	admin@10.10.1.2 (Local Database)
System	Microsoft Azure Netgate Device ID: 7d1f87011a94a068d995
BIOS	Vendor: American Megatrends Inc. Version: 090006 Release Date: Thu Apr 28 2016
Version	2.4.5-RELEASE-p1 (amd64) built on Tue Jun 02 17:51:17 EDT 2020 FreeBSD 11.3-STABLE
CPU Type	Intel(R) Xeon(R) Gold 6262V CPU @ 1.90GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	00 Hour 20 Minutes 29 Seconds

On the right, there is a Netgate Services And Support panel showing the following information:

Netgate Services And Support	
Contract type	Community Support Community Support Only

Below these panels, there is a section titled "NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES" containing the following text and links:

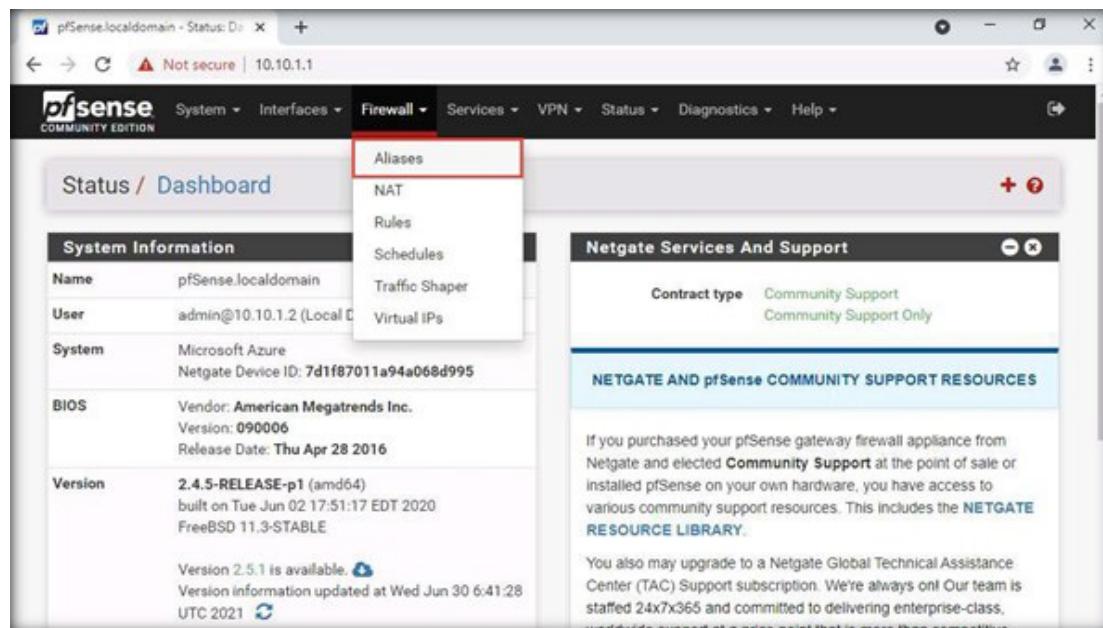
If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the [NETGATE RESOURCE LIBRARY](#).

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

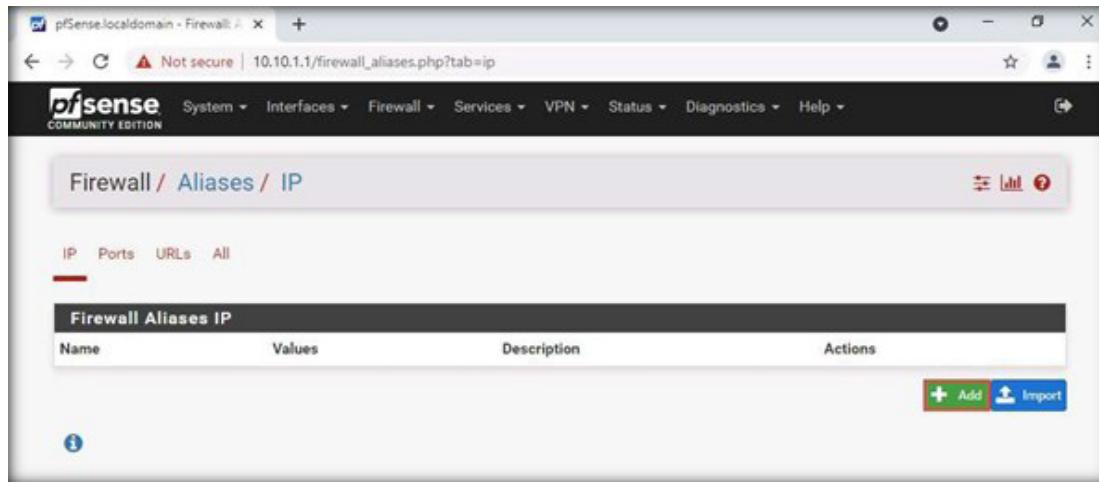
- Upgrade Your Support
- Netgate Global Support FAQ
- Netgate Professional
- Community Support Resources
- Official pfSense Training by Netgate
- Visit [Netgate.com](#)

10. Navigate to the **Firewall > Aliases** option menu from the main menu to add the list of websites for restricting access.

EXERCISE 3: IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK UNWANTED WEBSITE ACCESS USING PFSENSE FIREWALL



11. The **Firewall/ Aliases/ IP** page will appear. Click on the **Add** button.



The screenshot shows the pfSense Firewall / Aliases / IP configuration page. The browser title is "pfSense.localdomain - Firewall: /". The URL is "10.10.1.1/firewall_aliases.php?tab=ip". The pfSense logo is visible in the top left. The main header says "Firewall / Aliases / IP". Below it, there are tabs: IP (selected), Ports, URLs, and All. A table titled "Firewall Aliases IP" is displayed with columns: Name, Values, Description, and Actions. At the bottom right of the table area, there is a green "Add" button with a plus sign and a blue "Import" button with a downward arrow. A small blue info icon is located at the bottom left of the table area.

EXERCISE 3: IMPLEMENT NETWORK- BASED FIREWALL FUNCTIONALITY: BLOCK UNWANTED WEBSITE ACCESS USING PFSENSE FIREWALL

12. Next, we will check the domain IP address of (www.rediff.com) website to block. Minimize the browser.

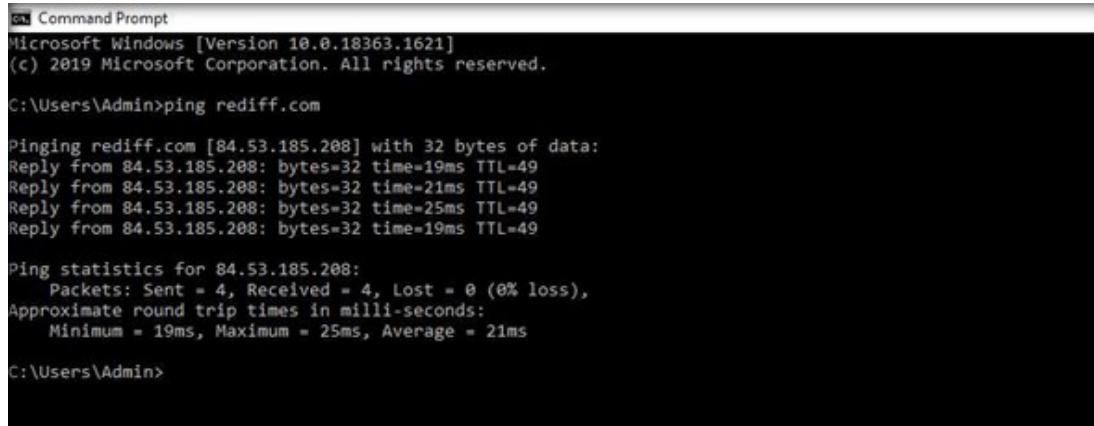
13. To check the domain address of rediff.com, we need to ping the domain. To open the command prompt, type **cmd** in the windows search option and click **Command Prompt** app.

14. The **Command Prompt** will appear. To ping the domain name, type the command **ping rediff.com**, and press **Enter** as shown in the below screenshot.

15. The result of ping **rediff.com** shows the IP address of the **rediff.com** server. Note down the **IP address** to include it in the aliases list of pfSense firewall.

Note: Ensure that you have added all IP addresses related to **rediff.com**. As, sometimes, one domain name might have multiple IP addresses and these IP addresses are changed timely. Similarly, you can also add other unwanted hosts also within the alias.

Note: IP address may differ from the one shown in the above screenshot. Ensure that you have noted all IP addresses related to **rediff.com**. As, sometimes, one domain name might have multiple IP addresses.



```
Windows PowerShell
Copyright © Microsoft Corporation. All rights reserved.

PS C:\Users\Admin> ping rediff.com

Pinging rediff.com [84.53.185.208] with 32 bytes of data:
Reply from 84.53.185.208: bytes=32 time=19ms TTL=49
Reply from 84.53.185.208: bytes=32 time=21ms TTL=49
Reply from 84.53.185.208: bytes=32 time=25ms TTL=49
Reply from 84.53.185.208: bytes=32 time=19ms TTL=49

Ping statistics for 84.53.185.208:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 19ms, Maximum = 25ms, Average = 21ms

PS C:\Users\Admin>
```

EXERCISE 3: IMPLEMENT NETWORK- BASED FIREWALL FUNCTIONALITY: BLOCK UNWANTED WEBSITE ACCESS USING PFSENSE FIREWALL

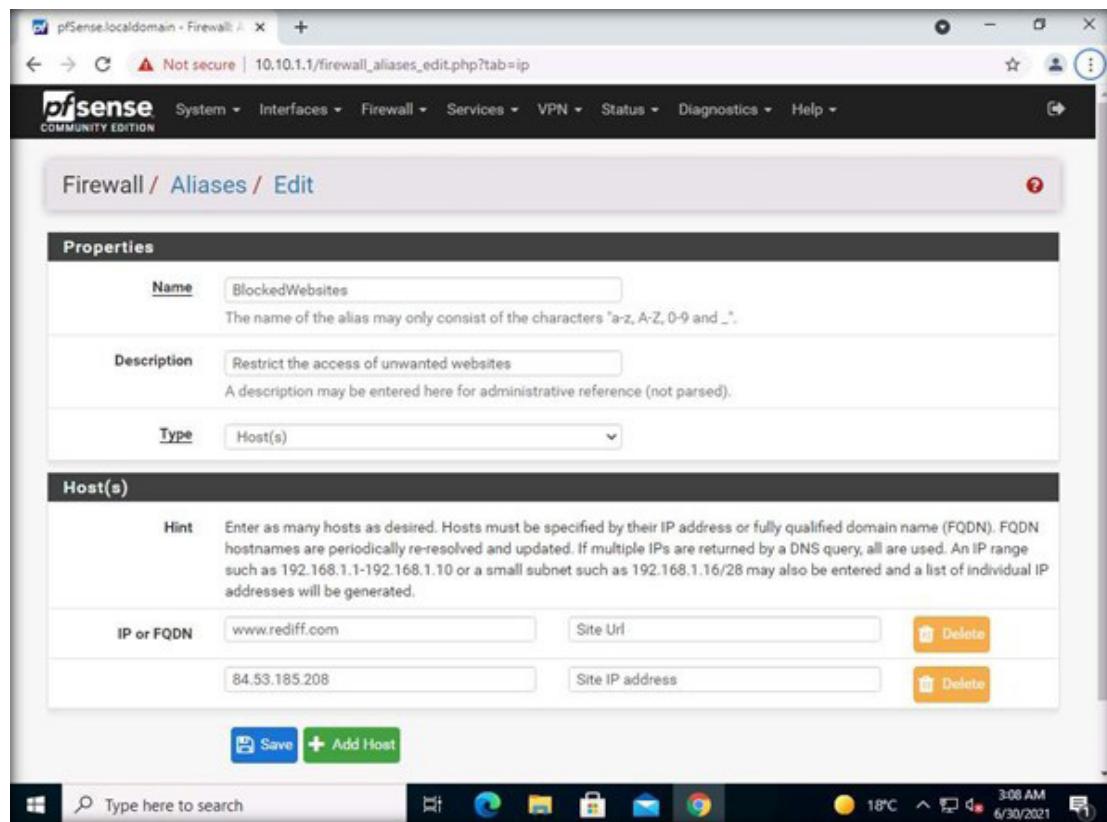
16. Next, switch to the **Google Chrome** web browser and add the following details. Under the Properties section, enter the following in the respective fields as shown in the following screenshot.

- **Name:** BlockedWebsites
- **Description:** Restrict the access of unwanted websites
- **Type:** Host(s)

Under the Host(s) section, add domain url and IP addresses for the aliases list:

- **IP or FQDN:** www.rediff.com
 - **Description:** Site Url
- Click **Add Host** button and add following IP address and description.
- **IP or FQDN:** 84.53.185.208 (Viewed rediff.com IP address from Command Prompt)
 - **Description:** Site IP address

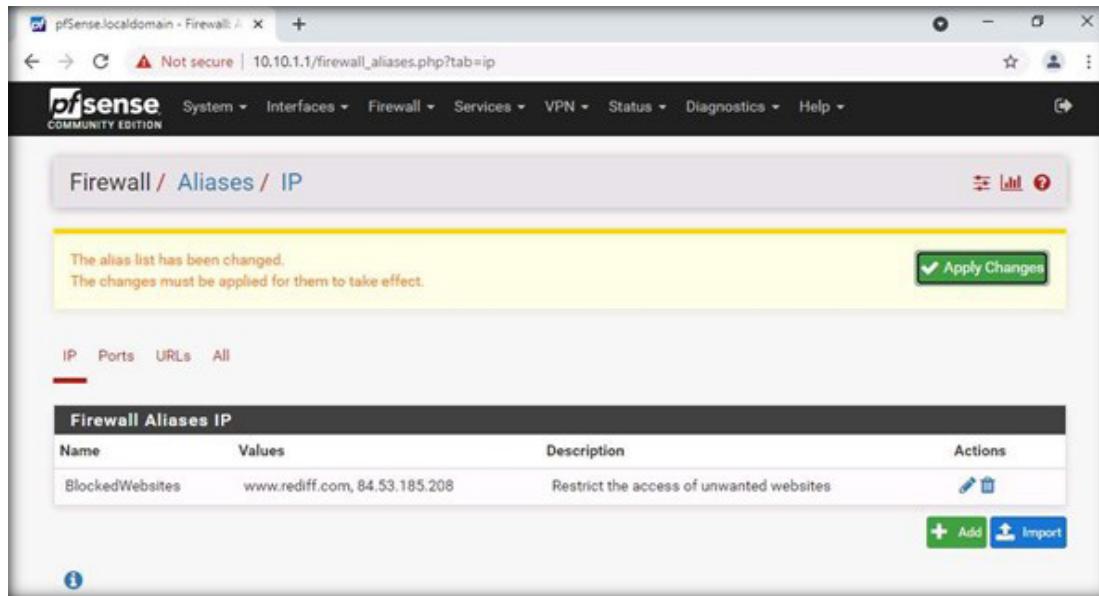
EXERCISE 3: IMPLEMENT NETWORK- BASED FIREWALL FUNCTIONALITY: BLOCK UNWANTED WEBSITE ACCESS USING PFSENSE FIREWALL



17. Click **Save**.

18. Click on **Apply Changes** button.

EXERCISE 3: IMPLEMENT NETWORK- BASED FIREWALL FUNCTIONALITY: BLOCK UNWANTED WEBSITE ACCESS USING PFSENSE FIREWALL



The screenshot shows the pfSense Firewall Aliases IP configuration page. A message at the top states: "The alias list has been changed. The changes must be applied for them to take effect." Below this is a green "Apply Changes" button. The main table lists a single entry:

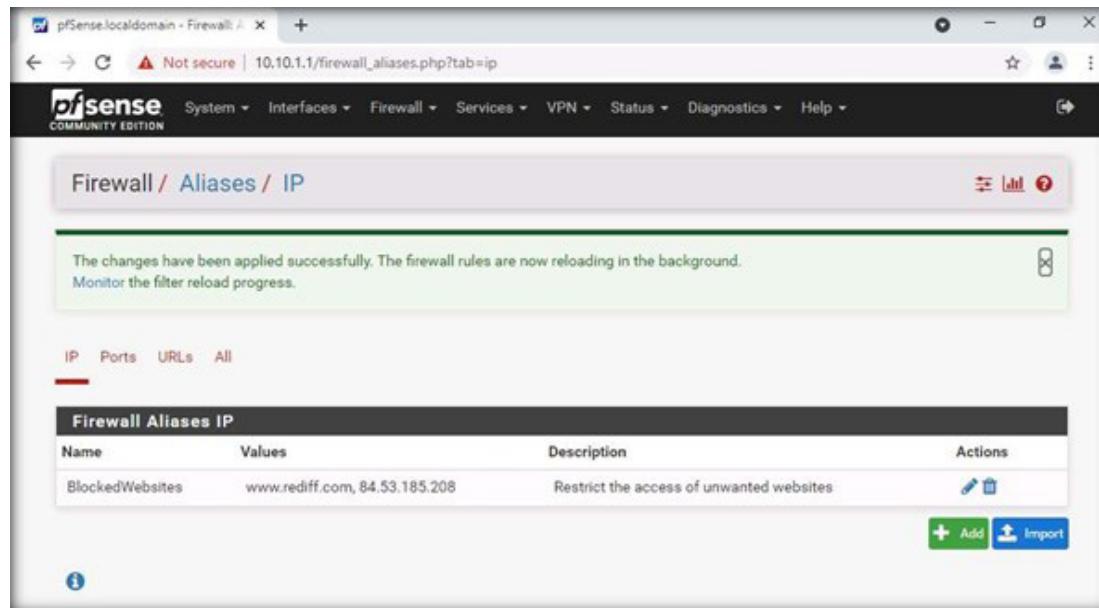
Name	Values	Description	Actions
BlockedWebsites	www.rediff.com, 84.53.185.208	Restrict the access of unwanted websites	

At the bottom are "Add" and "Import" buttons.

19. You will see the following message:

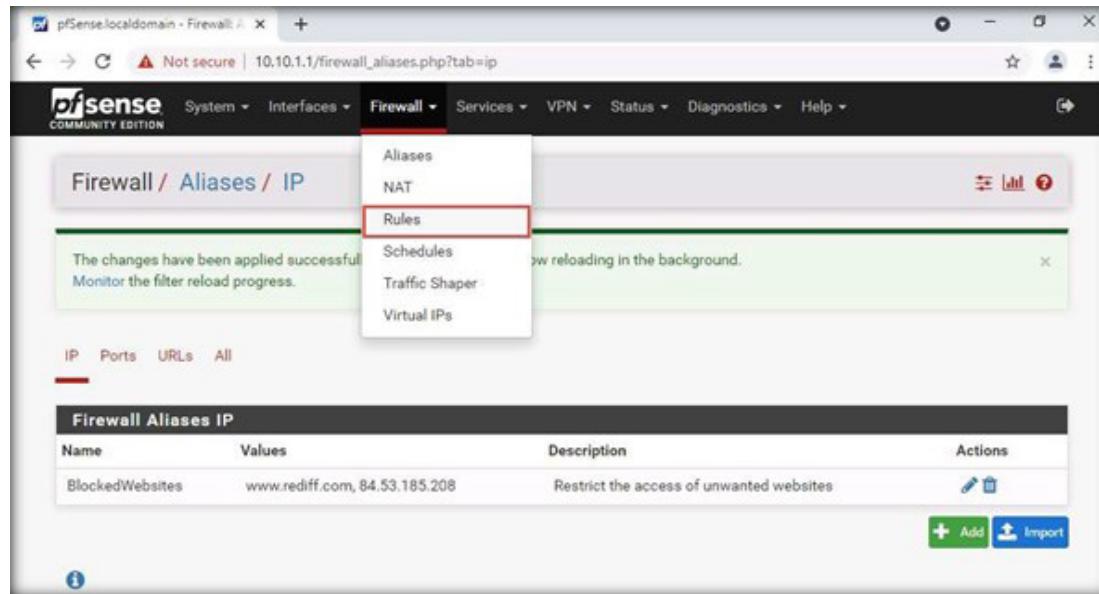
The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload process.

EXERCISE 3: IMPLEMENT NETWORK- BASED FIREWALL FUNCTIONALITY: BLOCK UNWANTED WEBSITE ACCESS USING PFSENSE FIREWALL



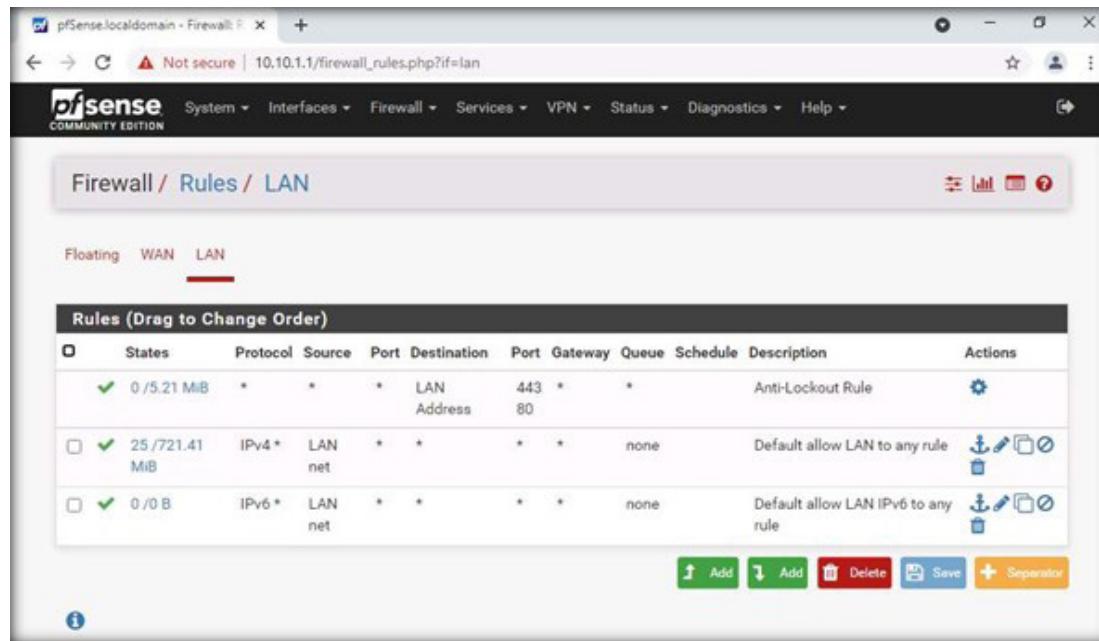
20. Next, we will add a firewall rule in pfSense to block the websites listed in the aliases. To add the rule, click on **Firewall > Rules** from the main menu in the pfSense web interface as shown in the screenshot below.

EXERCISE 3: IMPLEMENT NETWORK- BASED FIREWALL FUNCTIONALITY: BLOCK UNWANTED WEBSITE ACCESS USING PFSENSE FIREWALL



21. The Rules page will appear. Select the **LAN** option to see the default rules list as shown in the screenshot below.

EXERCISE 3: IMPLEMENT NETWORK- BASED FIREWALL FUNCTIONALITY: BLOCK UNWANTED WEBSITE ACCESS USING PFSENSE FIREWALL



The screenshot shows the pfSense Firewall Rules LAN page. The title bar reads "pfSense.localdomain - Firewall: F x +". The address bar says "Not secure | 10.10.1.1/firewall_rules.php?if=lan". The navigation menu includes System, Interfaces, Firewall (selected), Services, VPN, Status, Diagnostics, and Help. The main content area is titled "Firewall / Rules / LAN". Below it, there are tabs for Floating, WAN, and LAN, with LAN selected. A table titled "Rules (Drag to Change Order)" lists three rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0 / 5.21 MiB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	
✗ ✓ 25 / 721.41 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✗ ✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

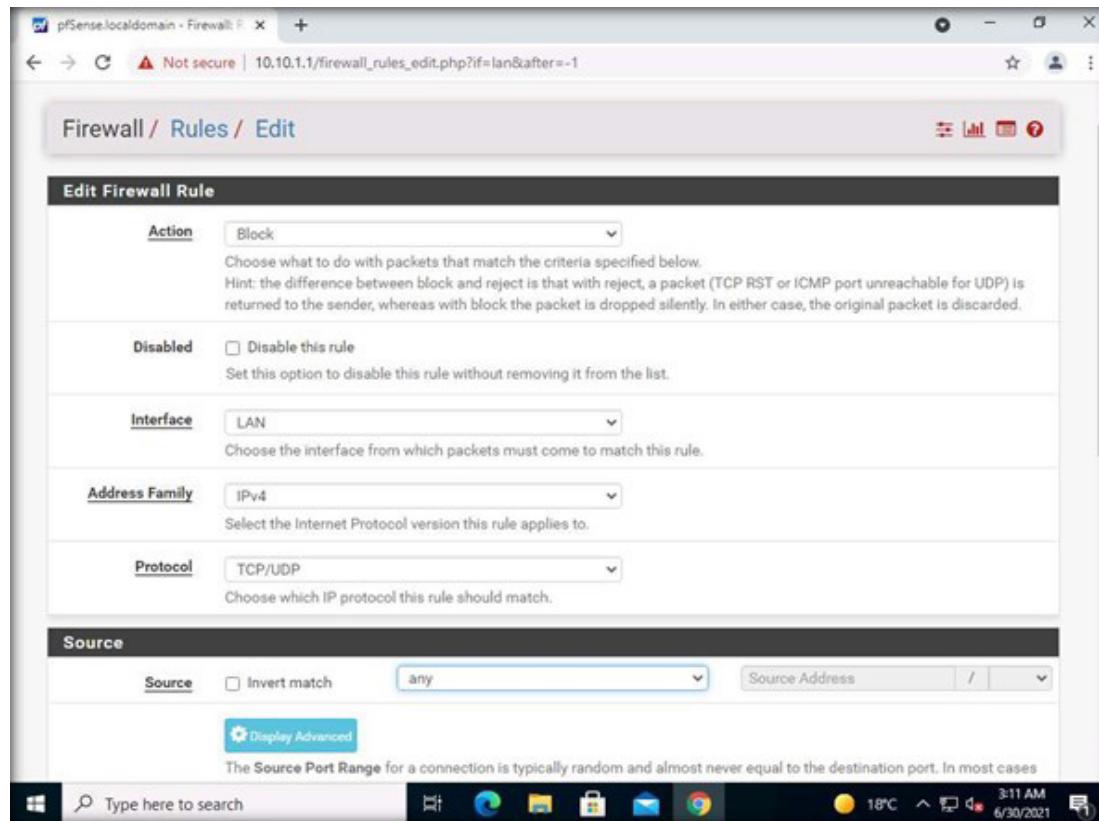
At the bottom are buttons for Add, Delete, Save, and Separator.

22. Click upper arrow **Add** to set a new rule on top of the default rule.

23. Under **Edit Firewall Rule** section, set below details.

- **Action:** Block
- **Interface:** LAN
- **Address Family:** IPv4
- **Protocol:** TCP/UDP

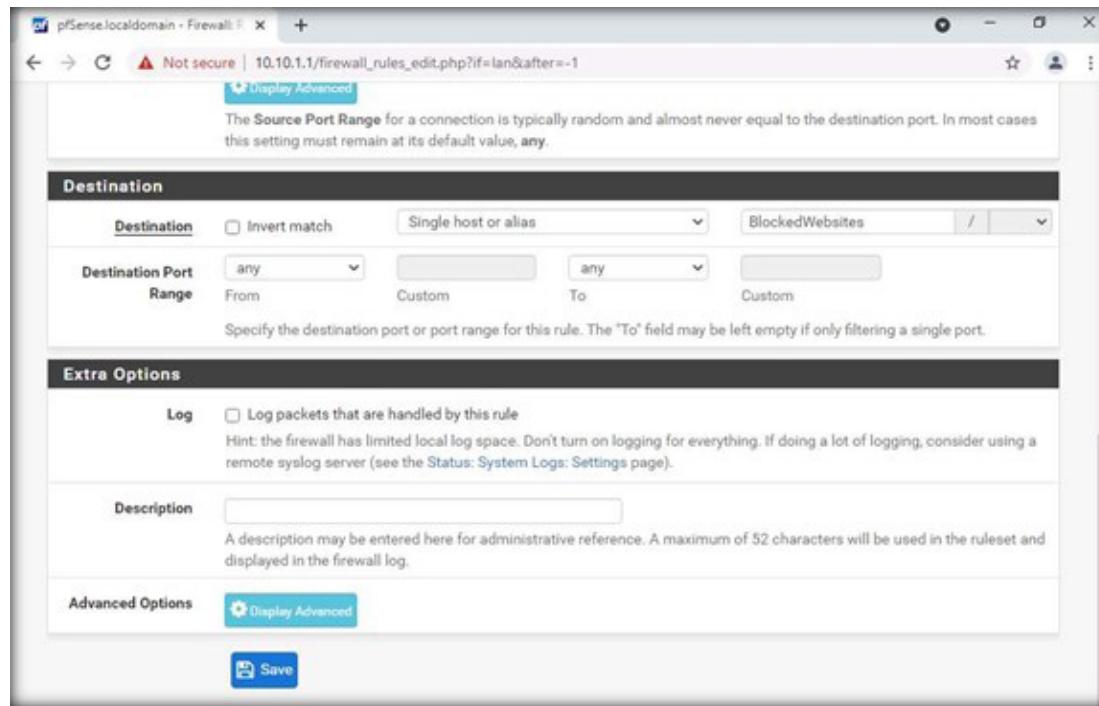
Under **Source** section, select **any** from the dropdown.



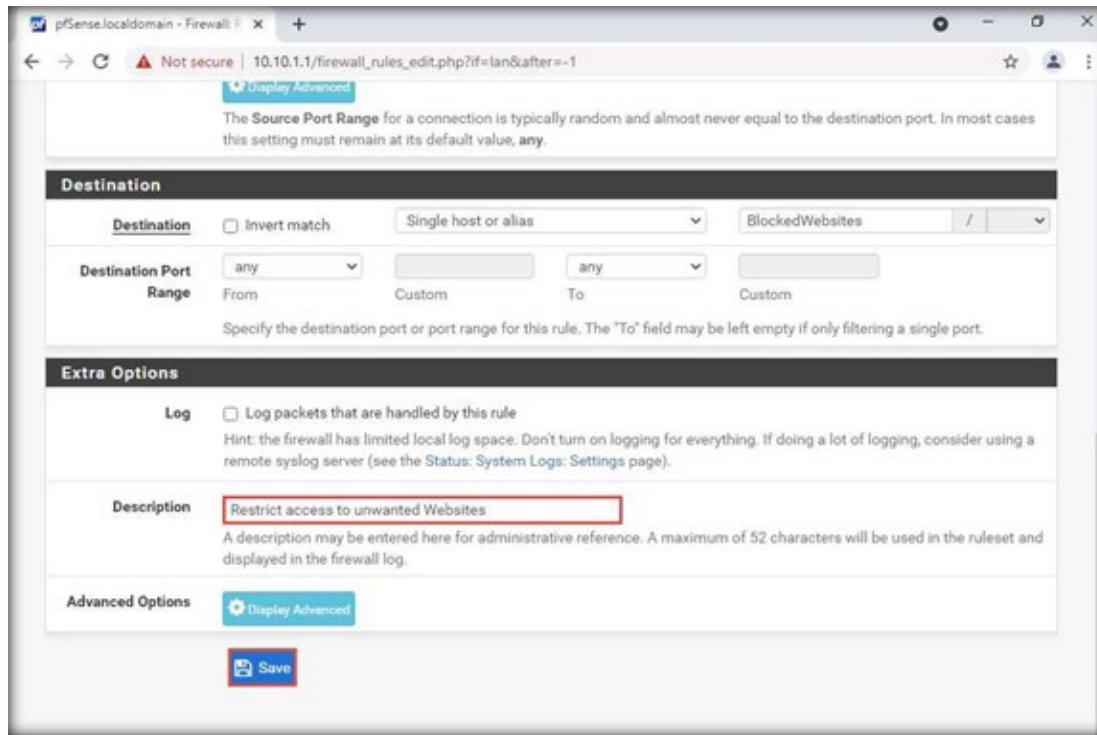
EXERCISE 3: IMPLEMENT NETWORK- BASED FIREWALL FUNCTIONALITY: BLOCK UNWANTED WEBSITE ACCESS USING PFSENSE FIREWALL

24. Under **Destination**, select **Single host or alias** from the dropdown and type **BlockedWebsites** in the text box, select **Destination Port Range as any**.

EXERCISE 3: IMPLEMENT NETWORK- BASED FIREWALL FUNCTIONALITY: BLOCK UNWANTED WEBSITE ACCESS USING PFSENSE FIREWALL



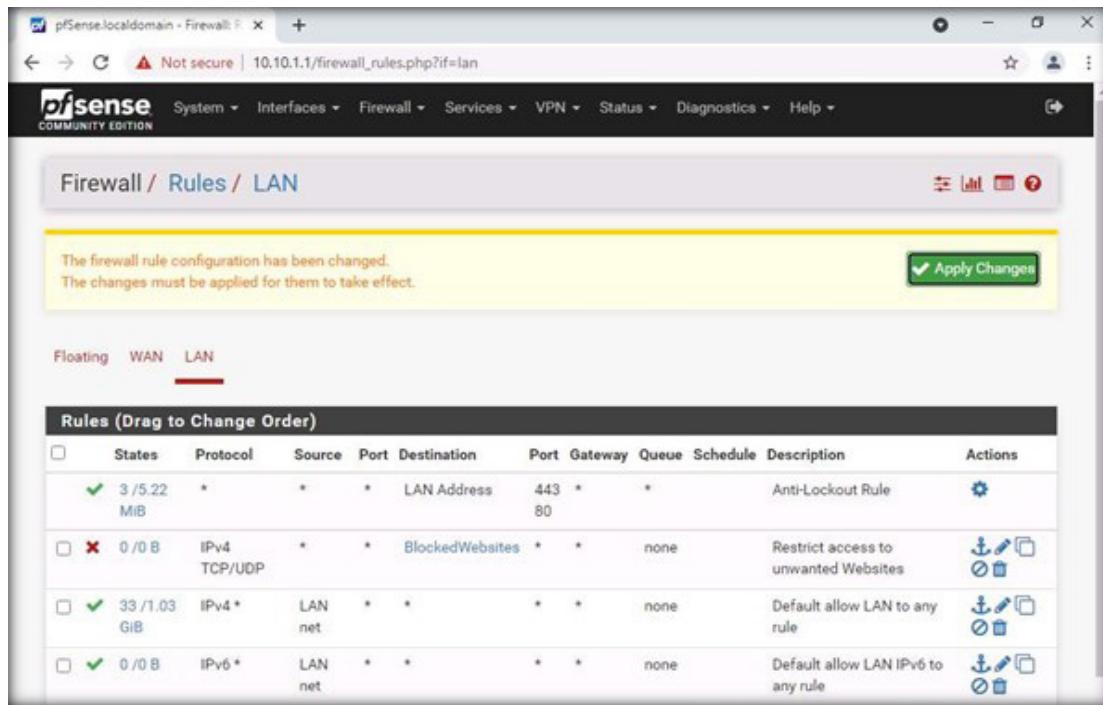
25. Scroll down, enter the text **Restrict access to unwanted Websites** in the **Description** field, and click **Save**.



EXERCISE 3: IMPLEMENT NETWORK- BASED FIREWALL FUNCTIONALITY: BLOCK UNWANTED WEBSITE ACCESS USING PFSENSE FIREWALL

26. The page will redirect to the **Firewall/ Rules** page. Click **Apply Changes**.

EXERCISE 3: IMPLEMENT NETWORK- BASED FIREWALL FUNCTIONALITY: BLOCK UNWANTED WEBSITE ACCESS USING PFSENSE FIREWALL

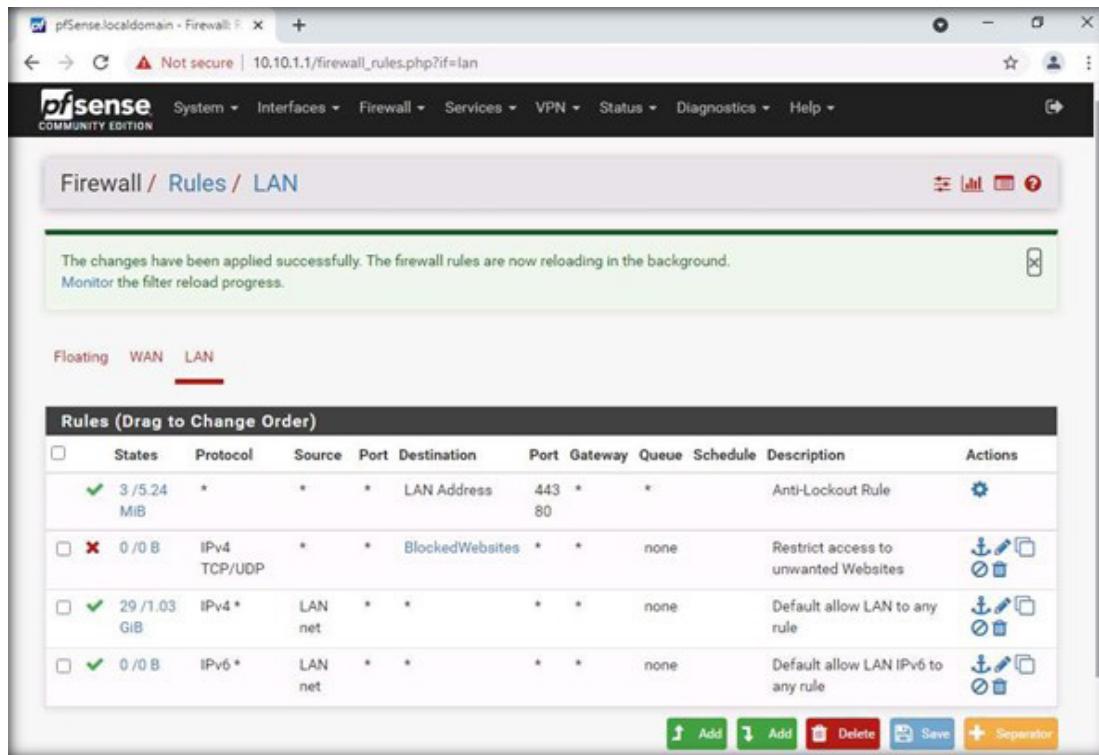


The screenshot shows the pfSense Firewall Rules LAN page. A yellow message box at the top states: "The firewall rule configuration has been changed. The changes must be applied for them to take effect." To the right of this message is a green "Apply Changes" button with a checkmark. Below the message, there are tabs for Floating, WAN, and LAN, with LAN selected. The main area displays a table titled "Rules (Drag to Change Order)". The table lists four rules:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	3 / 5.22. MiB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	*	*	BlockedWebsites	*	*	none		Restrict access to unwanted Websites	
<input type="checkbox"/>	33 / 1.03. GIB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

27. The firewall rule has been successfully created as shown in the screenshot below.

EXERCISE 3: IMPLEMENT NETWORK- BASED FIREWALL FUNCTIONALITY: BLOCK UNWANTED WEBSITE ACCESS USING PFSENSE FIREWALL



The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
3 / 5.24 MiB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	
0 / 0 B	IPv4 TCP/UDP	*	*	BlockedWebsites	*	*	none		Restrict access to unwanted Websites	
29 / 1.03 GiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

28. Close all open windows.

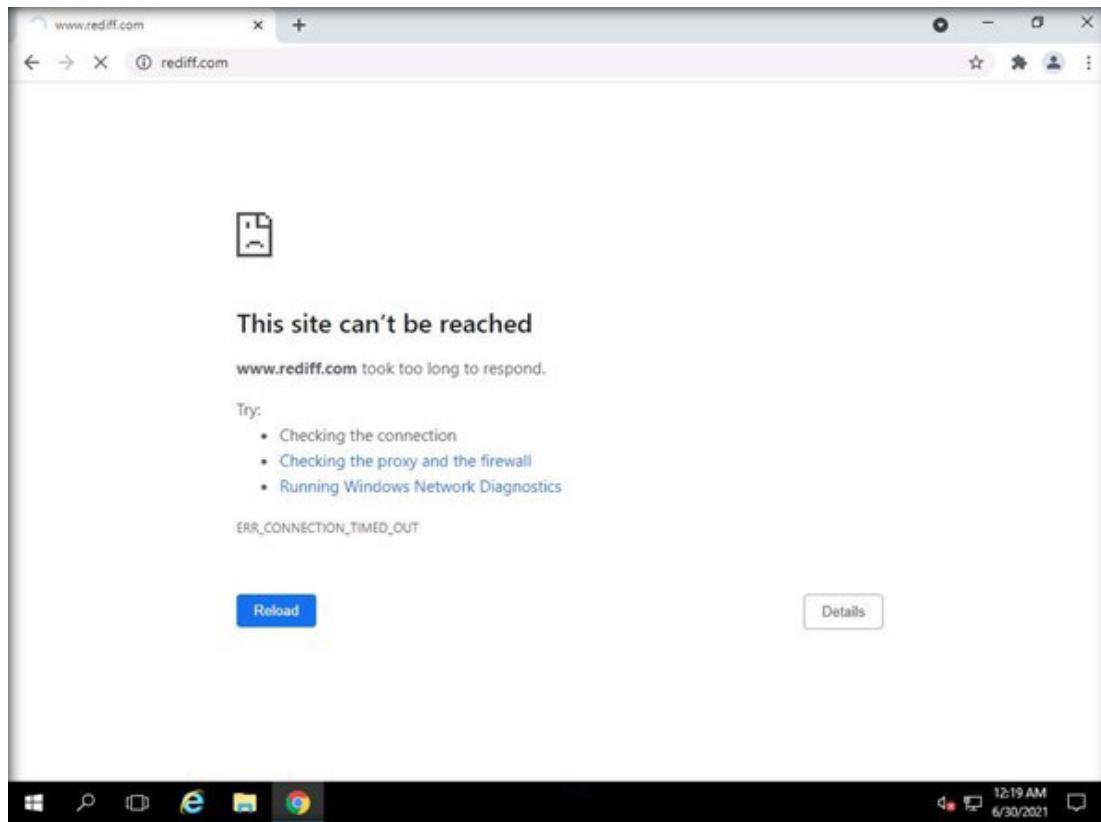
29. Switch to the **Web Server** virtual machine.

Note: If you are already logged into the **Web Server** virtual machine, then skip to **Step#31**.

30. Log in with the credentials **Administrator** and **admin@123**.

31. Open the browser and type **www.rediff.com** to check if rediff is accessible. You will see the following message: **This site can't be reached**.

EXERCISE 3:
**IMPLEMENT NETWORK-
BASED FIREWALL
FUNCTIONALITY: BLOCK
UNWANTED WEBSITE ACCESS
USING PFSENSE FIREWALL**



32. This indicates that the firewall is blocking the website listed in the firewall rule.

33. Close all open windows.

34. Turn off the **AD Domain Controller** virtual machine.

EXERCISE 4: IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL

Firewall rules allow a computer to send or receive packets from a program, services, computers, and/or users.

LAB SCENARIO

To keep the computer resources of the organization secure, the security professional needs to configure outbound traffic because outbound traffic leaves the network vulnerable to malware that targets organizational resources. These threats can be protected by using firewall rules. The pfSense firewall allows specific traffic on specific ports while blocking all other traffic.

LAB OBJECTIVE

This lab will demonstrate how to block insecure ports using the pfSense firewall and protect endpoints within the network using the pfSense firewall.

OVERVIEW OF FIREWALL RULES

Firewall rules can be created for either inbound or outbound traffic.

- An inbound firewall rule protects the network against incoming malicious traffic from the Internet or other network segments.
 - An outbound firewall protects against outgoing traffic originating inside an enterprise network.
- Firewall rules can be configured to specify computers, users, programs, services, ports, and protocols.

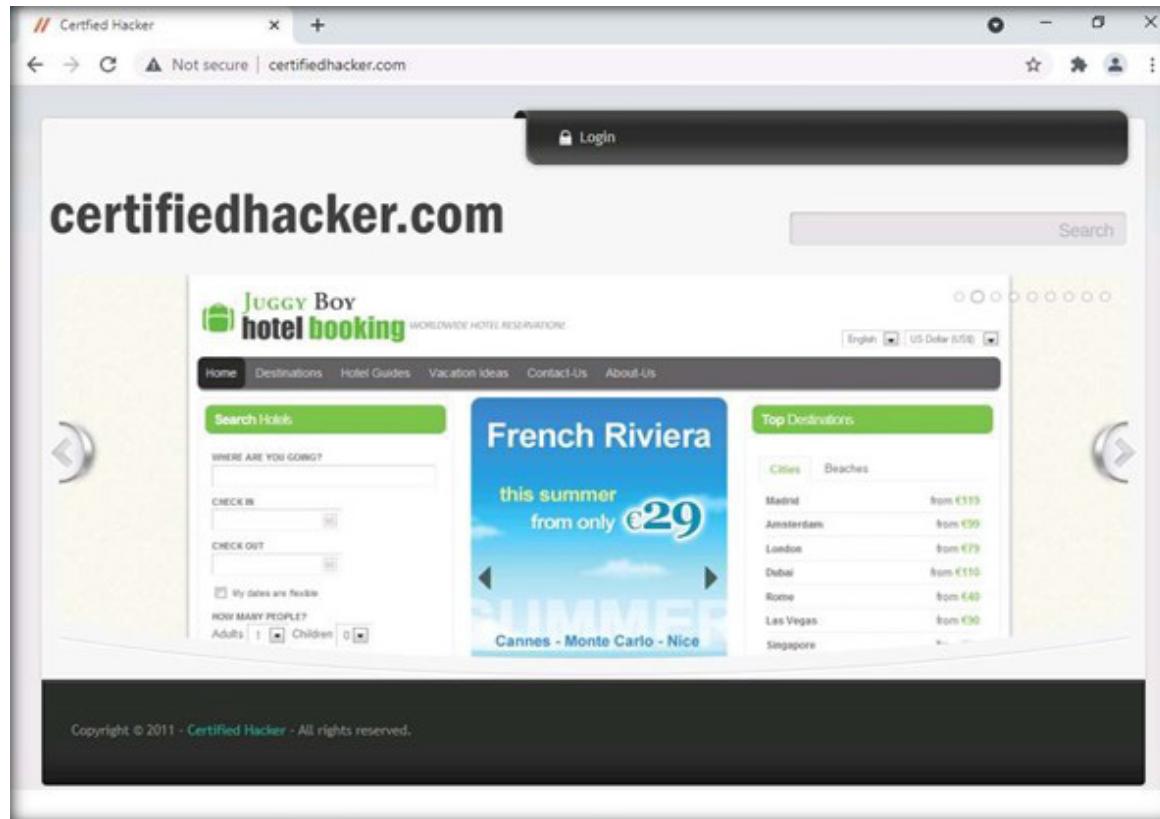
LAB TASKS

Note: Ensure that **Admin Machine-1**, **Web Server** and **PfSense Firewall** virtual machines are running.

1. Turn on the **AD Domain Controller** virtual machine.
2. Log in with the credentials **CCT\Administrator** and **admin@123**.
Note: If the network screen appears, click **Yes**.
3. Switch to the **Web Server** virtual machine.
Note: If you are not logged into the machine, then log in using credentials **Administrator / admin@123**.
4. In **Web Server** virtual machine, to open the browser, double click the **Google Chrome** icon on the **Desktop**.

5. Type <http://certifiedhacker.com> in the address bar, and press **Enter**. You will be able to access the web page, as shown in the below screenshot.

EXERCISE 4
**IMPLEMENT NETWORK-
BASED FIREWALL
FUNCTIONALITY: BLOCK
INSECURE PORTS USING
PFSENSE FIREWALL**



6. Next, we shall create a rule to restrict a user from accessing **HTTP-enabled websites (by blocking port http 80)**, so that they can access only https-enabled websites on the Internet.

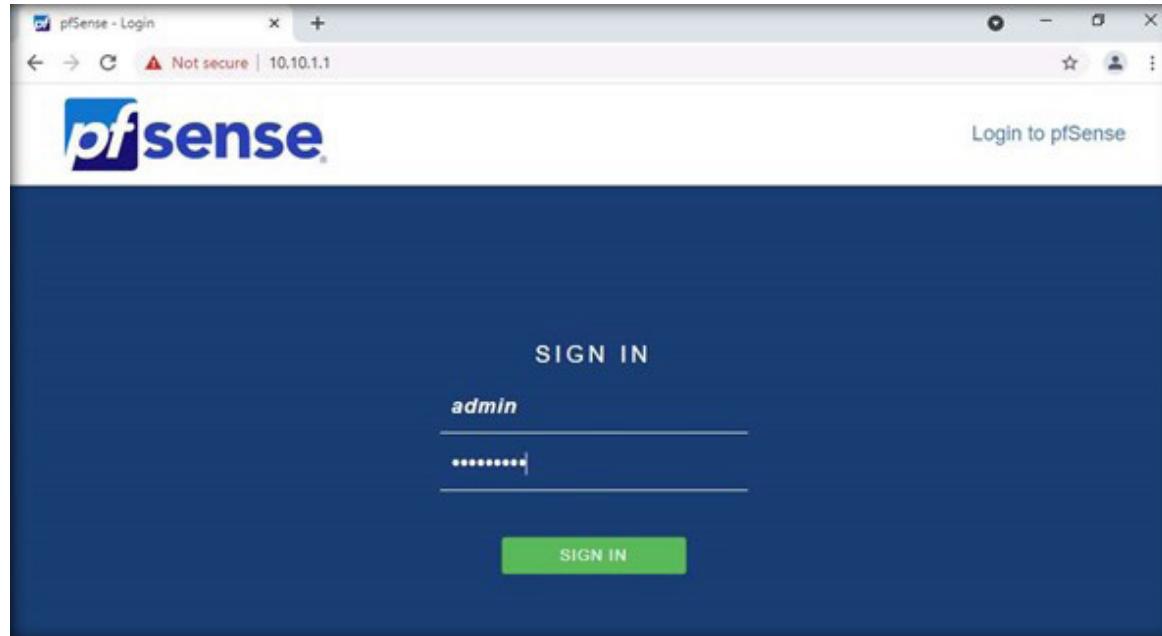
7. Switch to the **Admin Machine-1** virtual machine.

Note: If you are not logged into the machine, then log in with the credentials **Admin** and **admin@123**.

8. To open the browser, double click the **Google Chrome** icon on the **Desktop**.

9. Browse pfSense web interface. Type **https://10.10.1.1** in the address bar, and press **Enter**. Click **Advanced** button and click proceed to **10.10.1.1 (unsafe)** link.

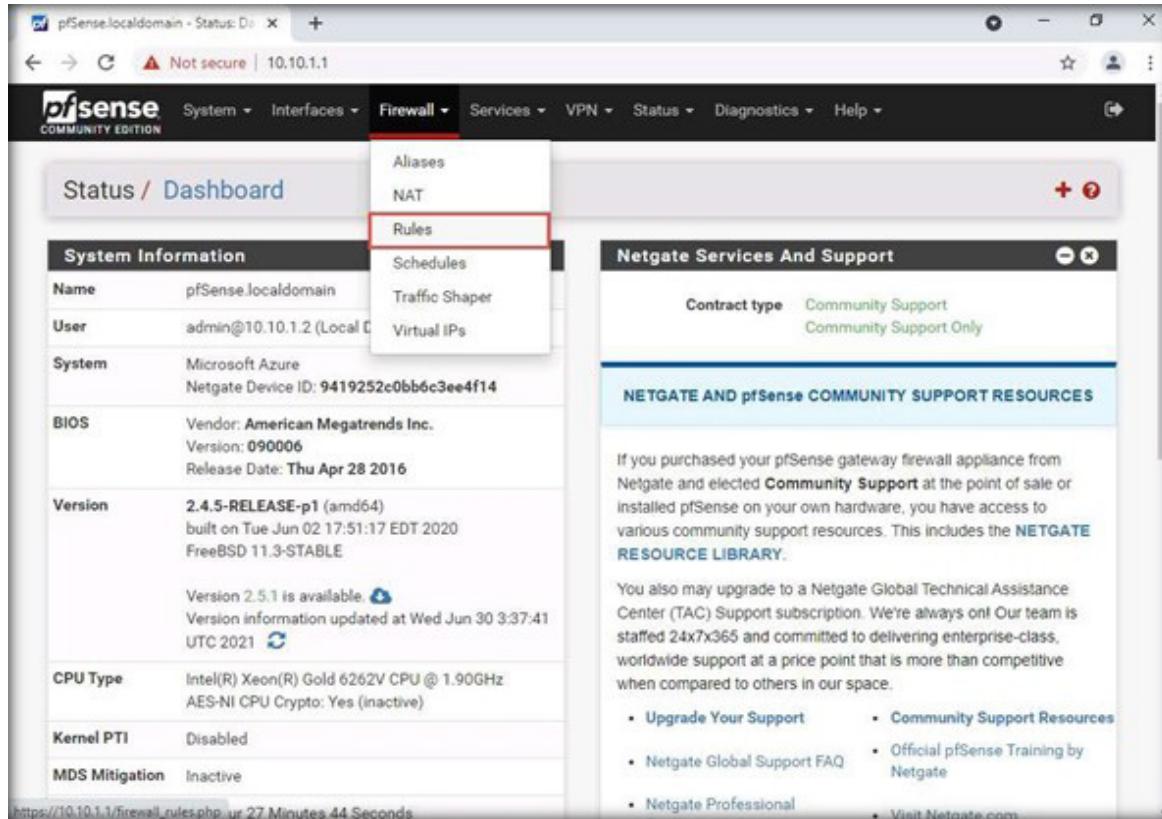
10. The pfSense login page will appear. Type the username as **admin** and password as **admin@123**, and click the **SIGN IN** button, as shown in the screenshot below.



EXERCISE 4^o
**IMPLEMENT NETWORK-
BASED FIREWALL
FUNCTIONALITY: BLOCK
INSECURE PORTS USING
PFSENSE FIREWALL**

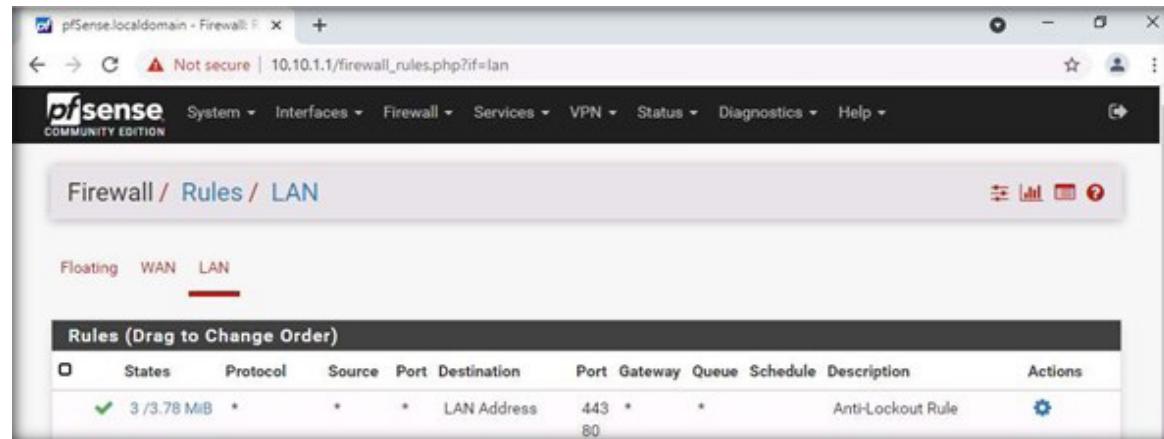
EXERCISE 4
IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING pfSense FIREWALL

11. The pfSense Dashboard will appear. Navigate to **Firewall > Rules** from the main menu.



The screenshot shows the pfSense Community Edition dashboard. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The Firewall menu is currently active, with its sub-options Aliases, NAT, and Rules visible. The Rules option is highlighted with a red box. Below the navigation bar, there's a 'Status / Dashboard' section and a 'System Information' table. To the right, there's a 'Netgate Services And Support' sidebar with information about contract types and support resources. At the bottom, there's a link to the firewall rules configuration page.

12. The **Firewall/Rules/WAN** page will appear. Click the **LAN** option.



The screenshot shows the pfSense Firewall Rules LAN page. The URL in the browser is `10.10.1.1/firewall_rules.php?if=lan`. The pfSense logo is visible at the top left. The main title is "Firewall / Rules / LAN". Below it, there are tabs for "Floating", "WAN", and "LAN", with "LAN" being the active tab. A table titled "Rules (Drag to Change Order)" lists one rule:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	3 / 3.78 MiB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	
						80					

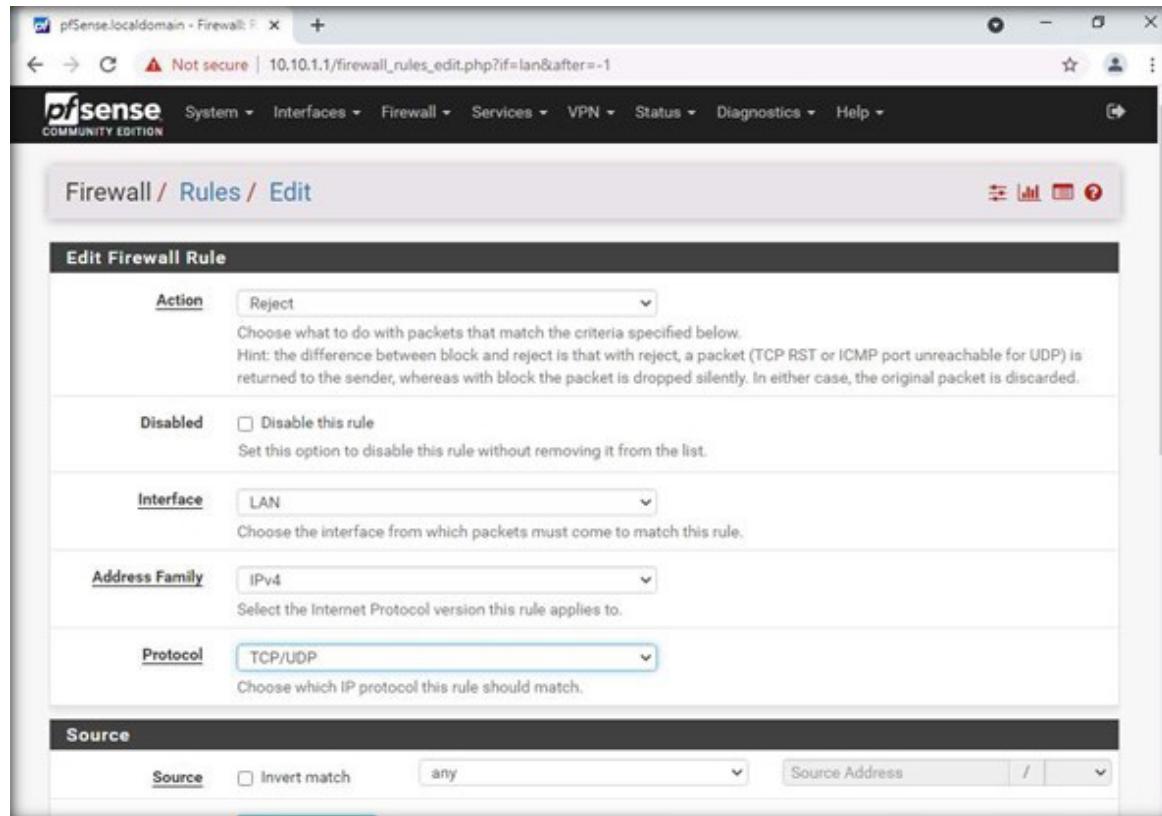
EXERCISE 4
IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL

13. To create a rule, click the up arrow Add button.

14. Set the following details under Edit Firewall Rule section:

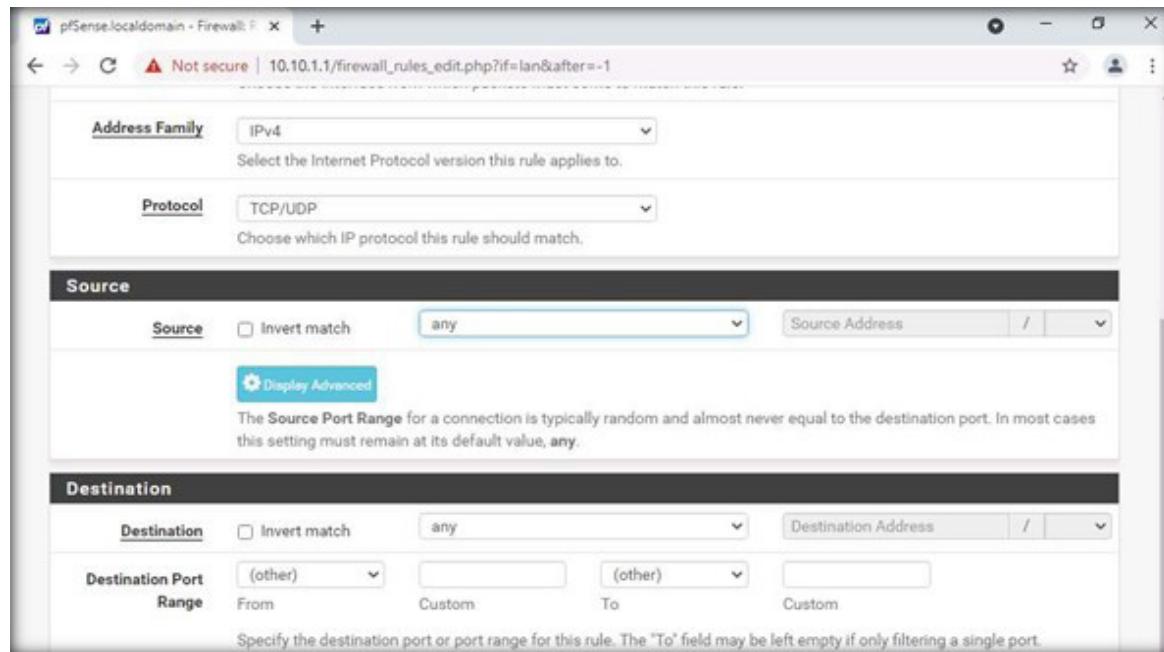
- Action > Reject
- Interface > LAN
- Address Family > IPv4
- Protocol > TCP/UDP.

EXERCISE 4
IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL



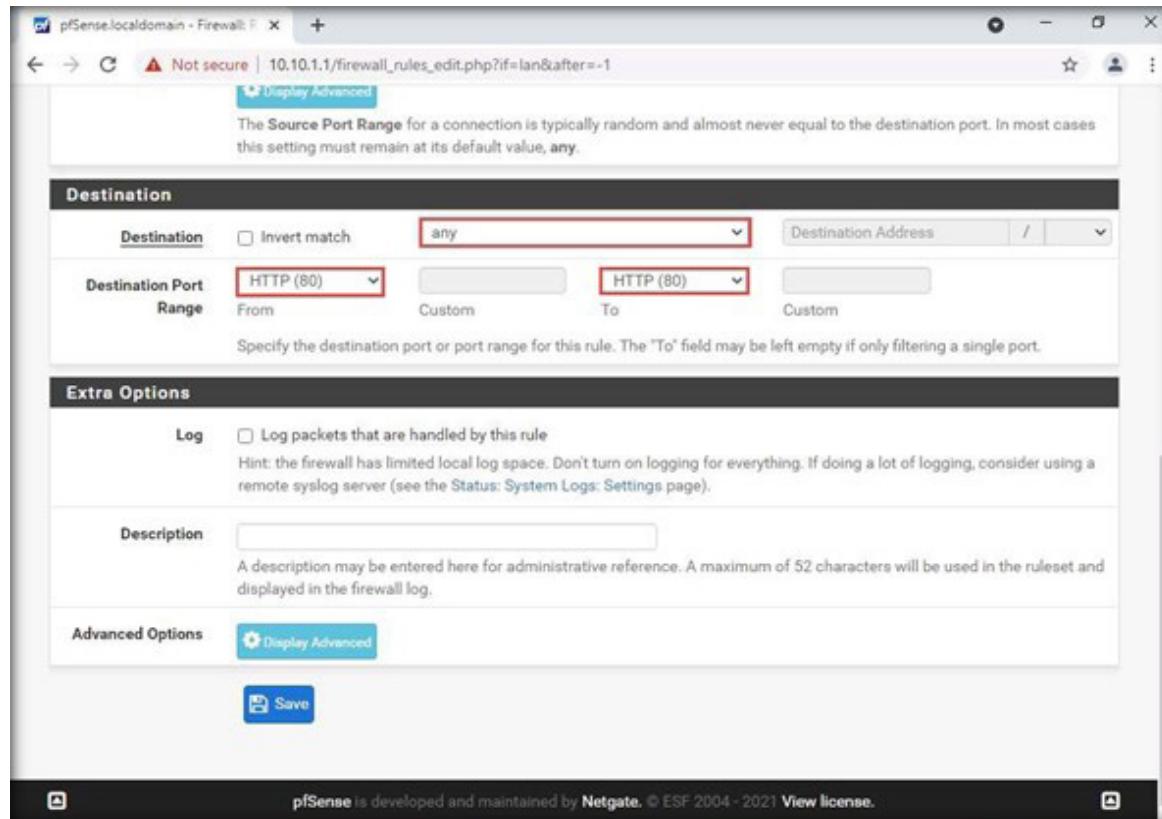
EXERCISE 4
IMPLEMENT NETWORK-
BASED FIREWALL
FUNCTIONALITY: BLOCK
INSECURE PORTS USING
PFSENSE FIREWALL

15. Under **Source** section, select **any** from the dropdown as shown in the below screenshot.

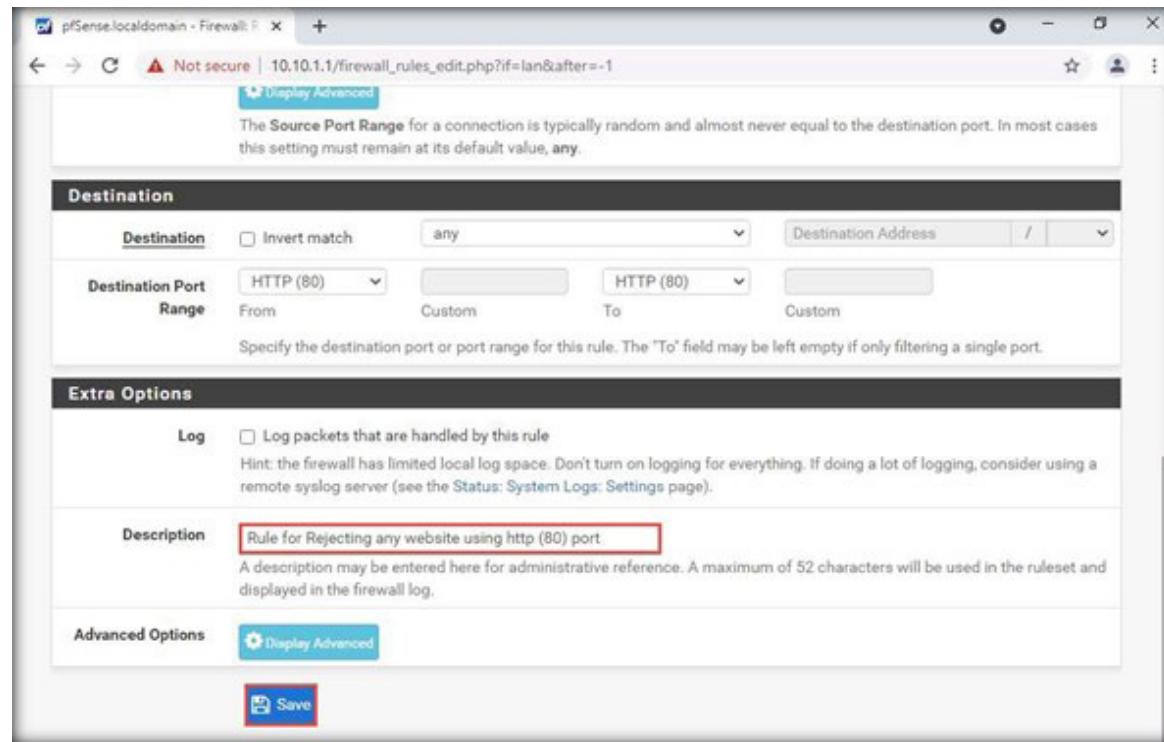


16. Under **Destination** section, select **any** from the dropdown and set **Destination Port Range to HTTP (80)** from the dropdown.

EXERCISE 4
IMPLEMENT NETWORK-
BASED FIREWALL
FUNCTIONALITY: BLOCK
INSECURE PORTS USING
PFSENSE FIREWALL

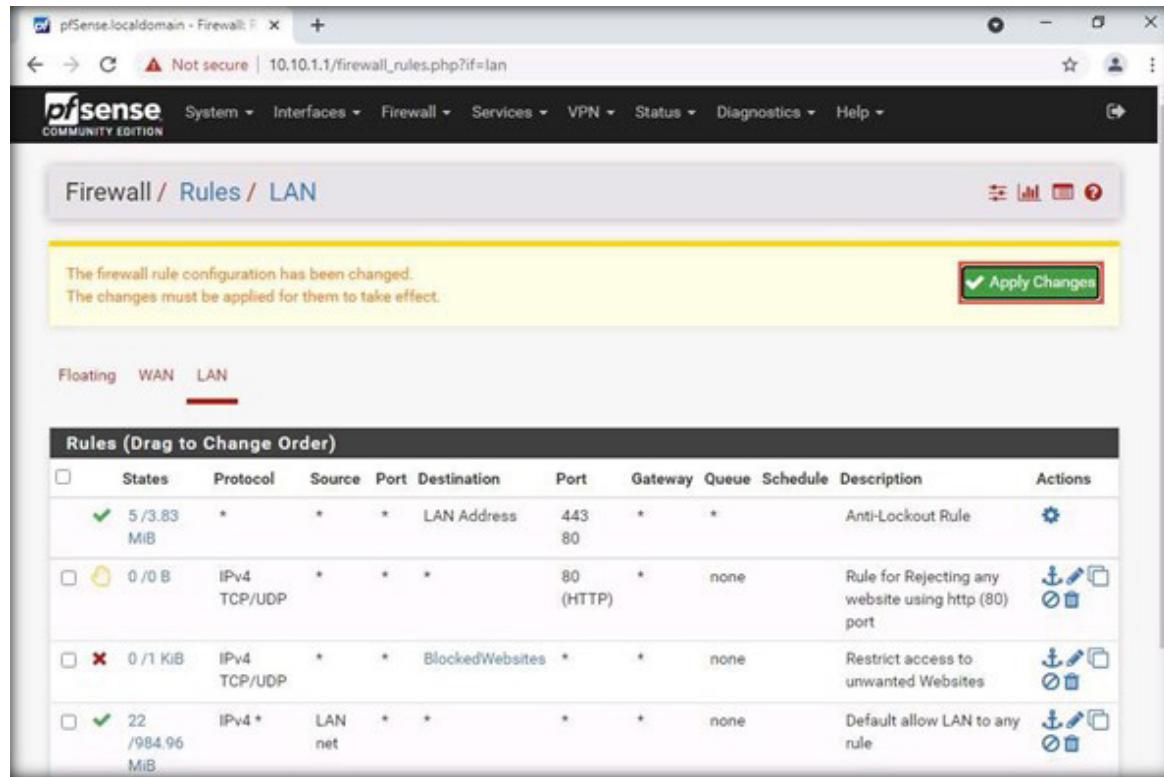


EXERCISE 4
IMPLEMENT NETWORK-
BASED FIREWALL
FUNCTIONALITY: BLOCK
INSECURE PORTS USING
PFSENSE FIREWALL



18. The page will redirect to the **Firewall/Rules/LAN** page. Click **Apply Changes**.

EXERCISE 4: IMPLEMENT NETWORK- BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL



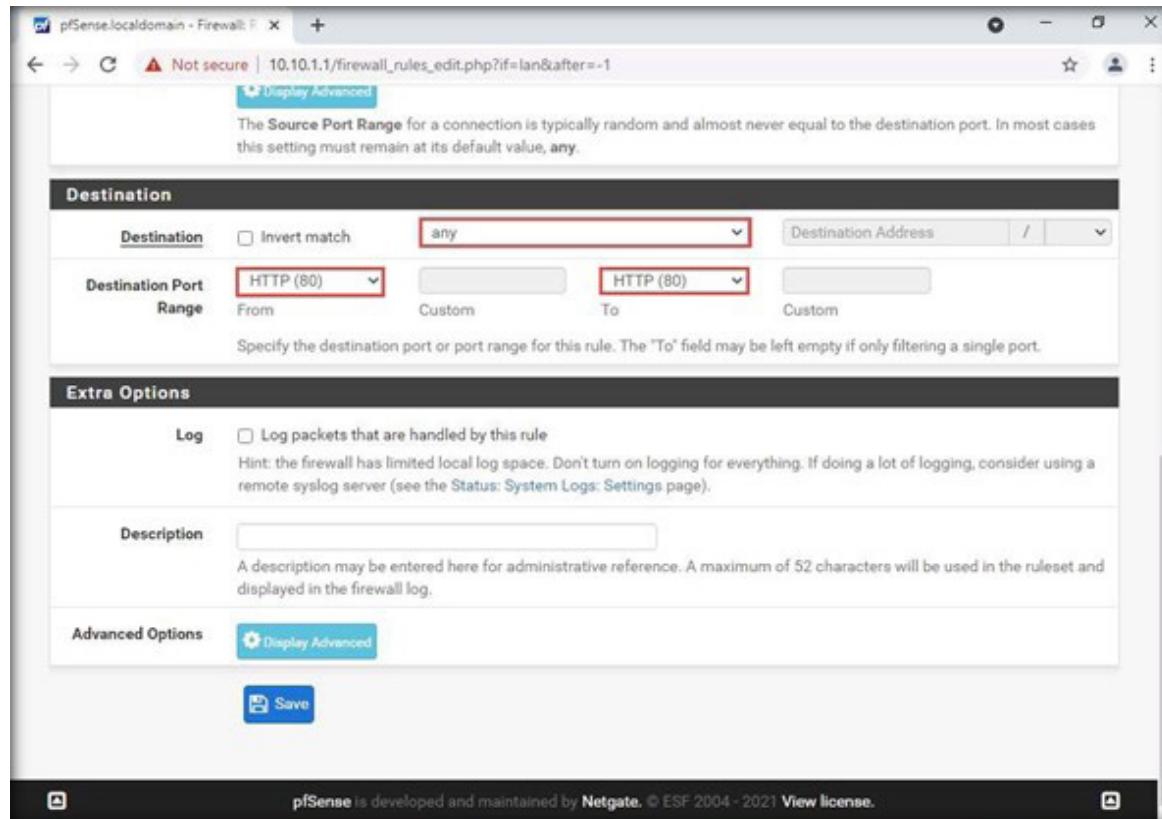
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
5 / 3.83 MIB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
0 / 0 B	IPv4 TCP/UDP	*	*	*	80 (HTTP)	*	none		Rule for Rejecting any website using http (80) port	
0 / 1 kB	IPv4 TCP/UDP	*	*	BlockedWebsites	*	*	none		Restrict access to unwanted Websites	
22 /984.96 MIB	IPv4 *	LAN net	*	*	*	*	*	none	Default allow LAN to any rule	

19. The firewall rule has been successfully created.

20. Close browser window.

21. Switch back to the **Web Server** virtual machine.

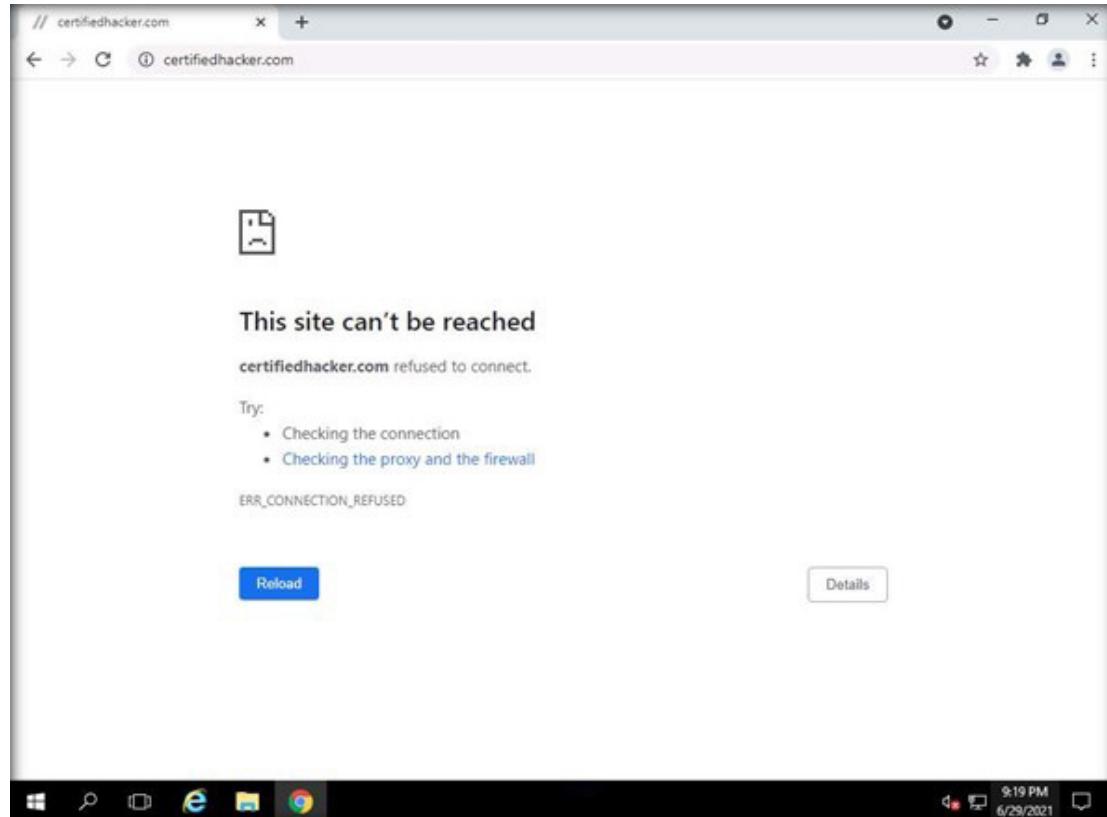
EXERCISE 4 IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL



22. In the Chrome browser (it is already opened, or you can launch a new window), enter <http://certifiedhacker.com> in the address bar, and press **Enter**. You will see the message as **This site can't be reached**. This is because the pfSense firewall rule is now preventing the traffic from the port http.

Note: If changes are not affecting, then reboot the pfSense firewall and clear the Chrome browser cache.

EXERCISE 4
IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL

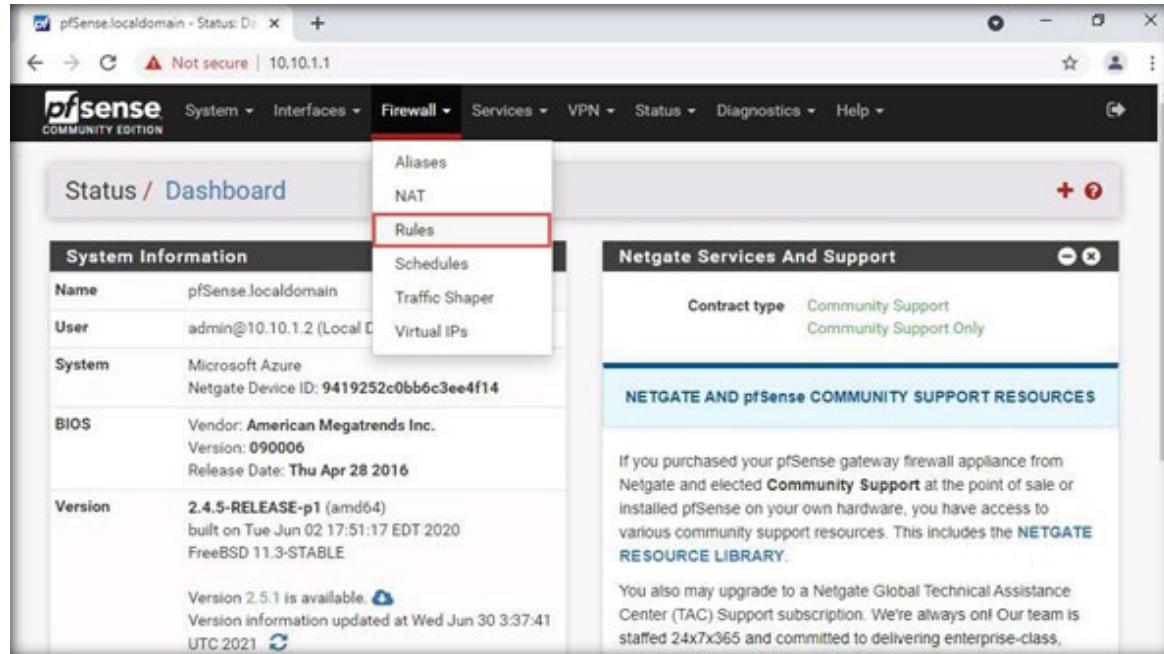


23. Close browser window.

24. Delete the firewall rules created in this exercise and previous exercise.

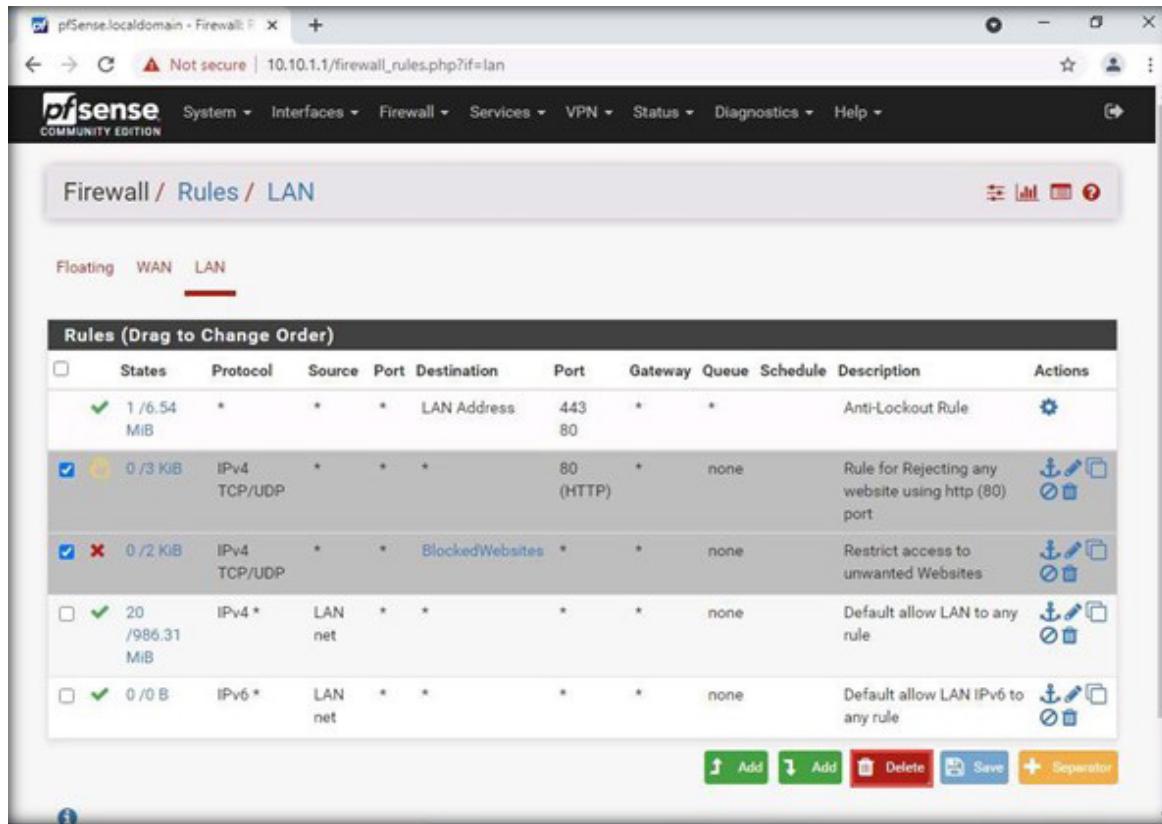
25. To delete the firewall rules, switch to **Admin Machine-1** virtual machine. Repeat steps **Step 9** to **Step 11**. Navigate to **Firewall > Rules** from the main menu.

EXERCISE 4
IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL



26. The Firewall/Rules/WAN page will appear. Click the **LAN** option. Select both the created rules by checking the checkboxes against the rules. and click **Delete** button.

EXERCISE 4
IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL

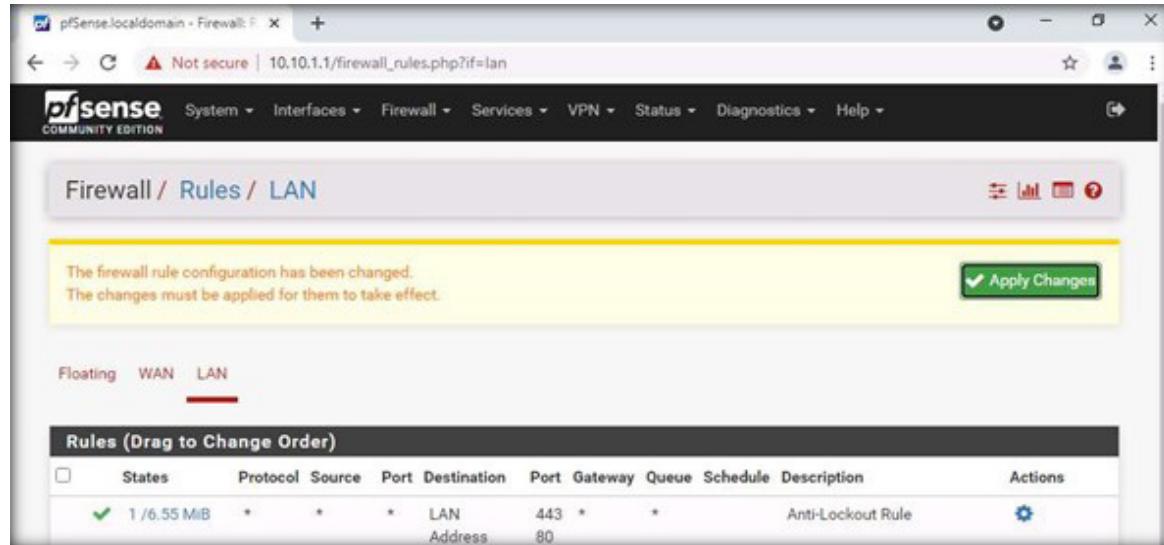


The screenshot shows the pfSense Firewall Rules LAN page. The interface includes a navigation bar with links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation is a breadcrumb trail: Firewall / Rules / LAN. A tab bar at the top of the main content area has tabs for Floating, WAN, and LAN, with LAN being the active tab. The main content area displays a table titled "Rules (Drag to Change Order)". The table has columns for States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. There are five rows in the table:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1 / 6.54 MiB	*	*	*	LAN Address	443 80	*	*	*	Anti-Lockout Rule	
✗ 0 / 3 kB	IPv4 TCP/UDP	*	*	*	80 (HTTP)	*	none		Rule for Rejecting any website using http (80) port	
✗ 0 / 2 kB	IPv4 TCP/UDP	*	*	BlockedWebsites	*	*	none		Restrict access to unwanted Websites	
✓ 20 /986.31 MiB	IPv4 *	LAN net	*	*	*	*	*	none	Default allow LAN to any rule	
✓ 0 /0 B	IPv6 *	LAN net	*	*	*	*	*	none	Default allow LAN IPv6 to any rule	

At the bottom of the table are several buttons: Add (green), Add (blue), Delete (red), Save (blue), and Separator (orange).

27. Click **OK** in the Rule deletion confirmation pop-up.
28. The page will redirect to the Firewall/Rules/LAN page. Click **Apply Changes**.



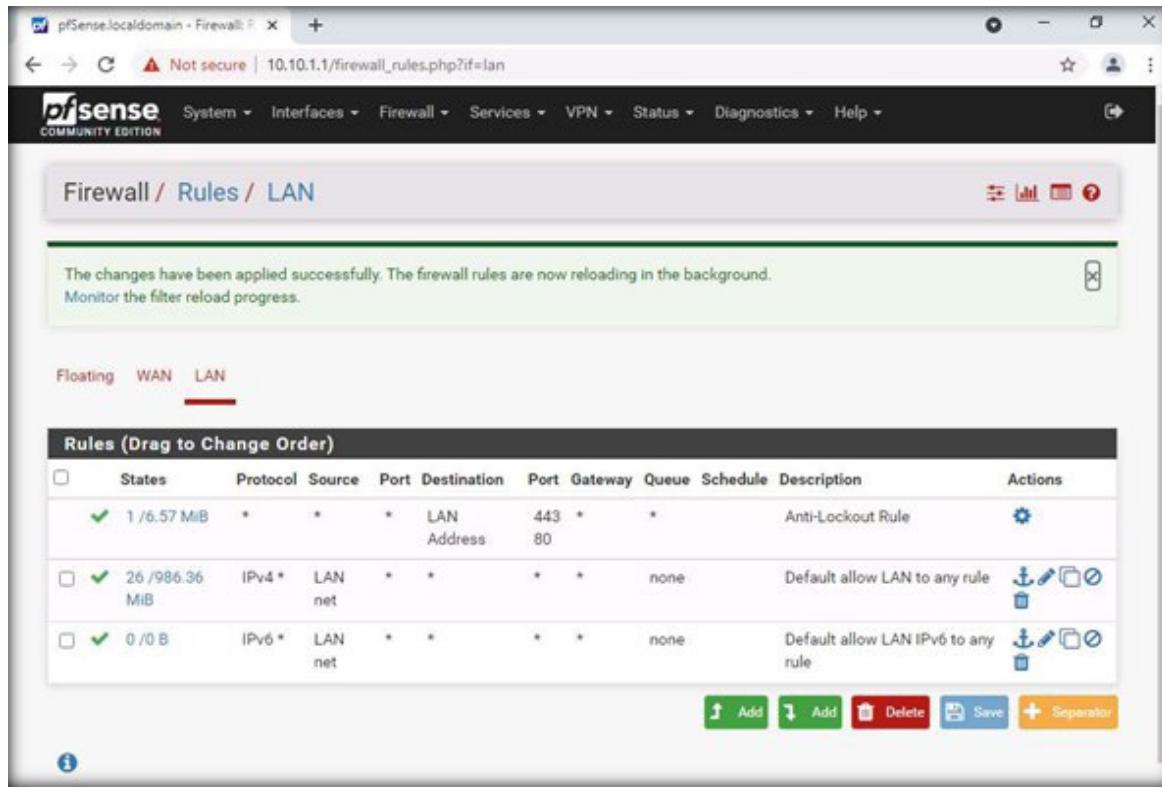
The screenshot shows the pfSense Firewall/Rules/LAN configuration interface. At the top, there is a message: "The firewall rule configuration has been changed. The changes must be applied for them to take effect." Below this is a green "Apply Changes" button. The main table displays a single rule:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1 / 6.55 MiB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	

EXERCISE 4
IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL

29. The selected rules will be deleted.

EXERCISE 4: IMPLEMENT NETWORK- BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL



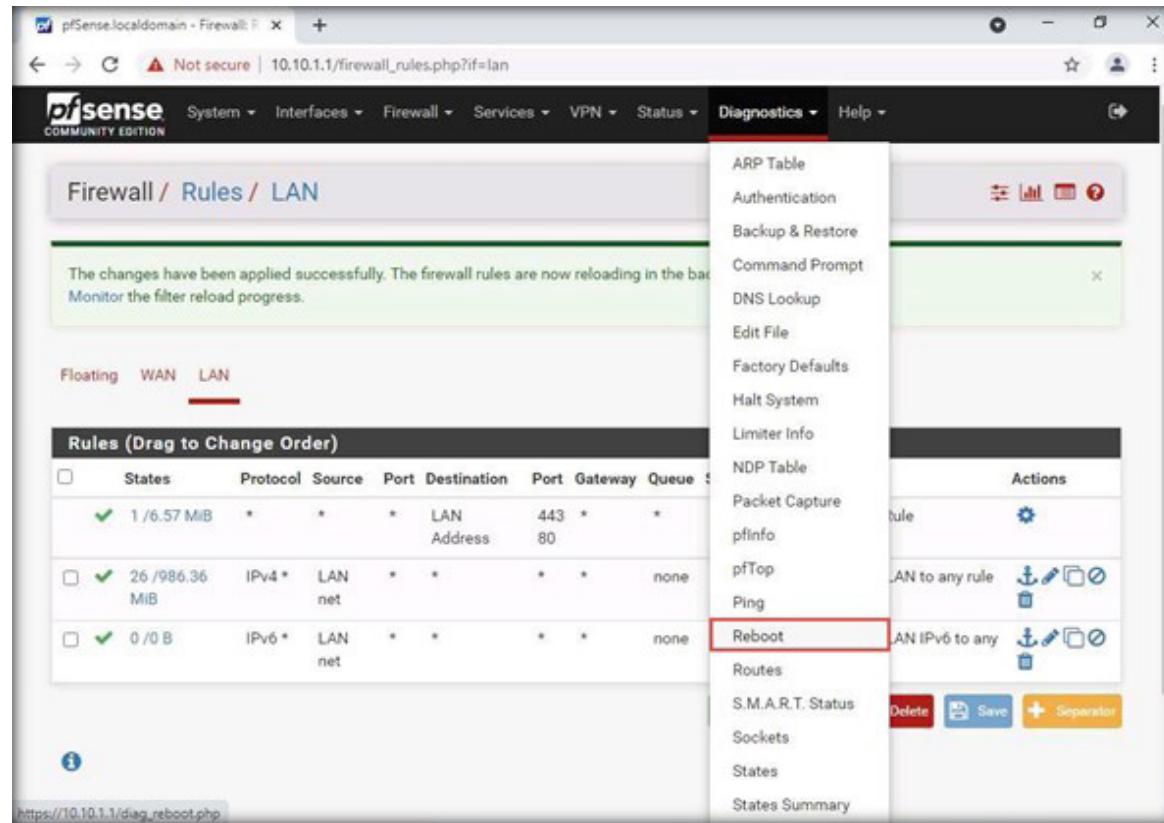
The screenshot shows the pfSense LAN firewall rules configuration. The title bar reads "pfSense.localdomain - Firewall: F". The URL in the address bar is "Not secure | 10.10.1.1/firewall_rules.php?if=lan". The pfSense logo is visible in the top left. The main menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The current page is "Firewall / Rules / LAN". A message box at the top states: "The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress." Below this, there are tabs for Floating, WAN, and LAN, with LAN selected. A table titled "Rules (Drag to Change Order)" lists three rules:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1 / 6.57 MiB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	26 / 986.36 MiB	IPv4	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0 / 0 B	IPv6	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

At the bottom are buttons for Add, Save, and Separator.

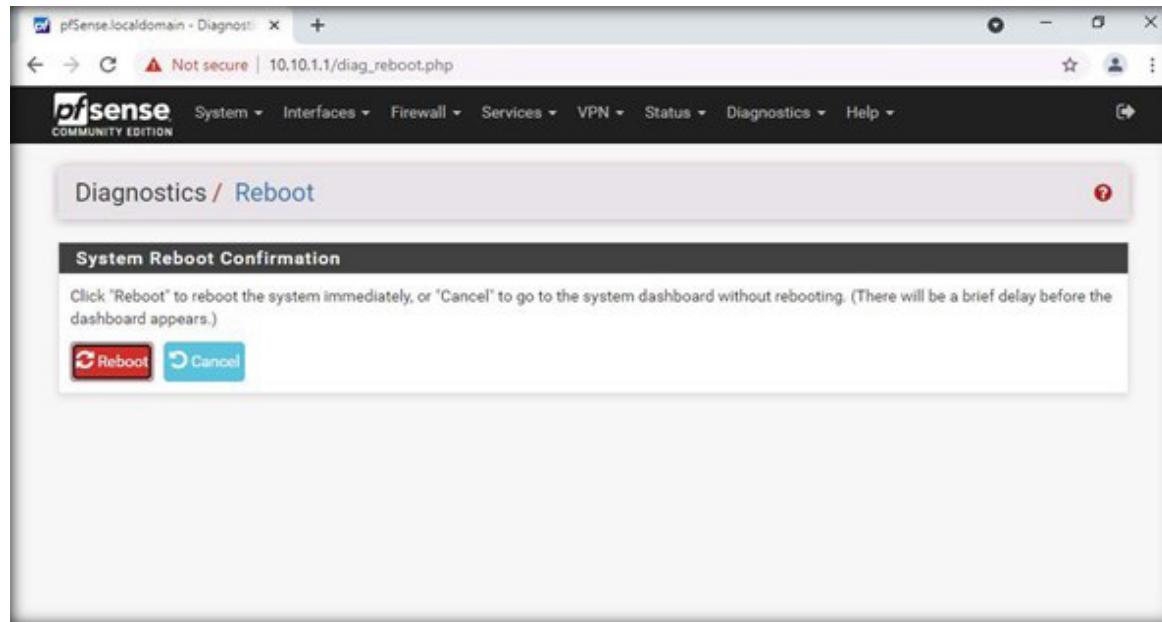
30. To reboot pfSense, navigate to **Diagnostics > Reboot** option from the main menu.

EXERCISE 4
IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL



31. Click on **Reboot** button.

EXERCISE 4^o
**IMPLEMENT NETWORK-
BASED FIREWALL
FUNCTIONALITY: BLOCK
INSECURE PORTS USING
PFSENSE FIREWALL**

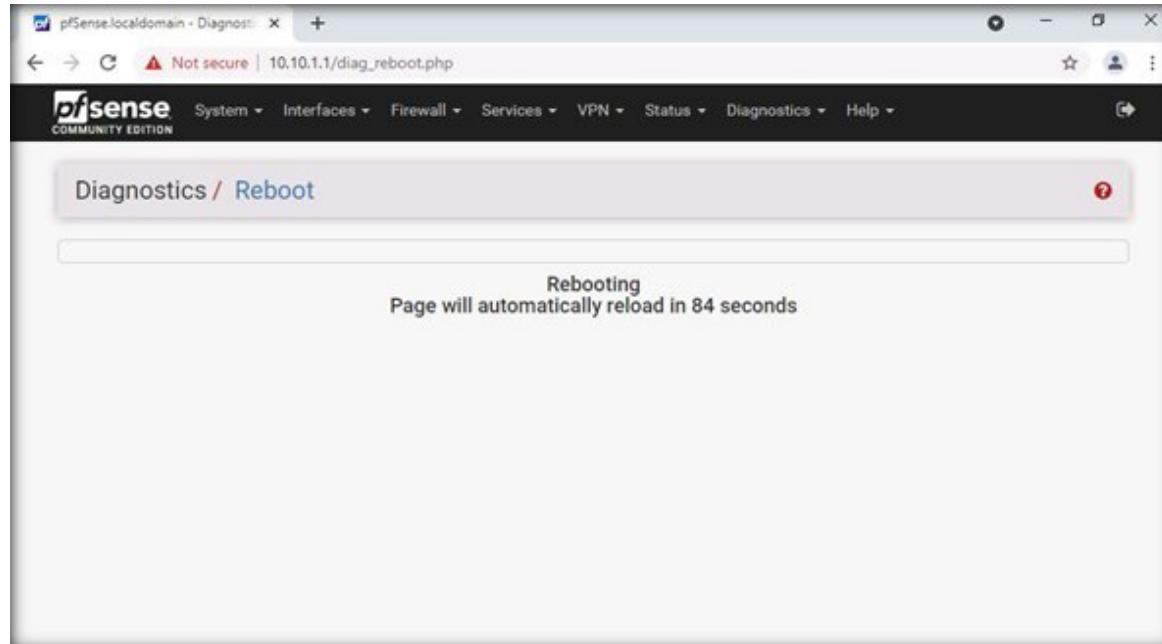


32. Click **OK** in the Reboot confirmation pop-up.

33. The pfSense firewall will reboot and load automatically.

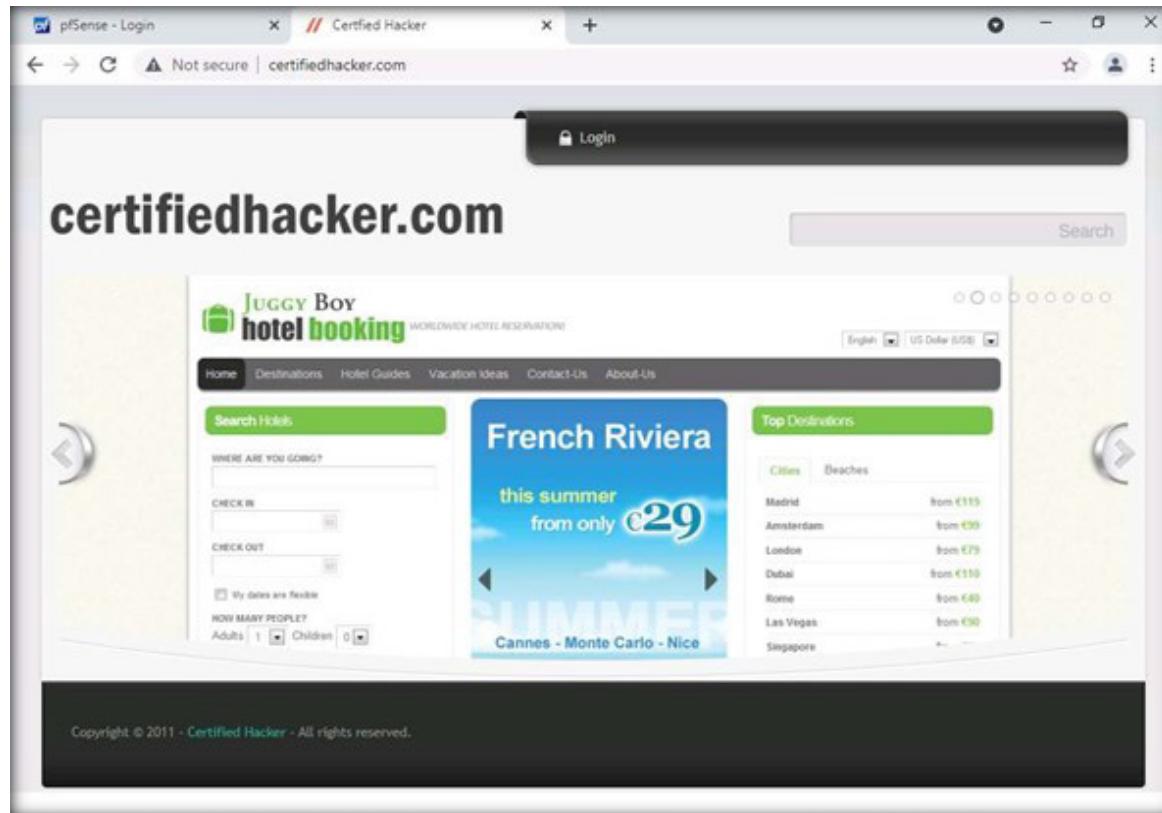
EXERCISE 4^o

IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL



34. The pfSense Sign in page will appear.

35. Now Open a new tab in Chrome browser and type <http://certifiedhacker.com/> in the address bar, and press **Enter**. You will be able to access the web page as shown in the below screenshot:



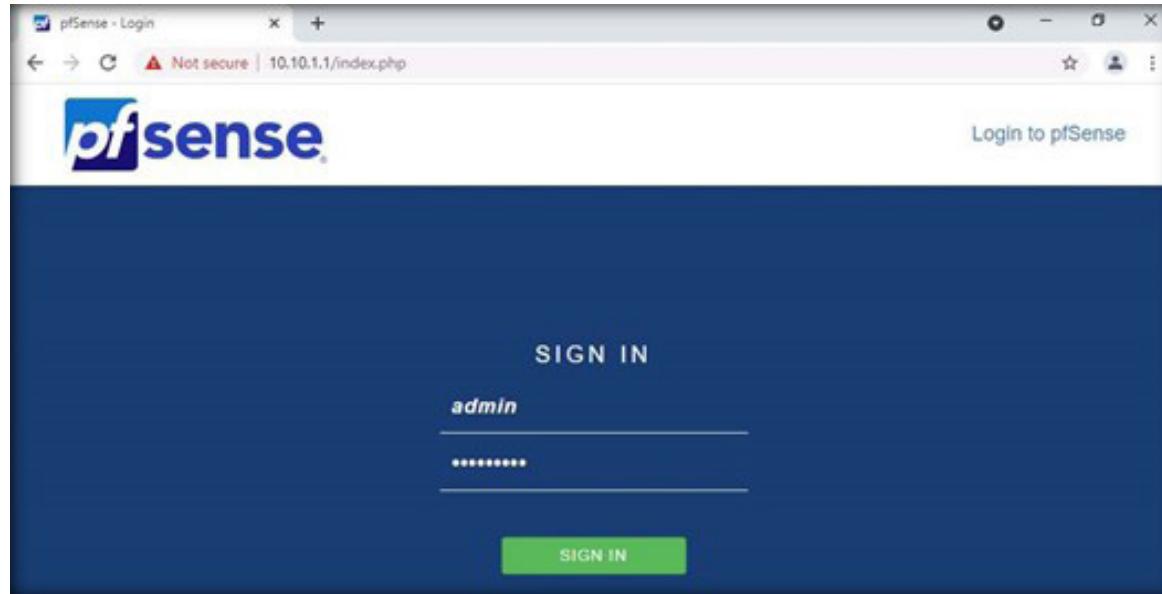
EXERCISE 4o

IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL

36. Close the tab and navigate to the pfSense **SIGN IN** page.

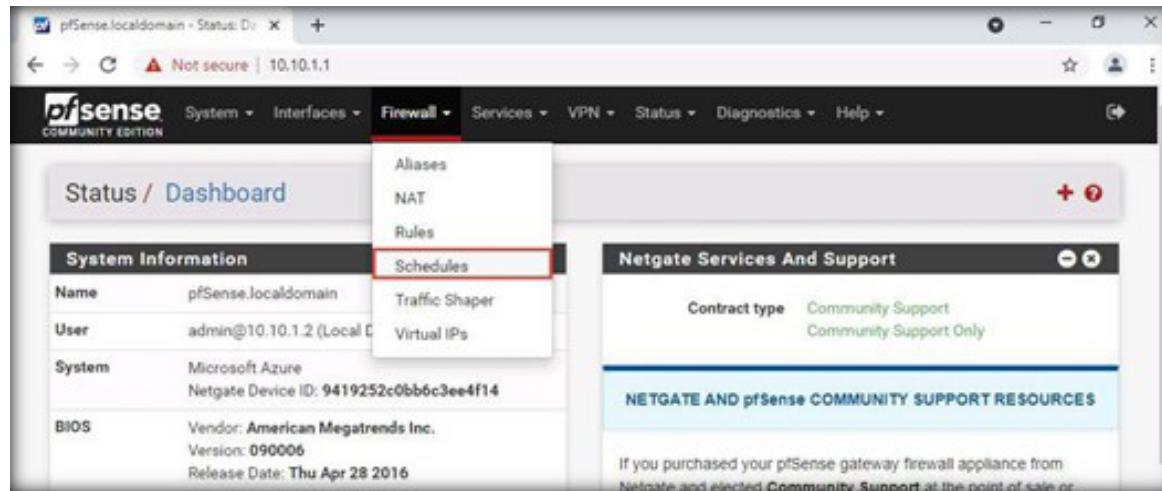
37. Now we will configure schedules for time-based rules

38. Type the username **admin** and password **admin@123** and click the **SIGN IN** button, as shown in the screenshot below.



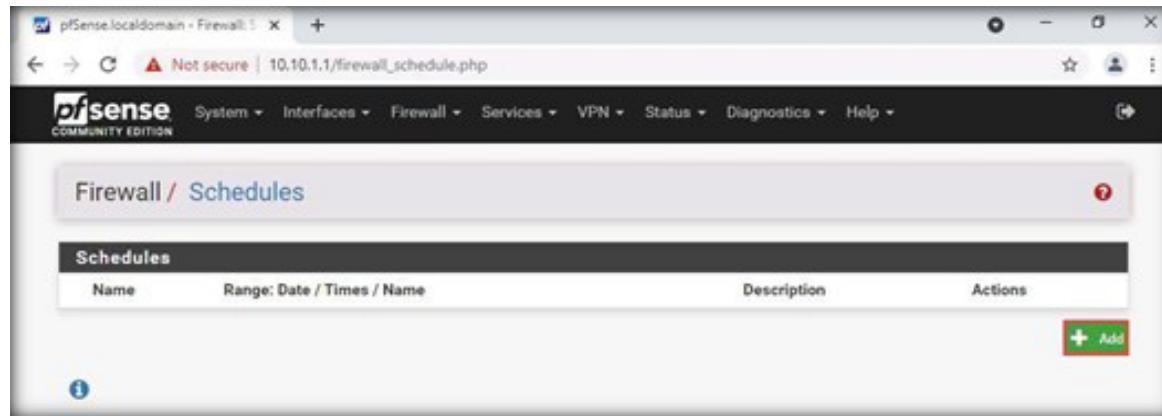
EXERCISE 4
**IMPLEMENT NETWORK-
BASED FIREWALL
FUNCTIONALITY: BLOCK
INSECURE PORTS USING
PFSENSE FIREWALL**

39. The pfSense Dashboard will appear. Navigate to **Firewall > Schedules** from the main menu.



EXERCISE 4^o
IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL

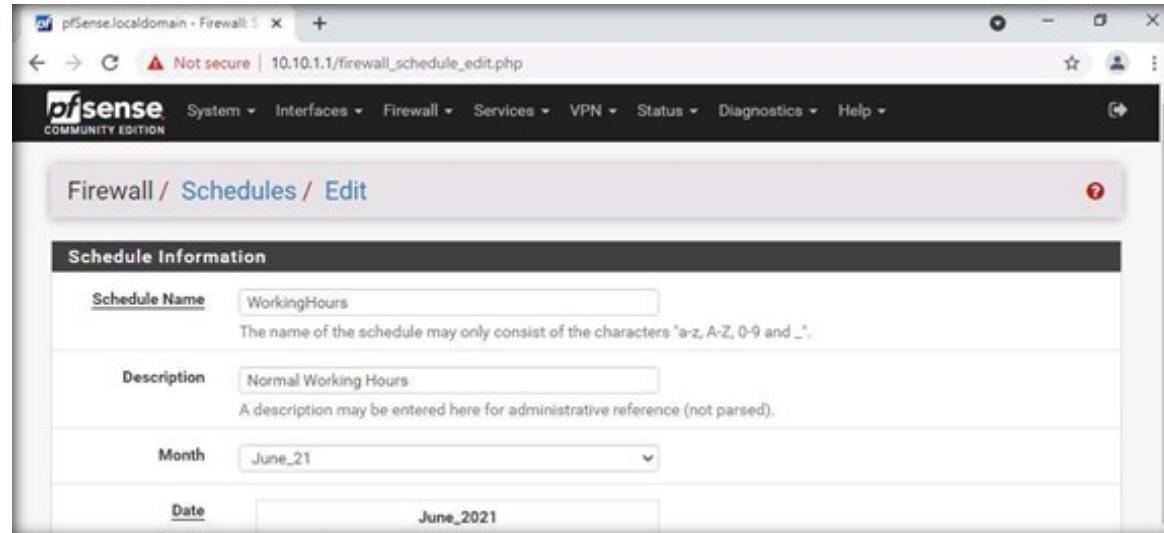
40. Click + Add button in the **Firewall/ Schedules** window.



EXERCISE 4^o
**IMPLEMENT NETWORK-
BASED FIREWALL
FUNCTIONALITY: BLOCK
INSECURE PORTS USING
PFSENSE FIREWALL**

41. The **Firewall/Schedules/Edit** window opens. Enter a name in the **Schedule Name** section under **Schedule Information** and enter description in the **Description** field.

Note: Schedule name must only contain letters and digits, no spaces. Here we have given the name as **WorkingHours** and **Normal Working Hours** as **Description**.

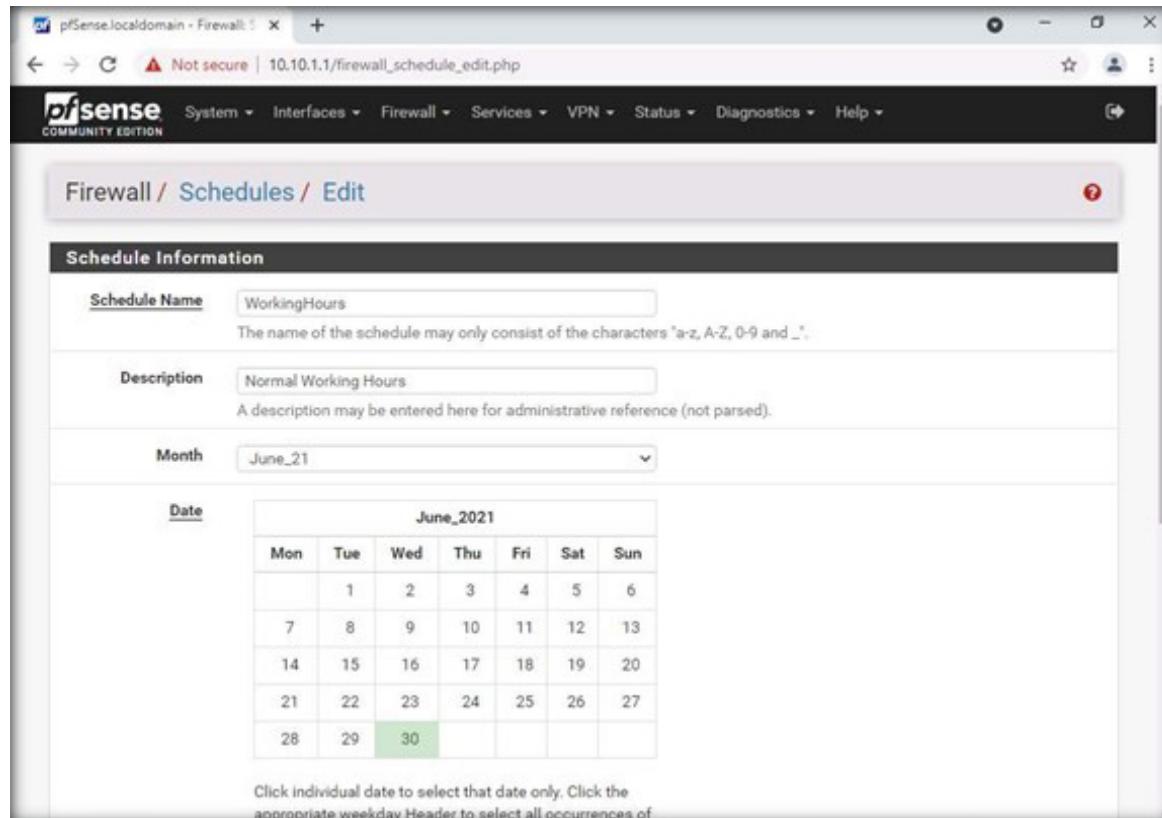


EXERCISE 4
IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL

42. Now set the **Month** by selecting a specific month and days, or by clicking the day of the week header for weekly recurring schedules.

Note: Here we are selecting a single day in a month.

EXERCISE 4 IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL

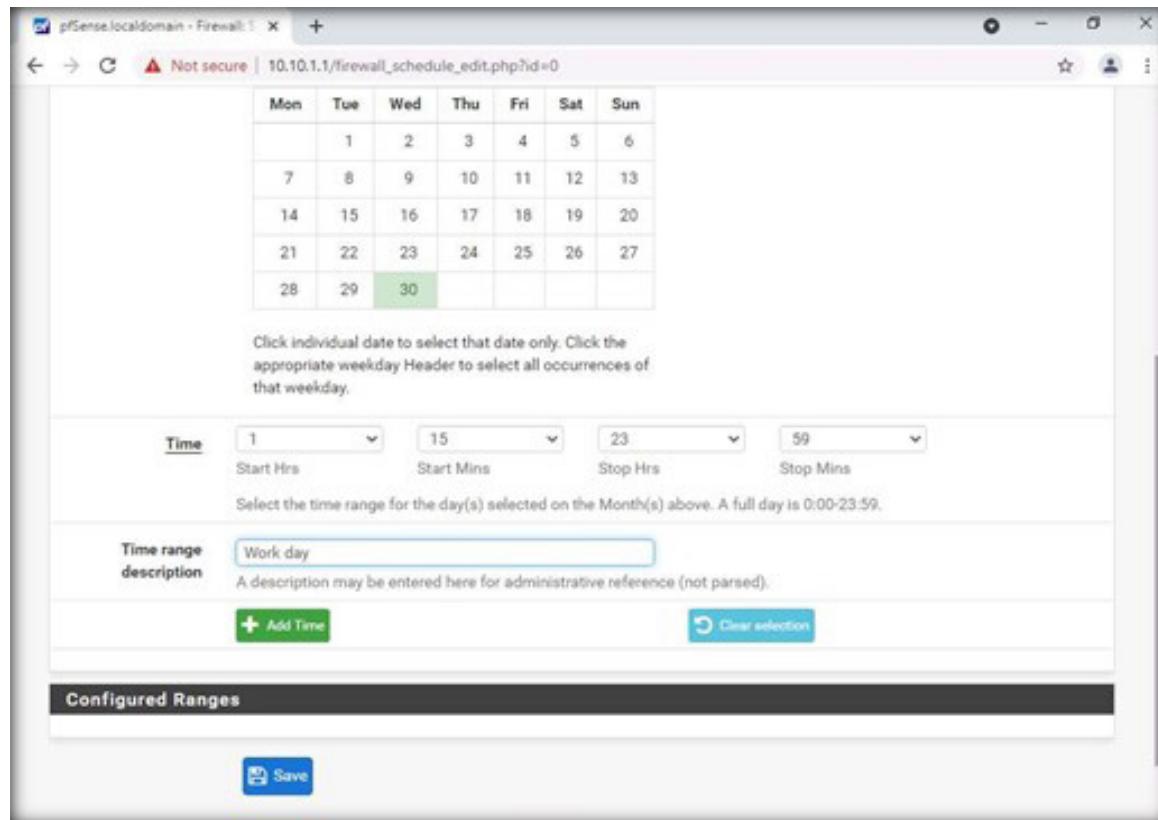


43. Choose a **Start Time** and **Stop Time** which control when the rule is active on the selected days. Enter an optional Time Range Description for this specific range.

Note: The time cannot cross midnight on any day. A full day is 0:00 to 23:59.

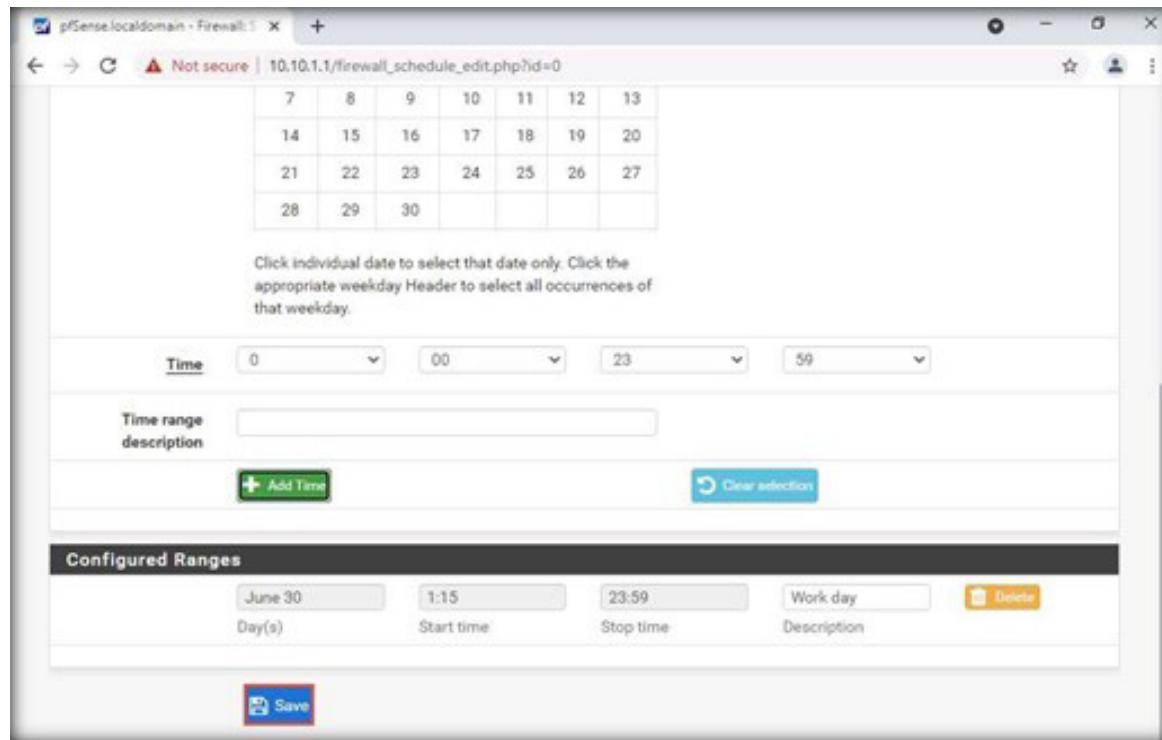
Note: While performing the task in the lab, make sure that the time you are selecting is 5 to 10 minutes ahead of the time.

EXERCISE 4
IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL

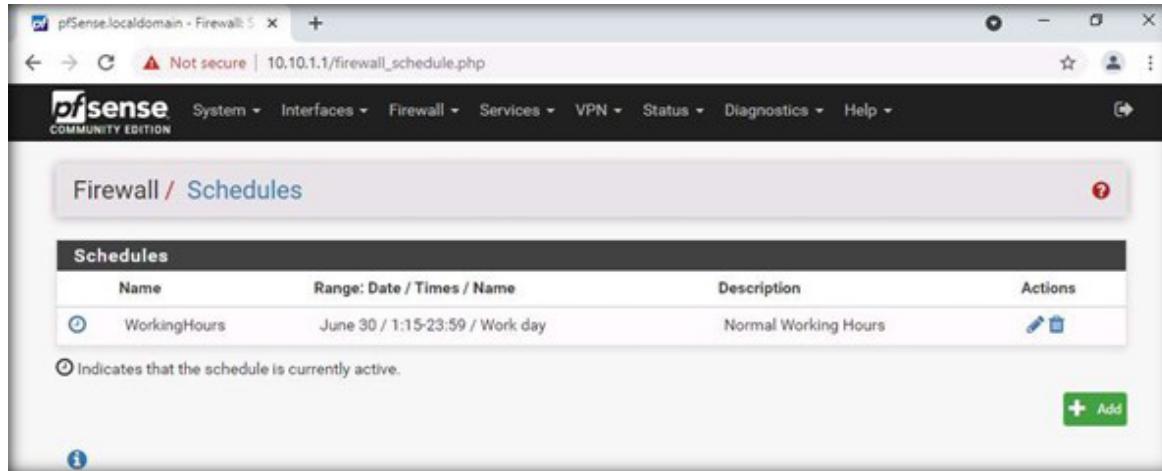


44. Click on **+ Add Time** to add the choices as range and click **Save**.

EXERCISE 4^o
**IMPLEMENT NETWORK-
BASED FIREWALL
FUNCTIONALITY: BLOCK
INSECURE PORTS USING
PFSENSE FIREWALL**



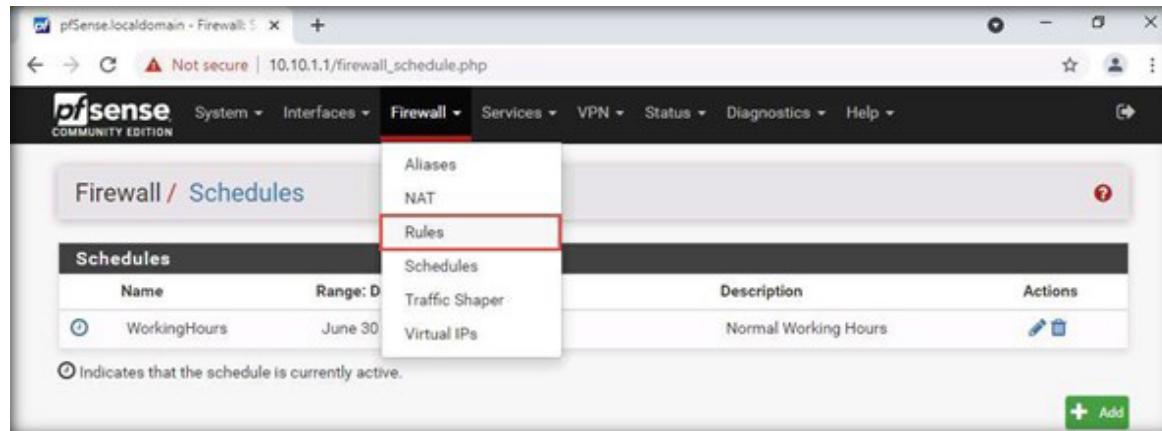
45. You will be redirected to the **Firewall / Schedules** page with the new schedule listed.



The screenshot shows a web browser window for the pfSense Community Edition interface. The title bar reads "pfSense.localdomain - Firewall: S". The address bar shows "Not secure | 10.10.1.1/firewall_schedule.php". The main content area is titled "Firewall / Schedules". Below it is a table titled "Schedules" with columns: Name, Range: Date / Times / Name, Description, and Actions. There is one entry: "WorkingHours" with the range "June 30 / 1:15-23:59 / Work day" and the description "Normal Working Hours". A note below the table says "(i) Indicates that the schedule is currently active." At the bottom right of the table is a green "Add" button with a plus sign.

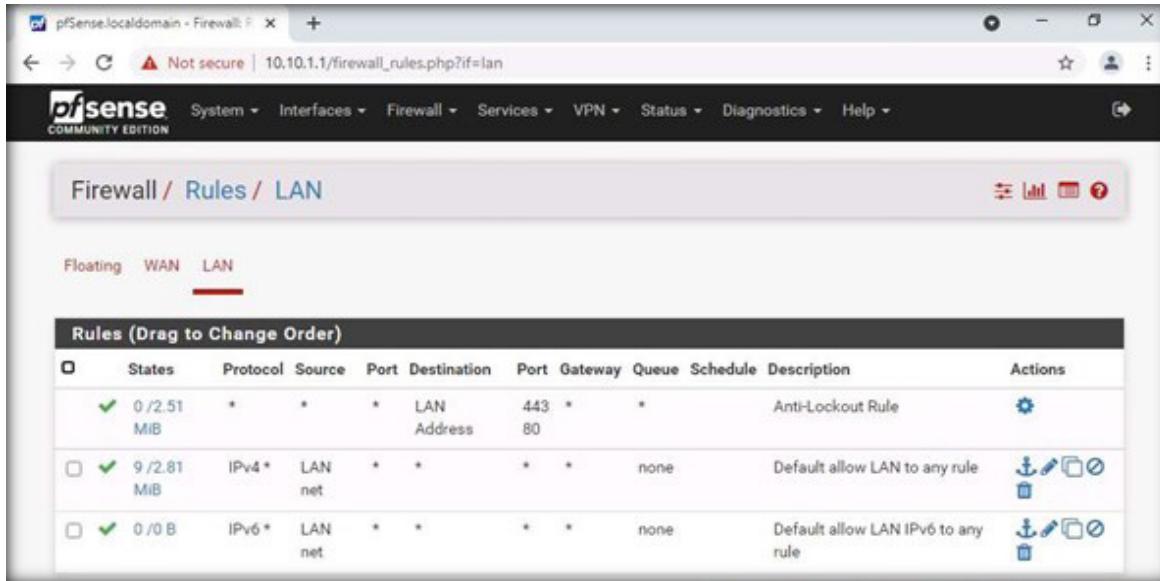
EXERCISE 4:
IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL

46. To create a new firewall rule, navigate to **Firewall > Rules** from the main menu.



EXERCISE 4^o
IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL

47. The **Firewall/Rules/WAN** page will appear. Click the **LAN** option.



The screenshot shows the pfSense Firewall Rules LAN page. The browser title is "pfSense.localdomain - Firewall: R". The address bar shows "Not secure | 10.10.1.1/firewall_rules.php?if=lan". The pfSense logo is at the top left. The navigation menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main title is "Firewall / Rules / LAN". Below it, there are tabs for Floating, WAN, and LAN, with LAN selected. A table titled "Rules (Drag to Change Order)" lists three rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0 / 2.51 MiB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	
✗ ✓ 9 / 2.81 MiB	IPv4	*	LAN net	*	*	*	*	none	Default allow LAN to any rule	
✗ ✓ 0 / 0 B	IPv6	*	LAN net	*	*	*	*	none	Default allow LAN IPv6 to any rule	

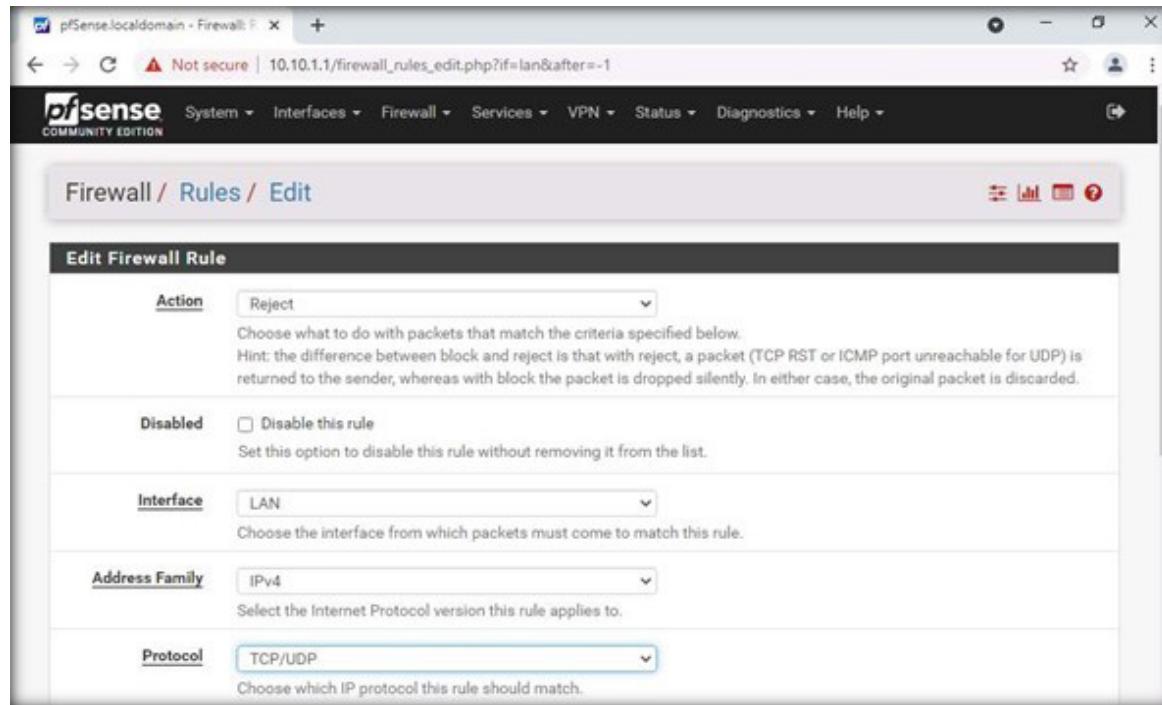
EXERCISE 4
IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL

48. To create a rule, click the up arrow **Add** button.

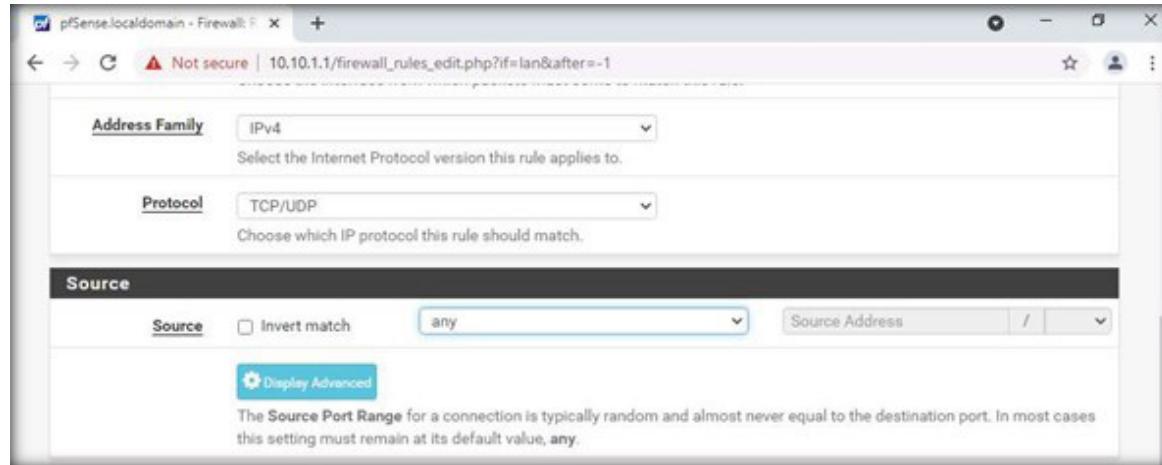
49. Set following details under **Edit Firewall Rule** section

- **Action** > Reject
- **Interface** > LAN
- **Address Family** > IPv4
- **Protocol** > TCP/UDP.

EXERCISE 4
IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL



50. Under **Source** section, select **any** from the dropdown as shown in the below screenshot.

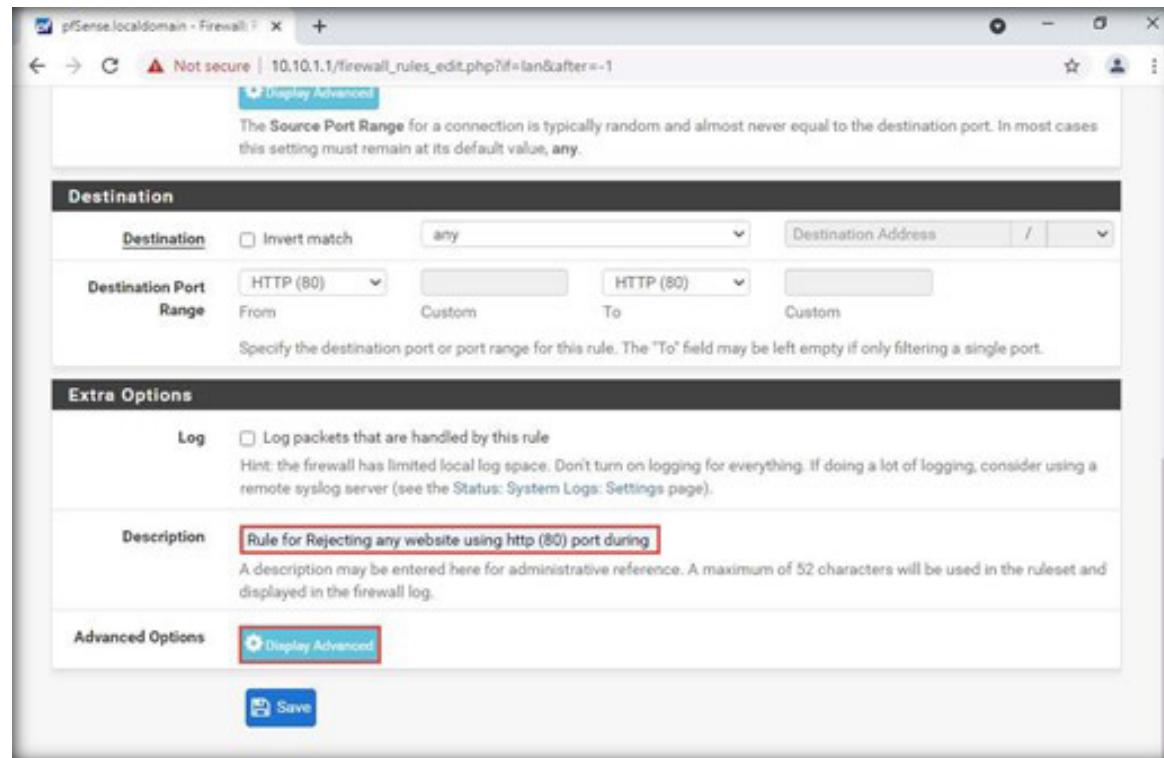


EXERCISE 4
IMPLEMENT NETWORK-
BASED FIREWALL
FUNCTIONALITY: BLOCK
INSECURE PORTS USING
PFSENSE FIREWALL

51. Under **Destination** section, select **any** from the dropdown and set **Destination Port Range** to **HTTP (80)** from the dropdown.

52. Scroll down. Under **Extra Options**, enter **Rule for Rejecting any website using http (80) port during Working Hours** in the **Description** field, and click on **Display Advanced**.

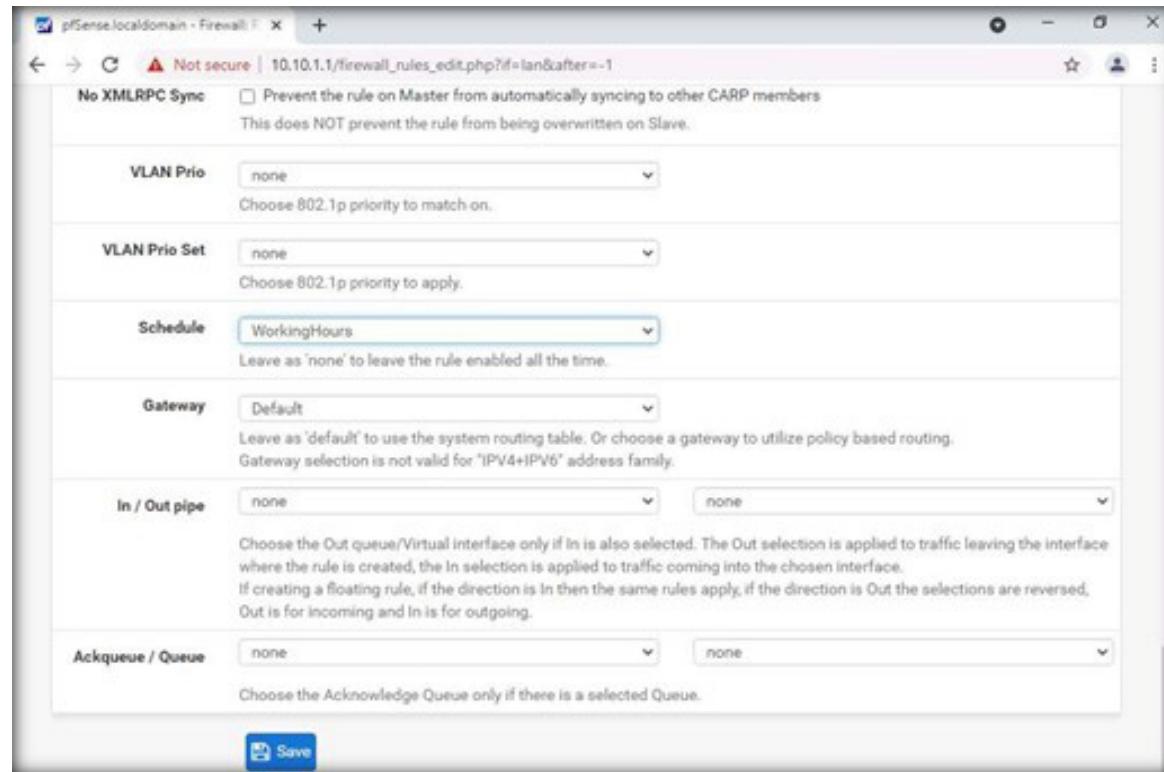
EXERCISE 4 IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL



53. In **Advanced Options** go to **Schedule** section and select the newly created **WorkingHours** Schedule from the drop down.

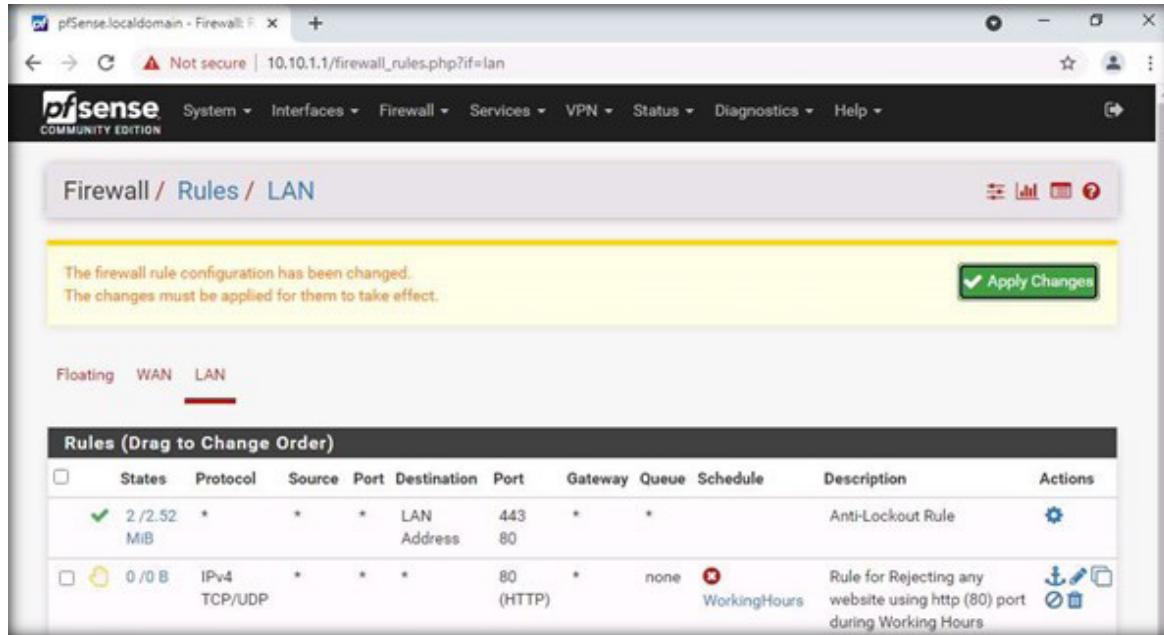
54. Leaving the other options set to default scroll down the page and click on **Save**.

EXERCISE 4
IMPLEMENT NETWORK-
BASED FIREWALL
FUNCTIONALITY: BLOCK
INSECURE PORTS USING
PFSENSE FIREWALL



55. The page will redirect to the Firewall/Rules/LAN page. Click **Apply Changes**.

EXERCISE 4
**IMPLEMENT NETWORK-
BASED FIREWALL
FUNCTIONALITY: BLOCK
INSECURE PORTS USING
PFSENSE FIREWALL**



The screenshot shows the pfSense Firewall Rules LAN page. A yellow message bar at the top states: "The firewall rule configuration has been changed. The changes must be applied for them to take effect." A green "Apply Changes" button is visible. Below the message, there are tabs for Floating, WAN, and LAN, with LAN selected. The main table displays two rules:

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	2 / 2.52 MIB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	*	*	*	80 (HTTP)	*	none WorkingHours	WorkingHours	Rule for Rejecting any website using http (80) port during Working Hours	

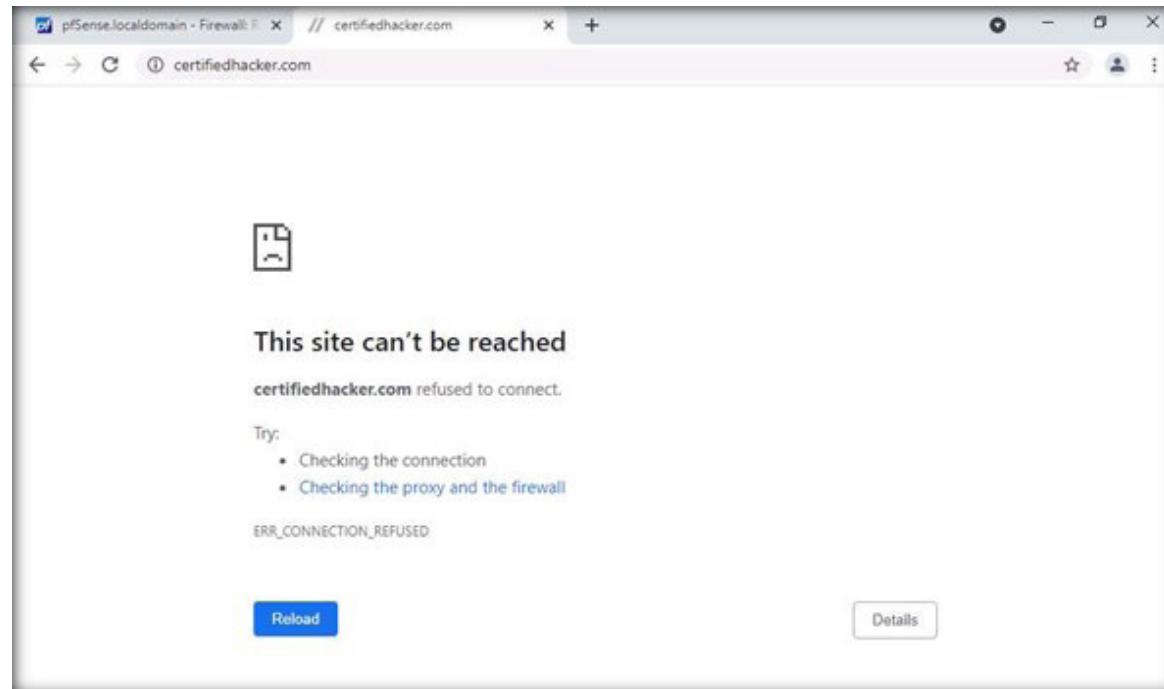
56. Reload the webpage and open a new tab in chrome browser and type <http://certifiedhacker.com/> in the address bar, and press **Enter**

Note: If a pop-up appears while reloading webpage, click on **Continue**.

Note: If changes are not affecting, then reboot the pfSense firewall and clear the Chrome browser cache.

EXERCISE 4^o

IMPLEMENT NETWORK-BASED FIREWALL FUNCTIONALITY: BLOCK INSECURE PORTS USING PFSENSE FIREWALL



57. You will see the message as **This site can't be reached**. This is because the pfSense firewall rule is now preventing port http.
58. Delete the newly created firewall rule before proceeding to the next lab.
59. Close the current tab and perform **Step 25 to Step 34** to delete the newly created rule and to reboot the pfSense firewall.
60. After the pfSense firewall is rebooted, close all open windows.
61. Turn off **Admin Machine-1** and **AD Domain Controller** virtual machines.

EXERCISE 5: IMPLEMENT HOST-BASED IDS FUNCTIONALITY USING WAZUH HIDS

Host-based Intrusion Detection Systems (HIDS) detect the events on the server and generate alerts.

LAB SCENARIO

Intrusion Detection Systems (IDS) helps monitor network activity. HIDS enables a security professional to monitor the network traffic for malicious activity or policy violations. Using Wazuh enables security professionals to perform continuous monitoring and respond to advanced threats.

LAB OBJECTIVE

This lab will demonstrate the use of Wazuh HIDS and agent to capture network traffic and show how to monitor the captured traffic for malicious activities. In this lab, you will learn the following:

- Installing and configuring Wazuh HIDS and Wazuh agent
- Monitoring network traffic for malicious activity using Sguil

OVERVIEW OF THE LAB

Host Intrusion Detection is a requirement for today's networks. Attacks and threats can be monitored easily because the full communication stream can be inspected using HIDS. Host-based IDS (HIDS) deployment is done with proper planning and care, as deploying these on a large-scale environment has the potential to generate numerous false alarms, which can get quite difficult to manage. Initial deployment of a HIDS is done on critical servers only. Security professional must consider implementing an IDS management console before adding additional hosts.

LAB TASKS

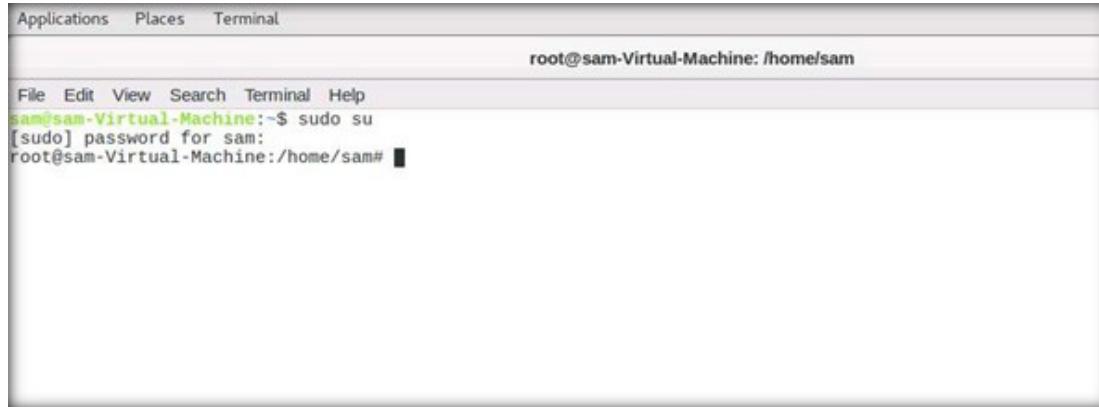
Note: Ensure that **Web Server** and **PfSense Firewall** virtual machines are running.

- EXERCISE 5:
**IMPLEMENT HOST-BASED
IDS FUNCTIONALITY USING
WAZUH HIDS**
1. Turn on **Admin Machine-2** and **Attacker Machine-1** virtual machines.
 2. Log in with the username **sam** and password **admin@123**.
 3. To configure Wazuh HIDS for detecting endpoint suspicious activity, right-click on the desktop, and select the **Open Terminal** option from the pop-up list as shown in the screenshot below.



4. When the terminal window appears, type command **sudo su**, and press the **Enter** button. When it prompts for the password, type the system password **admin@123** and press **Enter**.

Note: The password that you type will not be visible.

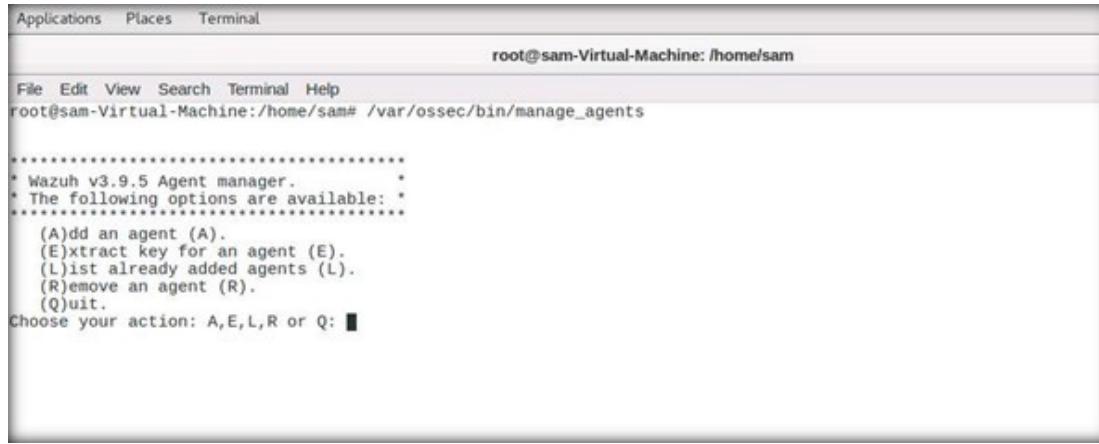


The screenshot shows a terminal window with a menu bar at the top labeled "Applications", "Places", and "Terminal". The main area of the terminal shows the following text:

```
root@sam-Virtual-Machine: /home/sam
File Edit View Search Terminal Help
sam@sam-Virtual-Machine:~$ sudo su
[sudo] password for sam:
root@sam-Virtual-Machine:/home/sam#
```

EXERCISE 5: IMPLEMENT HOST-BASED IDS FUNCTIONALITY USING WAZUH HIDS

5. To add the **Web Server** virtual machine as the Wazuh agent, type command **/var/ossec/bin/manage_agents** and press **Enter**, as shown in the screenshot below.



The terminal window shows the following output:

```
root@sam-Virtual-Machine: /home/sam#
File Edit View Search Terminal Help
root@sam-Virtual-Machine:/home/sam# /var/ossec/bin/manage_agents

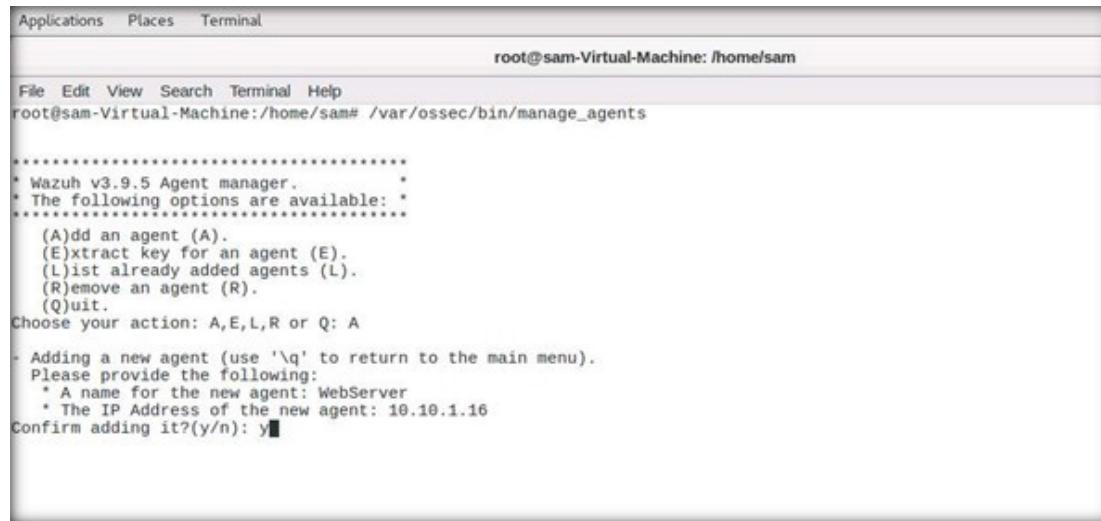
*****
* Wazuh v3.9.5 Agent manager.          *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: ■
```

EXERCISE 5:
**IMPLEMENT HOST-BASED
IDS FUNCTIONALITY USING
WAZUH HIDS**

6. The list of options is displayed. Type **A** to add the new agent (**Web Server**) for the monitor and press **Enter**.

7. You will be prompted to add new agent details. Provide the following details as shown in the screenshot below, and press **Enter**:

- **A name for the new agent:** WebServer
- **The IP address of the new agent:** 10.10.1.16
- **Confirm adding it? (y/n):** y



The terminal window shows the Wazuh v3.9.5 Agent manager interface. The user has run the command `/var/ossec/bin/manage_agents`. The screen displays a menu with the following options:

```
File Edit View Search Terminal Help
root@sam-Virtual-Machine:/home/sam# /var/ossec/bin/manage_agents

*****
* Wazuh v3.9.5 Agent manager.          *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.

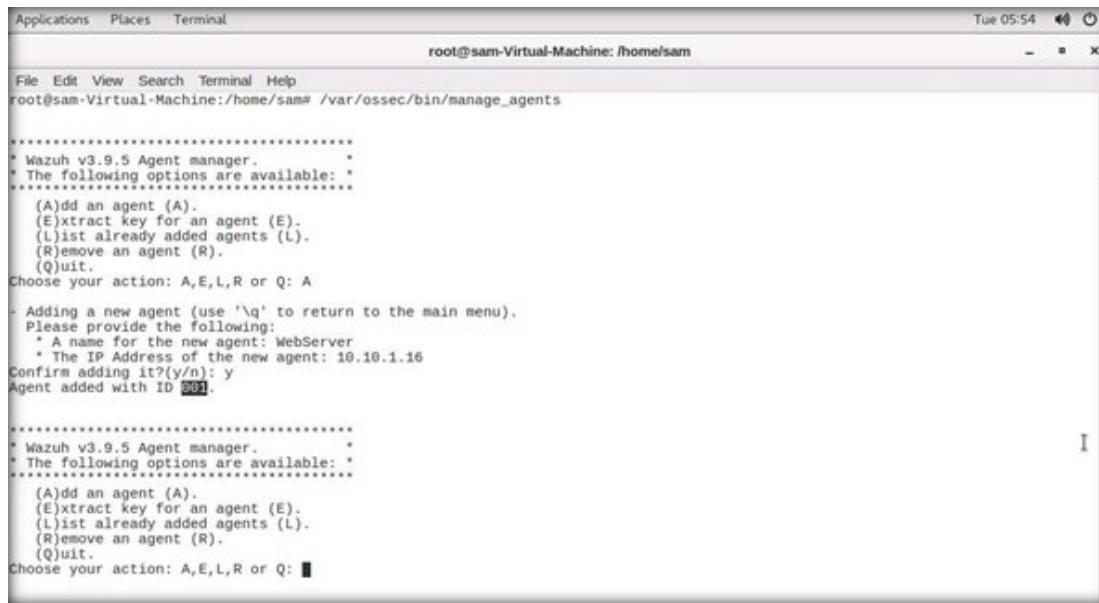
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
Please provide the following:
* A name for the new agent: WebServer
* The IP Address of the new agent: 10.10.1.16
Confirm adding it?(y/n): y
```

**EXERCISE 5:
IMPLEMENT HOST-BASED
IDS FUNCTIONALITY USING
WAZUH HIDS**

8. The Wazuh agent manager will add a new agent. The agent ID here is **001**. (It may differ in your lab).

EXERCISE 5: IMPLEMENT HOST-BASED IDS FUNCTIONALITY USING WAZUH HIDS



The screenshot shows a terminal window titled 'root@sam-Virtual-Machine: /home/sam'. The command '/var/ossec/bin/manage_agents' was run, which prompted the user to add a new agent. The user chose option 'A' to add a new agent, provided a name 'WebServer', and specified the IP address '10.10.1.16'. The confirmation step showed 'Agent added with ID 001'. The process was then repeated, showing the same options and steps.

```
root@sam-Virtual-Machine: /home/sam# /var/ossec/bin/manage_agents

*****
* Wazuh v3.9.5 Agent manager.
* The following options are available:
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.

Choose your action: A,E,L,R or Q: A

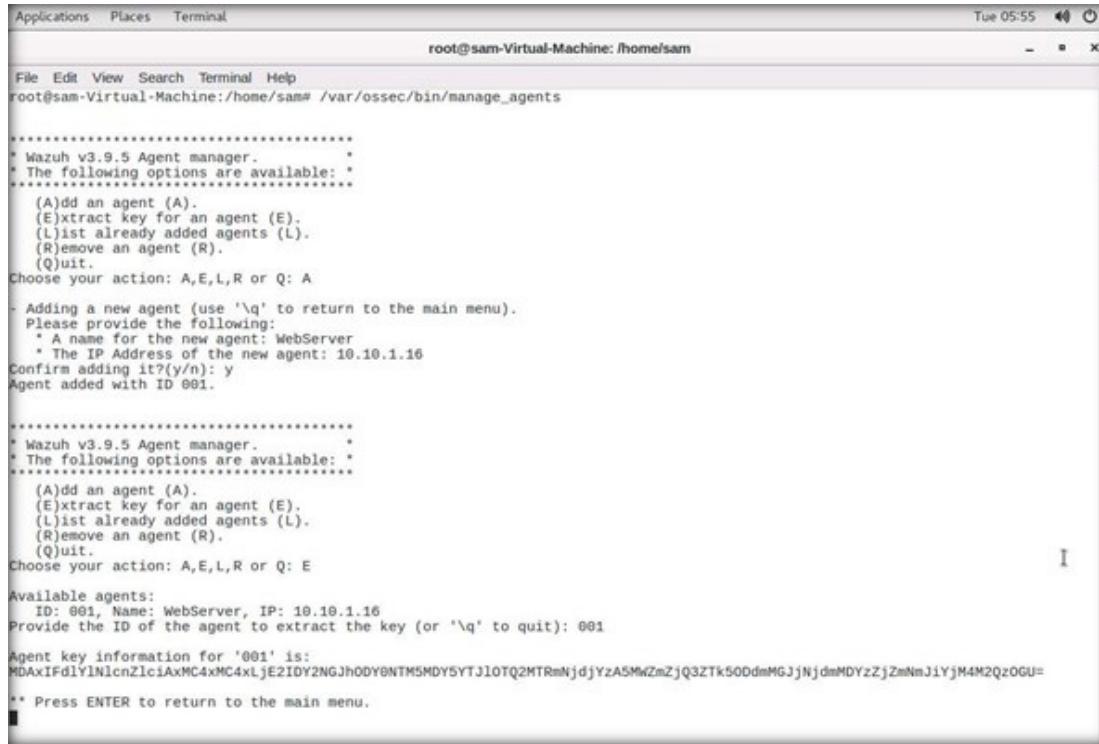
- Adding a new agent (use '\q' to return to the main menu).
Please provide the following:
* A name for the new agent: WebServer
* The IP Address of the new agent: 10.10.1.16
Confirm adding it?(y/n): y
Agent added with ID 001.

*****
* Wazuh v3.9.5 Agent manager.
* The following options are available:
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.

Choose your action: A,E,L,R or Q: ■
```

9. To extract the key for the agent (WebServer), type **E** and press **Enter**. You will be prompted to provide the agent ID to extract the key. Type **001** (In your lab, it may differ).

EXERCISE 5: IMPLEMENT HOST-BASED IDS FUNCTIONALITY USING WAZUH HIDS



```
root@sam-Virtual-Machine: /home/sam# /var/ossec/bin/manage_agents

*****
* Wazuh v3.9.5 Agent manager. *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.

Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
Please provide the following:
* A name for the new agent: WebServer
* The IP Address of the new agent: 10.10.1.16
Confirm adding it?(y/n): y
Agent added with ID 001.

*****
* Wazuh v3.9.5 Agent manager. *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.

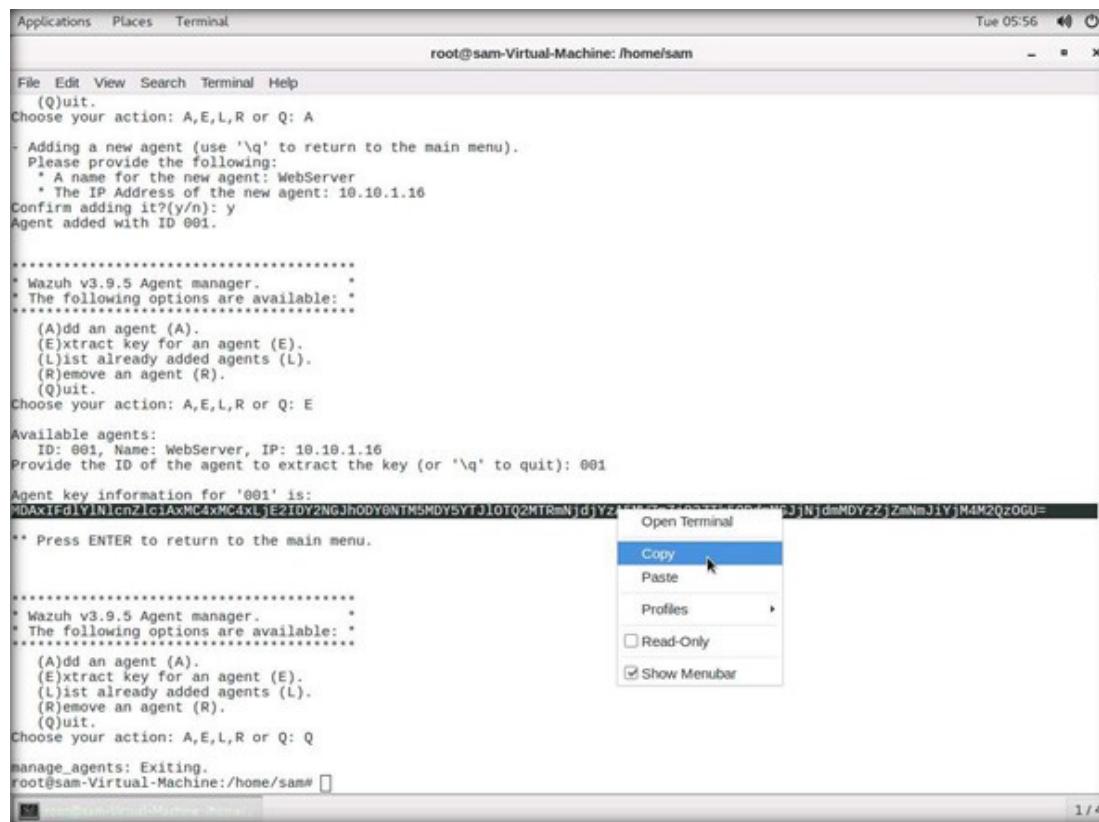
Choose your action: A,E,L,R or Q: E

Available agents:
ID: 001, Name: WebServer, IP: 10.10.1.16
Provide the ID of the agent to extract the key (or "\q" to quit): 001

Agent key information for '001' is:
MDAxIFd1YlNlcenZlciAxMC4xMC4xLjE2IDY2NGJhODY0NTM5MDY5YTJlOTQ2MTNmNjdjYzASMwZmZjQ3ZTk50DdmMGJjNjdmMDYzZjZmNmJ1YjN4M2QzOGU=
** Press ENTER to return to the main menu.
```

10. Press **Enter** to continue, and type **Q** to quit agent configuration. **Copy** the extracted **key**.

EXERCISE 5: IMPLEMENT HOST-BASED IDS FUNCTIONALITY USING WAZUH HIDS



```
root@sam-Virtual-Machine:/home/sam
File Edit View Search Terminal Help
  (Q)uit.
Choose your action: A,E,L,R or Q: A
- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
    * A name for the new agent: WebServer
    * The IP Address of the new agent: 10.10.1.16
Confirm adding it?(y/n): y
Agent added with ID 001.

*****
* Wazuh v3.9.5 Agent manager. *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: E

Available agents:
  ID: 001, Name: WebServer, IP: 10.10.1.16
Provide the ID of the agent to extract the key (or '\q' to quit): 001

Agent key information for '001' is:
W0AxIfdIYiNlcnZicIAxMC4xMC4xLjE2IDY2NGJhODY0NTM5MDY5YTJlOTQ2MTRmNjdjYzA...PQ= [REDACTED]
Open Terminal
  Copy [highlighted]
  Paste
  Profiles
   Read-Only
   Show Menubar

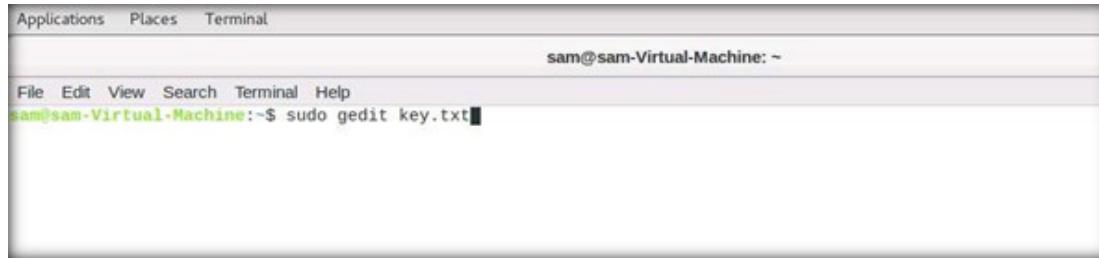
** Press ENTER to return to the main menu.

*****
* Wazuh v3.9.5 Agent manager. *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: Q

manage_agents: Exiting.
root@sam-Virtual-Machine:/home/sam#
```

11. Open another terminal window and type **sudo gedit key.txt**. Press **Enter**. If prompts for password type **admin@123** as password.

Note: The password that you type will not be visible.



The screenshot shows a terminal window with a light gray background and a dark gray header bar. The header bar contains the text "Applications", "Places", and "Terminal". Below the header bar, the terminal prompt "sam@sam-Virtual-Machine: ~" is displayed. The main area of the terminal shows the command "File Edit View Search Terminal Help" followed by the command "sam@sam-Virtual-Machine:~\$ sudo gedit key.txt". The cursor is positioned at the end of the command line.

EXERCISE 5:
**IMPLEMENT HOST-BASED
IDS FUNCTIONALITY USING
WAZUH HIDS**

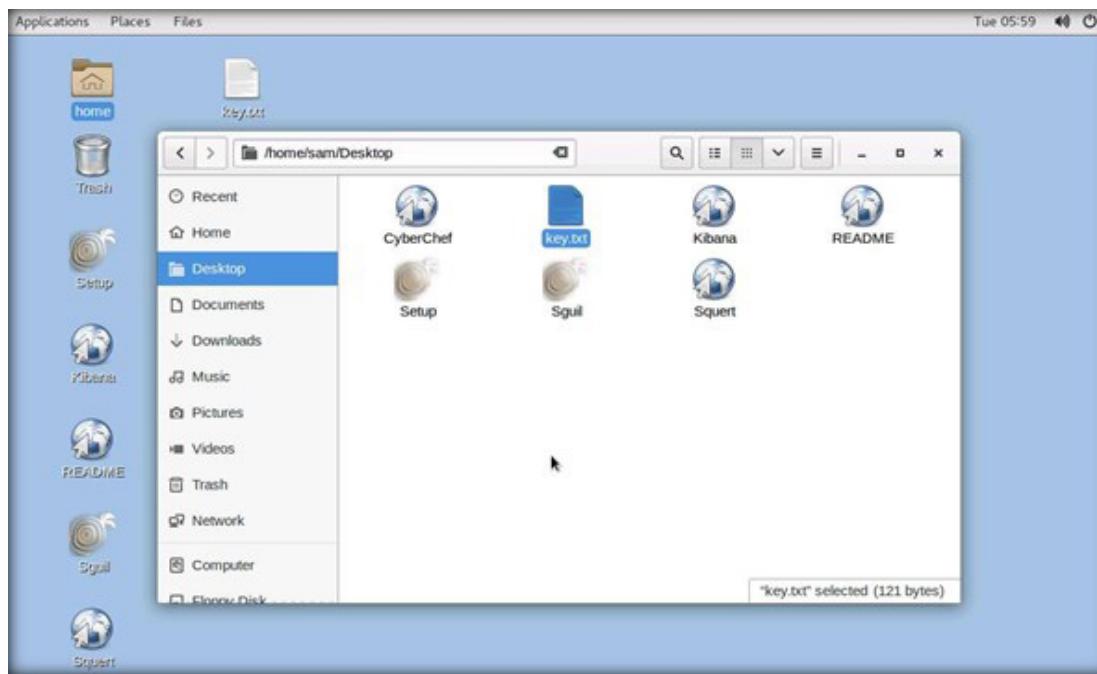
12. The new **key.txt** file opens. Paste the **copied extracted key**.



EXERCISE 5: IMPLEMENT HOST-BASED IDS FUNCTIONALITY USING WAZUH HIDS

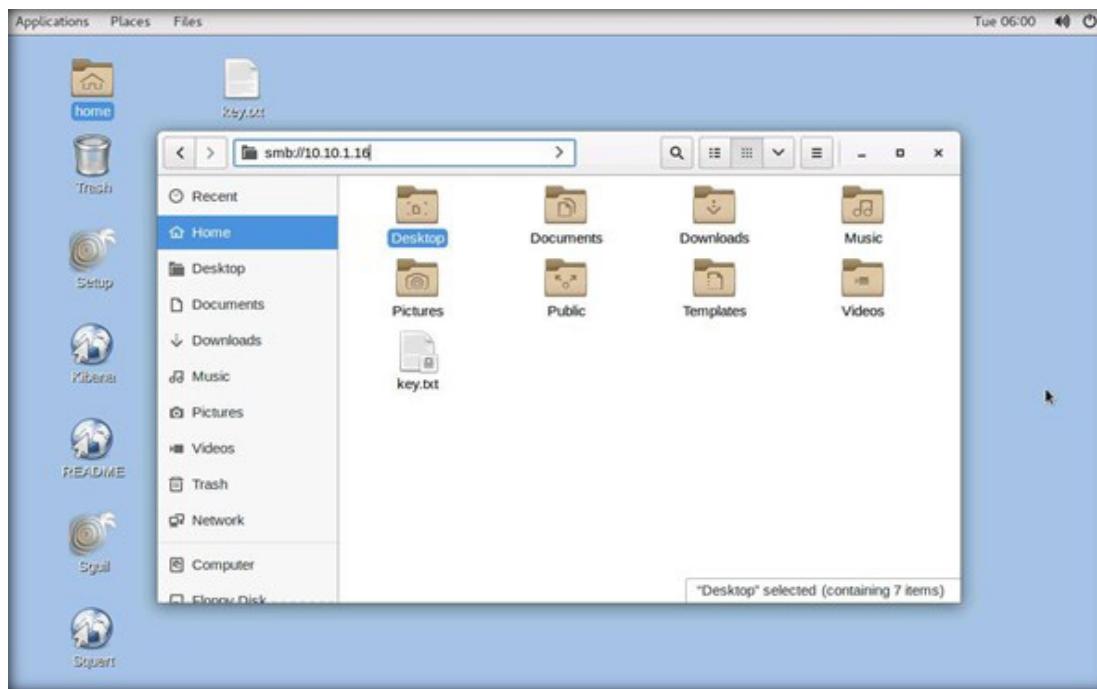
13. Save the file. Close all windows. Open **home** folder from **Desktop**, copy **key.txt** file to Desktop.

EXERCISE 5: IMPLEMENT HOST-BASED IDS FUNCTIONALITY USING WAZUH HIDS



14. Open the **home** folder from the Desktop and press **CTRL + L** This will enable the search textbox. Type **smb://10.10.1.16** and press the **Enter** button.

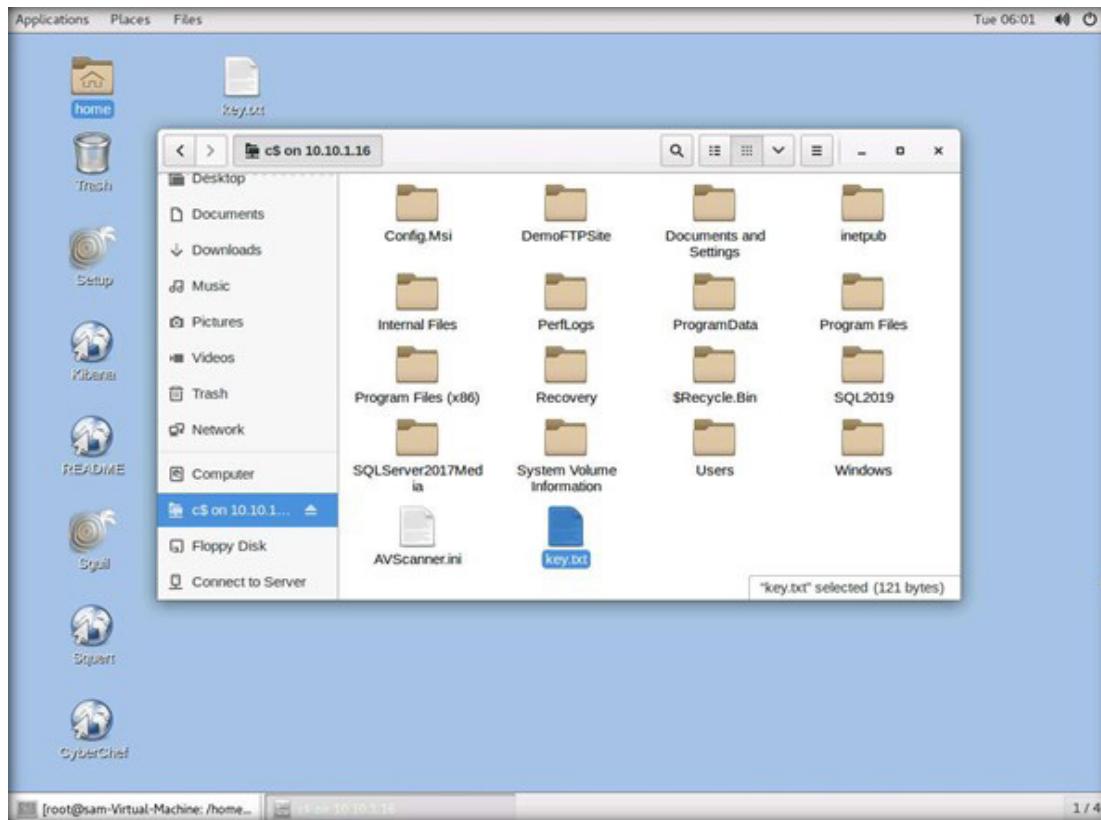
EXERCISE 5:
**IMPLEMENT HOST-BASED
IDS FUNCTIONALITY USING
WAZUH HIDS**



15. If prompted to enter the password, type the username **Administrator** and password **admin@123**. Click **Connect**.

16. The Windows share folder opens, open **C\$** folder. Go to the desktop and copy the **key.txt** file. Switch back to the Windows share folder, open the **C\$** folder, and paste the **key.txt** file.

EXERCISE 5: IMPLEMENT HOST-BASED IDS FUNCTIONALITY USING WAZUH HIDS



17. We have shared the agent key to **Web Server**. To configure the firewall to communicate with the agent, open terminal and type **sudo ufw allow proto udp from 10.10.1.16 to 10.10.1.79 port 1514** as shown in the screenshot below, and press the **Enter** button, if prompts for the password, then type **admin@123** as password and press **Enter** button.



The screenshot shows a terminal window with a grey header bar containing 'Applications', 'Places', and 'Terminal'. Below the header, the terminal prompt is 'sam@sam-Virtual-Machine: ~'. The user has typed the command 'sudo ufw allow proto udp from 10.10.1.16 to 10.10.1.79 port 1514' and is currently pressing the Enter key. The terminal window has a light grey background and a dark grey scroll bar on the right side.

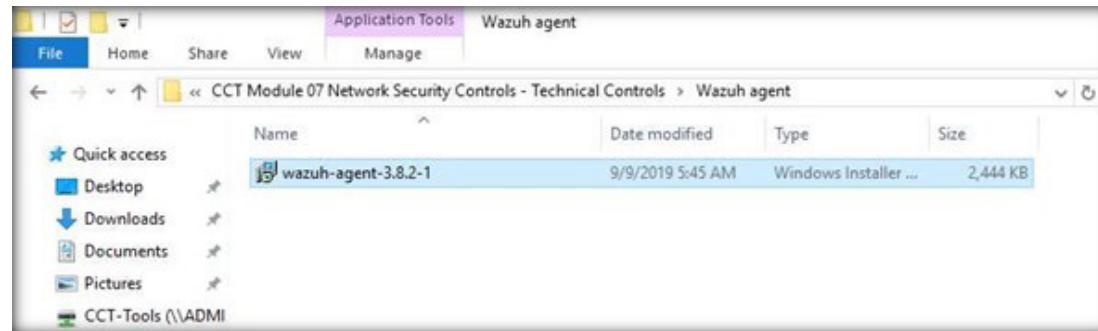
EXERCISE 5:
**IMPLEMENT HOST-BASED
IDS FUNCTIONALITY USING
WAZUH HIDS**

18. The firewall will be configured to allow communication between **Web Server** and **Admin Machine-2** machines.

19. Switch to the **Web Server** virtual machine.

Note: If you are not logged into the **Web Server** virtual machine, then log in using credentials **Administrator** and **admin@123**.

20. Navigate to **Z:\CCT Module 07 Network Security Controls - Technical Controls\Wazuh agent**. Double click **Wazuh-agent-3.8.2-1** and follow the wizard-driven installation.

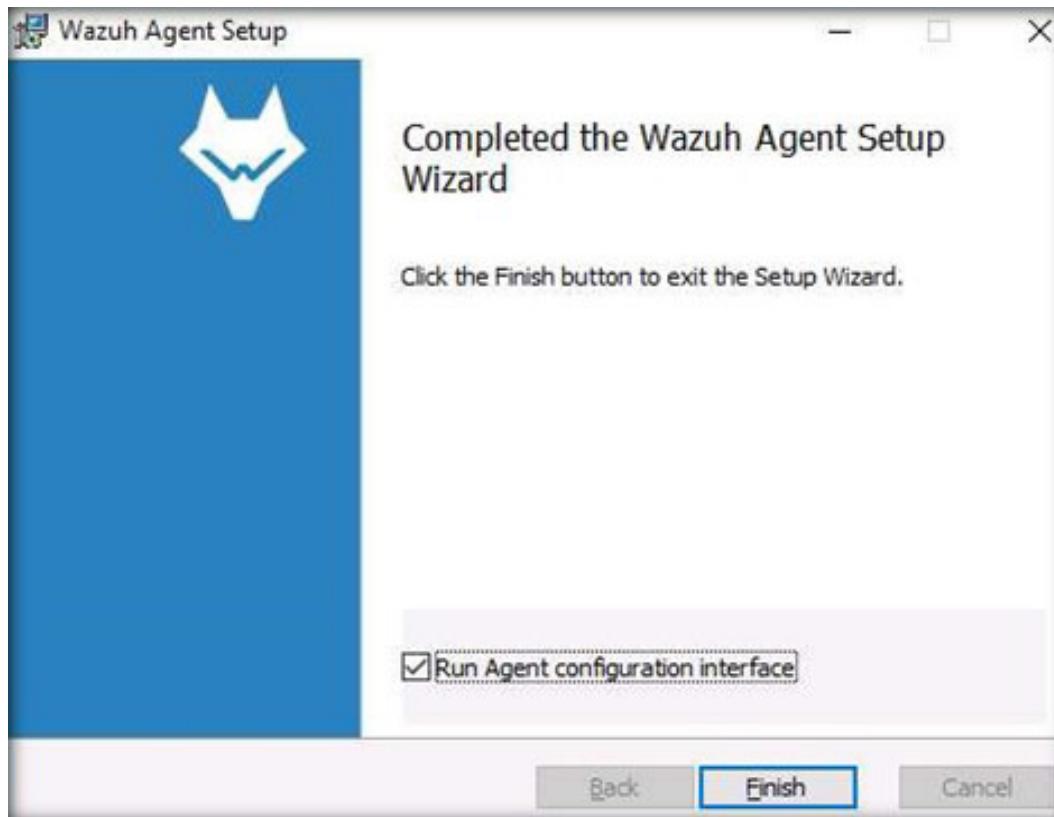


EXERCISE 5:
**IMPLEMENT HOST-BASED
IDS FUNCTIONALITY USING
WAZUH HIDS**

EXERCISE 5:
**IMPLEMENT HOST-BASED
IDS FUNCTIONALITY USING
WAZUH HIDS**

Note: If an **Open File-Security Warning** appears click **Run**.

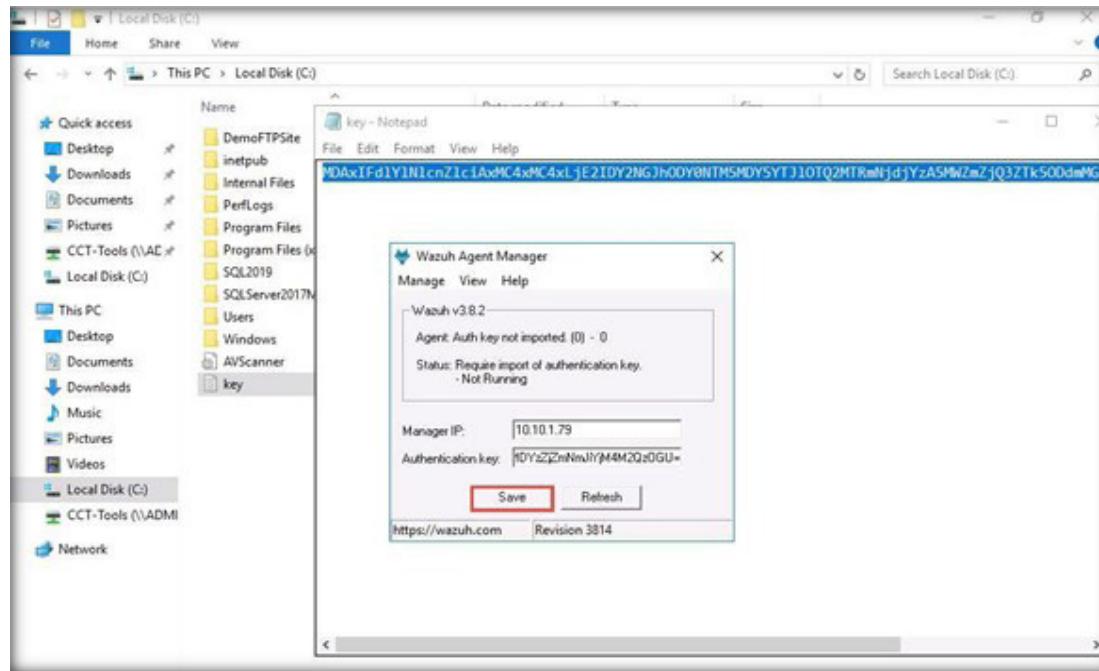
21. Check **I accept the terms in the License Agreement** and click **Install**.
22. Check **Run Agent configuration interface** and click **Finish** to complete the installation.



23. Once the installation is complete, the Wazuh Agent Manager window will open.

24. Type the IP address (**10.10.1.79**) of the Wazuh manager that is **Admin Machine-2** into the Manager IP field. Copy the agent key from the shared **C:\key.txt** file and paste into the Authentication key field. Click **Save**.

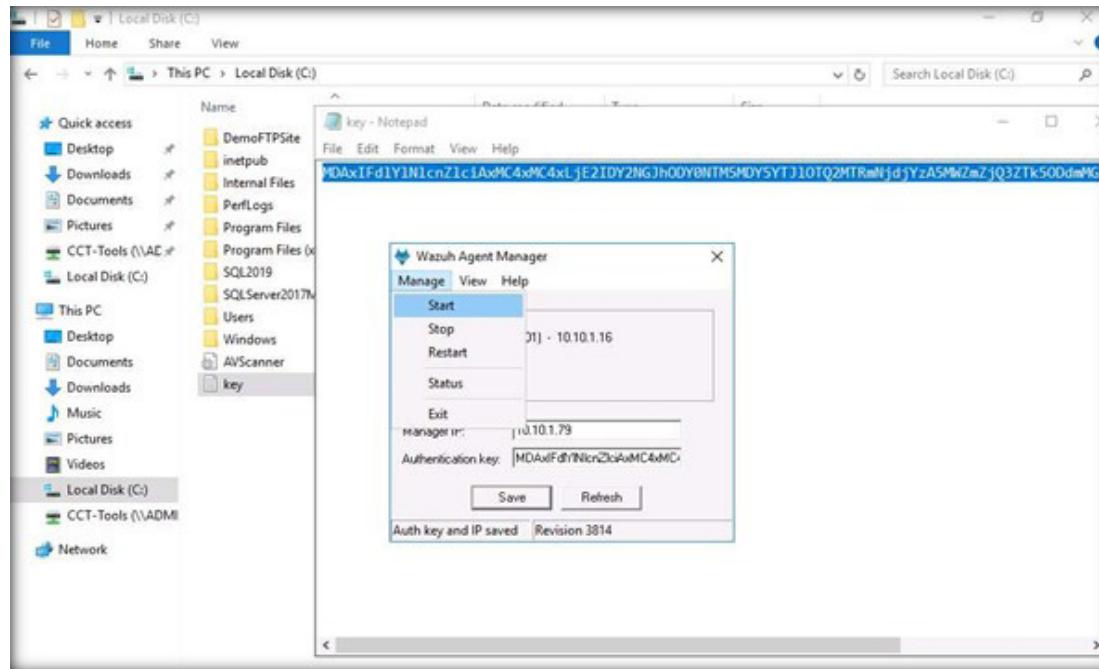
EXERCISE 5: IMPLEMENT HOST-BASED IDS FUNCTIONALITY USING WAZUH HIDS



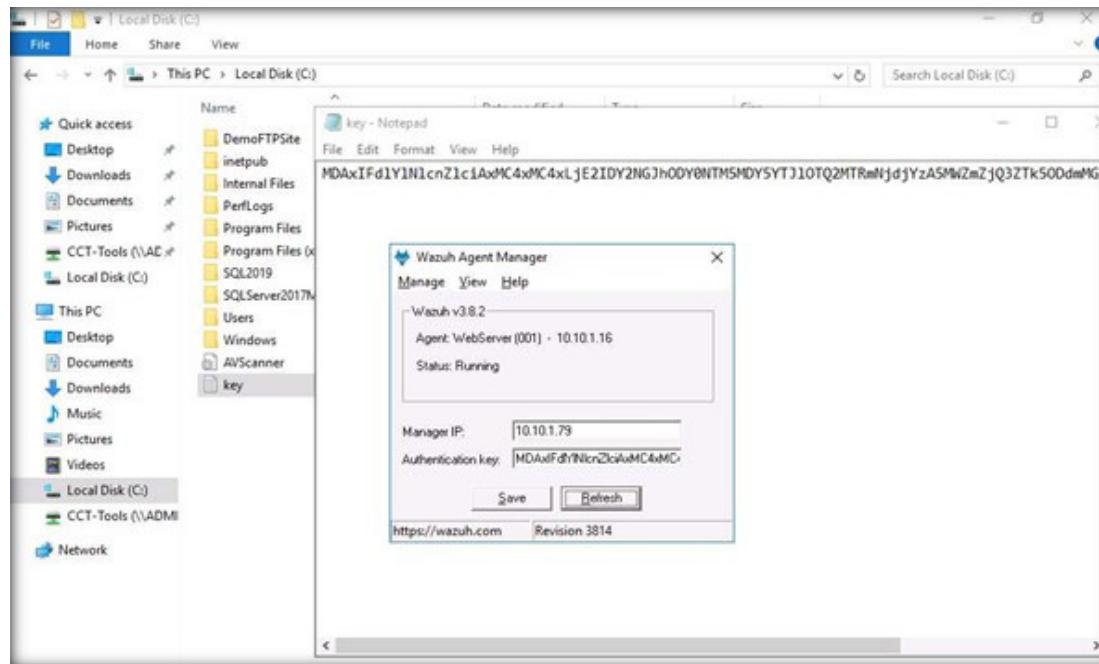
25. Click **OK** to confirm the importing key.

26. Manager IP will be added. By default, the Wazuh agent manager will be **stopped**. Select **Manage > Start** from the main menu and click **OK** for the prompted message.

EXERCISE 5: IMPLEMENT HOST-BASED IDS FUNCTIONALITY USING WAZUH HIDS



27. Click Refresh to view the **Running** status of the agent.



EXERCISE 5: IMPLEMENT HOST-BASED IDS FUNCTIONALITY USING WAZUH HIDS

28. Switch back to the **Admin Machine-2** virtual machine, login with password **admin@123**.

29. Open terminal in root privileges using **sudo su** command and type **/var/ossec/bin/ossec-control restart**, press **Enter**.

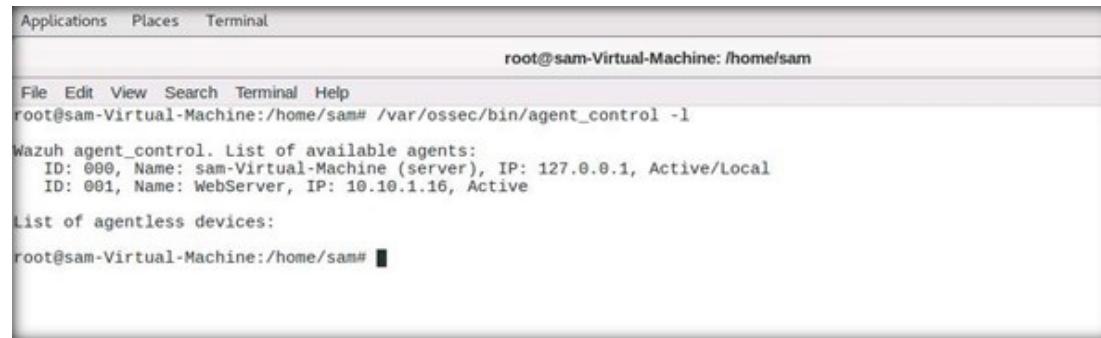


The screenshot shows a terminal window with a grey header bar containing "Applications", "Places", and "Terminal". The main area of the terminal shows the following text:

```
root@sam-Virtual-Machine: /home/sam
File Edit View Search Terminal Help
sam@sam-Virtual-Machine:~$ sudo su
[sudo] password for sam:
root@sam-Virtual-Machine:/home/sam# /var/ossec/bin/ossec-control restart
```

EXERCISE 5:
**IMPLEMENT HOST-BASED
IDS FUNCTIONALITY USING
WAZUH HIDS**

30. To check whether the agent is active, type **/var/ossec/bin/agent_control -l** and press **Enter**. You will see the **WebServer** agent that we added as Active.

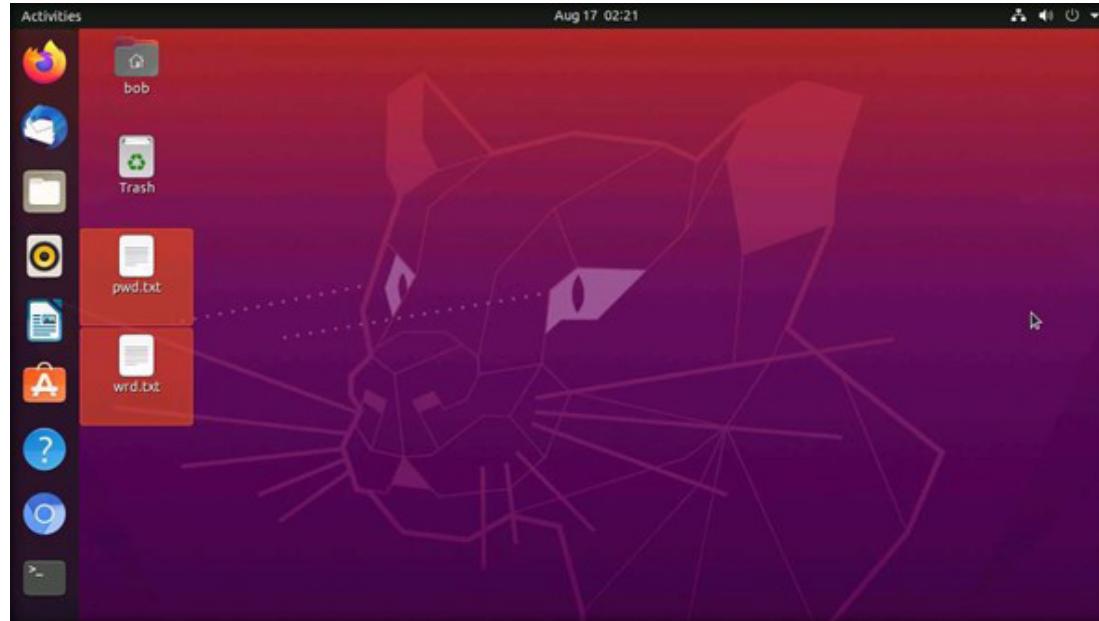


```
root@sam-Virtual-Machine:/home/sam
File Edit View Search Terminal Help
root@sam-Virtual-Machine:/home/sam# /var/ossec/bin/agent_control -l
Wazuh agent_control. List of available agents:
  ID: 000, Name: sam-Virtual-Machine (server), IP: 127.0.0.1, Active/Local
  ID: 001, Name: WebServer, IP: 10.10.1.16, Active
List of agentless devices:
root@sam-Virtual-Machine:/home/sam#
```

EXERCISE 5: IMPLEMENT HOST-BASED IDS FUNCTIONALITY USING WAZUH HIDS

31. Switch to the **Attacker Machine-1** virtual machine, select username as **Bob** and type password as **user@123**, press **Enter**.

32. Copy the **wrd.txt** file and **pwd.txt** file from the home directory (**bob**) and paste on the **Desktop**.

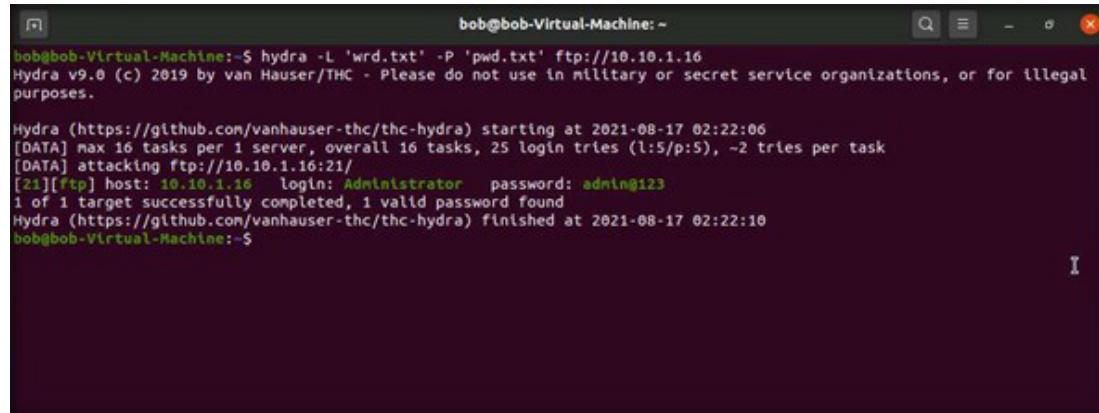


EXERCISE 5: IMPLEMENT HOST-BASED IDS FUNCTIONALITY USING WAZUH HIDS

33. Launch the **terminal** and type the below command to perform FTP attack on **Web Server**.

```
hydra -L 'wrd.txt' -P 'pwd.txt' ftp://10.10.1.16
```

EXERCISE 5:
**IMPLEMENT HOST-BASED
IDS FUNCTIONALITY USING
WAZUH HIDS**



```
bob@bob-Virtual-Machine:~$ hydra -L 'wrd.txt' -P 'pwd.txt' ftp://10.10.1.16
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-08-17 02:22:06
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (1:5/p:5), ~2 tries per task
[DATA] attacking ftp://10.10.1.16:21/
[21][ftp] host: 10.10.1.16 login: Administrator password: admin@123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-08-17 02:22:10
bob@bob-Virtual-Machine:~$
```

EXERCISE 5:
**IMPLEMENT HOST-BASED
IDS FUNCTIONALITY USING
WAZUH HIDS**

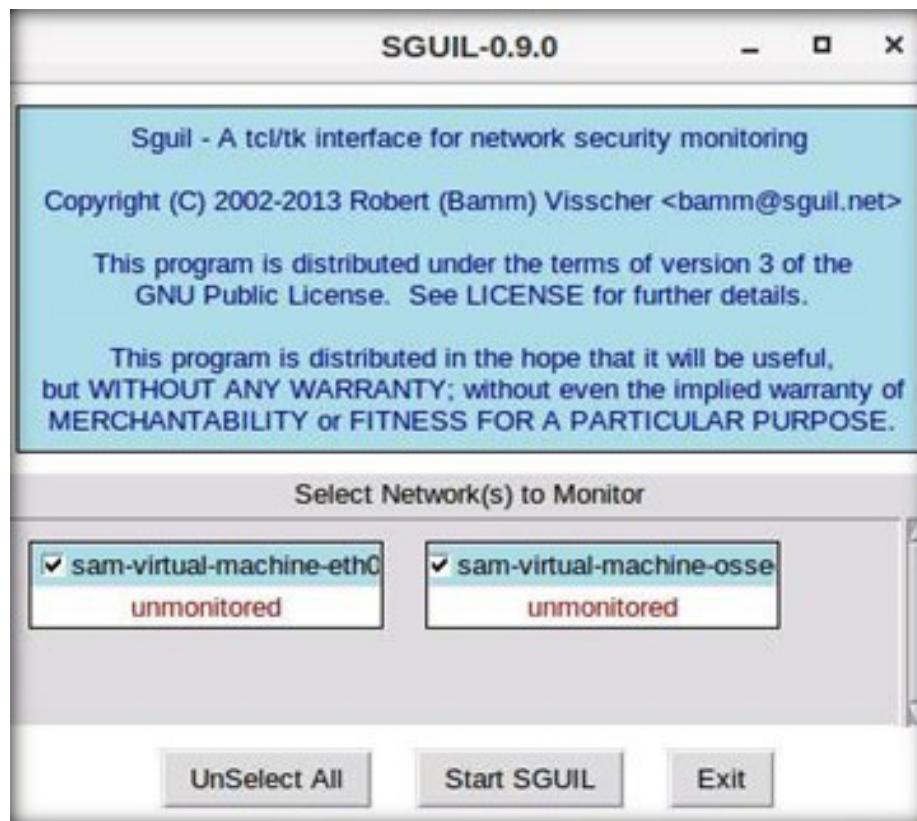
Note: Re-execute the command if you don't get the result showed in the above screenshot.

34. This indicates that the attacker can extract the FTP username and password over the network using insecure ports.
35. Switch to the **Admin Machine-2** machine. Login with password **admin@123**.
36. Launch the **sguil** application from the desktop.
37. The Sguil window appears. Type the username as **martin** and password as **user@123**. Click the **OK** button.



38. Network interfaces will be displayed. Click the **Select All** button.

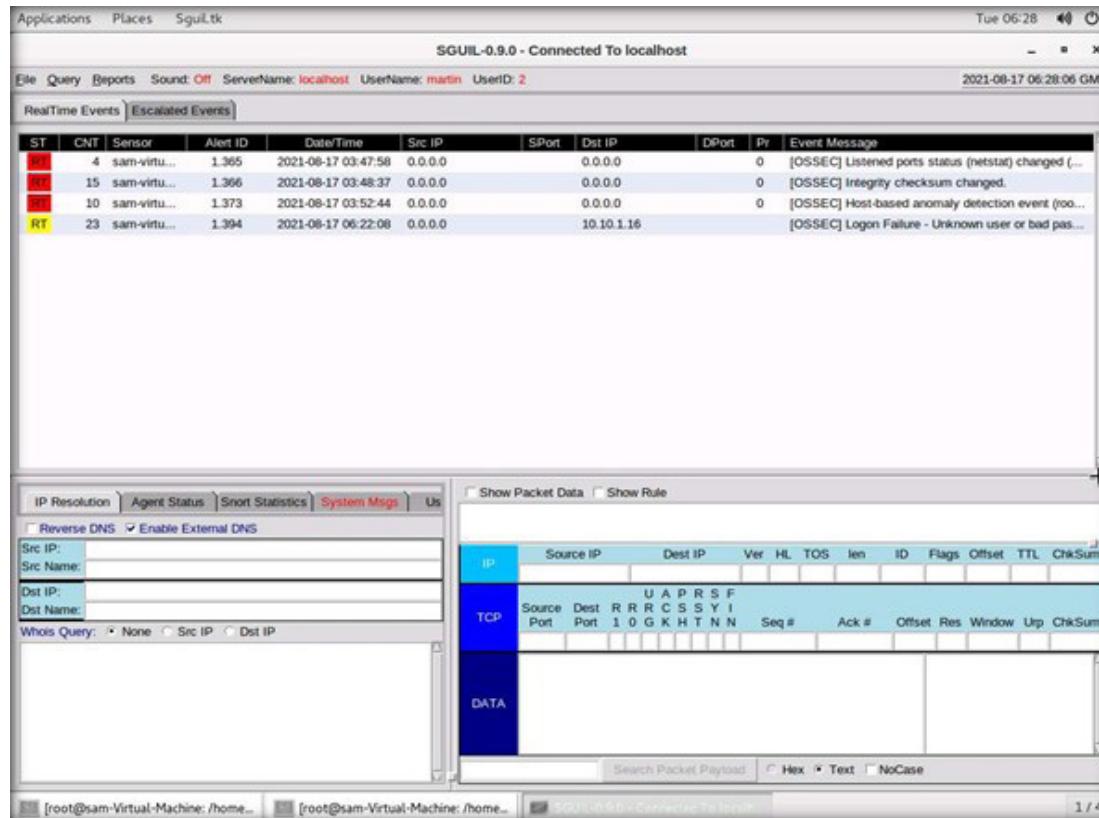
EXERCISE 5:
**IMPLEMENT HOST-BASED
IDS FUNCTIONALITY USING
WAZUH HIDS**



39. All available interfaces will be selected. Click the **Start SCUIL** button.

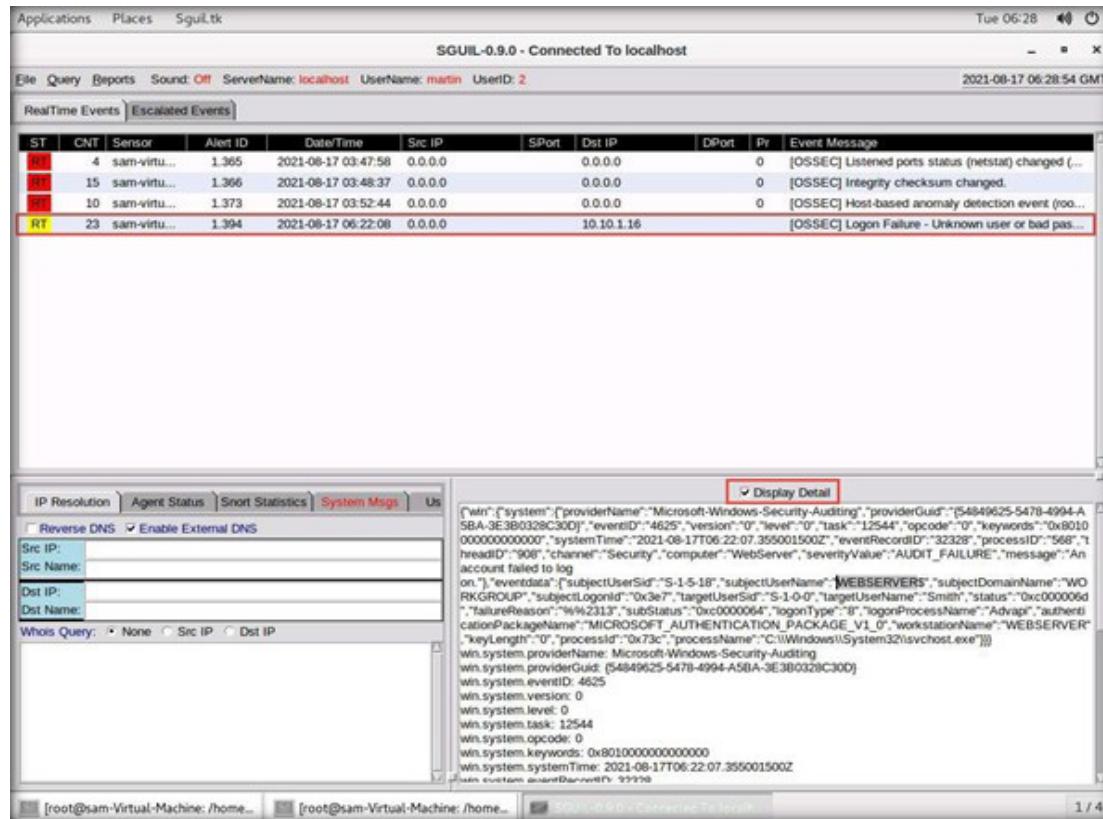
40. You will see the Sguil window, as shown in the screenshot below.

EXERCISE 5: IMPLEMENT HOST-BASED IDS FUNCTIONALITY USING WAZUH HIDS



41. The Windows Login Failure event is captured by the Wazuh agent.
42. You can observe the **Dst IP 10.10.1.16** OSSEC alert.
43. Click on the **OSSEC Windows: Logon Failure–unknown user record** from the list and check the **Display Detail** pane/option.

EXERCISE 5: IMPLEMENT HOST-BASED IDS FUNCTIONALITY USING WAZUH HIDS



The screenshot shows the SGUIL-0.9.0 interface connected to localhost. The RealTime Events tab is selected, displaying several alerts. One alert, entry number 23, is highlighted in yellow and has its details shown in the Display Detail pane below. The alert message is: "[OSSEC] Logon Failure - Unknown user or bad password". The Display Detail pane shows the raw JSON event data:

```

{
  "win": {
    "system": {
      "providerName": "Microsoft-Windows-Security-Auditing",
      "providerGuid": "{54849625-5478-4994-A5BA-3E3B0328C300}",
      "eventID": 4625,
      "version": 0,
      "level": 0,
      "task": 12544,
      "opcode": 0,
      "keywords": "0x8010000000000000"
    },
    "eventTime": "2021-08-17T06:22:07.355001500Z",
    "eventRecordID": "32328",
    "processID": "568",
    "threadID": "908",
    "channel": "Security",
    "computer": "WebServer",
    "severityValue": "AUDIT_FAILURE",
    "message": "An account failed to log on."
  },
  "eventData": [
    {
      "subjectUserId": "S-1-5-18",
      "subjectUserName": "WEBSERVER$",
      "subjectDomainName": "WORKGROUP",
      "subjectLogonId": "0x3e7",
      "targetUserId": "S-1-0-0",
      "targetUserName": "Smith",
      "status": "0xc000006d",
      "failureReason": "%42313",
      "subStatus": "0x0000004",
      "logonType": "8",
      "logonProcessName": "Advapi",
      "authenticationPackageName": "MICROSOFT_AUTHENTICATION_PACKAGE_V1_0",
      "workstationName": "WEBSERVER"
    }
  ],
  "keyLength": 0,
  "processID": "0x73c",
  "processName": "C:\Windows\System32\svchost.exe"
}
  
```

44. As described above, a security professional can use Wazuh to detect malicious activity on the host machine.

45. Close all open windows.

46. Turn off the **Admin Machine-2** virtual machine.

EXERCISE 6: IMPLEMENT NETWORK-BASED IDS FUNCTIONALITY USING SURICATA IDS

Network-based intrusion detection systems (NIDS) check every packet entering the network for the presence of anomalies and incorrect data.

LAB SCENARIO

A security professional must have the required knowledge to use Suricata for real-time Intrusion Detection System (IDS), inline Intrusion Prevention System (IPS), Network Security Monitoring (NSM), and offline pcap processing.

LAB OBJECTIVE

This lab will demonstrate how to use Suricata IDS. In this lab, you will also learn how to:

- Use the intrusion detection tool Suricata
- Review information in the Suricata Logs.

OVERVIEW OF NETWORK-BASED IDS

By limiting the firewall to drop large numbers of data packets, the NIDS checks every packet thoroughly. A NIDS captures and inspects all traffic. It generates alerts at the IP or application level based on the content. NIDS are more distributed than host-based IDS. The NIDS identifies the anomalies at the router and host levels. It audits the information contained in the data packets and logs the information of malicious packets; furthermore, it assigns a threat level to each risk after receiving the data packets.

LAB TASKS

Note: Ensure that Admin Machine-1, Web Server, Attacker Machine-1 and PfSense Firewall virtual machines are running.

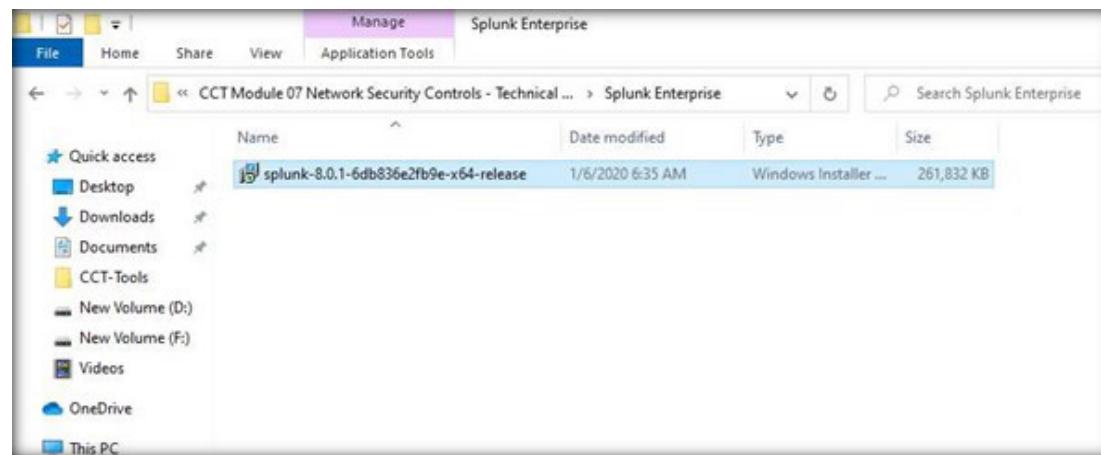
1. Switch to the **Admin Machine-1** virtual machine.

Note: If you are not logged into the machine, then log in using credentials **Admin** and **admin@123**.

2. Next, install Splunk Enterprise SIEM, to view the captured Suricata logs in SIEM.

3. Navigate to **Z:\CCT-Tools\CCT Module 07 Network Security Controls - Technical Controls\Splunk Enterprise**.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



EXERCISE 6: IMPLEMENT NETWORK-BASED IDS FUNCTIONALITY USING SURICATA IDS

4. Double-click **splunk-8.0.1-6db836e2fb9e-x64-release.msi** to start the installation. If the **Open File - Security Warning** pop-up appears, click **Run**.

Note: If a “SmartScreen has prevented the app from running” message appears, click **More info**, and then click **Run anyway**.

5. The **Splunk Enterprise Installer** window appears. Click checkbox to accept the license agreement and click **Next**.

6. Enter the credential for Splunk Enterprise with username **admin**, password and confirm password as **admin@123**. Click **Next**.



7. Click **Install** to install Splunk Enterprise.
8. The **User Account Control** pop-up window appears; click **Yes** to continue.
9. Wait for the installation to complete. Click **Finish** to complete the Splunk Enterprise setup.

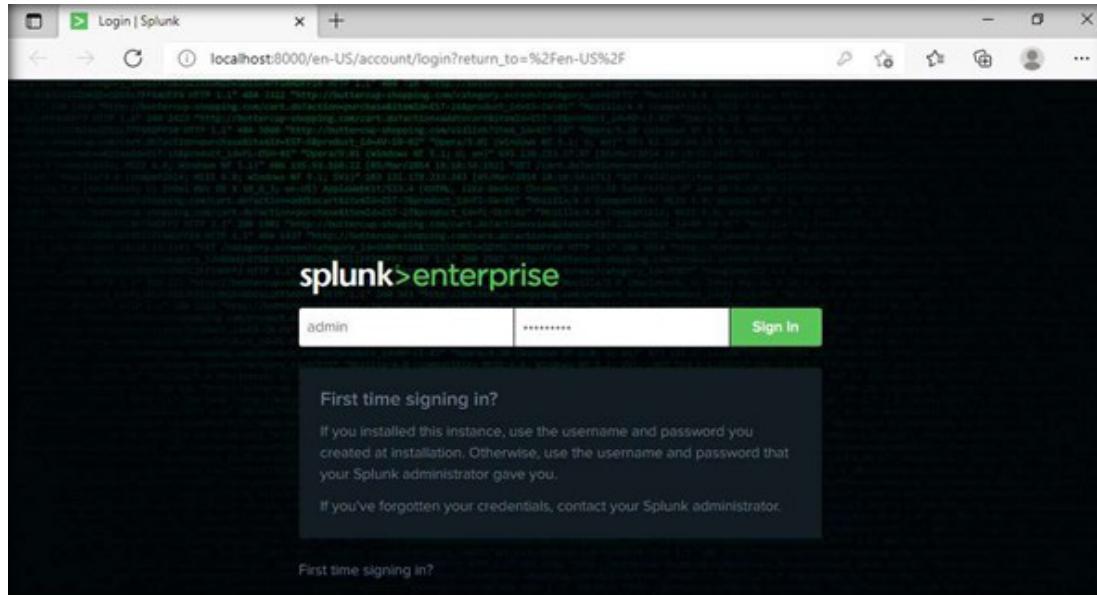
EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



10. Splunk Enterprise launches in your default browser.

11. The **First time signing in?** page appears. Enter the username (**admin**) and password (provided while installation as **admin@123**) in their respective fields and click **Sign In**.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS

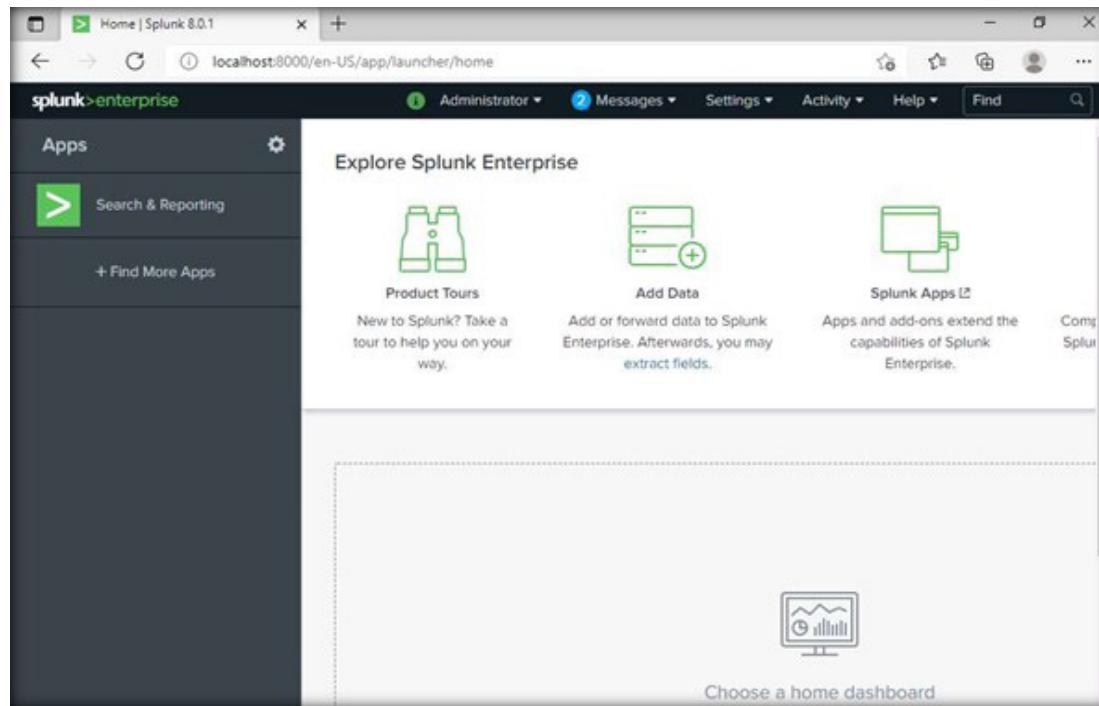


12. You will be successfully logged in to Splunk Enterprise.

Note: If **Helping You Get More Value from Splunk Software** window appears, click on **Got it!**, in **Important changes coming!** window click on **Don't show me this again**.

Note: If **Save password** pop-up appears, click on **Never**.

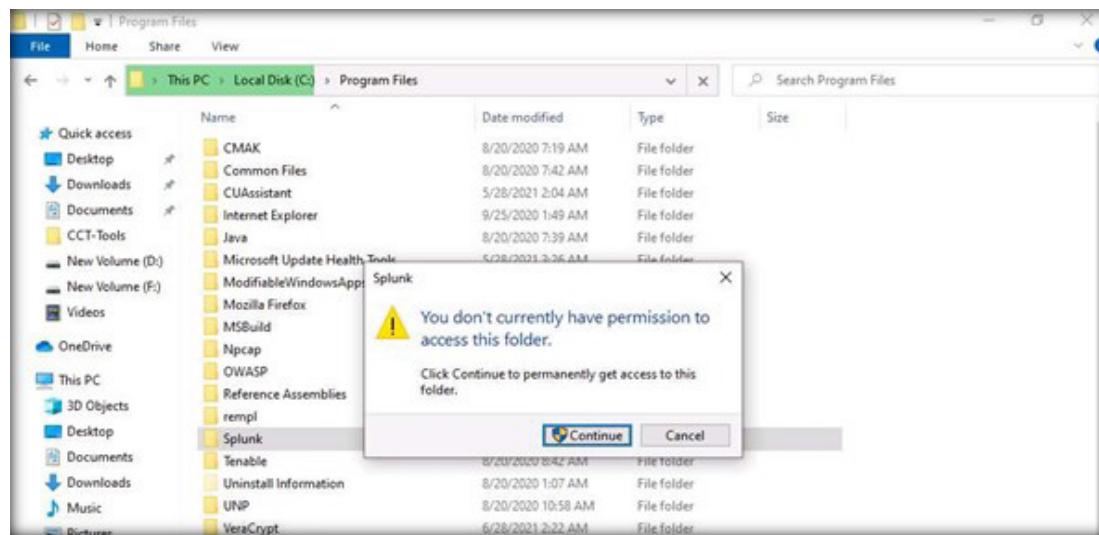
EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



13. Close the browser, to increase the default maximum number of concurrent searches per CUP in Splunk Enterprise, navigate to **C:\Program Files\Splunk\etc\system\default**.

14. If the permission alert window opens, click **Continue** to access the Splunk folder.

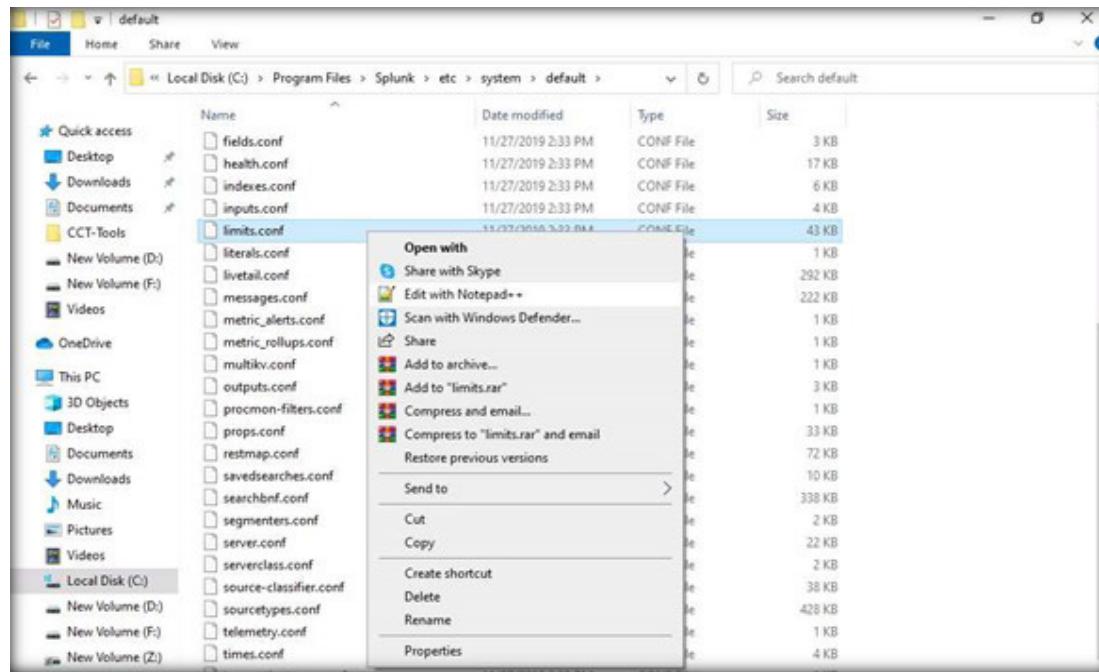
EXERCISE 6: IMPLEMENT NETWORK-BASED IDS FUNCTIONALITY USING SURICATA IDS



15. Open **limits.conf** with Notepad++.

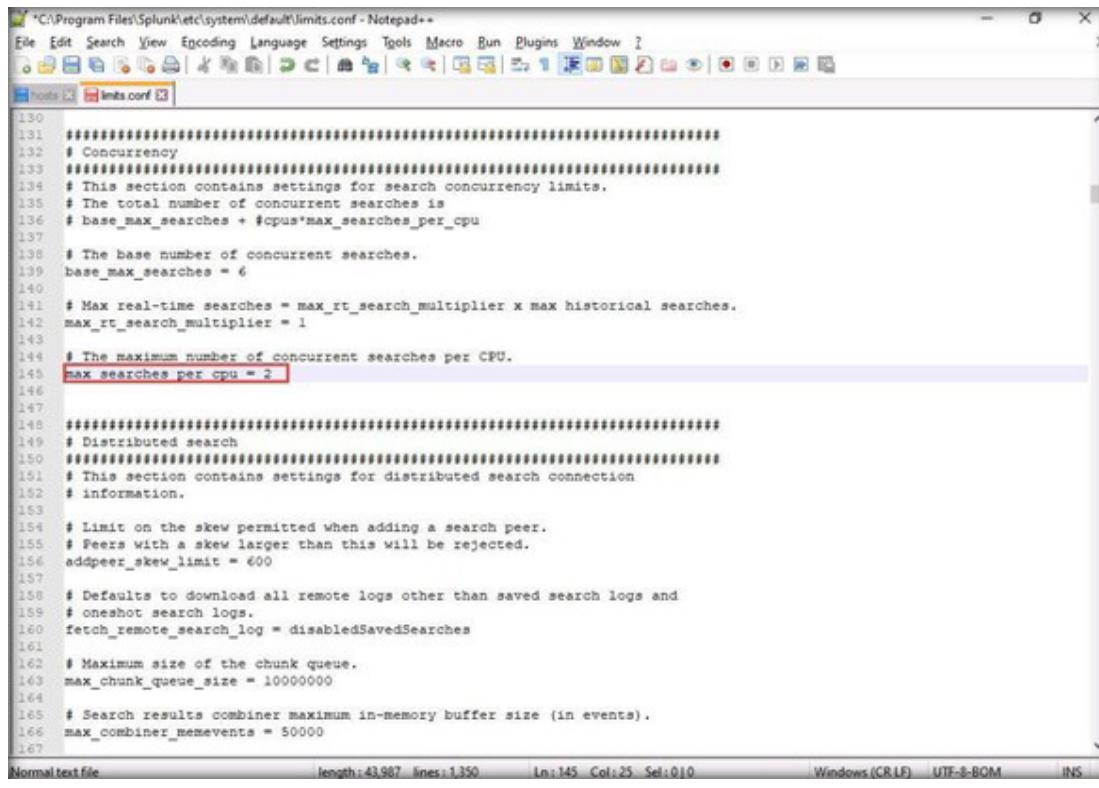
Note: If the **Notepad++ update** pop-up appears click **No**.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



16. Go to line number 145 and set **max_searches_per_cpu=2**; click save and close the file.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



The screenshot shows a Notepad++ window displaying the contents of the 'limits.conf' file located at 'C:\Program Files\Splunk\etc\system\default'. The file contains configuration settings for search concurrency. Line 145 is highlighted with a red rectangle, indicating the modification point. The configuration includes base_max_searches, max_rt_search_multiplier, and max_searches_per_cpu settings.

```
*C:\Program Files\Splunk\etc\system\default\limits.conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window I
o D E F G H C A B S T M L V N P R X
tools limits.conf
130
131 #####Concurrency#####
132 # This section contains settings for search concurrency limits.
133 #####
134 # The total number of concurrent searches is
135 # base_max_searches + #cpus*max_searches_per_cpu
136
137 # The base number of concurrent searches.
138 base_max_searches = 6
139
140 # Max real-time searches = max_rt_search_multiplier * max historical searches.
141 max_rt_search_multiplier = 1
142
143 # The maximum number of concurrent searches per CPU.
144 max_searches_per_cpu = 2
145
146
147 #####Distributed search#####
148 # Distributed search
149 #####
150 # This section contains settings for distributed search connection
151 # information.
152
153 # Limit on the skew permitted when adding a search peer.
154 # Peers with a skew larger than this will be rejected.
155 addpeer_skew_limit = 600
156
157 # Defaults to download all remote logs other than saved search logs and
158 # oneshot search logs.
159 fetch_remote_search_log = disabledSavedSearches
160
161 # Maximum size of the chunk queue.
162 max_chunk_queue_size = 10000000
163
164 # Search results combiner maximum in-memory buffer size (in events).
165 max_combiner_memevents = 50000
166
167
```

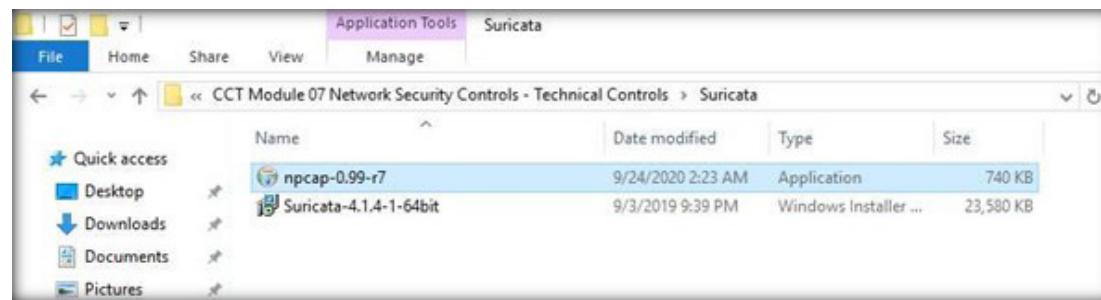
17. Restart the **Admin Machine-1** virtual machine.

18. The Suricata IDS configuration needs to be on the web server; therefore, we need to configure the Suricata IDS on Web Server.

19. Switch to the **Web Server** virtual machine.

Note: If you are note logged into the machine, then log in using credentials **Administrator** and **admin@123**.

20. Navigate to **Z:\CCT Module 07 Network Security Controls - Technical Controls\Suricata** and copy **npcap-0.99-r7.exe**.

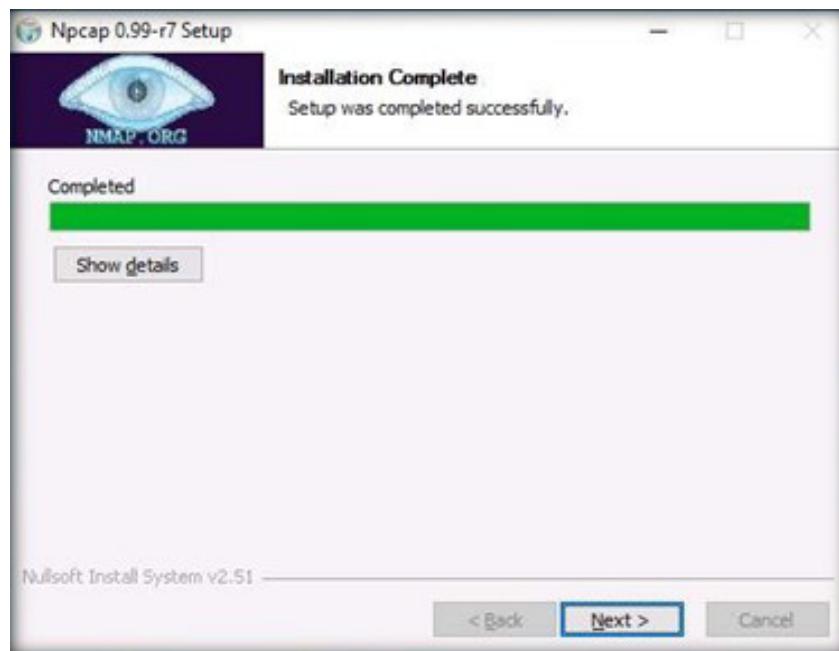


EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS

21. Paste the **npcap-0.99-r7.exe** file on the **Desktop**.
22. **Npcap** is a tool used for network packet capturing and injection library for Windows.
23. Suricata uses **npcap** for capturing network packets and alerts. The following steps demonstrate the installation of the npcap tool.
24. Double click on **npcap-0.99-r7.exe**. Click on **I Agree** to continue the installation.
Note: If the **Security Warning** pop-up appears, click **Run**.
25. Check **Install Npcap in WinPcap API-compatible Mode** and click **Install**.

26. The installation will start in a few seconds. Once the installation is completed successfully, click **Next** to continue.

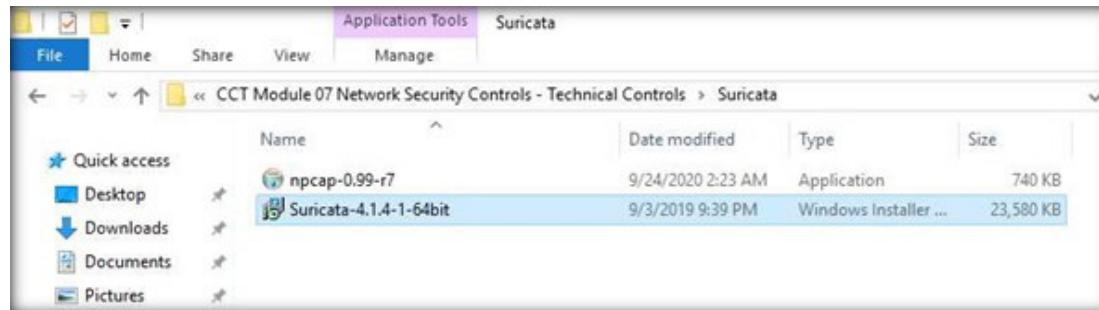
EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



27. Click **Finish** to complete the installation.

28. Navigate to **Z:\CCT-Tools\CCT Module 07 Network Security Controls - Technical Controls\Suricata** and copy **Suricata-4.1.4-1-64bit.msi**.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



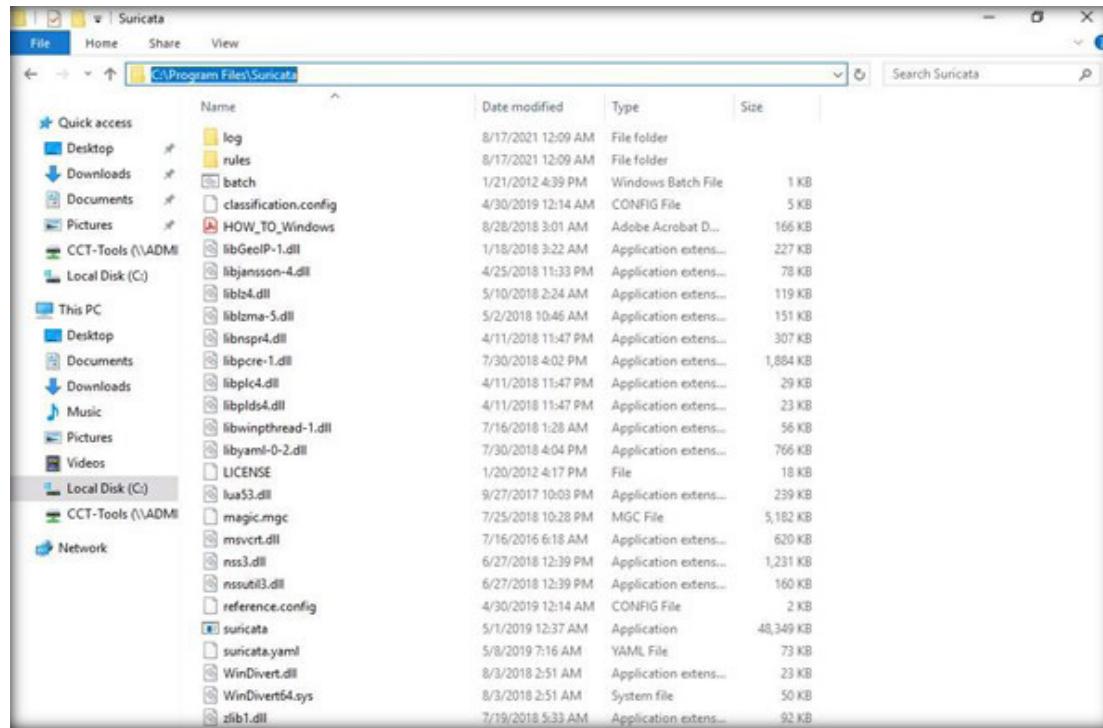
29. Paste the **Suricata-4.1.4-1-64bit.msi** file on the desktop.
30. Double click **Suricata-4.1.4-1-64bit.msi**. The **Suricata.IDS/IPS2.1.2-1-64bit Setup** window will appear. Click **Next**.
31. Check **I accept the terms in the License Agreement** to accept the license and click **Next**.
32. Click **Next** to continue the installation as shown in the screenshot below.
33. Click **Install** to continue the installation process.
34. Click **Finish** to complete the installation process.



EXERCISE 6:
**IMPLEMENT
NETWORK-BASED IDS
FUNCTIONALITY USING
SURICATA IDS**

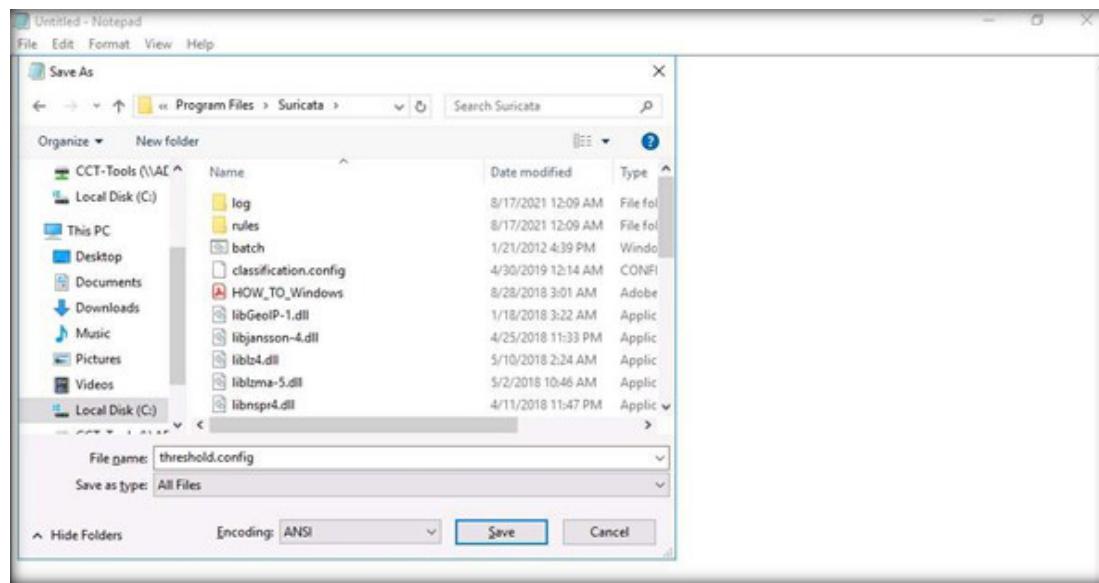
35. After Suricata IDS is successfully installed, the Suricata directory will be created under the **C:\Program Files\Suricata**.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



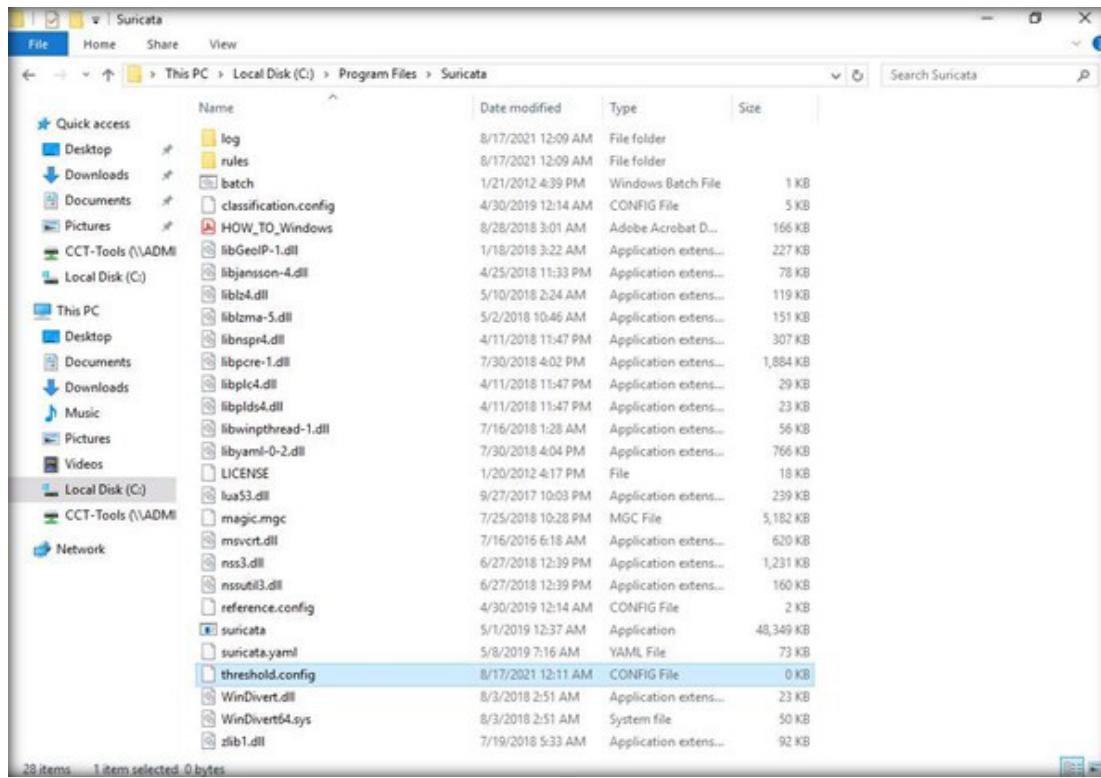
36. From Windows search, Open **Notepad** and save the empty **threshold.config** file under **C:\Program Files\Suricata** location, as shown in the screenshot below (ensure that you have selected **All Files** in the **Save as type:** option while saving the file).

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



37. The **threshold.config** file will be created, as shown in the screenshot below.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



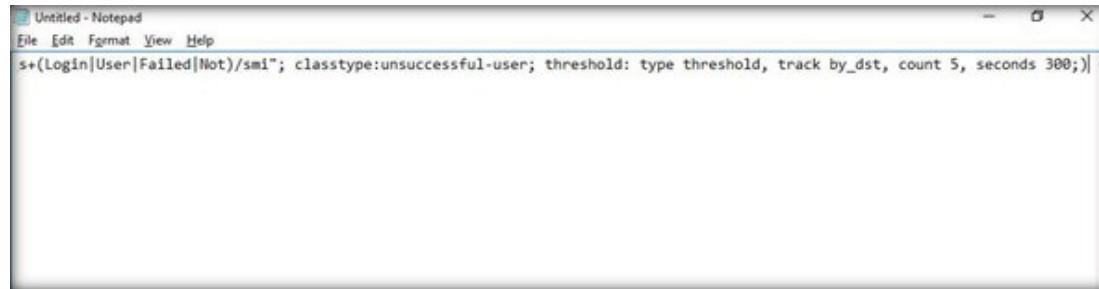
38. The Suricata IDS generates the alert based on the ruleset. A security professional can set the custom rule using the **.rule** file as shown in the following steps.

39. First, the **local.rules** file needs to be created. The **local.rules** file includes custom rules. We can create 'n' number of files for various rules (the rule file must have a **.rule** extension).

40. Here, we have created a rule for generating a **PING** alert.

41. Open **Notepad**, and type the following:

```
alert tcp any 21 -> any (msg:"ET SCAN Potential FTP Brute-Force attempt"; flow:from_server,established; dsize:<100; content:"530 "; depth:4; pcre:"/530\s+(Login|User|Failed|Not)/smi"; classtype:unsuccessful-user; threshold: type threshold, track by_dst, count 5, seconds 300;)
```



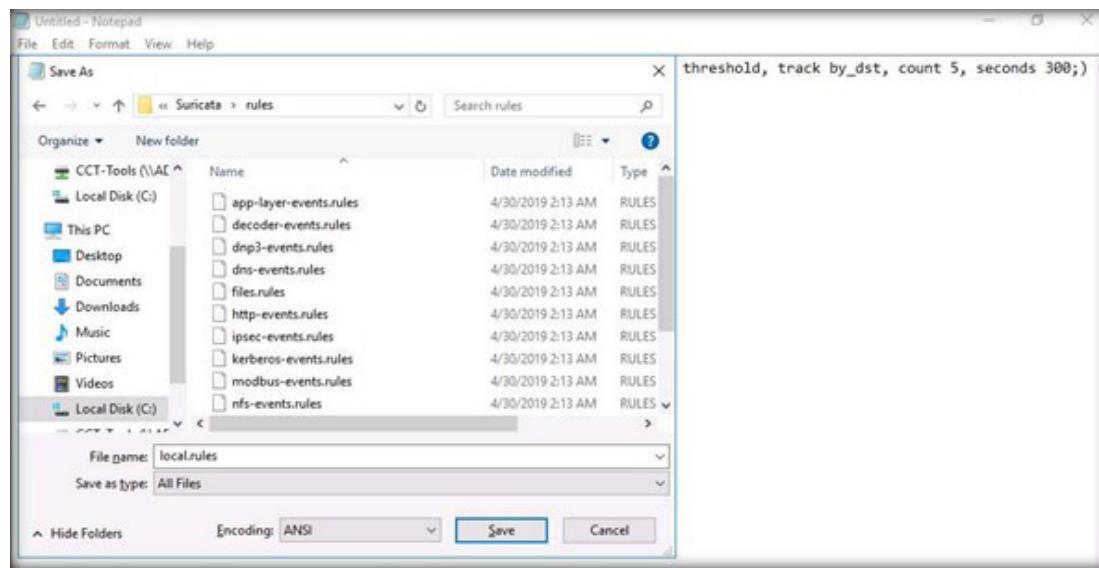
A screenshot of a Windows Notepad window titled "Untitled - Notepad". The window contains a single line of text representing a Suricata rule. The rule is defined as follows:

```
alert tcp any 21 -> any (msg:"ET SCAN Potential FTP Brute-Force attempt"; flow:from_server,established; dsize:<100; content:"530 "; depth:4; pcre:"/530\s+(Login|User|Failed|Not)/smi"; classtype:unsuccessful-user; threshold: type threshold, track by_dst, count 5, seconds 300;)
```

EXERCISE 6: IMPLEMENT NETWORK-BASED IDS FUNCTIONALITY USING SURICATA IDS

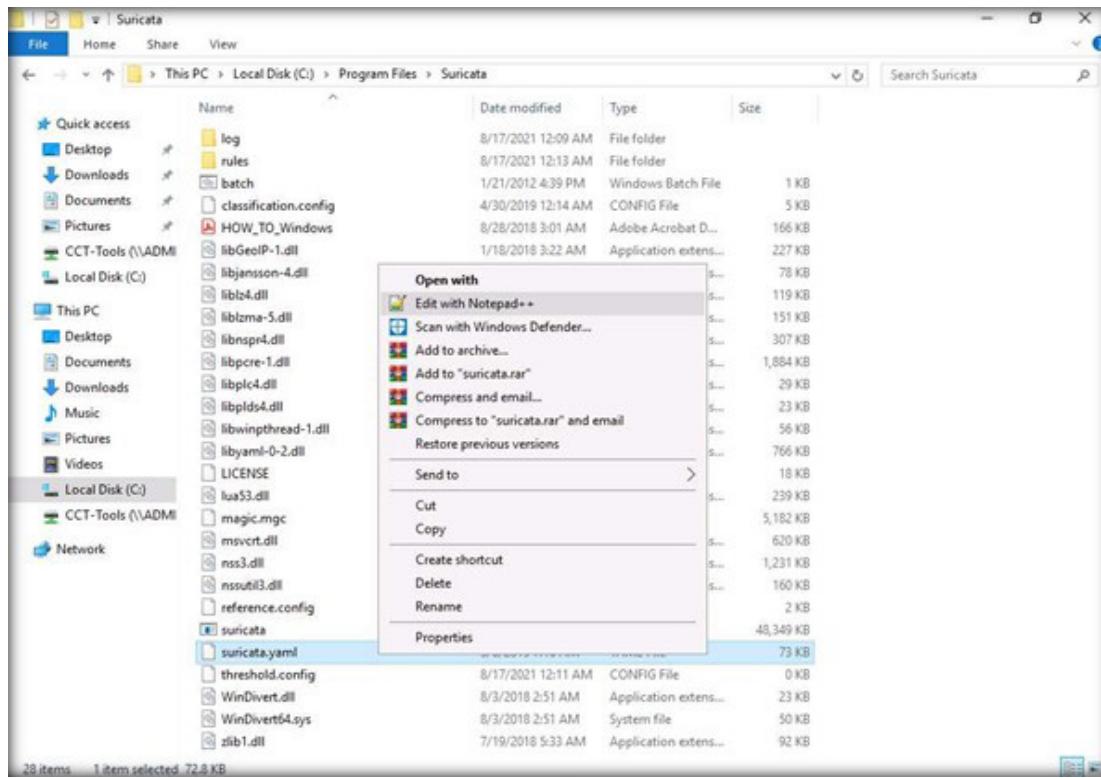
42. Save the file as **local.rules** under the **C:\Program Files\Suricata\rules** location as shown in the screenshot below (ensure that you have selected **All Files** in the Save as type option while saving the file).

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



43. Navigate to **C:\Program Files\Suricata**, and open **suricata.yaml** file in Notepad++.

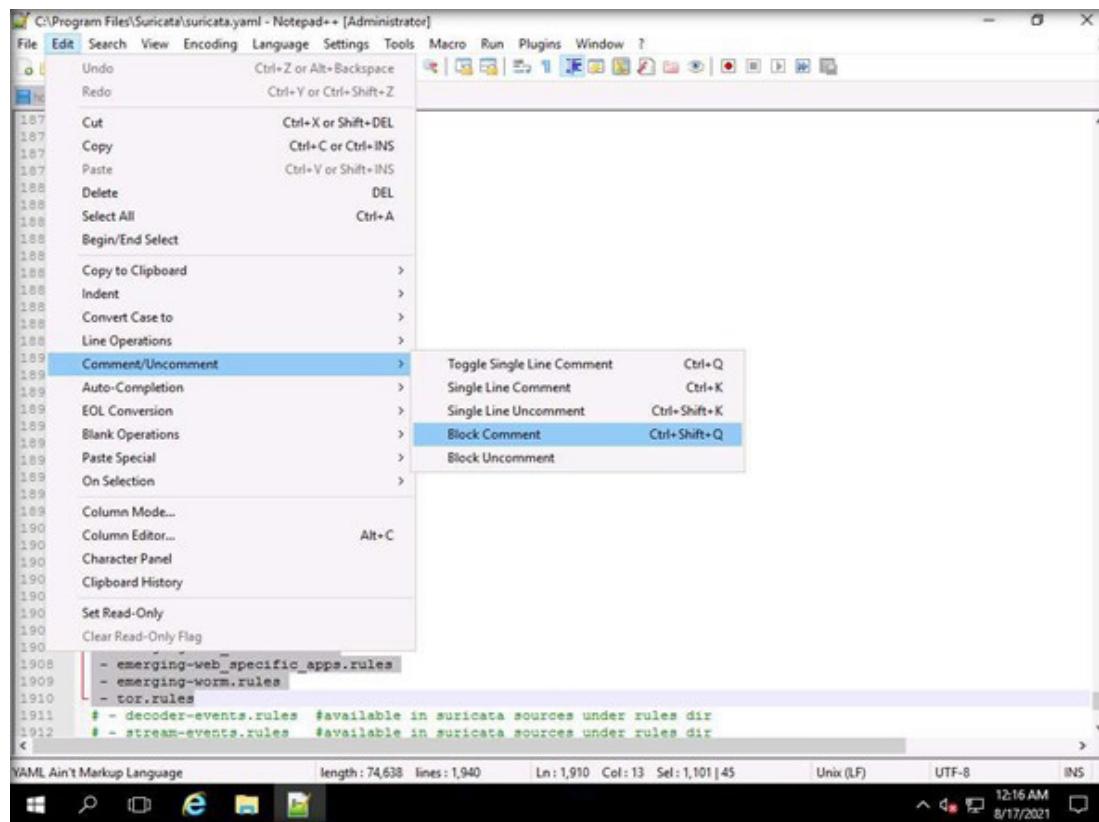
EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



44. The **suricata.yaml** file opens in Notepad++.

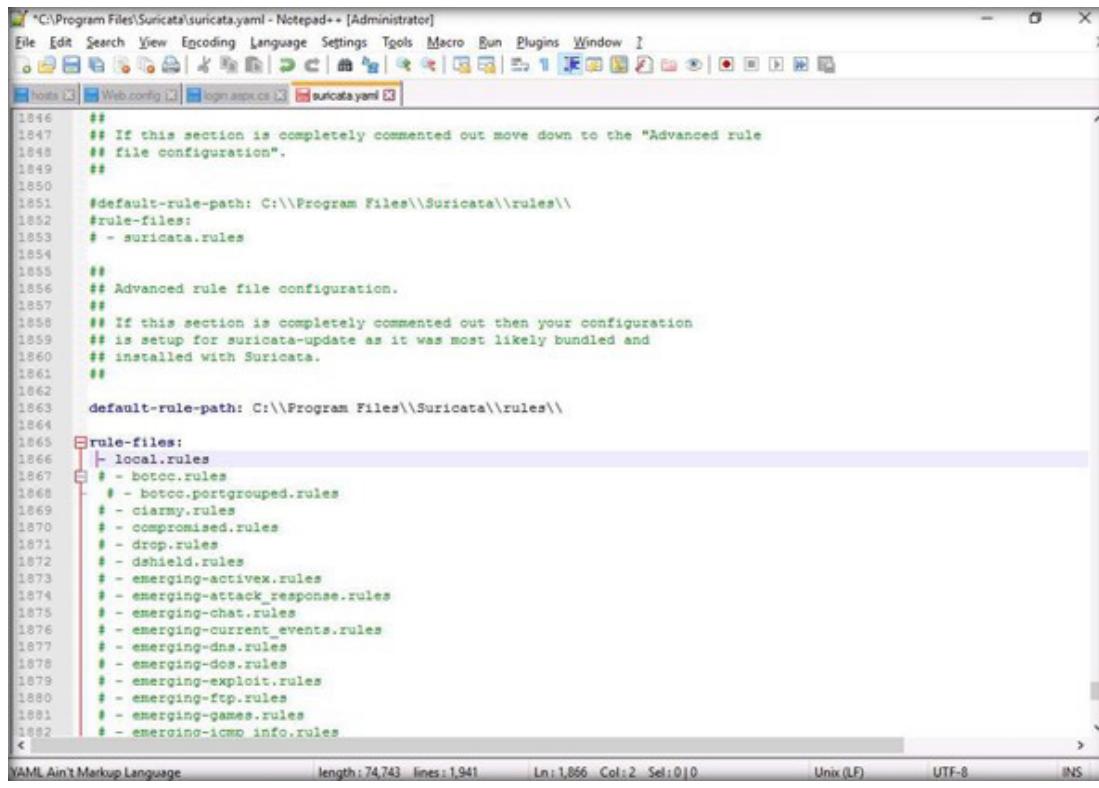
Note: If the Notepad++ update pop-up appears, click No.

45. To comment on the default rules files, select line numbers **1866** to **1910**, navigate to the **Edit** menu, and select **Comment/Uncomment > Block Comment** as shown in the screenshot below.



46. Add – **local.rules** below the line number **1865** as shown in the screenshot below and click **Save**.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



```
1846 ##  
1847 ## If this section is completely commented out move down to the "Advanced rule  
1848 ## file configuration".  
1849 ##  
1850 #default-rule-path: C:\\Program Files\\Suricata\\rules\\\\  
1851 #rule-files:  
1852 # - suricata.rules  
1853 ##  
1854 ## Advanced rule file configuration.  
1855 ##  
1856 ## If this section is completely commented out then your configuration  
1857 ## is setup for suricata-update as it was most likely bundled and  
1858 ## installed with Suricata.  
1859 ##  
1860 default-rule-path: C:\\Program Files\\Suricata\\rules\\\\  
1861  
1862  
1863  
1864  
1865 rule-files:  
1866   local.rules  
1867   botcc.rules  
1868   botcc.portgrouped.rules  
1869   clarify.rules  
1870   compromised.rules  
1871   drop.rules  
1872   dshield.rules  
1873   emerging-activex.rules  
1874   emerging-exploit.rules  
1875   emerging-chat.rules  
1876   emerging-current_events.rules  
1877   emerging-dns.rules  
1878   emerging-dos.rules  
1879   emerging-ftp.rules  
1880   emerging-games.rules  
1881   emerging-icmp.info.rules  
1882 <
```

47. Close all open folders and files.

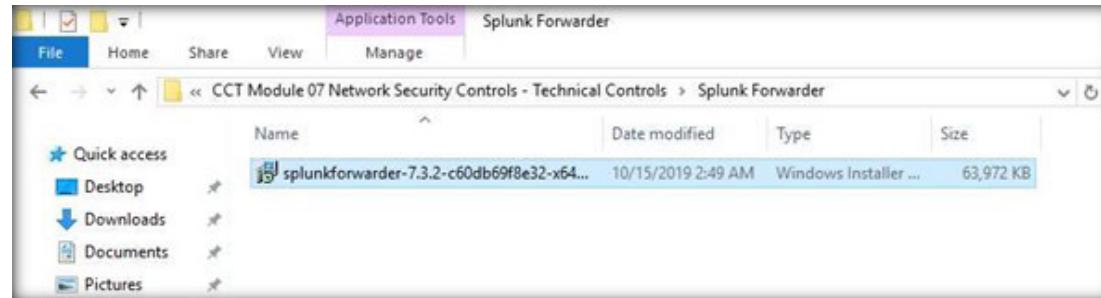
48. Navigate to **C:\Program Files\Suricata\log**. Observe that there is no log file under the **log\files** directory.

49. We will capture the Suricata logs in Splunk, next we forward Suricata logs to Splunk on the monitoring machine using Splunkforwarder.

50. To install Splunk forwarder, navigate to **Z:\CCT Module 07 Network Security Controls - Technical Controls\Splunk Forwarder**.

51. Double-click on **splunkforwarder-7.3.2-c60db69f8e32-x64-release.msi**.

Note: If a **Security Warning** pop-up appears, click on **Run**.



EXERCISE 6: IMPLEMENT NETWORK-BASED IDS FUNCTIONALITY USING SURICATA IDS

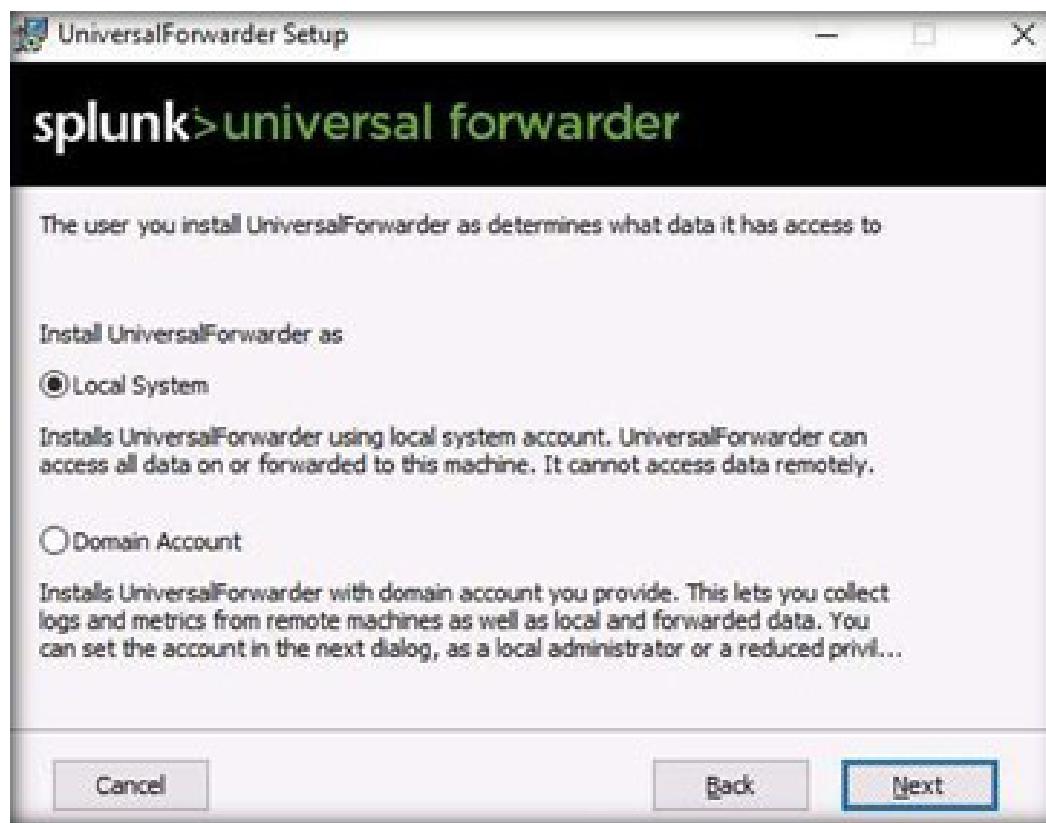
EXERCISE 6: IMPLEMENT NETWORK-BASED IDS FUNCTIONALITY USING SURICATA IDS

52. Once the UniversalForwarder Setup window appears, check **Check the box to accept the License Agreement** and click on **Customize Options**.

53. Leave the installation path set to the default location and click on **Next**.

54. Click on **Next** in the Splunk certificate section.

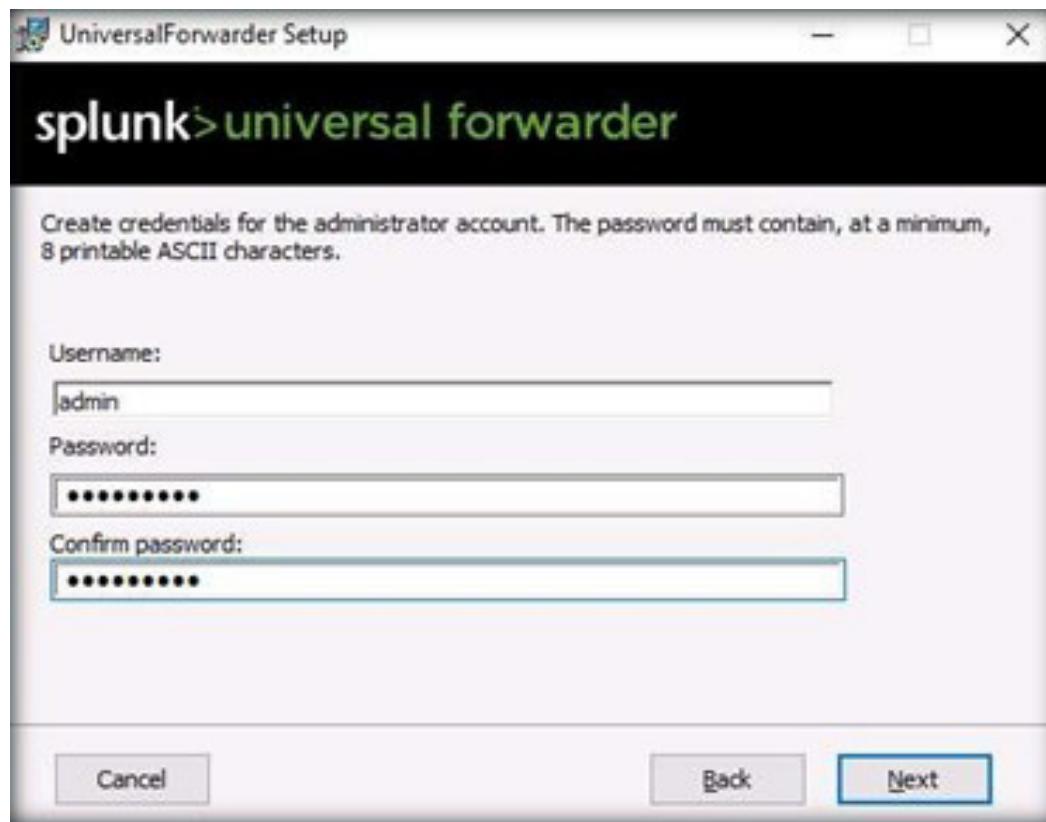
55. In the next step, select the Local System radio button to install Universal Forwarder as a **Local System** and then click on **Next**.



56. Next, check all entities under **Windows Event Logs**, **Active Directory Monitoring** and **Performance Monitor** and click on **Next**.

57. Create credentials for the administrator account; type username “**admin**” and password “**admin@123**” and click on **Next**.

EXERCISE 6:
IMPLEMENT NETWORK-
BASED IDS FUNCTIONALITY
USING SURICATA IDS



58. Leave the **Deployment Server** section without issuing the deployment IP and port number details and click on **Next**.

59. In the **Receiving Indexer** section, enter the IP address for **Admin Machine-1**, namely, **10.10.1.2** in the Hostname or IP field; enter Port **9997** in the port field and click on **Next**.

EXERCISE 6:
**IMPLEMENT NETWORK-BASED IDS FUNCTIONALITY
USING SURICATA IDS**



60. Once you are through with the configuration, click on Install. At this time, if a User Account Control pop-up appears, click on Yes.

61. Click on **Finish** after the installation completes.

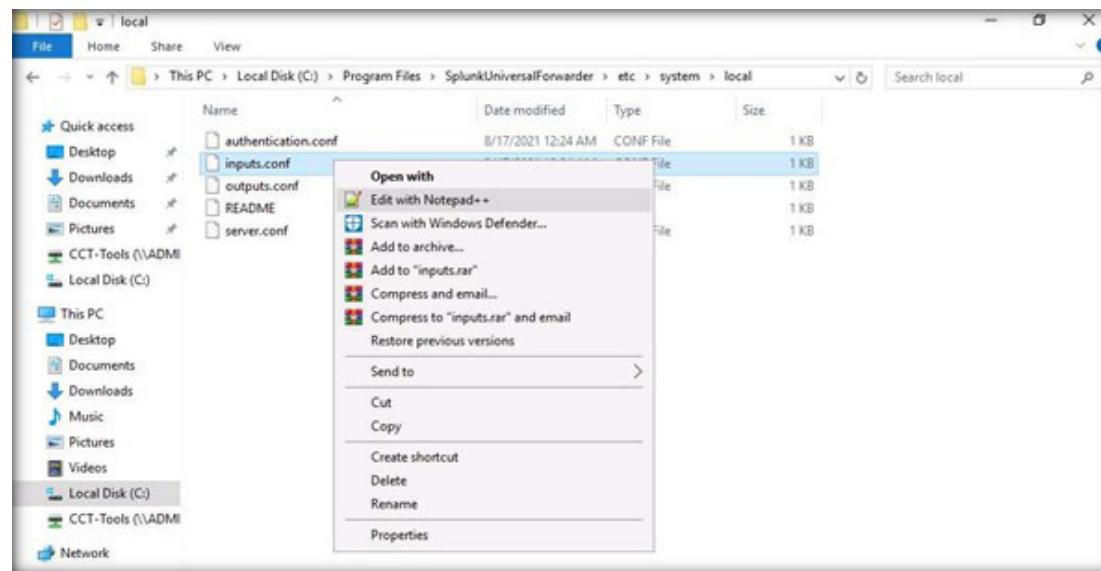
EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



Note: You do not need any explicit configuration for **Splunk Forwarder** to collect Windows event logs, since Splunk Forwarder has default configuration done during installation. You need to configure Splunk Forwarder explicitly to collect logs from IIS and Snort IDS.

62. To configure Splunk Universal Forwarder to collect IIS logs from the Web Server machine, go to the Web Server machine.
63. Navigate to **C:\Program Files\SplunkUniversalForwarder\etc\system\local**, right-click on **inputs.conf**, and then on **Edit with Notepad++**.

EXERCISE 6: IMPLEMENT NETWORK-BASED IDS FUNCTIONALITY USING SURICATA IDS



64. Add the following lines in the **inputs.conf** file like in the below screenshot.

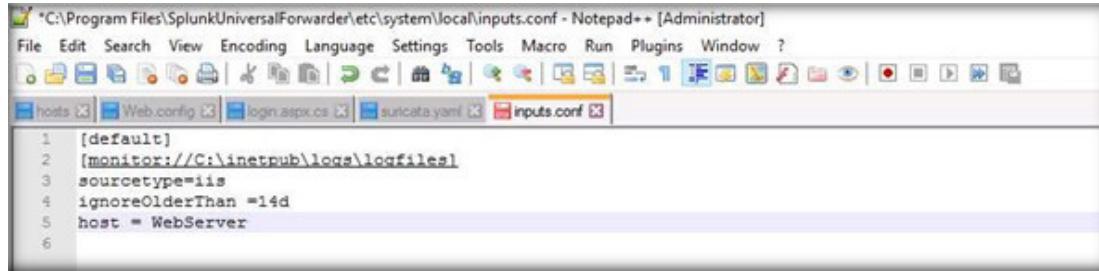
```
[monitor://C:\inetpub\logs\LogFiles]
```

```
sourcetype=iis
```

```
ignoreOlderThan =14d
```

```
host = WebServer
```

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



The screenshot shows a Notepad++ window with the title bar "C:\Program Files\SplunkUniversalForwarder\etc\system\local\inputs.conf - Notepad++ [Administrator]". The window contains the following configuration code:

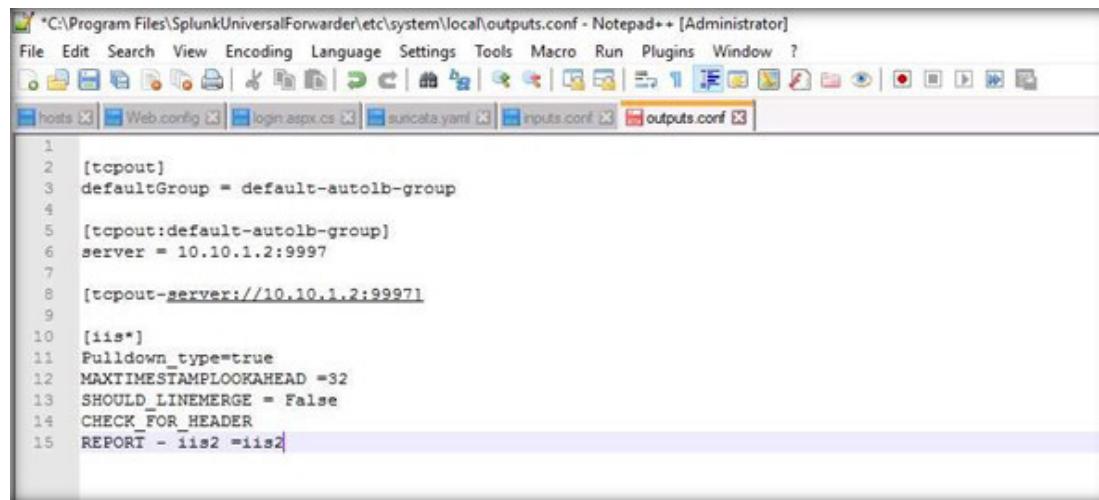
```
1 [default]
2 [monitor://C:\inetpub\logs\LogFiles]
3 sourcetype=iis
4 ignoreOlderThan =14d
5 host = WebServer
6
```

65. Click on **Save** to save the file and close it.

66. Right-click on **outputs.conf**, and then on **Edit with Notepad++**.

67. Add the following lines in the **outputs.conf** file, as shown in the screenshot below.

```
[iis*]
Pulldown_type=true
MAXTIMESTAMPLOOKAHEAD =32
SHOULD_LINEMERGE = False
CHECK_FOR_HEADER
REPORT - iis2 =iis2
```



```
*C:\Program Files\SplunkUniversalForwarder\etc\system\local\outputs.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
hosts Web config login.aspx.cs suncata.yaml inputs.conf outputs.conf

1
2 [tcpout]
3 defaultGroup = default-autolb-group
4
5 [tcpout:default-autolb-group]
6 server = 10.10.1.2:9997
7
8 [tcpout-server://10.10.1.2:9997]
9
10 [iis*]
11 Pulldown_type=true
12 MAXTIMESTAMPLOOKAHEAD =32
13 SHOULD_LINEMERGE = False
14 CHECK_FOR_HEADER
15 REPORT - iis2 =iis2
```

EXERCISE 6: IMPLEMENT NETWORK-BASED IDS FUNCTIONALITY USING SURICATA IDS

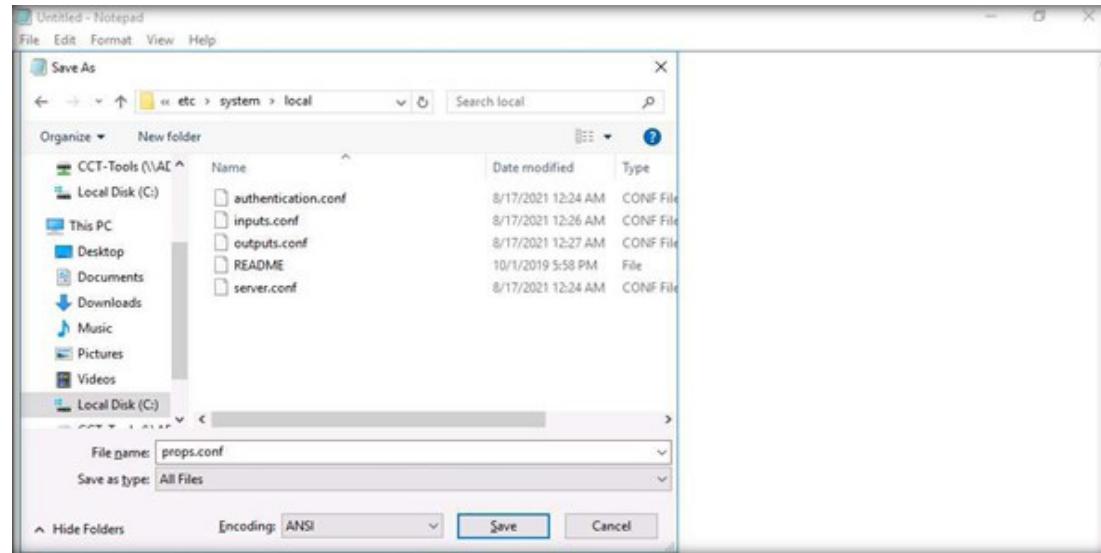
68. Click on **Save** to save the file and then **Close** it.

69. Open **Notepad** and type the below code.

```
[iis*]
Pulldown_type=true
MAXTIMESTAMPLOOKAHEAD =32
SHOULD_LINEMERGE =False
CHECK_FOR_HEADER
REPORT -iis2 =iis2
```

70. Save the notepad as **props.conf** at **C:\Program Files\SplunkUniversalForwarder\etc\system\local** path and close the file.

Note: Ensure you have selected **Save type as: All Files** while saving the props.conf file.



EXERCISE 6: IMPLEMENT NETWORK-BASED FUNCTIONALITY USING SURICATA IDS

71. Open Notepad again, add the following lines in the new opened file and save the file as **transforms.conf** at **C:\Program Files\SplunkUniversalForwarder\etc\system\local**.

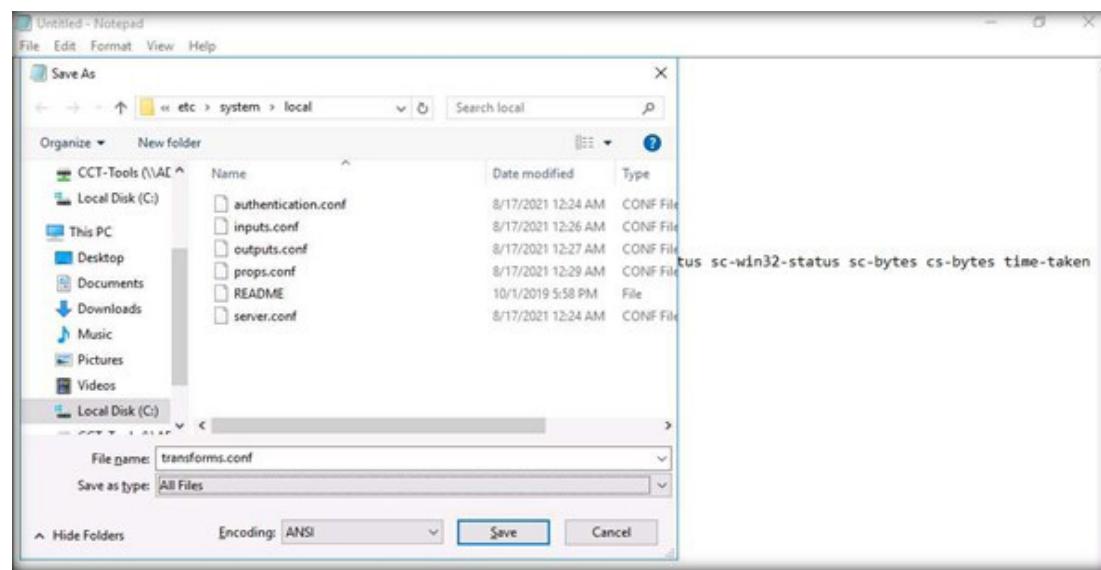
Note: Ensure you have selected **Save type as: All Files** while saving the transforms.conf file.

```
[default]
host -WebServer

[ignore_comments]
REGEX = ^#.*
DEST_KEY =queue
FORMAT =nullQueue

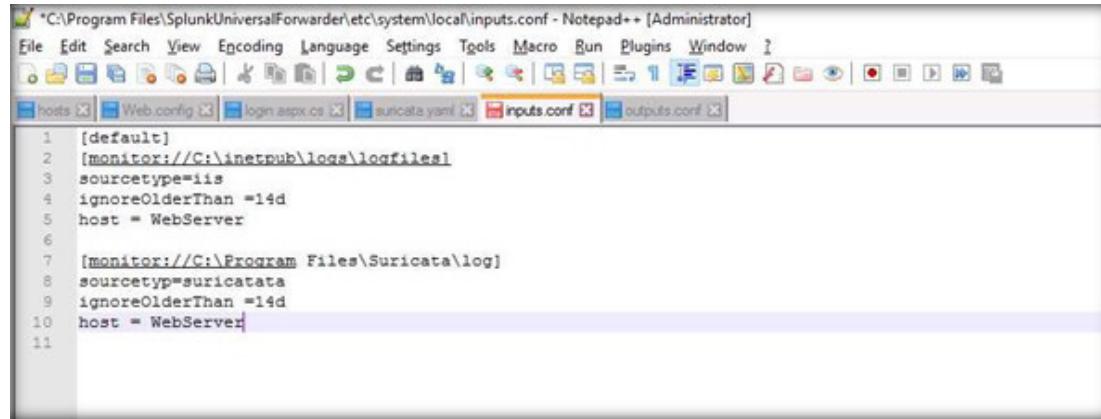
[iis2]
DELIMS =”“
FIELDS = date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Cookie) cs(Referer) cs-host sc-status sc-substatus
sc-win32-status sc-bytes cs-bytes time-taken
```

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



72. To forward the Suricata logs, navigate to the **C:\Program Files\SplunkUniversalForwarder\etc\system\local** folder and open **inputs.conf** file **Edit with Notepad++**. Add the following configuration lines of code at the end of the file and **Save**. Close the file.

```
[monitor://C:\Program Files\Suricata\log]
sourcetype=suricata
ignoreOlderThan =14d
host = WebServer
```



The screenshot shows a Notepad++ window titled "C:\Program Files\SplunkUniversalForwarder\etc\system\local\inputs.conf - Notepad++ [Administrator]". The window displays the following configuration file:

```
[default]
[monitor://C:\inetpub\logs\LogFiles]
sourcetype=iis
ignoreOlderThan =14d
host = WebServer

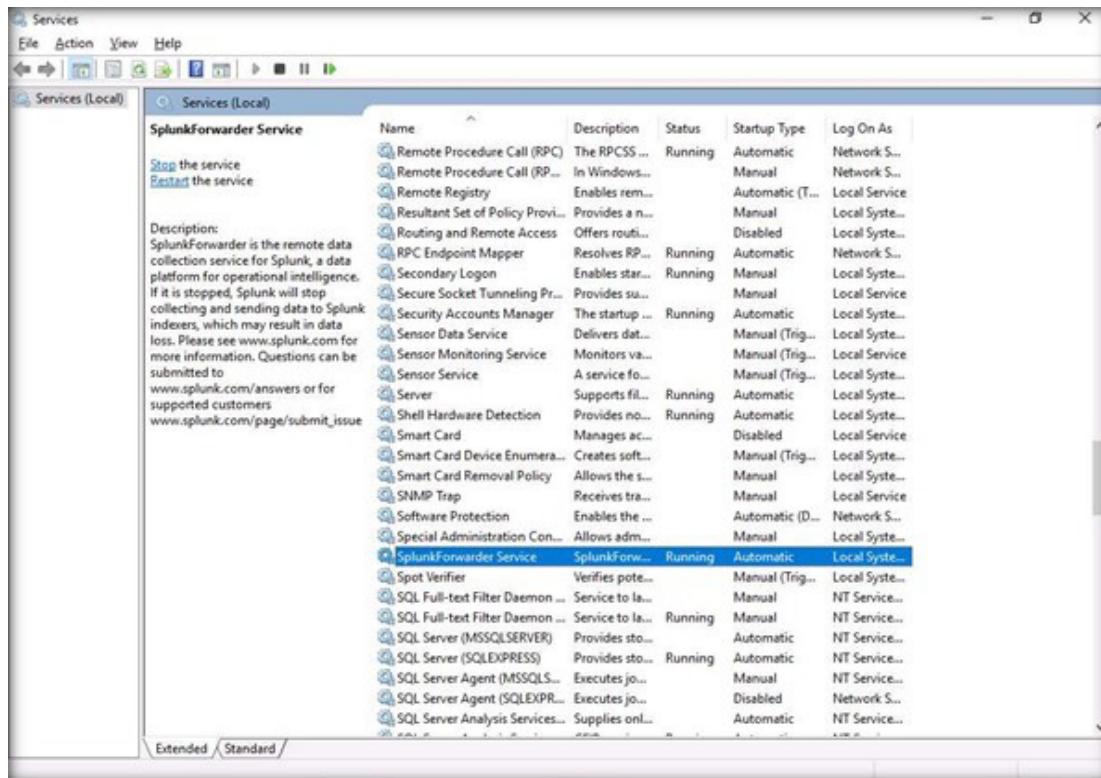
[monitor://C:\Program Files\Suricata\log]
sourcetype=suricata
ignoreOlderThan =14d
host = WebServer
```

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS

73. Close all open files in **Notepad**.

74. Navigate to **Windows Start > Administrative Tools**. Double-click on **Services** in the Administrative Tools window. The services window opens, search for **SplunkForwarder Service**.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



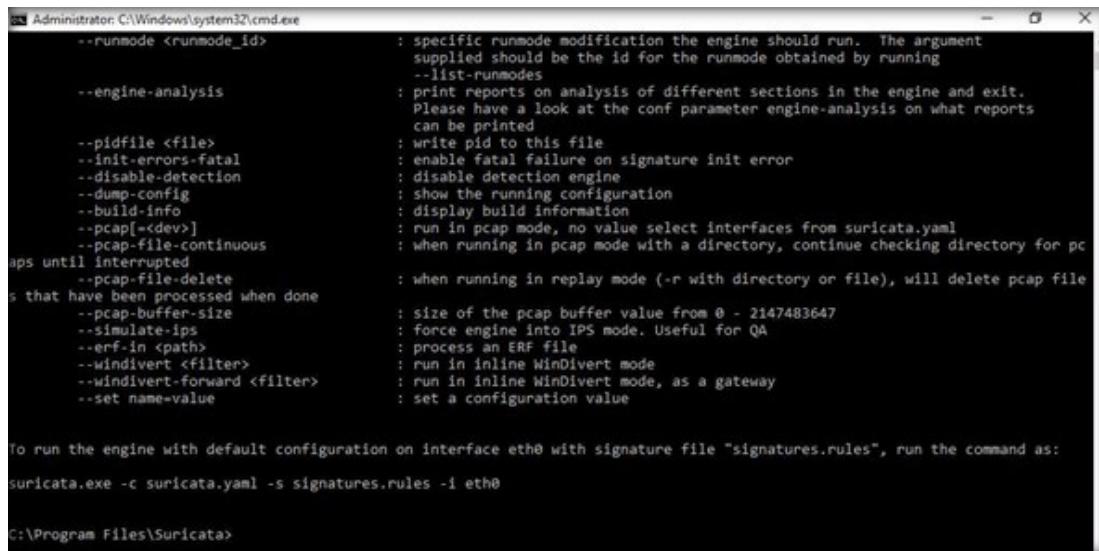
75. Click on **SplunkForwarder Service**, and then **Restart** the service.

Note: If an error occurs while restarting, click **Start** again.

76. Next, launch Suricata to capture the network traffic, navigate to the desktop, and double click the **Suricata-4.1.4-64bit IDS-IPS** shortcut.

77. The Suricata Command Prompt will open.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The window displays the command-line interface for the Suricata IDS/IPS system. The user has run the command "suricata --help", which outputs a detailed list of command-line options and their descriptions. The options include various modes like runmode, engine analysis, and file processing, along with their specific parameters and meanings. At the bottom of the output, there is a note about running the engine with default configuration on interface eth0.

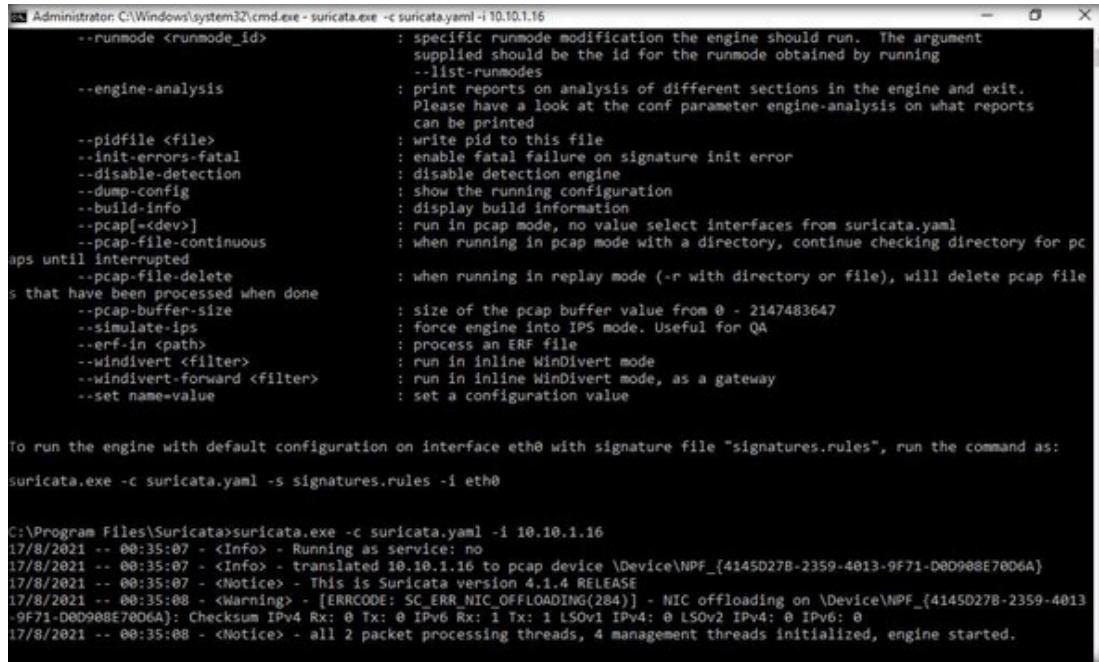
```
--runmode <runmode_id>
          : specific runmode modification the engine should run. The argument
          supplied should be the id for the runmode obtained by running
--list-runmodes
          : print reports on analysis of different sections in the engine and exit.
          Please have a look at the conf parameter engine-analysis on what reports
          can be printed
--pidfile <file>
          : write pid to this file
--init-errors-fatal
          : enable fatal failure on signature init error
--disable-detection
          : disable detection engine
--dump-config
          : show the running configuration
--build-info
          : display build information
--pcap[=<dev>]
          : run in pcap mode, no value select interfaces from suricata.yaml
--pcap-file-continuous
          : when running in pcap mode with a directory, continue checking directory for pc
aps until interrupted
          : when running in replay mode (-r with directory or file), will delete pcap file
--pcap-file-delete
          : when running in replay mode (-r with directory or file), will delete pcap file
          : that have been processed when done
--pcap-buffer-size
          : size of the pcap buffer value from 0 - 2147483647
--simulate-ips
          : force engine into IPS mode. Useful for QA
--erf-in <path>
          : process an ERF file
--windivert <filter>
          : run in inline WinDivert mode
--windivert-forward <filter>
          : run in inline WinDivert mode, as a gateway
--set name=value
          : set a configuration value

To run the engine with default configuration on interface eth0 with signature file "signatures.rules", run the command as:
suricata.exe -c suricata.yaml -s signatures.rules -i eth0

C:\Program Files\Suricata>
```

78. Type the **suricata.exe -c suricata.yaml -i 10.10.1.16** command to run Suricata for capturing network traffic, and press **Enter**.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The command entered is "suricata.exe -c suricata.yaml -i 10.10.1.16". The output displays the Suricata configuration options and their descriptions. It includes sections for runmode, engine analysis, pidfile, init-errors-fatal, disable-detection, dump-config, build-info, pcap, pcap-file-continuous, and pcap-file-delete. Below this, it provides instructions for running the engine with default configuration on interface eth0 with signature file "signatures.rules". The final part of the output shows the Suricata log starting at 17/8/2021, 00:35:07, indicating it is running as a service and providing version information.

```
Administrator: C:\Windows\system32\cmd.exe - suricata.exe -c suricata.yaml -i 10.10.1.16

--runmode <runmode_id> : specific runmode modification the engine should run. The argument supplied should be the id for the runmode obtained by running --list-runmodes

--engine-analysis : print reports on analysis of different sections in the engine and exit. Please have a look at the conf parameter engine-analysis on what reports can be printed

--pidfile <file> : write pid to this file
--init-errors-fatal : enable fatal failure on signature init error
--disable-detection : disable detection engine
--dump-config : show the running configuration
--build-info : display build information
--pcap[=<dev>] : run in pcap mode, no value select interfaces from suricata.yaml
--pcap-file-continuous : when running in pcap mode with a directory, continue checking directory for pcaps until interrupted
--pcap-file-delete : when running in replay mode (-r with directory or file), will delete pcap file
-s that have been processed when done
--pcap-buffer-size : size of the pcap buffer value from 0 - 2147483647
--simulate-ips : force engine into IPS mode. Useful for QA
--erf-in <path> : process an ERF file
--windivert <filter> : run in inline WinDivert mode
--windivert-forward <filter> : run in inline WinDivert mode, as a gateway
--set name=value : set a configuration value

To run the engine with default configuration on interface eth0 with signature file "signatures.rules", run the command as:
suricata.exe -c suricata.yaml -s signatures.rules -i eth0

C:\Program Files\Suricata>suricata.exe -c suricata.yaml -i 10.10.1.16
17/8/2021 -- 00:35:07 - <Info> - Running as service: no
17/8/2021 -- 00:35:07 - <Info> - translated 10.10.1.16 to pcap device \Device\NPF_{4145D27B-2359-4013-9F71-00D988E7006A}
17/8/2021 -- 00:35:07 - <Notice> - This is Suricata version 4.1.4 RELEASE
17/8/2021 -- 00:35:08 - <Warning> - [ERRCODE: SC_ERR_NIC_OFFLOADING(284)] - NIC offloading on \Device\NPF_{4145D27B-2359-4013-9F71-00D988E7006A}: Checksum IPv4 Rx: 0 Tx: 0 IPv6 Rx: 1 Tx: 1 LSOv1 IPv4: 0 LSOv2 IPv4: 0 IPv6: 0
17/8/2021 -- 00:35:08 - <Notice> - all 2 packet processing threads, 4 management threads initialized, engine started.
```

79. The Suricata engine will start. Leave the command prompt open and Suricata running.

80. We need to perform the attack from the attacker machine to the **Web Server**. Suricata will then generate the alert and store it in the **fast.log** file.

81. The **fast.log** file is the default alert log file that is already set into the suricatata.yaml file.

82. Switch to the **Attacker Machine-1** virtual machine.

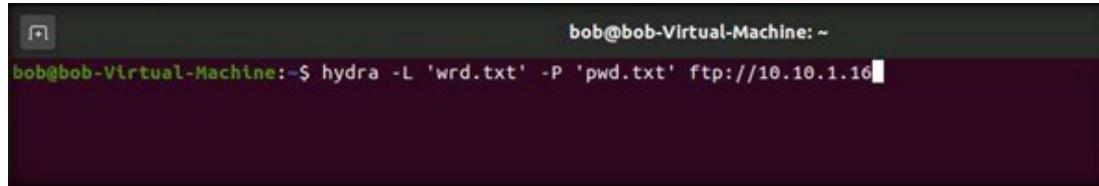
83. Select username as **Bob** and type password as **user@123** and press **Enter**.

84. To perform a brute-force attack, use the tool Hydra from Ubuntu OS (Attacker Machine).

Note: Hydra uses two files for performing a brute-force attack. The first file has the list of usernames, and the second file has a list of passwords. Hydra uses these lists of usernames and passwords for performing a brute-force attacks.

85. Press **Ctrl + Alt + T** to open the terminal, type **hydra -L 'wrd.txt' -P 'pwd.txt' ftp://10.10.1.16**, and press **Enter**.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS

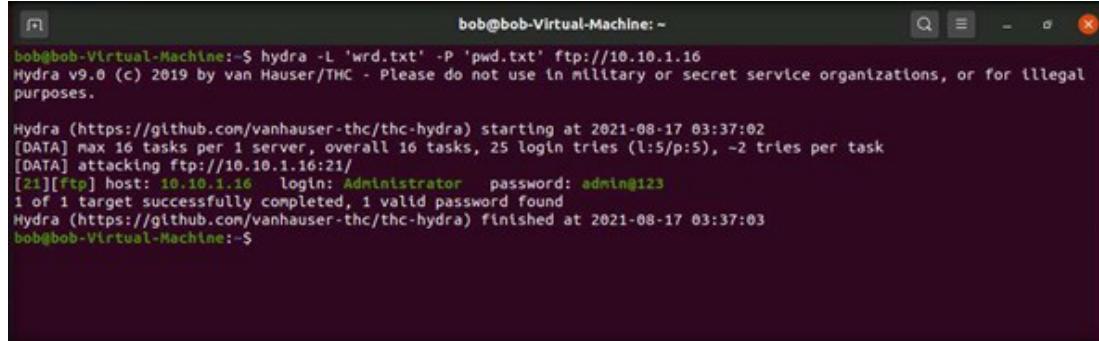


A screenshot of a terminal window titled "bob@bob-Virtual-Machine: ~". The command "hydra -L 'wrd.txt' -P 'pwd.txt' ftp://10.10.1.16" is typed into the terminal and is being executed.

86. The **Attacker Machine-1** will try to match the combination of usernames and passwords with the Web Server.

87. The matched username and password are shown in the terminal in green color. Close the terminal window.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



A terminal window titled "bob@bob-Virtual-Machine: ~" displays the output of a Hydra attack. The command used was "hydra -L 'wrd.txt' -P 'pwd.txt' ftp://10.10.1.16". The output shows Hydra version 9.6 from 2019, attacking an FTP server at 10.10.1.16:21. It lists 16 tasks per server, 25 login tries (l:5/p:5), and 2 tries per task. A successful login is shown in green: [21][FTP] host: 10.10.1.16 login: Administrator password: admin@123. The attack finished at 2021-08-17 03:37:03.

```
bob@bob-Virtual-Machine:~$ hydra -L 'wrd.txt' -P 'pwd.txt' ftp://10.10.1.16
Hydra v9.6 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal
purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-08-17 03:37:02
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5), -2 tries per task
[DATA] attacking ftp://10.10.1.16:21/
[21][FTP] host: 10.10.1.16 login: Administrator password: admin@123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-08-17 03:37:03
bob@bob-Virtual-Machine:~$
```

88. After the attack is complete, switch to the **Admin Machine-1** virtual machine.

89. Log in using the credentials **Admin** and **admin@123**.

Note: If the network screen appears, click **Yes**.

90. Launch the web browser, and access Splunk Enterprise with the URL <http://localhost:8000/en-US/account/login?> and press **Enter**.

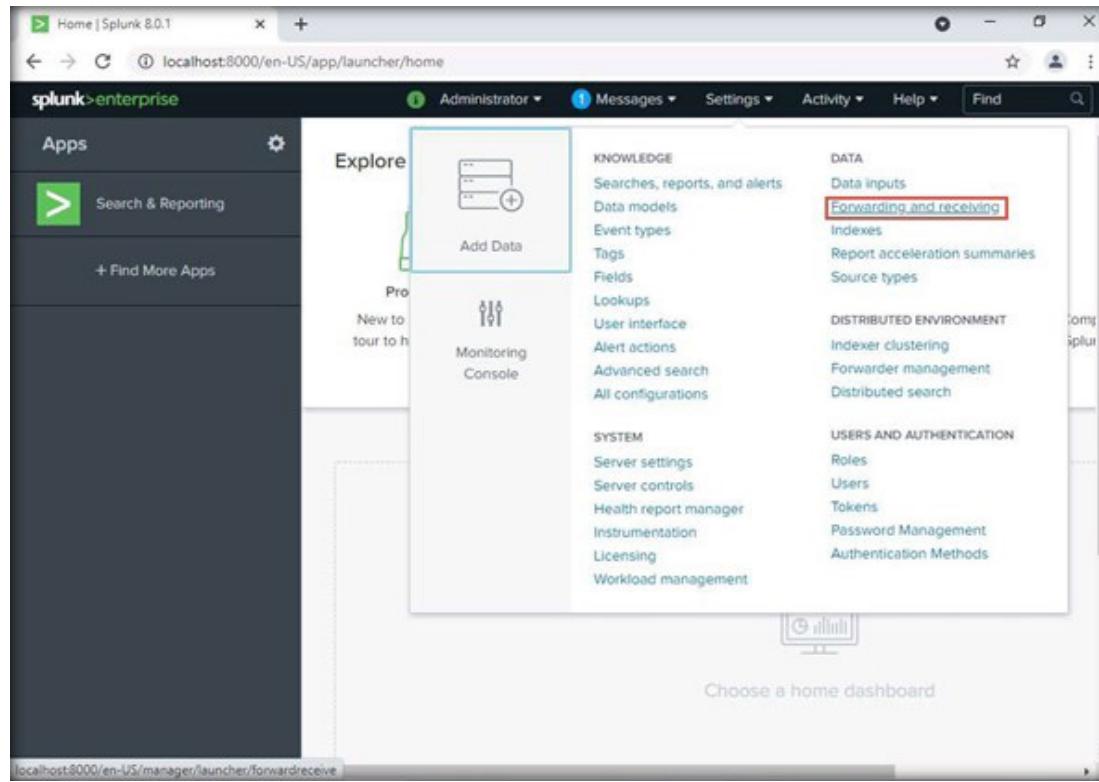
91. Log in with the username **admin** and password **admin@123**.

Note: If the Splunk Enterprise page is not opening, make sure the splunkd service is running. If not, then press “**Windows+R**” on your keyboard and type “**services.msc**”. Click on **OK**. Next, the Services window opens. Search for the **splunkd** service and **restart**. Wait for the service to start.

Note: If **Important Changes coming!** pop-up appears, click **Don't show me this again**.

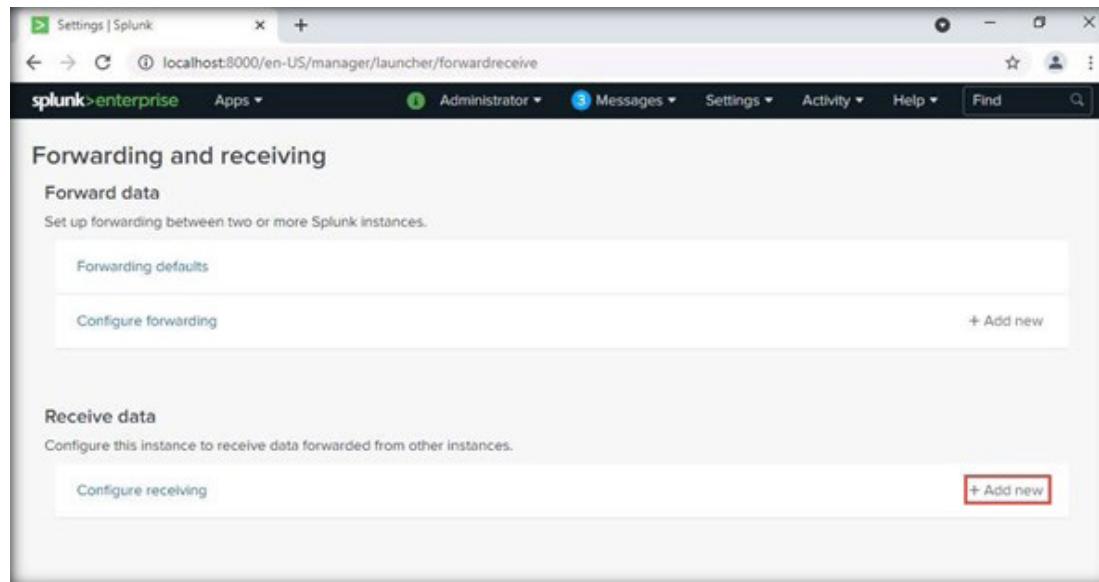
92. The Splunk web console appears; click **Settings** menu, select **Forwarding and receiving** link under the **DATA** section

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



93. The Forwarding and receiving console will appear. This is where a new instance will be added to receive the data forwarded from Universal Forwarder. Click on the **+Add new** link in the bottom right corner to **Configure receiving**.

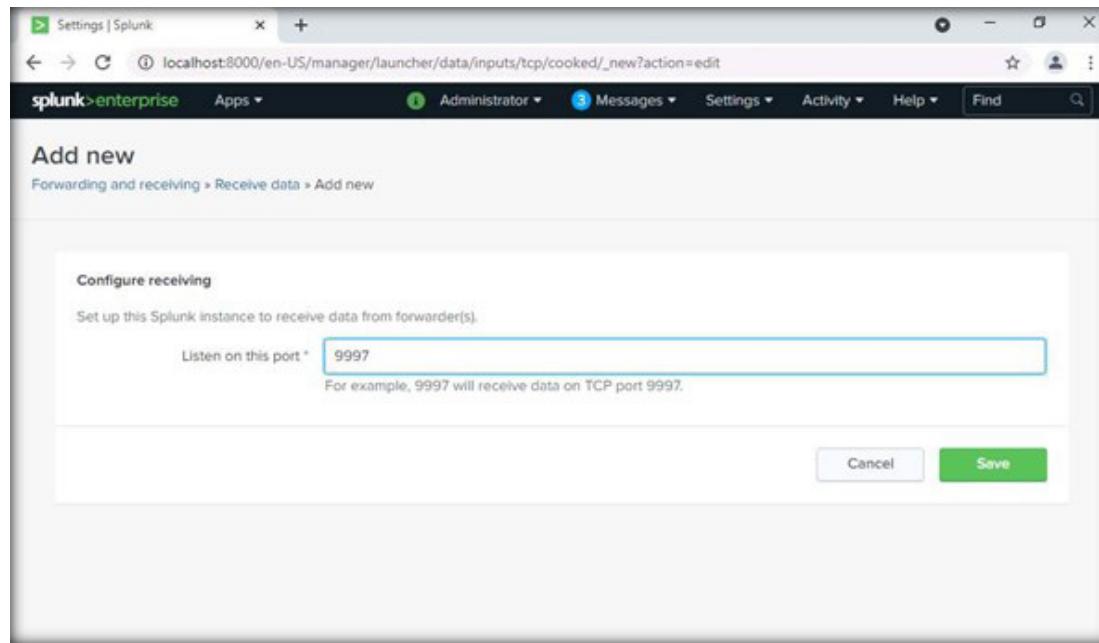
EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



The screenshot shows the 'Forwarding and receiving' configuration page in the Splunk web interface. The top navigation bar includes 'Settings | Splunk', a search bar, and user information ('Administrator'). Below the header, the URL 'localhost:8000/en-US/manager/launcher/forwardreceive' is visible. The main content area is titled 'Forwarding and receiving'. It contains two sections: 'Forward data' and 'Receive data'. The 'Forward data' section has a sub-section 'Forwarding defaults' and a button '+ Add new' next to 'Configure forwarding'. The 'Receive data' section has a sub-section 'Configure receiving' and a red-bordered button '+ Add new' next to it.

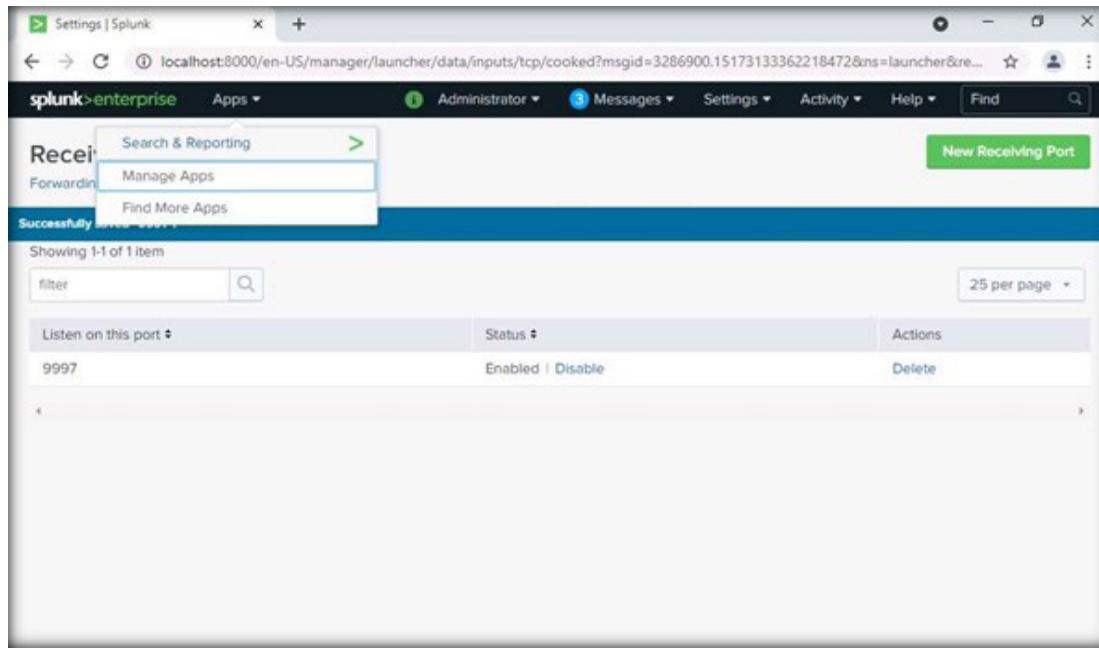
94. The **Add new** console appears; in the **Listen on this port*** field, type **9997** and click on **Save**.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



95. Once the port is added, go to **Apps** menu, and then select **Manage Apps**.

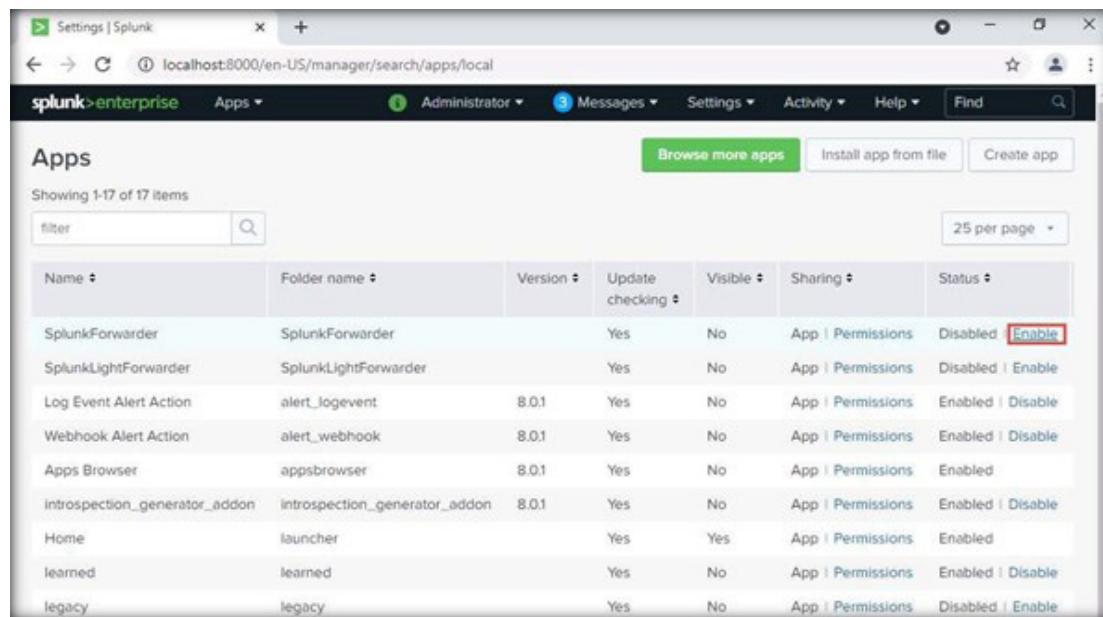
EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



The screenshot shows the Splunk Enterprise Settings interface. At the top, there's a navigation bar with links for Settings, Apps (which is currently selected), Administrator, Messages, Activity, Help, and Find. Below the navigation bar, a dropdown menu is open under the Apps link, showing options: Search & Reporting, Manage Apps (which is highlighted with a blue background), and Find More Apps. A green button labeled "New Receiving Port" is visible on the right. The main content area has a header "Successfully" and a message "Your port was successfully added". It shows a table with one item: "9997" under "Listen on this port", "Enabled | Disable" under "Status", and a "Delete" button under "Actions". There are also "filter" and "25 per page" buttons at the bottom of the table.

96. The Apps console appears; click on the **Enable** link toward the extreme right associated with the **SplunkForwarder** application.

EXERCISE 6: IMPLEMENT NETWORK-BASED IDS FUNCTIONALITY USING SURICATA IDS

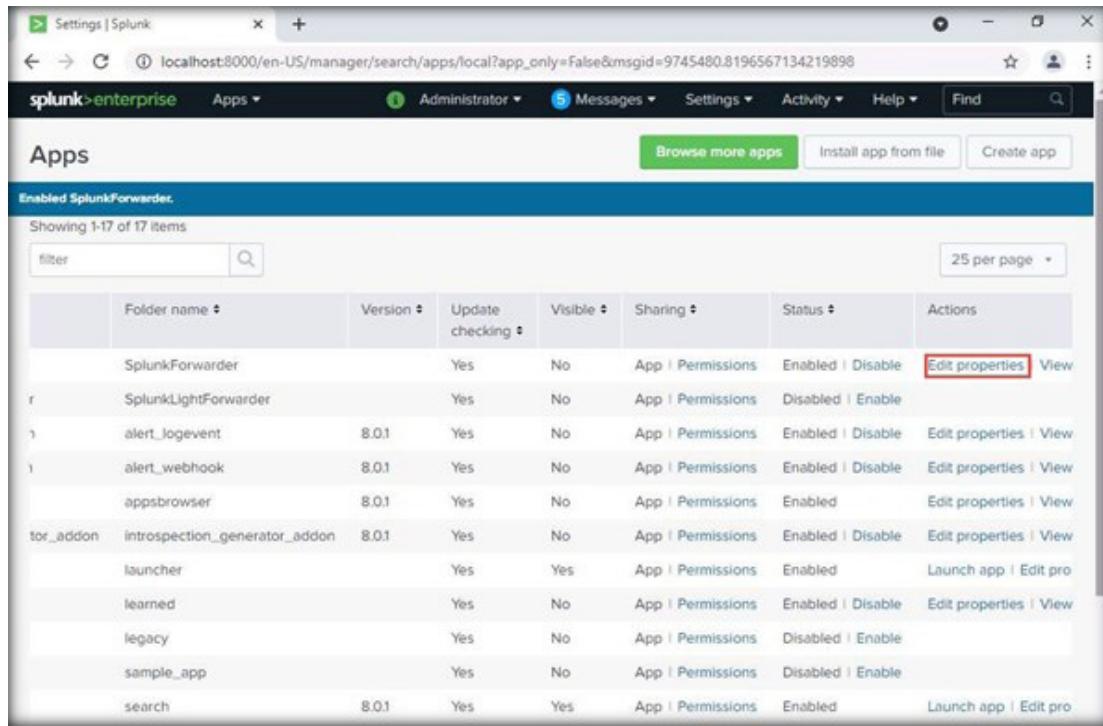


The screenshot shows the Splunk Apps console interface. The title bar reads "Settings | Splunk" and the URL is "localhost:8000/en-USmanager/search/apps/local". The top navigation bar includes "splunk>enterprise", "Apps", "Administrator", "Messages", "Settings", "Activity", "Help", and "Find". Below the navigation is a search bar and a "Browse more apps" button. A "Create app" button is also present. The main area is titled "Apps" and displays a table of 17 items. The columns are: Name, Folder name, Version, Update checking, Visible, Sharing, and Status. The "Status" column contains links like "App | Permissions" and "Enabled | Disable". The "SplunkForwarder" row is highlighted, and the "Enabled | Disable" link is circled in red.

Name	Folder name	Version	Update checking	Visible	Sharing	Status
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable
Log Event Alert Action	alert_logevent	8.0.1	Yes	No	App Permissions	Enabled Disable
Webhook Alert Action	alert_webhook	8.0.1	Yes	No	App Permissions	Enabled Disable
Apps Browser	appsbrowser	8.0.1	Yes	No	App Permissions	Enabled
introspection_generator_addon	introspection_generator_addon	8.0.1	Yes	No	App Permissions	Enabled Disable
Home	launcher		Yes	Yes	App Permissions	Enabled
learned	learned		Yes	No	App Permissions	Enabled Disable
legacy	legacy		Yes	No	App Permissions	Disabled Enable

97. When the application is enabled, click on **Edit properties** under **Actions** column associated with **SplunkForwarder**.

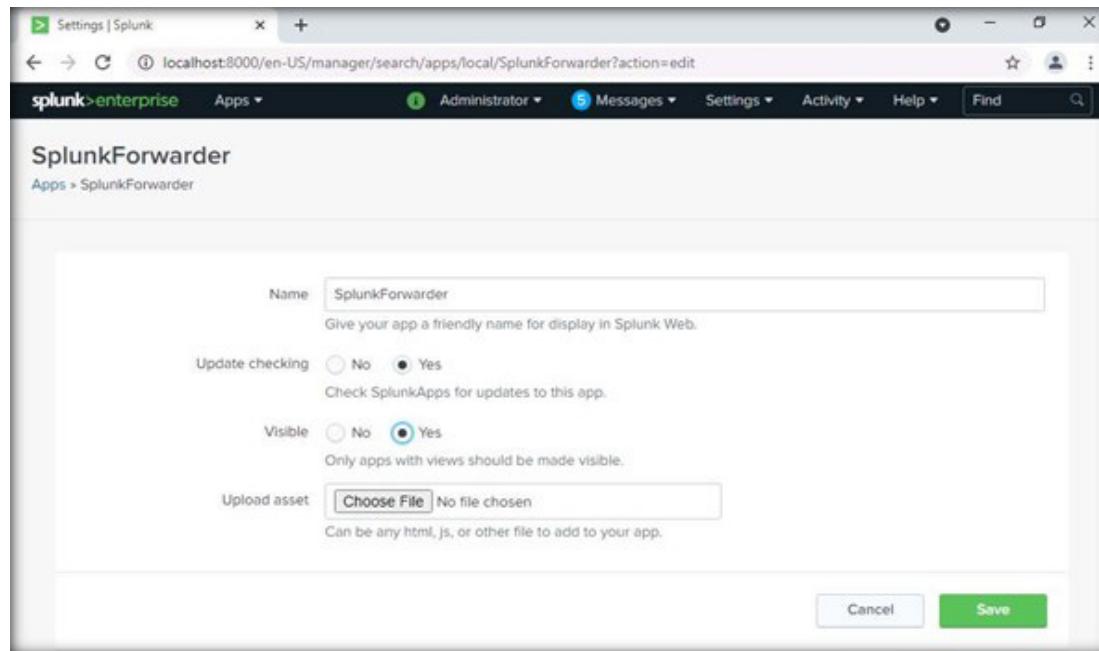
EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder		Yes	No	App Permissions	Enabled Disable	Edit properties View
SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable	Edit properties View
alert_logevent	8.0.1	Yes	No	App Permissions	Enabled Disable	Edit properties View
alert_webhook	8.0.1	Yes	No	App Permissions	Enabled Disable	Edit properties View
appsbrowser	8.0.1	Yes	No	App Permissions	Enabled	Edit properties View
tor-addon	introspection_generatorAddon	8.0.1	Yes	No	App Permissions	Enabled Disable
launcher		Yes	Yes	App Permissions	Enabled	Launch app Edit pro
learned		Yes	No	App Permissions	Enabled Disable	Edit properties View
legacy		Yes	No	App Permissions	Disabled Enable	Edit properties View
sample_app		Yes	No	App Permissions	Disabled Enable	Edit properties View
search	8.0.1	Yes	Yes	App Permissions	Enabled	Launch app Edit pro

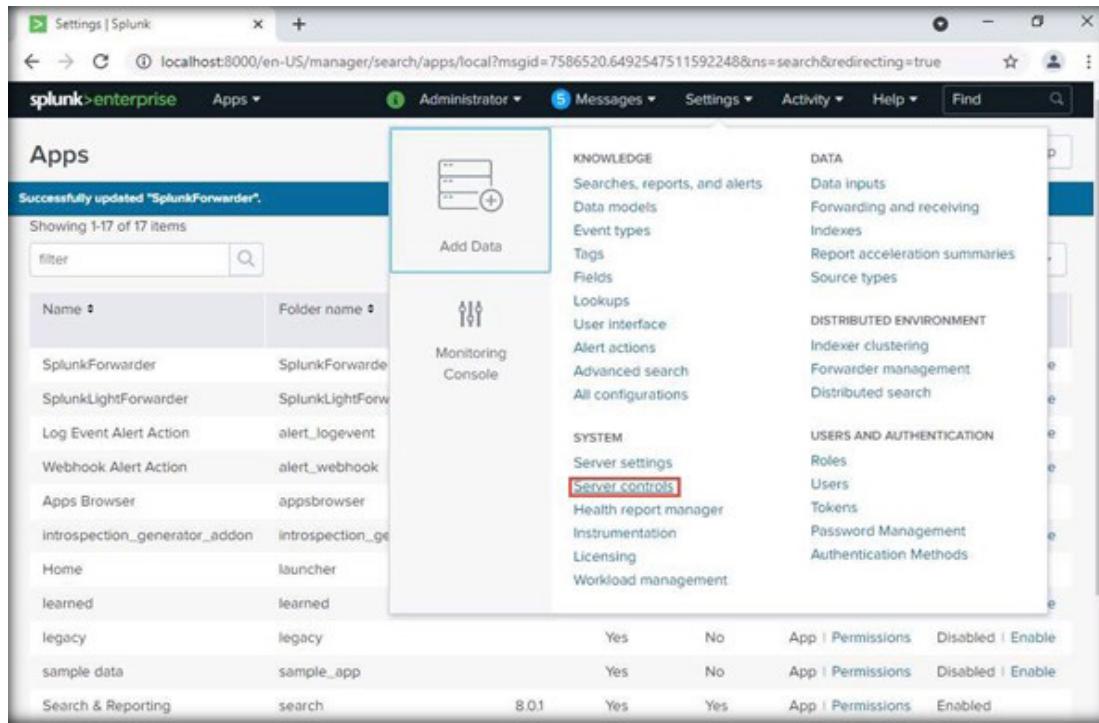
98. The SplunkForwarder console appears; click on **Yes** under the **Visible** section, and then on **Save**.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



99. Go to **Settings** and select **Server controls** under the **SYSTEM** section.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS

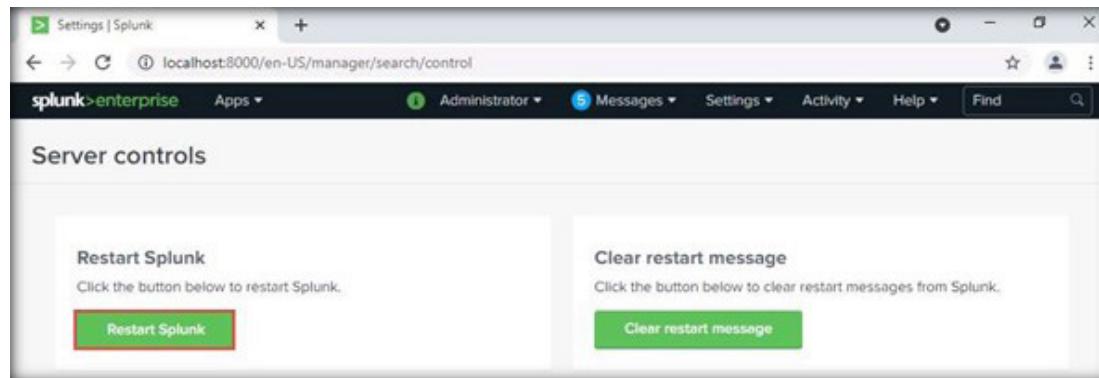


The screenshot shows the Splunk Enterprise Settings interface. On the left, there is a list of apps, including SplunkForwarder, SplunkLightForwarder, Log Event Alert Action, Webhook Alert Action, Apps Browser, introspection_generator_addon, Home, learned, legacy, sample data, and Search & Reporting. In the center, there is a sidebar with sections for KNOWLEDGE, DATA, DISTRIBUTED ENVIRONMENT, SYSTEM, and USERS AND AUTHENTICATION. Under the SYSTEM section, the 'Server settings' and 'Server controls' options are listed. A red box highlights the 'Server controls' link. On the right, there is a table showing app details like Name, Folder name, Monitoring Console, Status, App permissions, and Permissions status.

Name	Folder name	Monitoring Console	Status	App permissions	Permissions
SplunkForwarder	SplunkForwarder		Yes	App	Enabled
SplunkLightForwarder	SplunkLightForw		Yes	App	Disabled
Log Event Alert Action	alert_logevent		No		Enable
Webhook Alert Action	alert_webhook		No		Enable
Apps Browser	appsbrowser		Yes	App	Enabled
introspection_generator_addon	introspection_ge		Yes	App	Enabled
Home	launcher		Yes	App	Enabled
learned	learned		Yes	App	Enabled
legacy	legacy		Yes	App	Enabled
sample data	sample_app		Yes	App	Enabled
Search & Reporting	search		Yes	App	Enabled

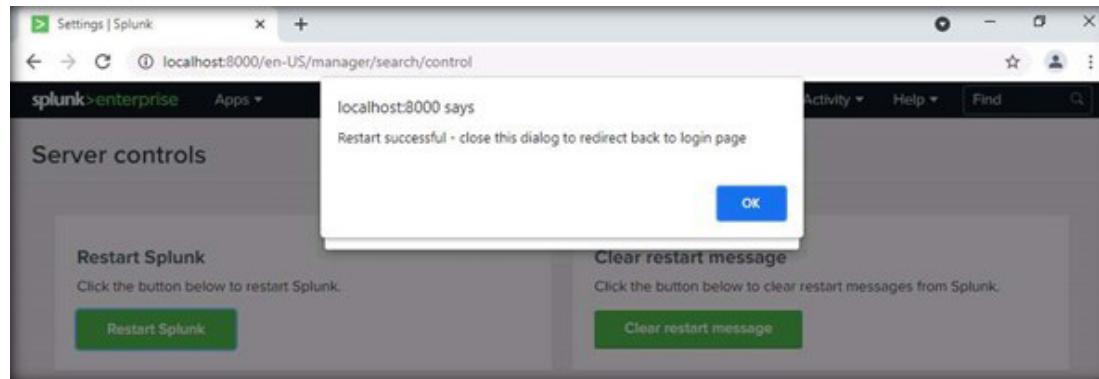
100. The **Server controls** console appears; click on **Restart Splunk**. A confirmation pop-up appears; click on **OK**.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



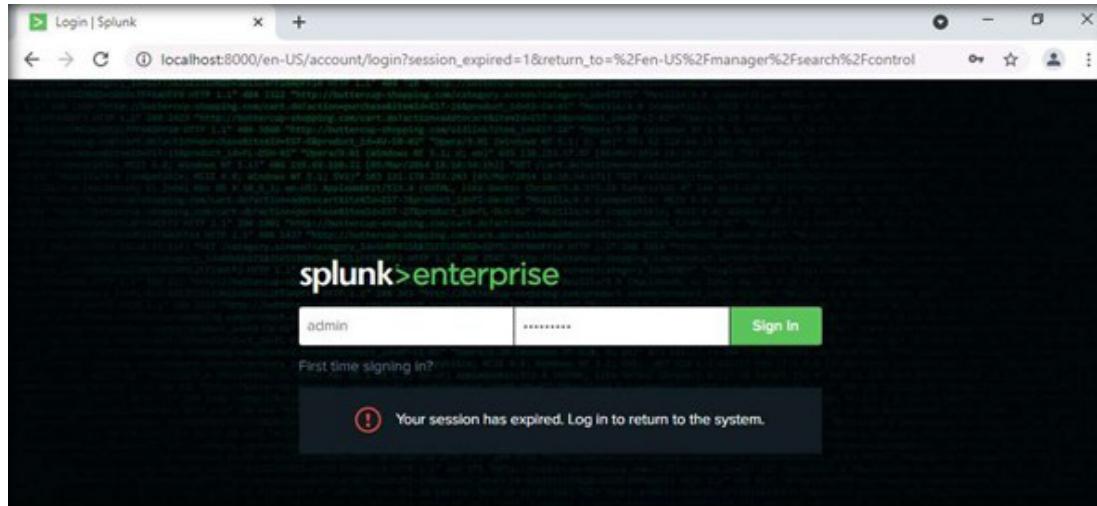
101. Wait for few seconds, on a successful restart, a pop-up appears with the message “**Restart successful**”. Click **OK** to log back into Splunk. Click on **OK**.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



102. You will be redirected to the login page. Enter the user credentials (username **admin** and password **admin@123**) and click on **Sign In**.

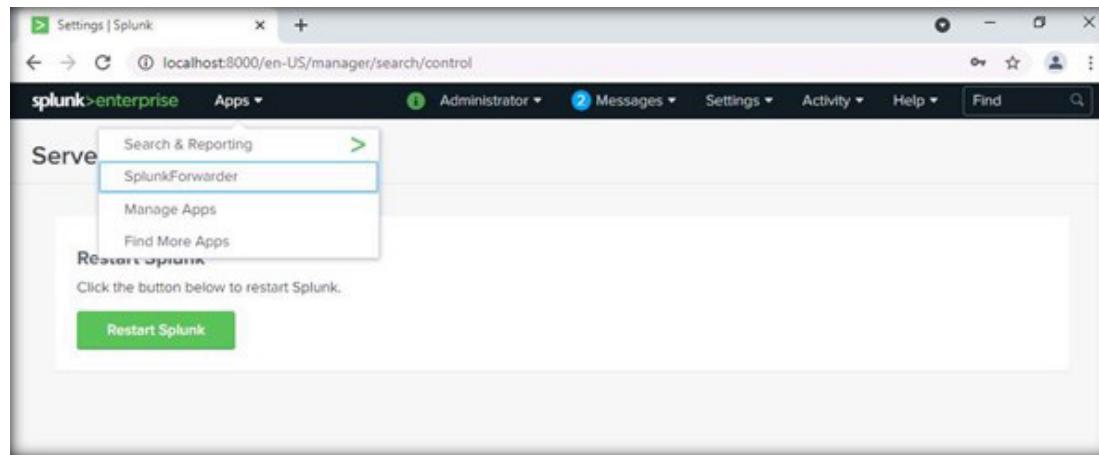
EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS

Note: If Splunk is properly not restarted, click **Restart Splunk again**.

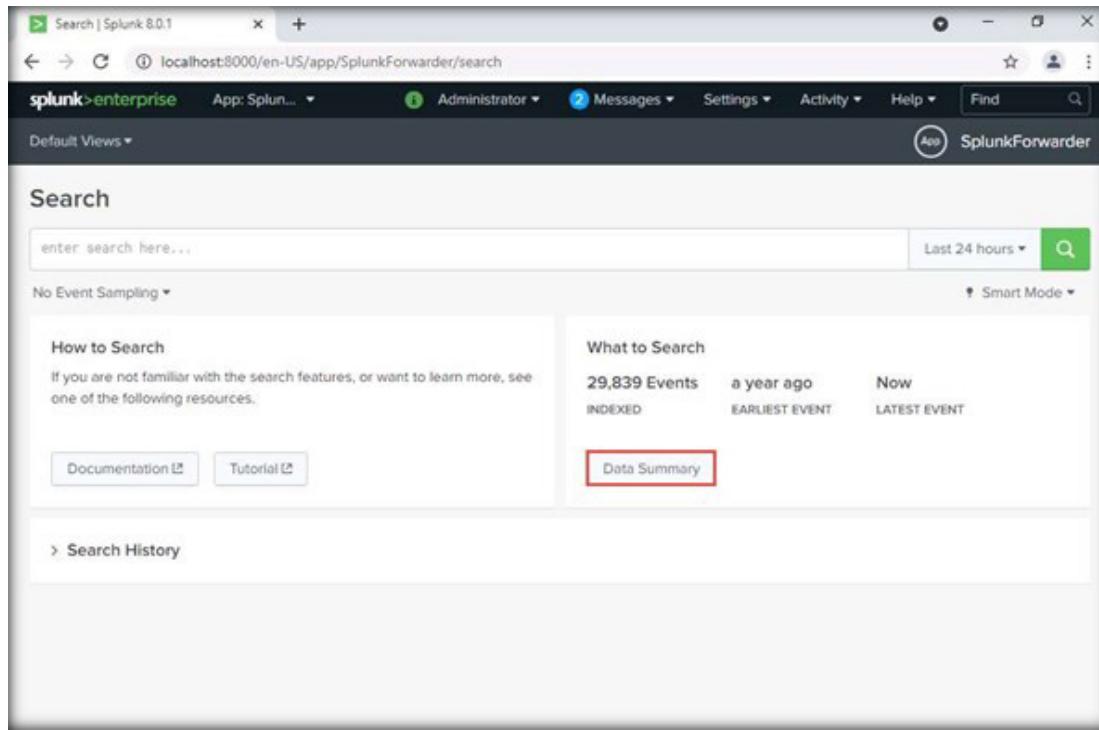
103. Once you log in, click on **Apps > SplunkForwarder** from menu.



EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS

Note: Make sure Splunk Forwarder service is running. If it is not running, start the Splunkforwarder service in Windows services.

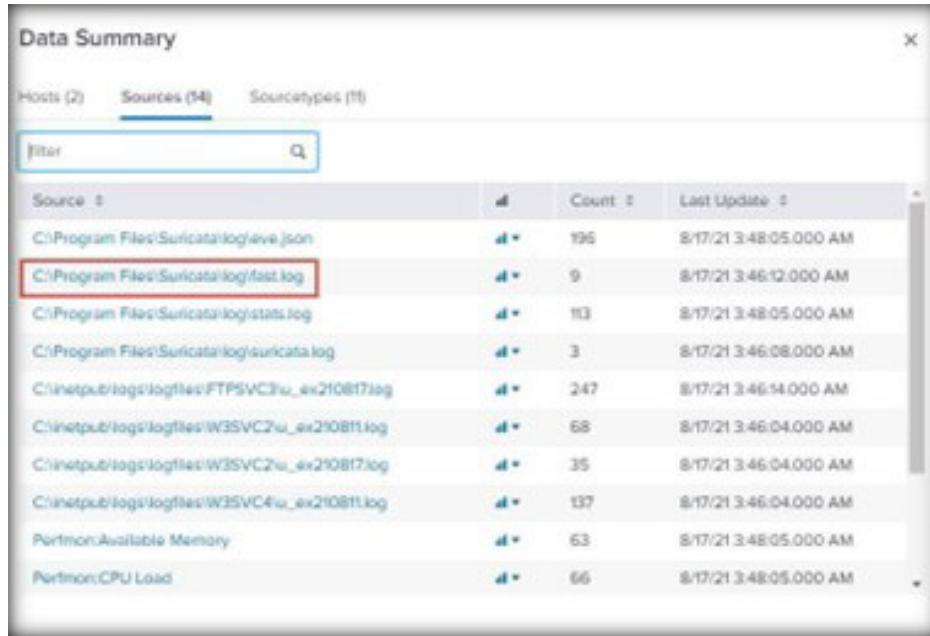
104. The **Search** console appears; click on **Data Summary** under the **What to Search** section.



The screenshot shows the Splunk 8.0.1 search interface. At the top, the URL is localhost:8000/en-US/app/SplunkForwarder/search. The main area is titled "Search" with a search bar containing "enter search here...". Below the search bar are sections for "How to Search" and "What to Search". The "How to Search" section includes links for "Documentation" and "Tutorial". The "What to Search" section displays statistics: 29,839 Events (INDEXED), a year ago (EARLIEST EVENT), Now (LATEST EVENT), and a button labeled "Data Summary" which is highlighted with a red box. At the bottom left, there is a link to "Search History".

105. The **Data Summary** pop-up appears. Select the **Sources (14)** tab, wait for some time, and then click the **C:\Program Files\Suricata\log\fast.log** link to continue.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



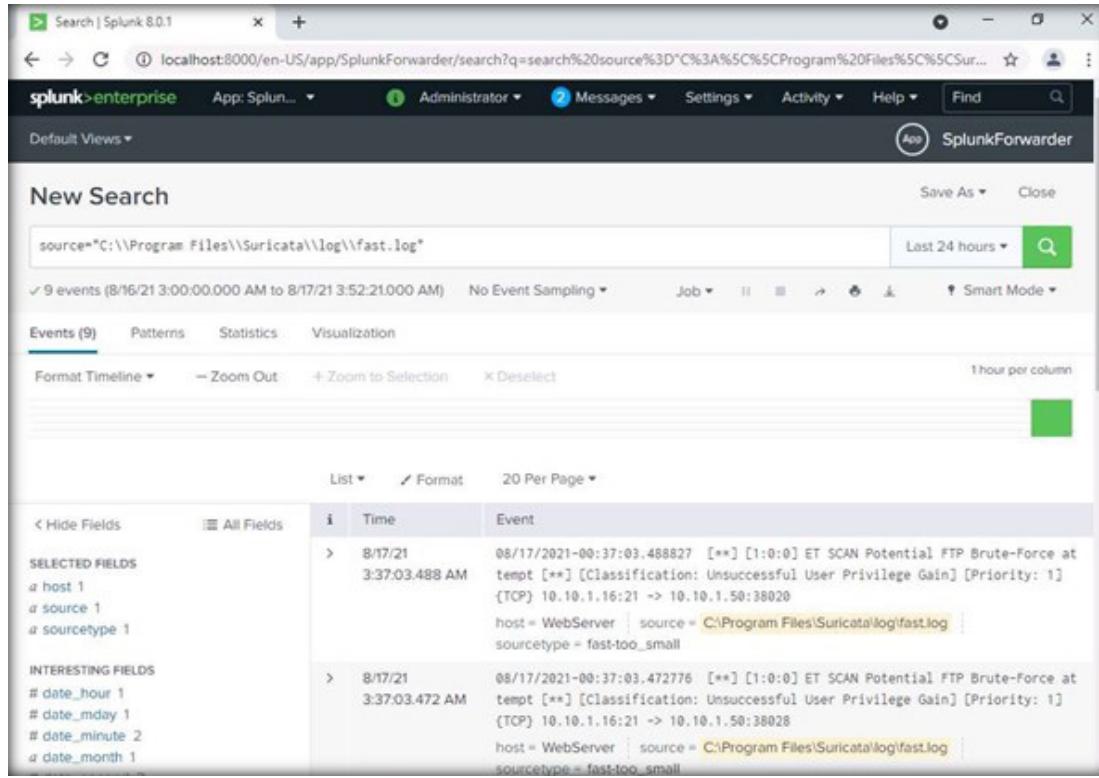
Source	Count	Last Update
C:\Program Files\Suricata\log\eve.json	195	8/17/21 3:48:05.000 AM
C:\Program Files\Suricata\log\fast.log	9	8/17/21 3:46:12.000 AM
C:\Program Files\Suricata\log\stats.log	103	8/17/21 3:48:05.000 AM
C:\Program Files\Suricata\log\suricata.log	3	8/17/21 3:46:08.000 AM
Chinetpub\logs\logfiles\FTPSVC1\w_ex210817.log	247	8/17/21 3:46:14.000 AM
Chinetpub\logs\logfiles\W3SVC2\w_ex210811.log	68	8/17/21 3:46:04.000 AM
Chinetpub\logs\logfiles\W3SVC2\w_ex210817.log	35	8/17/21 3:46:04.000 AM
Chinetpub\logs\logfiles\W3SVC4\w_ex210811.log	137	8/17/21 3:46:04.000 AM
Portmon:Available Memory	63	8/17/21 3:48:05.000 AM
Portmon:CPU Load	66	8/17/21 3:48:05.000 AM

106. Once the **fast.log** file is selected, the page redirects to the search page and displays the detailed logs.

107. The brute-force attempt was made from Attacker Machine-1 (**10.10.1.50**) to the Web Server (**10.10.1.16**).

Note: The number of **Events** might vary in your lab environment.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



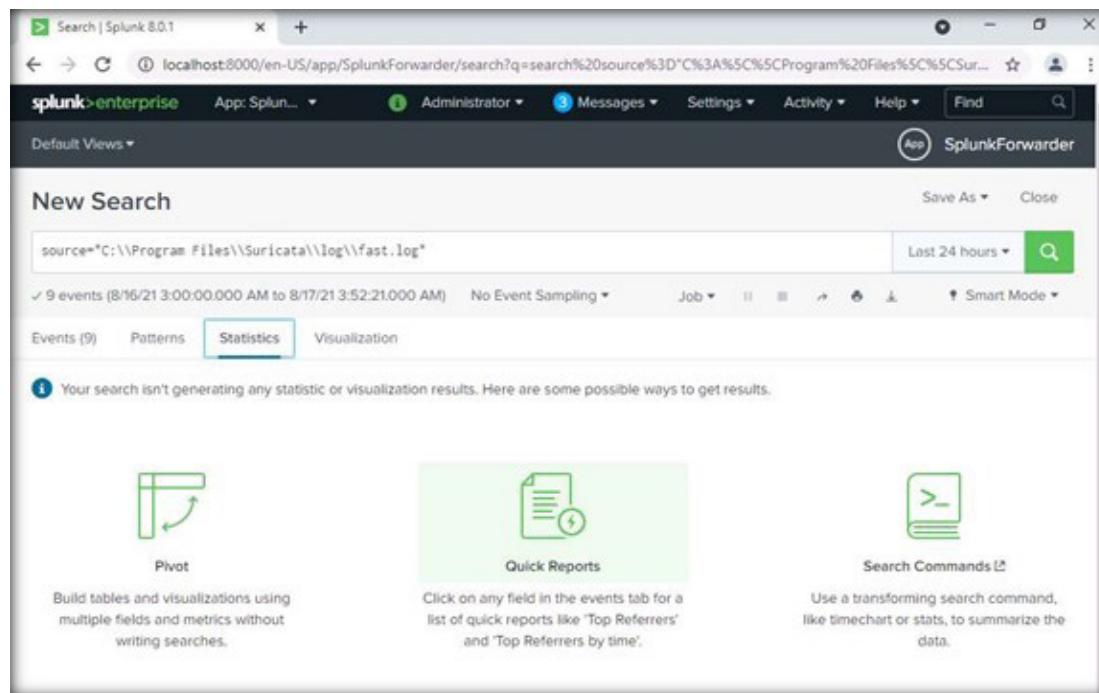
The screenshot shows the Splunk 8.0.1 interface with the following details:

- Search Bar:** source="C:\Program Files\Suricata\log\fast.log"
- Results Summary:** ✓ 9 events (8/16/21 3:00:00.000 AM to 8/17/21 3:52:21.000 AM) | No Event Sampling | Job | Smart Mode
- Event List:** Shows 9 events in a table format. The first two events are listed below:

Time	Event
8/17/21 3:37:03.488 AM	08/17/2021-00:37:03,488827 [**] [1:0:0] ET SCAN Potential FTP Brute-Force attempt [**] [Classification: Unsuccessful User Privilege Gain] [Priority: 1] {TCP} 10.10.1.16:21 -> 10.10.1.50:38020 host = WebServer source = C:\Program Files\Suricata\log\fast.log sourcetype = fast-too_small
8/17/21 3:37:03.472 AM	08/17/2021-00:37:03,472776 [**] [1:0:0] ET SCAN Potential FTP Brute-Force attempt [**] [Classification: Unsuccessful User Privilege Gain] [Priority: 1] {TCP} 10.10.1.16:21 -> 10.10.1.50:38028 host = WebServer source = C:\Program Files\Suricata\log\fast.log sourcetype = fast-too_small

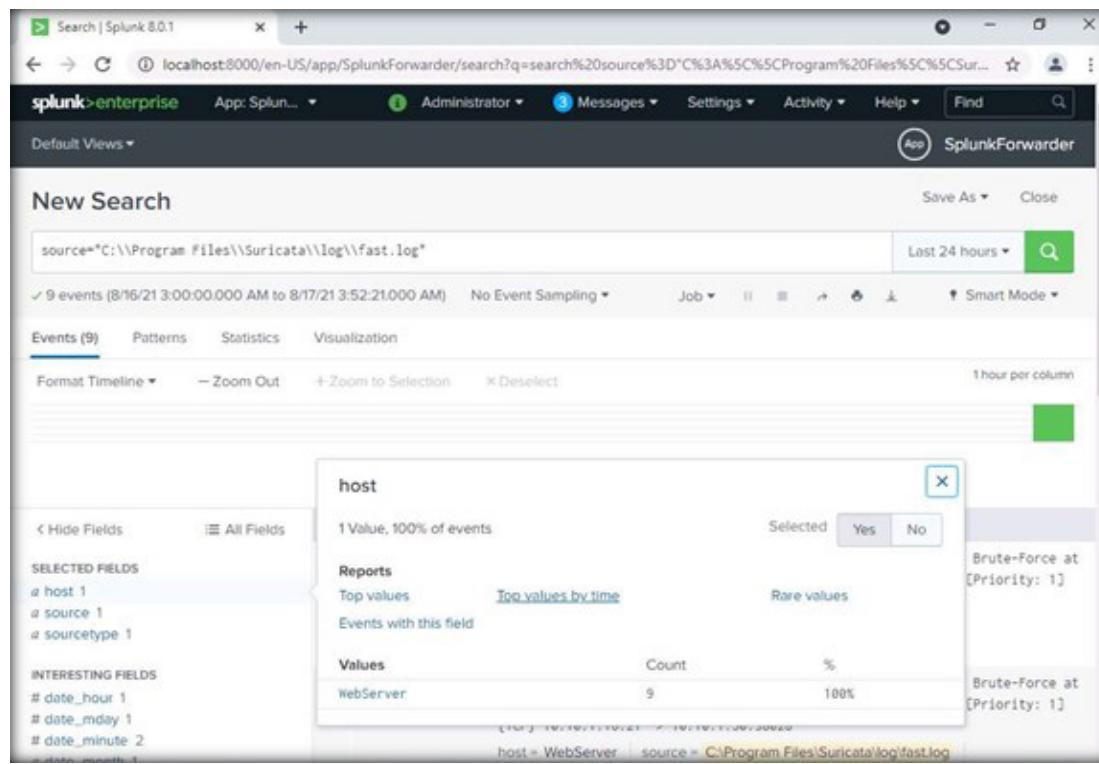
108. Click on **Statistics** tab and **Quick Reports**.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



109. You will be redirected to the host window, in the host window click on any value under Reports to see the graphical representation of that value. Here we are selecting **Top values by time**.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS

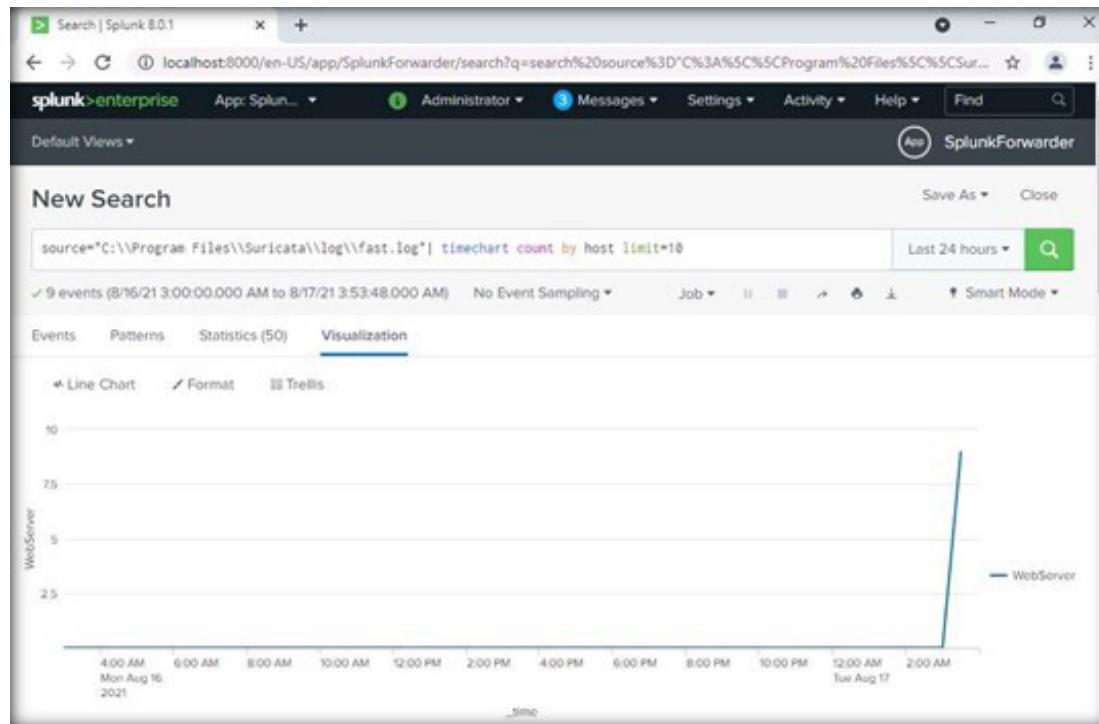


The screenshot shows the Splunk 8.0.1 interface with a search bar containing "source=C:\Program Files\Suricata\log\fast.log". The search results show 9 events from August 16, 2021, to August 17, 2021. A context menu is open over the "host" field, with "Top values by time" selected. The "Values" table shows:

Values	Count	%
WebServer	9	100%

110. You will be redirected to **Visualization** tab where you can find the **Line Chart** of the selected option.

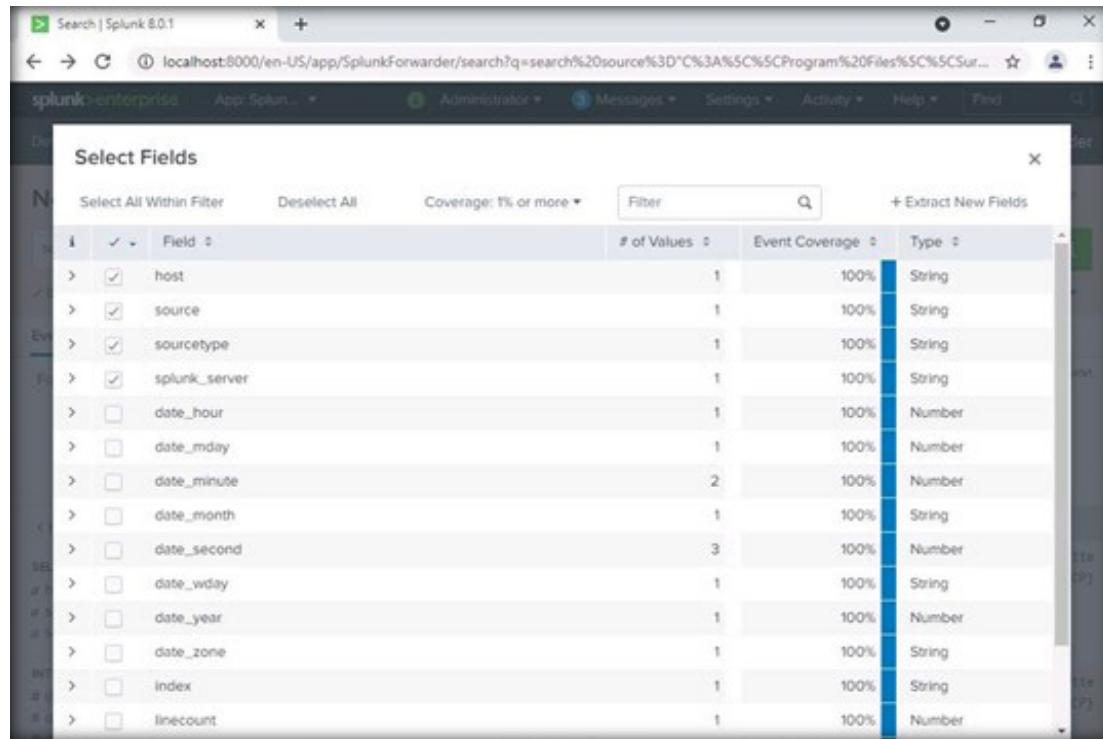
EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



111. Click on back button on the chrome browser to get back to the **Events** tab.

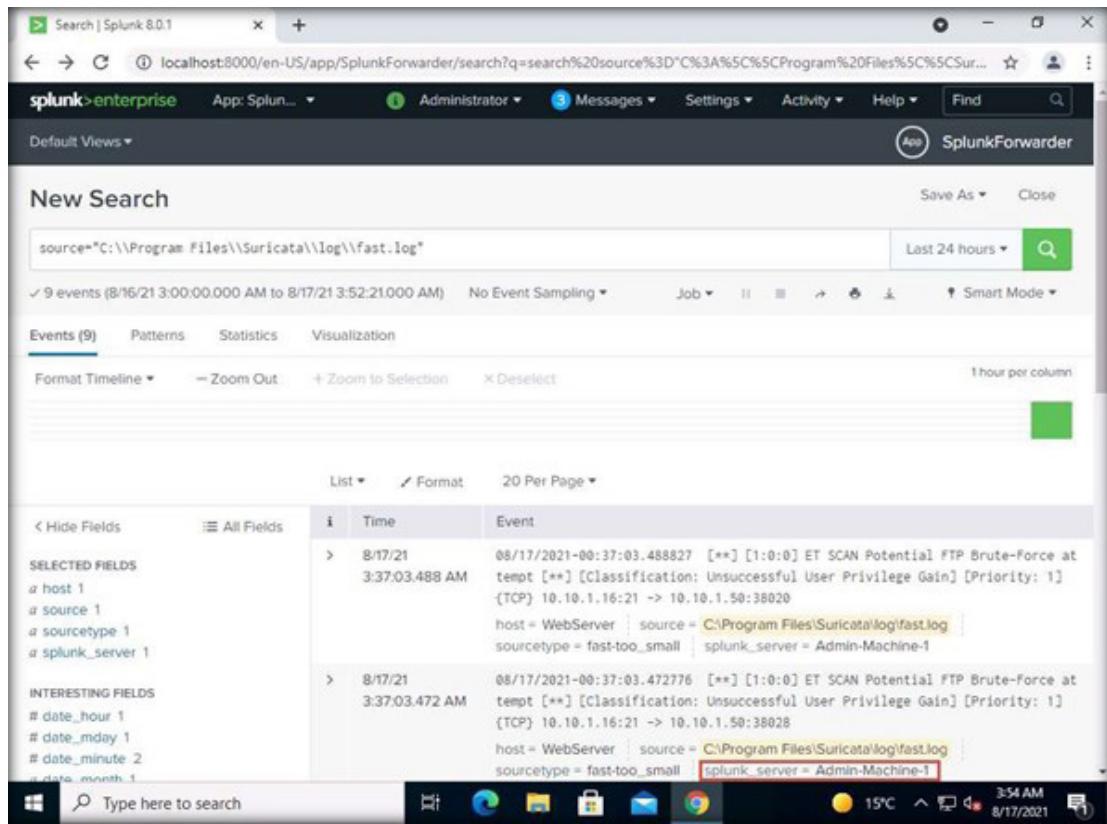
112. Click on **All Fields** option at the left panel of the window to select the options that can be visible in the events tab. Here we are selecting **splunk_server** option, after selecting the options close the **Select Fields** window.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



113. We can see that the **splunk_server (Admin Machine-1)** is visible in the **Event** tab.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS

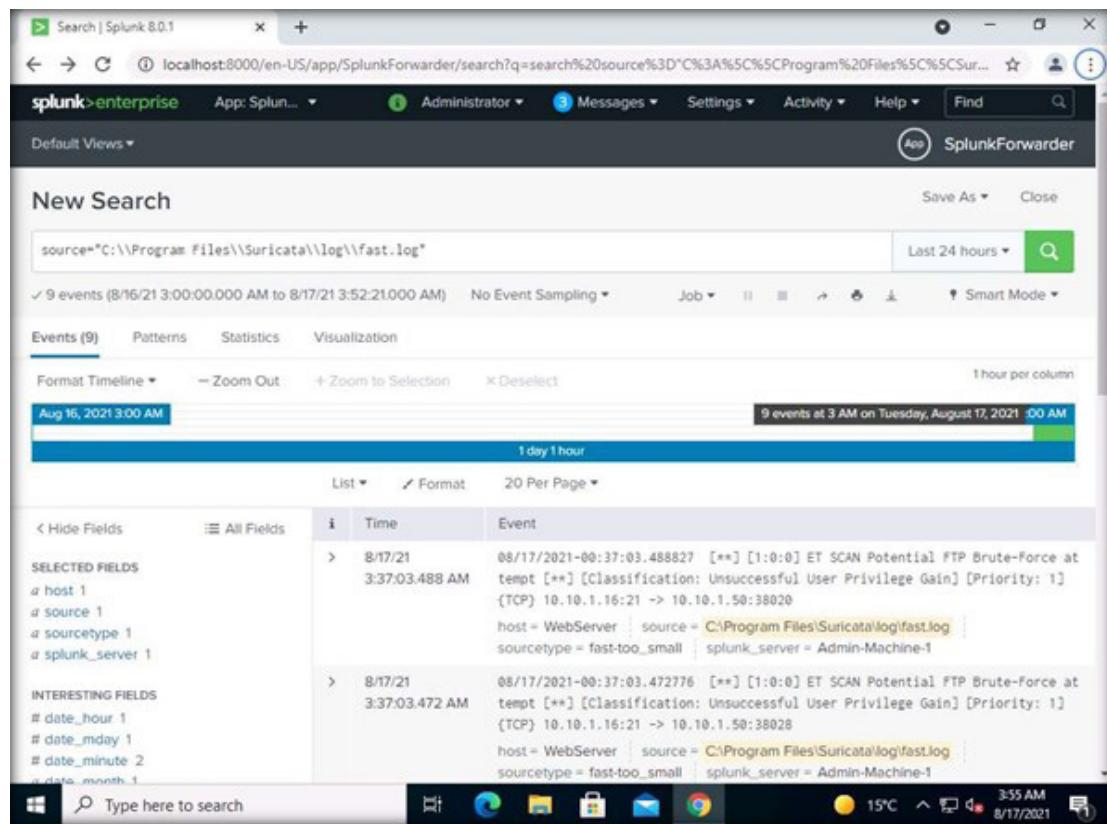


The screenshot shows the Splunk 8.0.1 interface with a search query: `source="C:\Program Files\Suricata\log\fast.log"`. The results table displays 9 events from August 17, 2021, between 3:00:00.000 AM and 3:52:21.000 AM. The table includes columns for Time, Event, host, source, sourcetype, and splunk_server. The last two columns are highlighted with a red box, showing the value `splunk_server = Admin-Machine-1`.

Time	Event	host	source	sourcetype	splunk_server
8/17/21 3:37:03.488 AM	08/17/2021-00:37:03.488827 [**] [1:0:0] ET SCAN Potential FTP Brute-Force at tempt [*] [Classification: Unsuccessful User Privilege Gain] [Priority: 1] {TCP} 10.10.1.16:21 -> 10.10.1.50:38020	host = WebServer	source = C:\Program Files\Suricata\log\fast.log	sourcetype = fast-too_small	splunk_server = Admin-Machine-1
8/17/21 3:37:03.472 AM	08/17/2021-00:37:03.472776 [**] [1:0:0] ET SCAN Potential FTP Brute-Force at tempt [*] [Classification: Unsuccessful User Privilege Gain] [Priority: 1] {TCP} 10.10.1.16:21 -> 10.10.1.50:38028	host = WebServer	source = C:\Program Files\Suricata\log\fast.log	sourcetype = fast-too_small	splunk_server = Admin-Machine-1

114. Scroll the cursor under the **Format Timeline** option you can see that the events are recorded in hourly basis, in real time the Administrator can just click on the time in which he wants to review the information.

EXERCISE 6: IMPLEMENT NETWORK- BASED IDS FUNCTIONALITY USING SURICATA IDS



Time	Event
08/17/2021 3:37:03.488 AM	08/17/2021-00:37:03.488827 [**] [1:0:0] ET SCAN Potential FTP Brute-Force attempt [**] [Classification: Unsuccessful User Privilege Gain] [Priority: 1] {TCP} 10.10.1.16:21 -> 10.10.1.50:38020 host = WebServer source = C:\Program Files\Suricata\log\fast.log sourcetype = fast-too_small splunk_server = Admin-Machine-1
08/17/2021 3:37:03.472 AM	08/17/2021-00:37:03.472776 [**] [1:0:0] ET SCAN Potential FTP Brute-Force attempt [**] [Classification: Unsuccessful User Privilege Gain] [Priority: 1] {TCP} 10.10.1.16:21 -> 10.10.1.50:38028 host = WebServer source = C:\Program Files\Suricata\log\fast.log sourcetype = fast-too_small splunk_server = Admin-Machine-1

115. Close the web browser in **Admin Machine-1** virtual machine.

116. Close all open windows in **Web Server** virtual machine.

117. Turn off the **Web Server** virtual machine.

EXERCISE 7: DETECT MALICIOUS NETWORK TRAFFIC USING HONEYBOT

Network traffic monitoring is the process of capturing network traffic and inspecting it closely to determine what is happening on the network.

LAB SCENARIO

A security professional must have the required knowledge to detect malicious traffic in the network. You should constantly strive to maintain smooth network operation. If a network goes down even for a small period, productivity within a company may decline. To be proactive rather than reactive, the traffic movement and performance must be monitored to ensure that no security breach occurs within the network.

LAB OBJECTIVE

This lab demonstrates how to detect malicious network traffic using HoneyBOT.

OVERVIEW OF NETWORK TRAFFIC MONITORING

The network monitoring process involves sniffing the traffic flowing through the network. For this purpose, network packets must be captured, and a signature analysis must be conducted to identify any malicious activity.

Networking monitoring assists security professionals in identifying possible issues before they affect business continuity. If an issue occurs in the network, the root cause can be determined easily with network monitoring, and with network automation tools, the problem can be fixed automatically. Networking monitoring not only prevents outages but also gives visibility to potential issues. Continuous network monitoring minimizes downtime and increases the performance of the network.

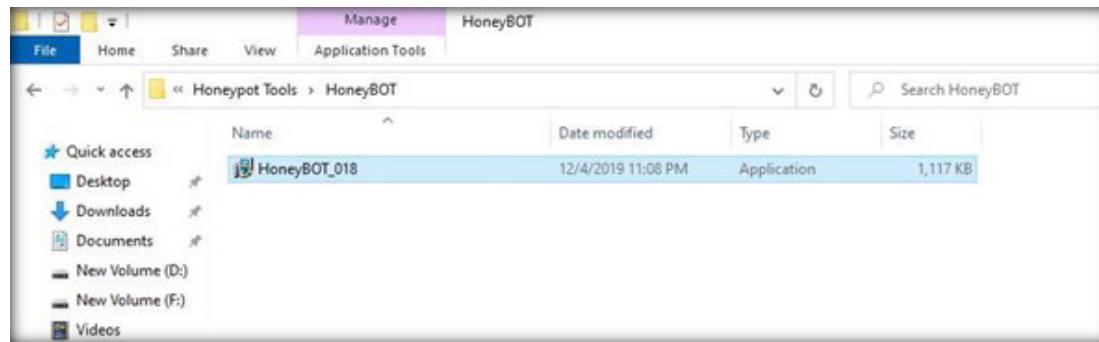
LAB TASKS

Note: Ensure that **Admin Machine-1**, **Attacker Machine-1** and **PfSense Firewall** are running.

1. Switch to the **Admin Machine-1** virtual machine.

2. Navigate to **Z:\CCT-Tools\CCT Module 07 Network Security Controls - Technical Controls\Honeypot Tools\HoneyBOT**. Double-click **HoneyBOT_018.exe** to launch the HoneyBOT installer. Follow the wizard-driven steps to install HoneyBOT.

Note: If the **User Account Control** window appears, click **Yes**.

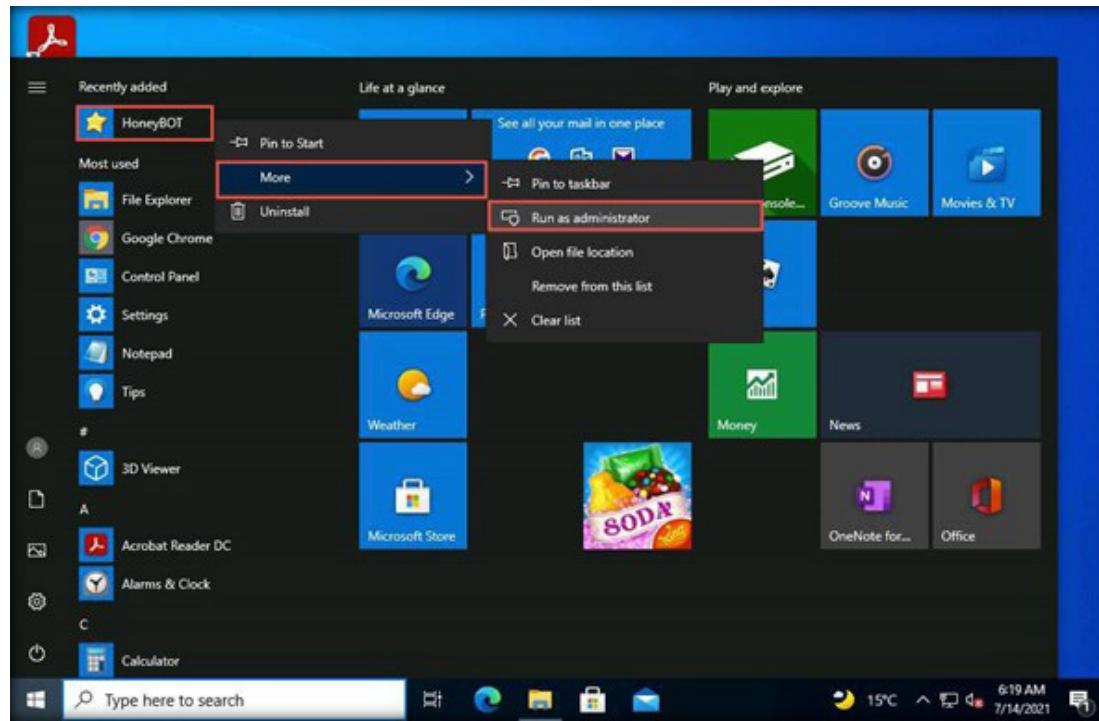


EXERCISE 7:
**DETECT MALICIOUS
NETWORK TRAFFIC USING
HONEYBOT**

3. Once the installation of HoneyBOT completes, in the **Completing the HoneyBot Setup Wizard** window, uncheck the **Launch HoneyBOT** option, click **Finish**.

4. Now, click the **Start** icon from the left-bottom of **Desktop**. Under **Recently added** applications, right-click **HoneyBOT > More > Run as administrator**, as shown in the screenshot.

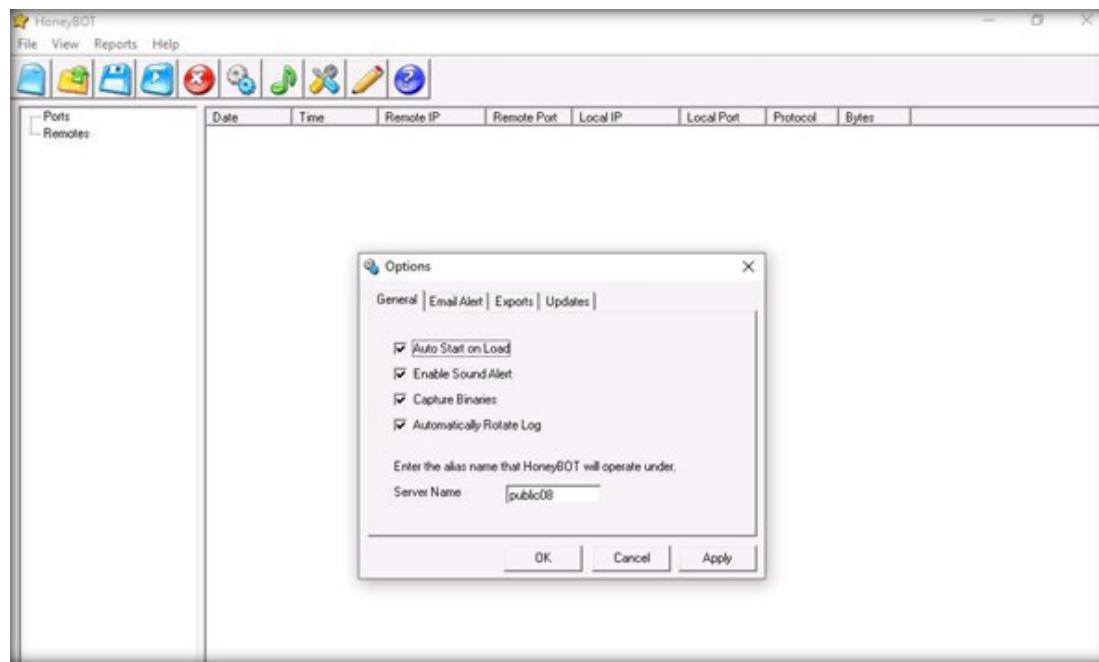
Note: If the **User Account Control** window appears, click **Yes**.



5. The **HoneyBOT** configuration pop-up appears; click **Yes** to configure HoneyBOT.

6. The HoneyBOT **Options** window appears with default options checked on the **General** settings tab. Leave the default settings or modify them accordingly.

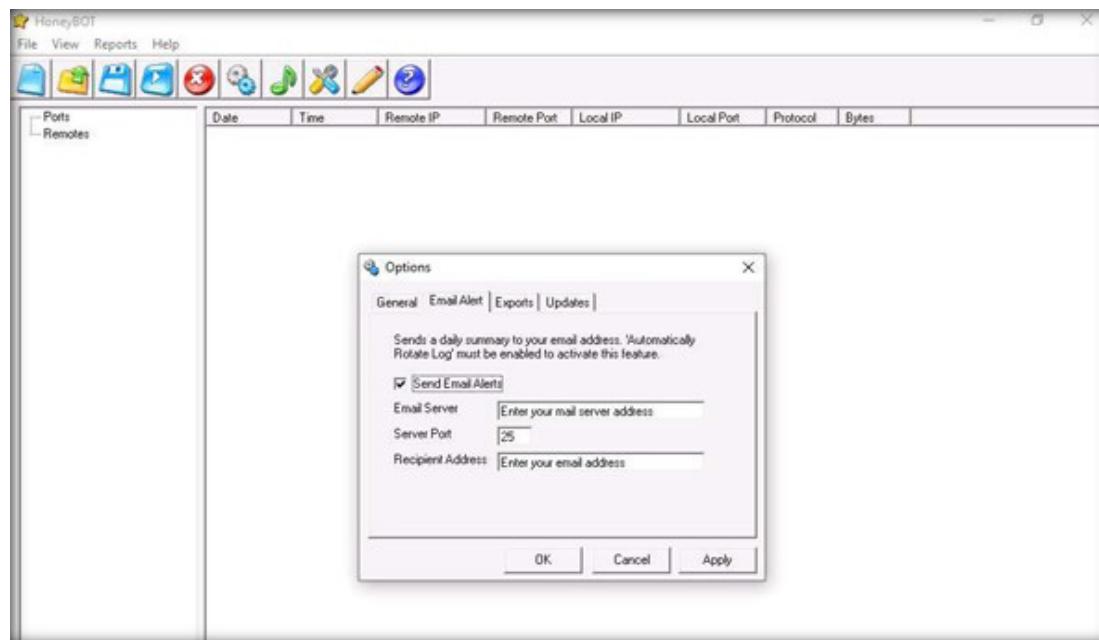
7. In this task, we are leaving the settings on default for the **General** tab in the **Options** window.



8. Click the **Email Alert** tab; if you want HoneyBOT to send you email alerts, check **Send Email Alerts**, and fill in the respective fields.

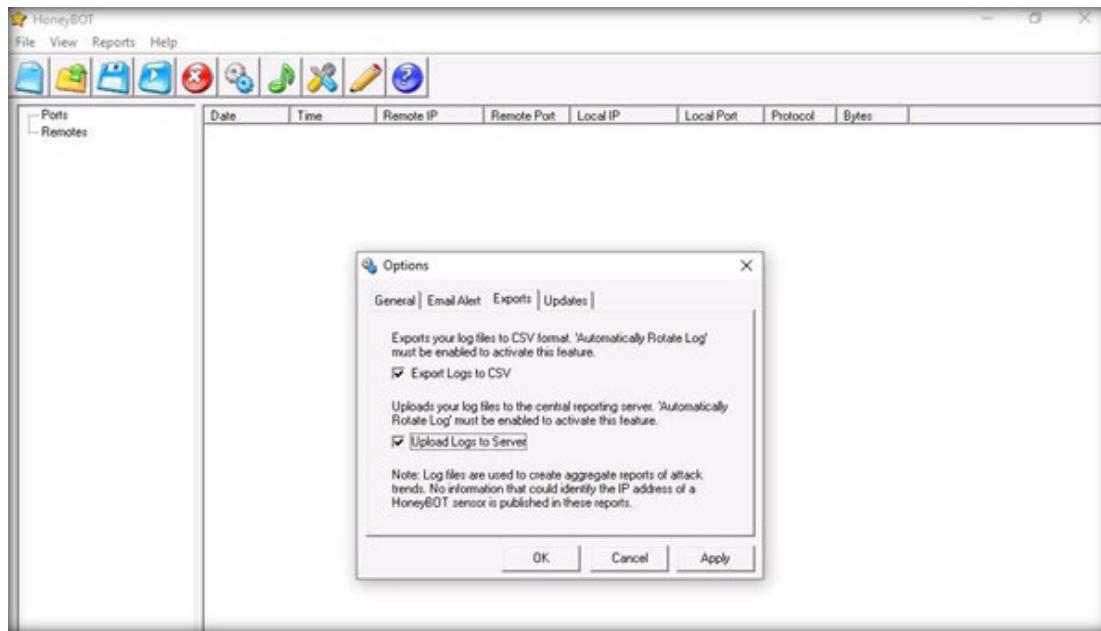
Note: In this task, we will not be providing any details for email alerts.

EXERCISE 7:
DETECT MALICIOUS
NETWORK TRAFFIC USING
HONEYBOT



9. On the **Exports** tab, in which you can export the logs recorded by HoneyBOT, choose the required option to view the reports, and then proceed to the next step. (Here, **Export Logs to CSV** and **Upload Logs to Server** checkbox are selected)

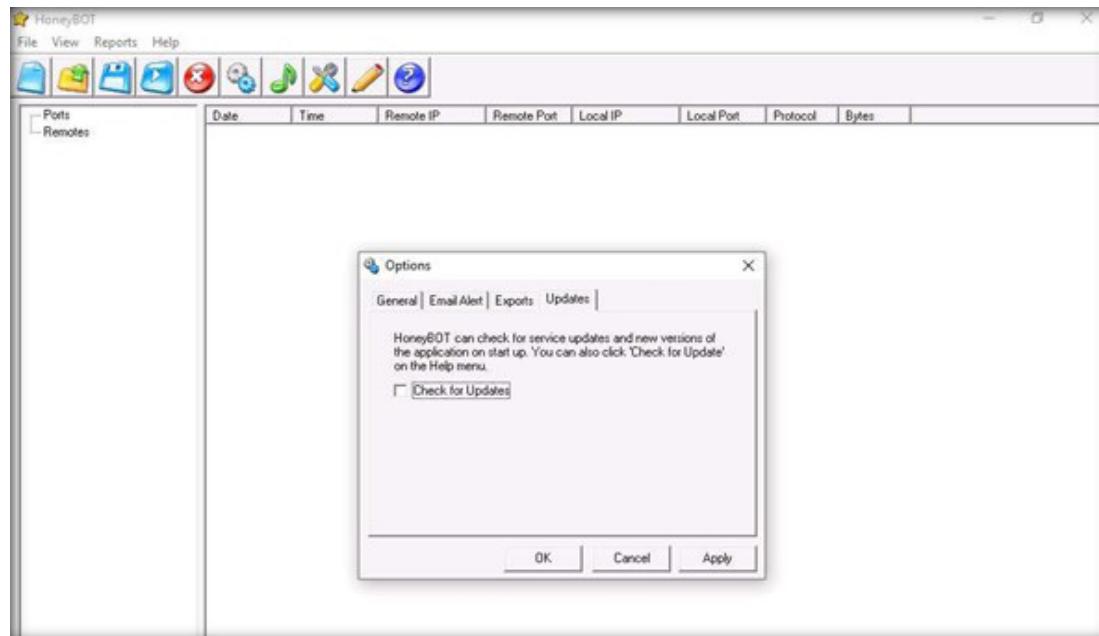
EXERCISE 7:
DETECT MALICIOUS
NETWORK TRAFFIC USING
HONEYBOT



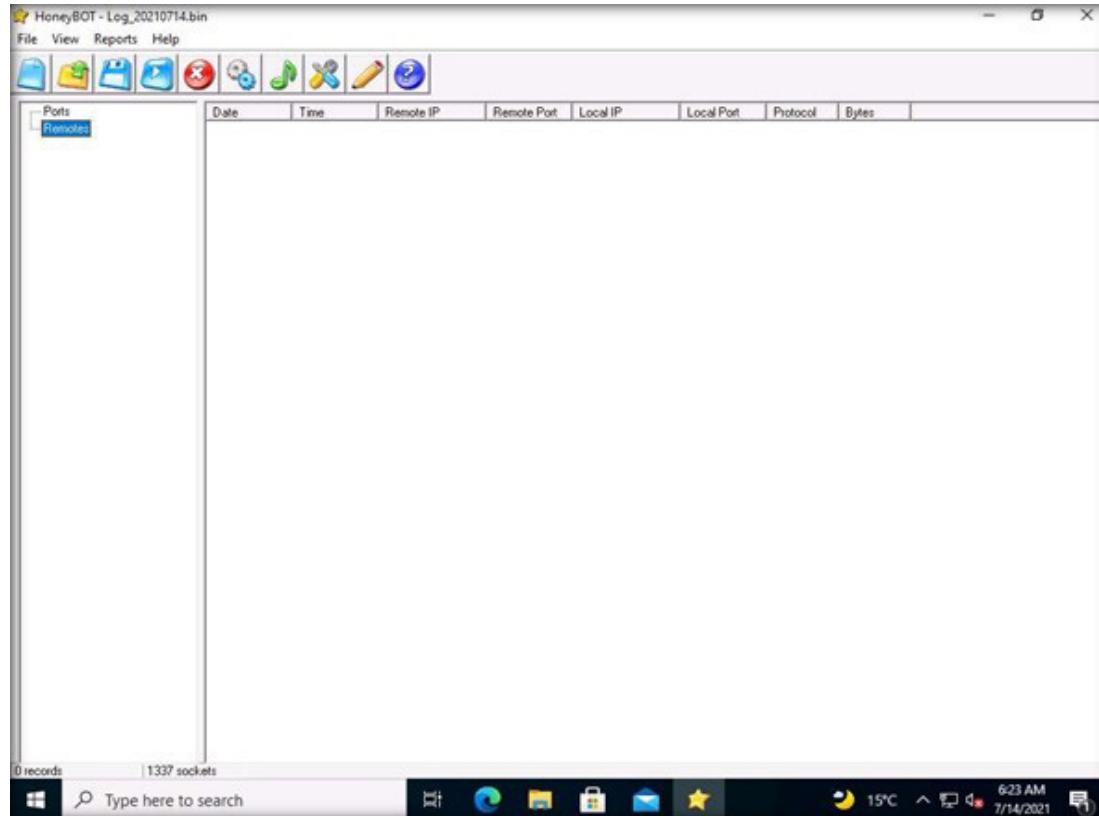
10. On the **Updates** tab, uncheck **Check for Updates**; click **Apply** and click **OK** to continue.

Note: If a **Bindings** pop-up appears, click **OK** to continue.

EXERCISE 7:
DETECT MALICIOUS
NETWORK TRAFFIC USING
HONEYBOT



11. The **HoneyBOT** main window appears, as shown in the screenshot.



EXERCISE 7:
**DETECT MALICIOUS
NETWORK TRAFFIC USING
HONEYBOT**

12. Now, leave the HoneyBOT window running on **Admin Machine-1** virtual machine.

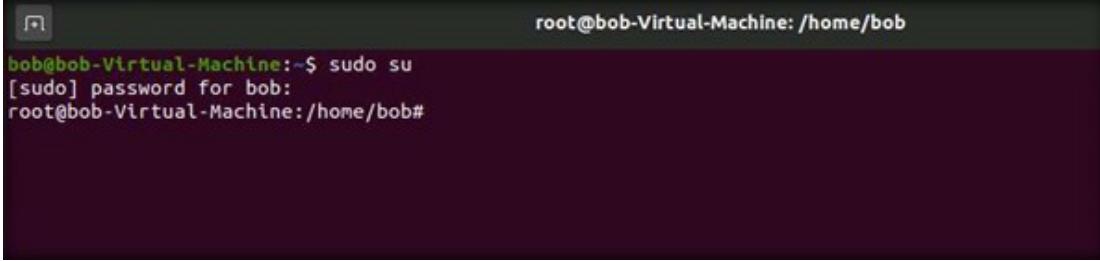
13. Switch to the **Attacker Machine-1** virtual machine.

14. Select User **Bob** and type password **user@123** press the **Enter** button.

15. Press **ALT + CTL + T** to open the terminal, type the **sudo su** command for the root user, and press **Enter**.

16. When prompted for the password, type the password for the root user (here the **root** user password is **user@123**), and press **Enter**.

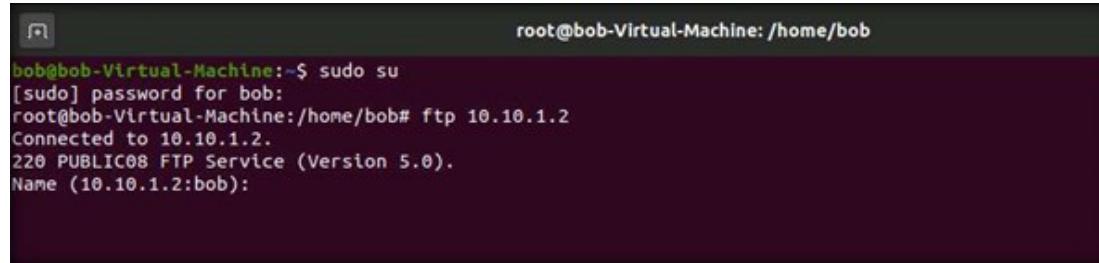
Note: The password that you type will not be visible.



The screenshot shows a terminal window with a dark background and light-colored text. At the top, it says "root@bob-Virtual-Machine: /home/bob". Below that, the command "bob@bob-Virtual-Machine:~\$ sudo su" is entered. A prompt "[sudo] password for bob:" appears, followed by the root password "root@bob-Virtual-Machine:/home/bob#".

EXERCISE 7.
DETECT MALICIOUS
NETWORK TRAFFIC
USING HONEYBOT

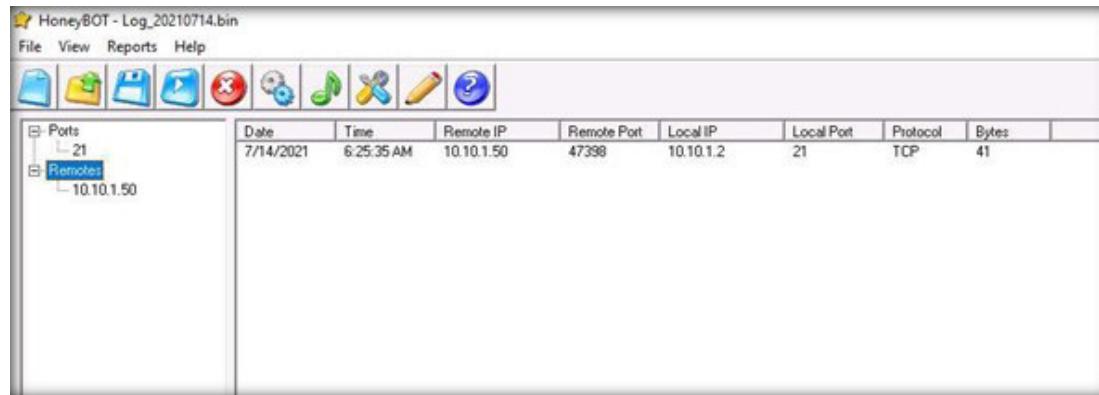
17. In the terminal window, type **ftp [IP Address of the Admin Machine-1]** and press **Enter**.
18. You will be prompted for the ftp credentials of the **Admin Machine-1** machine.
19. In this task, the IP address of **Admin Machine-1** is **10.10.1.2**; this may differ in your lab environment.



```
root@bob-Virtual-Machine: /home/bob
bob@bob-Virtual-Machine:~$ sudo su
[sudo] password for bob:
root@bob-Virtual-Machine:/home/bob# ftp 10.10.1.2
Connected to 10.10.1.2.
220 PUBLIC08 FTP Service (Version 5.0).
Name (10.10.1.2:bob):
```

EXERCISE 7:
DETECT MALICIOUS
NETWORK TRAFFIC USING
HONEYBOT

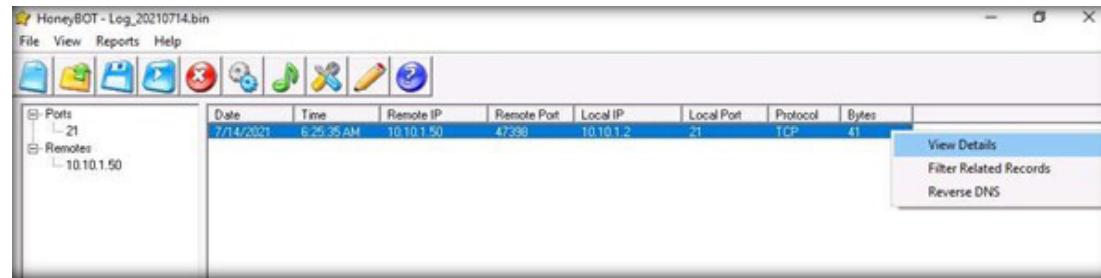
- EXERCISE 7: DETECT MALICIOUS NETWORK TRAFFIC USING HONEYBOT
20. Switch back to the **Admin Machine-1** virtual machine. In the **HoneyBOT** window, expand the **Ports** and **Remotes** node from the left-pane.
 21. Under **Ports**, you can see the port numbers from which **Admin Machine-1** received requests or attacks.
 22. Under **Remotes**, you can view the recorded IP addresses through which Admin Machine-1 received requests.



The screenshot shows the HoneyBOT application window. At the top, there's a menu bar with File, View, Reports, and Help. Below the menu is a toolbar with various icons. The main interface has two panes. The left pane shows a tree view with 'Ports' expanded, showing '21' and 'Remotes' expanded, showing '10.10.1.50'. The right pane is a table of network traffic logs:

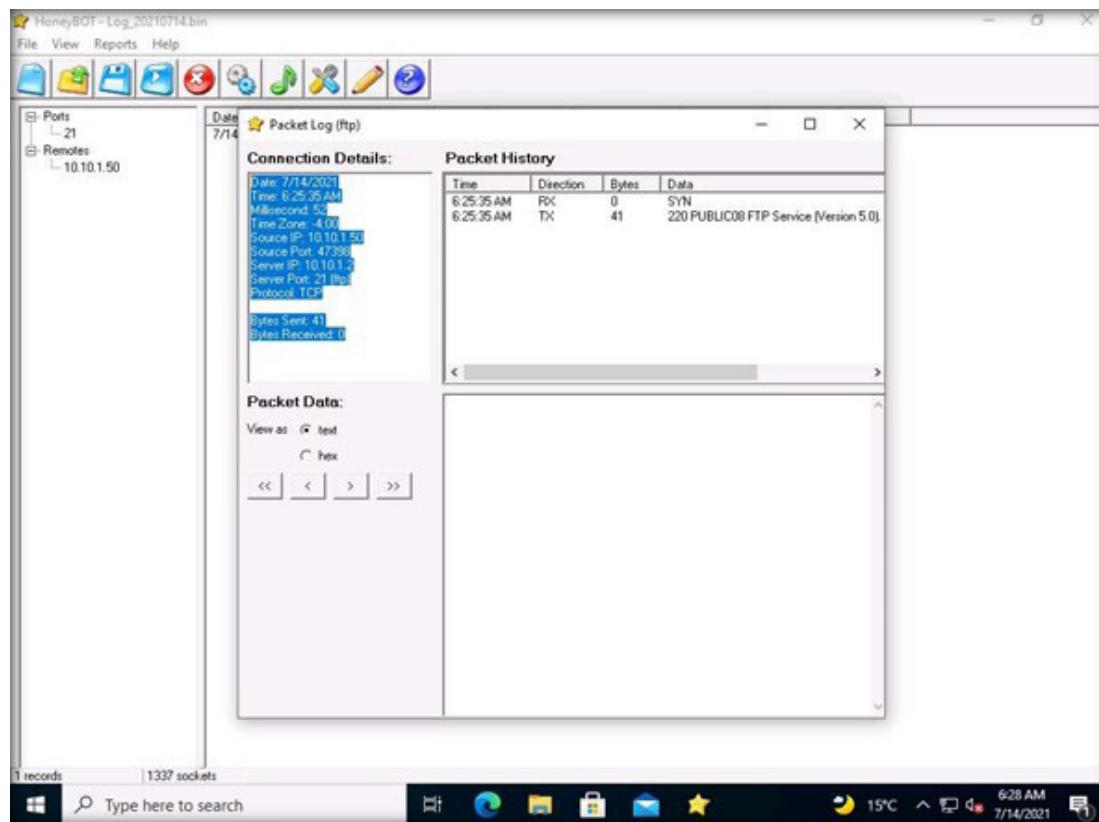
Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
7/14/2021	6:25:35 AM	10.10.1.50	47398	10.10.1.2	21	TCP	41

23. Now, right-click any IP address or Port on the left, and click **View Details**, as shown in the screenshot, to view the complete details of the request or attack recorded by HoneyBOT.



EXERCISE 7:
DETECT MALICIOUS
NETWORK TRAFFIC USING
HONEYBOT

24. The **Packet Log** window appears, as shown in the screenshot. This displays the complete log details of the request captured by HoneyBOT.
25. In the screenshot, under **Connection Details**, you can view the **Date** and **Time** of the connection established as well as the protocol used.
26. **Connection Details** also shows the **Source IP**, **Port**, and **Server Port**, as shown below.



EXERCISE 7:
**DETECT MALICIOUS
NETWORK TRAFFIC USING
HONEYBOT**

27. Similarly, you can run the telnet command on the **Attacker Machine-1** virtual machine and observe the log recorded by **HoneyBOT** on **Admin Machine-1**.
28. After the completion of this task, open **Control Panel** in the **Admin Machine-1** and uninstall **HoneyBOT**.
29. Turn off the **Attacker Machine-1** virtual machine.

EXERCISE 8: ESTABLISH VIRTUAL PRIVATE NETWORK CONNECTION USING SOFTETHER VPN

Virtual private network is a private network that uses a public network to connect users/sites remotely.

LAB SCENARIO

Most of the organization has its offices located at different locations around the world. There is a need for establishing a remote connection between these offices as a result. Previously, remote access was established through leased lines with the help of dial-up telephone links such as ISDN, DSL, cable modem, satellite, and mobile broadband. However, establishing remote connections with these leased lines is quite expensive and the costs rise when the distance between the offices increases.

A security professional must have the required knowledge to establish a VPN connection to provide a secure remote access to organization's employees and distant offices.

LAB OBJECTIVE

This lab will demonstrate how to establish a Virtual Private Network (VPN) connection using SoftEther VPN.

OVERVIEW OF VIRTUAL PRIVATE NETWORK

A virtual private network (VPN) offers an attractive solution for security professionals to connect their organization's network securely over the Internet. VPN is used to connect distant offices or individual users to their organization's network over a secure channel. VPN uses a tunneling process to transport encrypted data over the internet.

IPsec is the common protocol used in VPN at the IP level. VPN ensures the data integrity check by using a message digest and ensures data transmission is not tampered with. VPN guarantees the quality of service (QoS) through service level agreements (SLA's) with the service provider.

LAB TASKS

Note: Before starting this lab exercise, make a note of your public IP. To know your public IP, open up any web browser and browse for google.com. In the Google search, type **what is my IP** and click **search**. Your public IP will be displayed.

Note: Ensure that **Admin Machine-1** and **PfSense Firewall** virtual machines are running.

1. Turn on the **AD Domain Controller** virtual machine.
2. Log in with the credentials **CCT\Administrator** and **admin@123**.

Note: If the network screen appears, click **Yes**.

3. To install **SoftEther VPN Server**, navigate to **Z:\CCT Module 07 Network Security Controls - Technical Controls\SoftEther VPN\SoftEther VPN Server**. Double click **softether-vpnserver_vpnbridge-v4.30-9696-beta-2019.07.08-windows-x86_x64-intel**.

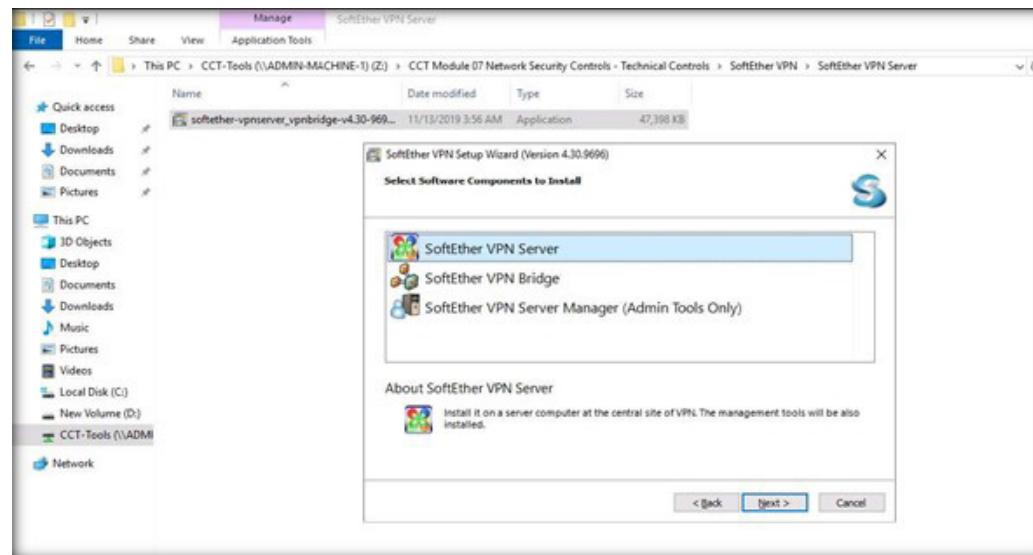
Note: If the **Open File – Security Warning** window appears, click **Run**.

Note: You can download the latest version of **SoftEther VPN Server** from <https://www.softether-download.com>. If you use the downloaded file, the screenshots in the lab may vary.

4. The **SoftEther VPN Setup Wizard** appears. Click **Next**.

5. In the **Select Software Components to Install** wizard, **SoftEther VPN Server** is selected by default. Retain the default selection and click **Next**.

EXERCISE 8:
ESTABLISH VIRTUAL PRIVATE NETWORK CONNECTION USING SOFTETHER VPN

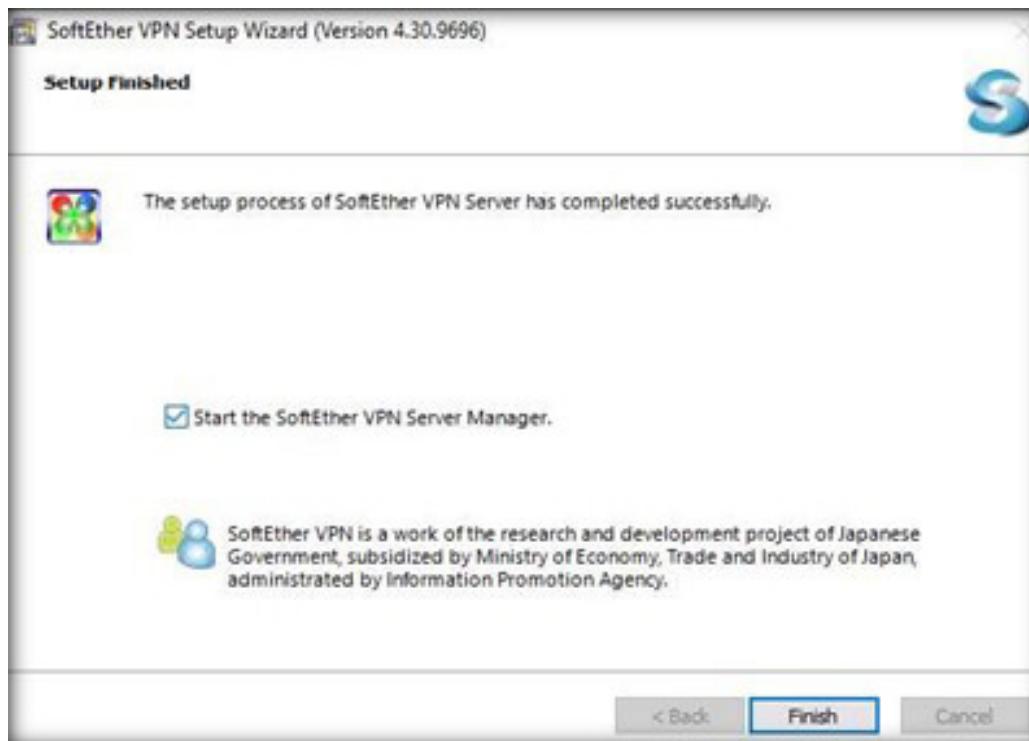


6. The **End User License Agreement** wizard appears. Check **I agree to the End User License Agreement**. Click **Next**. Follow the wizard-driven installation steps to install **SoftEther VPN Server Manager**.

7. The **Important Notice** window appears. Click **Next**.

8. Continue the installation until you see the **Setup Finished** wizard appears. Ensure that the **Start the SoftEther VPN Server Manager** option is checked to launch it automatically. Click **Finish**.

Note: Alternatively, you can also launch the application by double-clicking the shortcut icon on the Desktop.



EXERCISE 8: ESTABLISH VIRTUAL PRIVATE NETWORK CONNECTION USING SOFTETHER VPN

9. The **SoftEther VPN Server Manager** window appears. Click the **Connect** button to configure the VPN Server.

Note: If an **Update Available** pop-up appears, click on **Do Not Show this Message Again**.

EXERCISE 8:
**ESTABLISH VIRTUAL
PRIVATE NETWORK
CONNECTION USING
SOFTETHER VPN**



10. When you connect for the first time, you will be prompted to set the Administrator password for the Server Manager. Type in the password in the **New Password** field and retype the same password in the **Confirm Password** field (in this lab, the password was set to **user@123**). Click **OK**.



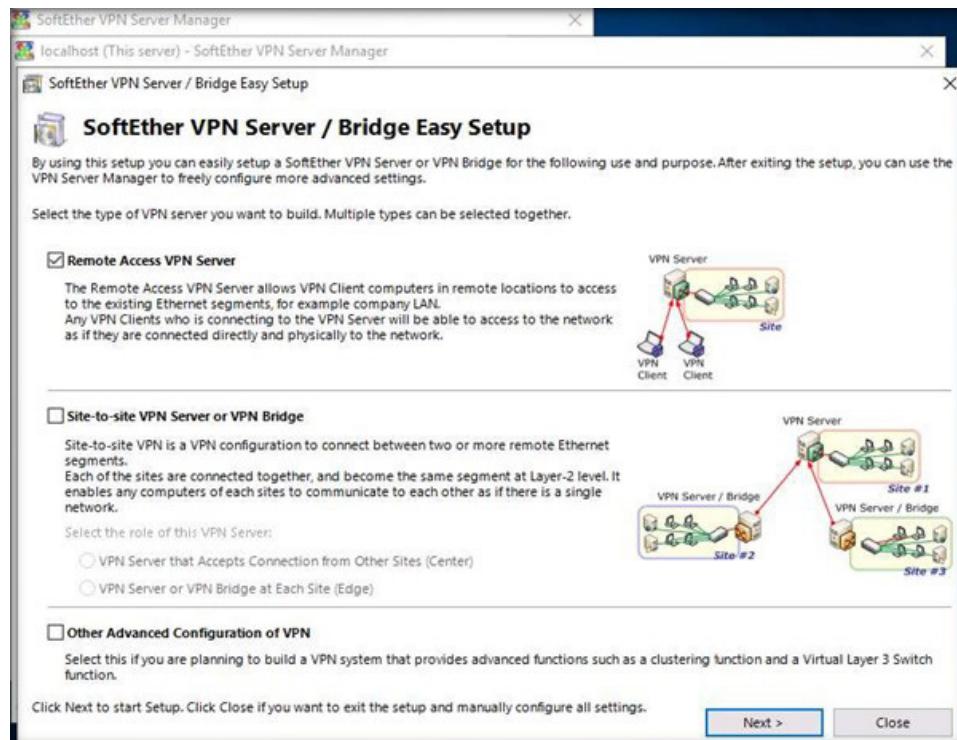
EXERCISE 8:
ESTABLISH VIRTUAL
PRIVATE NETWORK
CONNECTION USING
SOFTETHER VPN

11. After this, the password will be changed. A confirmation pop-up appears. Click **OK**.

12. The **SoftEther VPN Server / Bridge Easy Setup** wizard appears. Check **Remote Access VPN Server**. Click **Next**.

Note: If an **Update Available** pop-up appears, click on **Do Not Show this Message Again**.

EXERCISE 8 ESTABLISH VIRTUAL PRIVATE NETWORK CONNECTION USING SOFTETHER VPN



13. The **SoftEther VPN Server Manager** pop-up appears. Click **Yes**.

14. The **Easy Setup - Decide the Virtual Hub Name** pop-up appears. Specify the **Virtual Hub Name** in the field (in this exercise, the name is set as **CCT-VPN**) and click **OK**.

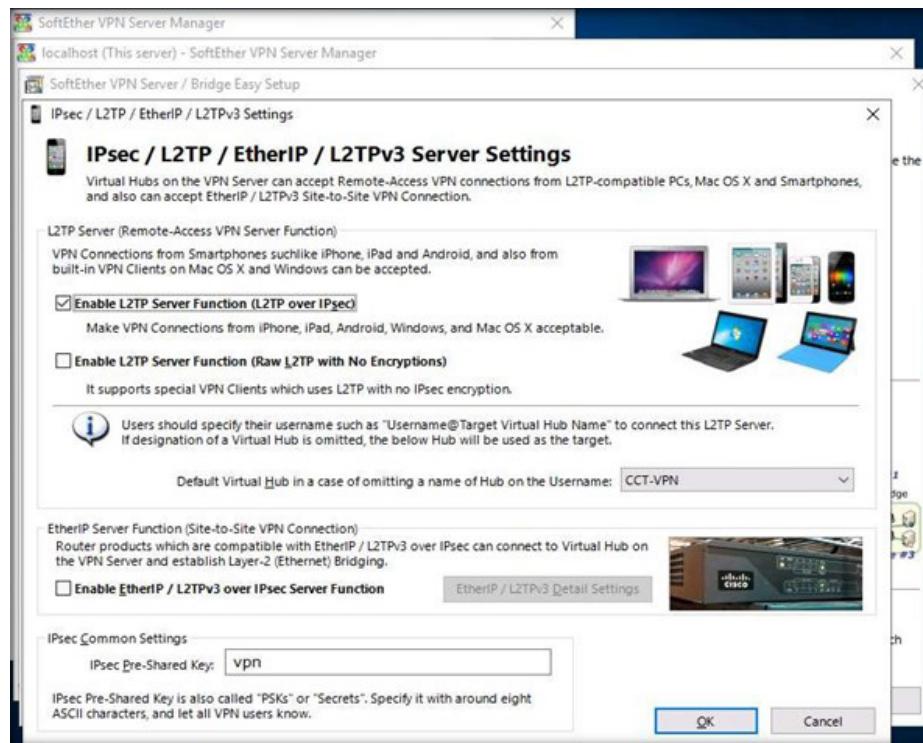


EXERCISE 8:
**ESTABLISH VIRTUAL
PRIVATE NETWORK
CONNECTION USING
SOFTETHER VPN**

15. The **Dynamic DNS Function** window appears. Click **Exit** to continue.

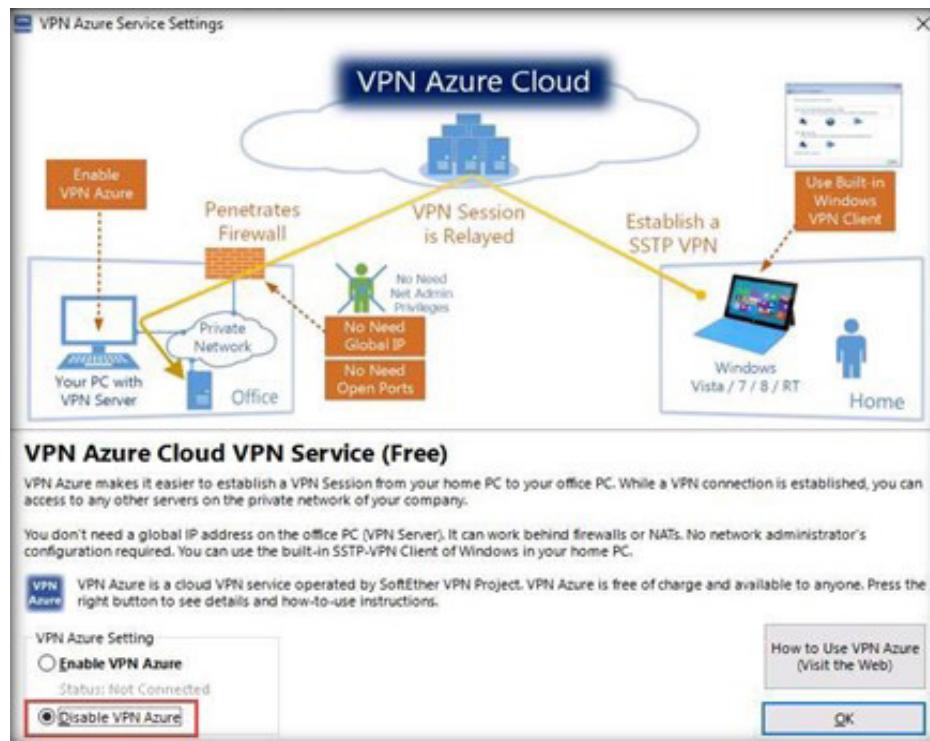
16. The **IPsec / L2TP / EtherIP / L2TPv3 Server Settings** window appears. Check **Enable L2TP Server Function (L2TP over IPsec)**. Retain the other settings as default and click **OK**.

EXERCISE 8: ESTABLISH VIRTUAL PRIVATE NETWORK CONNECTION USING SOFTETHER VPN



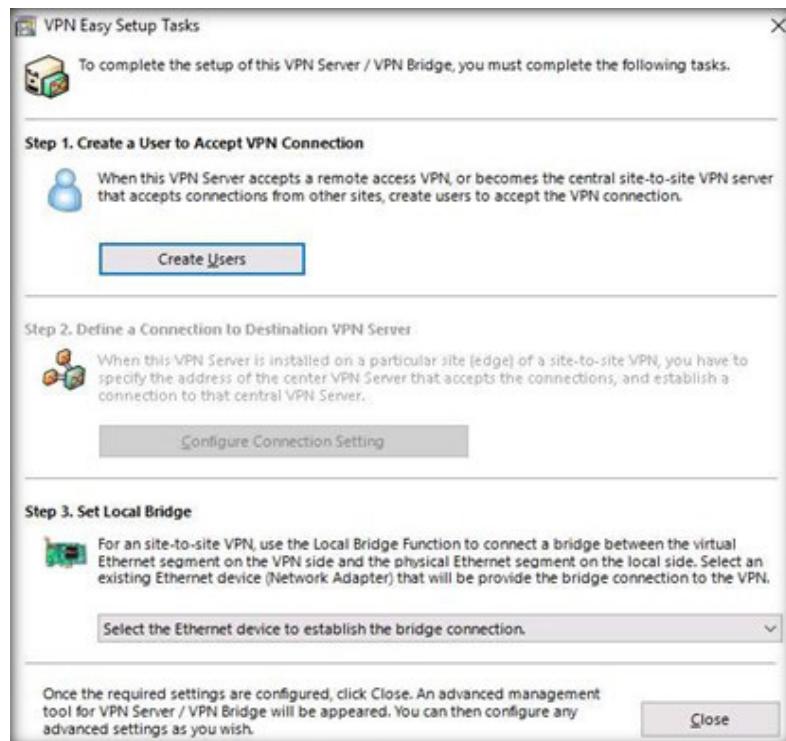
EXERCISE 8: ESTABLISH VIRTUAL PRIVATE NETWORK CONNECTION USING SOFTETHER VPN

17. The **VPN Azure Service Settings** wizard appears. You can choose any option according to your organization network policy. In this exercise, we select the **Disable VPN Azure** radio button. Click **OK**.

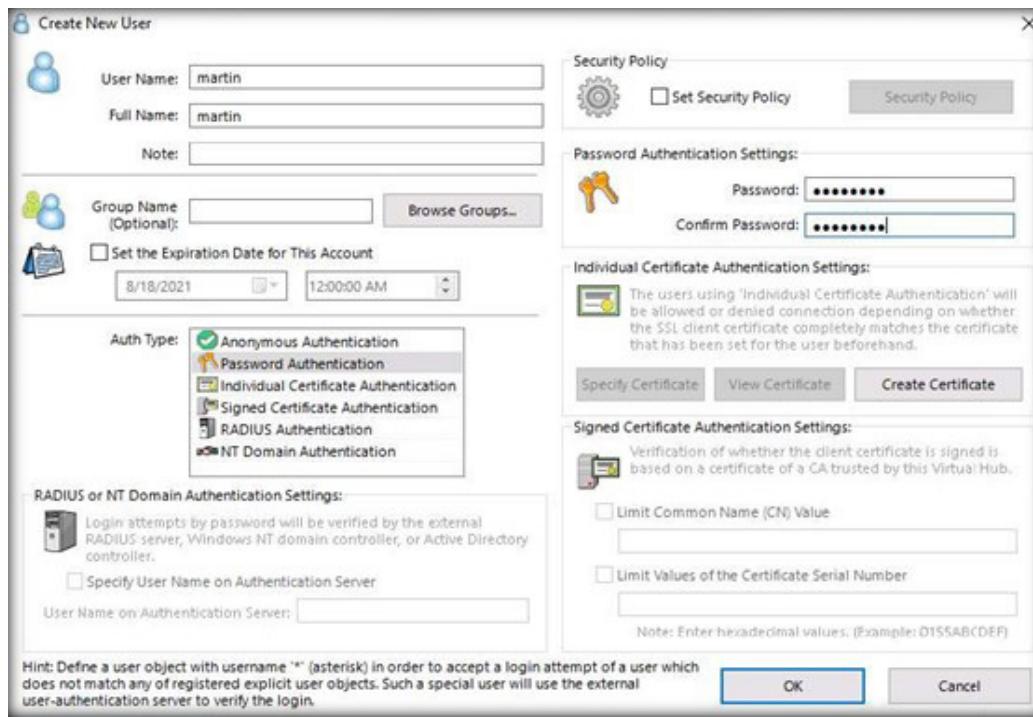


18. The **VPN Easy Setup Tasks** wizard appears; in this wizard, we create users who can access the organization network using VPN. To create new users, click **Create Users**.

EXERCISE 8
ESTABLISH VIRTUAL PRIVATE NETWORK CONNECTION USING SOFTWARE VPN



19. The **Create New User** wizard appears. Fill in the required details. As can be seen, we have created a new username **martin** and password **user@123**. Click **OK**.

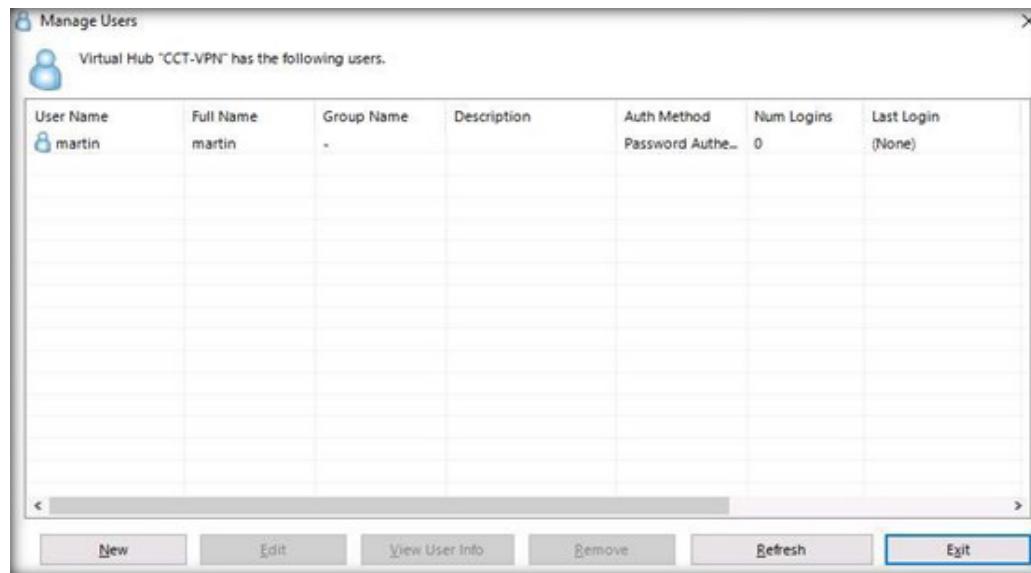


EXERCISE 8: ESTABLISH VIRTUAL PRIVATE NETWORK CONNECTION USING SOFTETHER VPN

20. A pop-up notifying that the user has been created appears. Click **OK**.

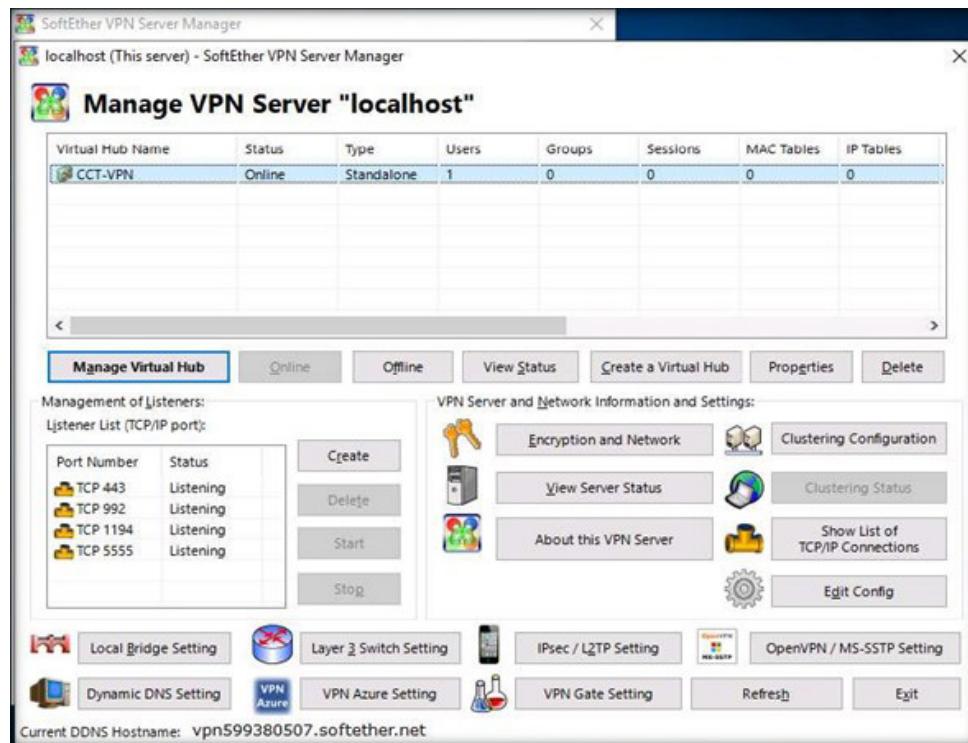
21. The **Manage Users** window appears. Here, you can create new users, edit created users, view user information, and remove users. Click the **Exit** button.

EXERCISE 8:
**ESTABLISH VIRTUAL
PRIVATE NETWORK
CONNECTION USING
SOFTETHER VPN**



22. The **VPN Easy Setup Tasks** wizard appears. Click **Close**.

23. The **Manage VPN Server** “localhost” dashboard appears. Here, you can see the connected users through the VPN network. You can also manage the VPN settings using different options on this dashboard.



EXERCISE 8

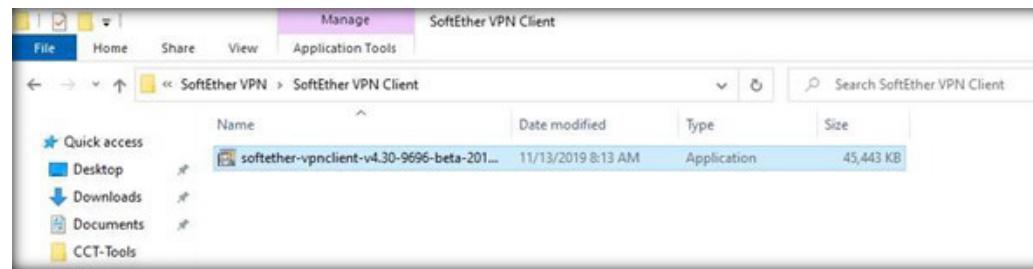
ESTABLISH VIRTUAL PRIVATE NETWORK CONNECTION USING SOFTETHER VPN

24. Switch to the **Admin Machine-1** virtual machine.

Note: If you are not logged into the machine, then login with the credentials **Admin** and **admin@123**.

25. To install the **SoftEther VPN client**, navigate to **Z:\CCT-Tools\CCT Module 07 Network Security Controls - Technical Controls\SoftEther VPN\SoftEther VPN Client**.

26. Double-click **softether-vpnclient-v4.30-9696-beta-2019.07.08-windows-x86_x64-intel.exe**.



EXERCISE 8
ESTABLISH VIRTUAL
PRIVATE NETWORK
CONNECTION USING
SOFTETHER VPN

EXERCISE 8:
ESTABLISH VIRTUAL
PRIVATE NETWORK
CONNECTION USING
SOFTETHER VPN

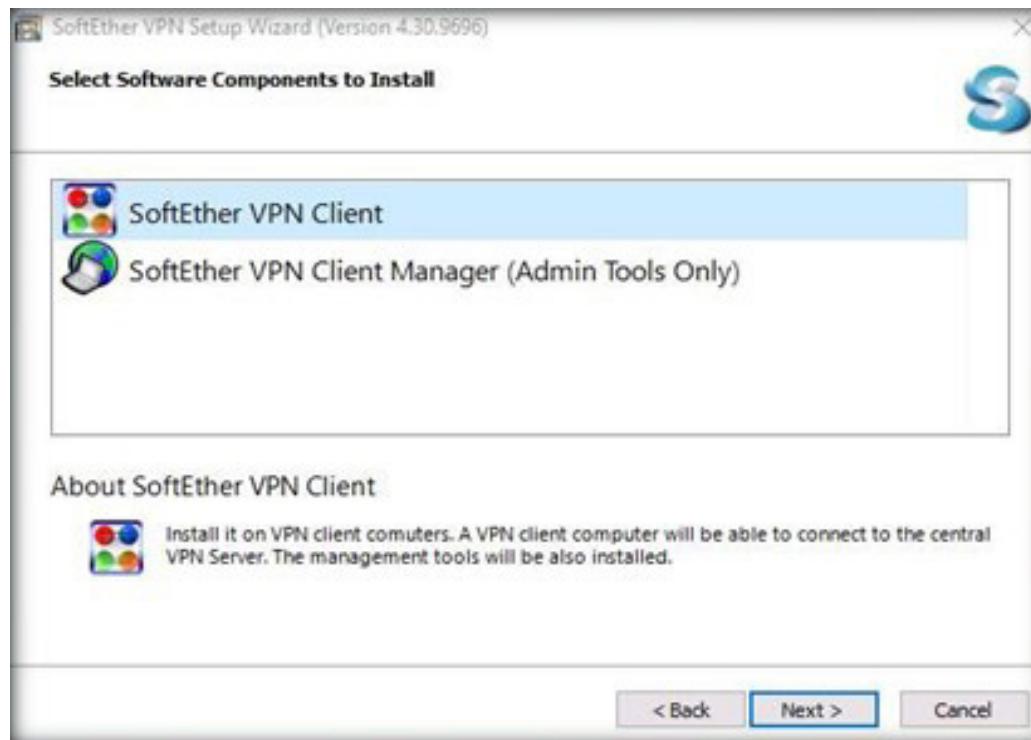
Note: You can download the latest version of SoftEther VPN Client from <https://www.softether-download.com>. If you use the downloaded file, then the screenshots may not exactly match the version you will use.

Note: If an **Open File - Security Warning** window appears, click **Run**.

27. The **SoftEther VPN Setup Wizard** appears. Click **Next**.

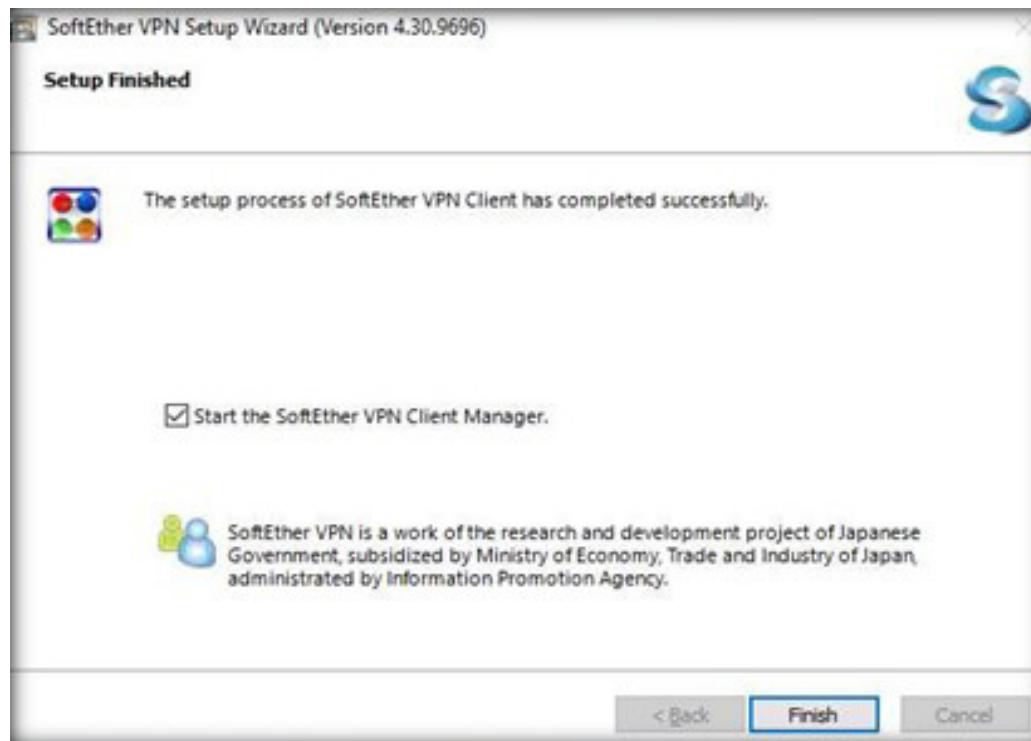
Note: If **User Account Control** window appears, click **Yes**.

28. The **Select Software Components to Install** wizard appears. Choose the **SoftEther VPN Client**. Click **Next**.



29. Follow the wizard-driven installation steps to complete the installation process. When the **Setup Finished** wizard appears, ensure that **Start the SoftEther VPN Client Manager** is checked to launch the application automatically. Click **Finish**.

EXERCISE 8:
**ESTABLISH VIRTUAL
PRIVATE NETWORK
CONNECTION USING
SOFTETHER VPN**

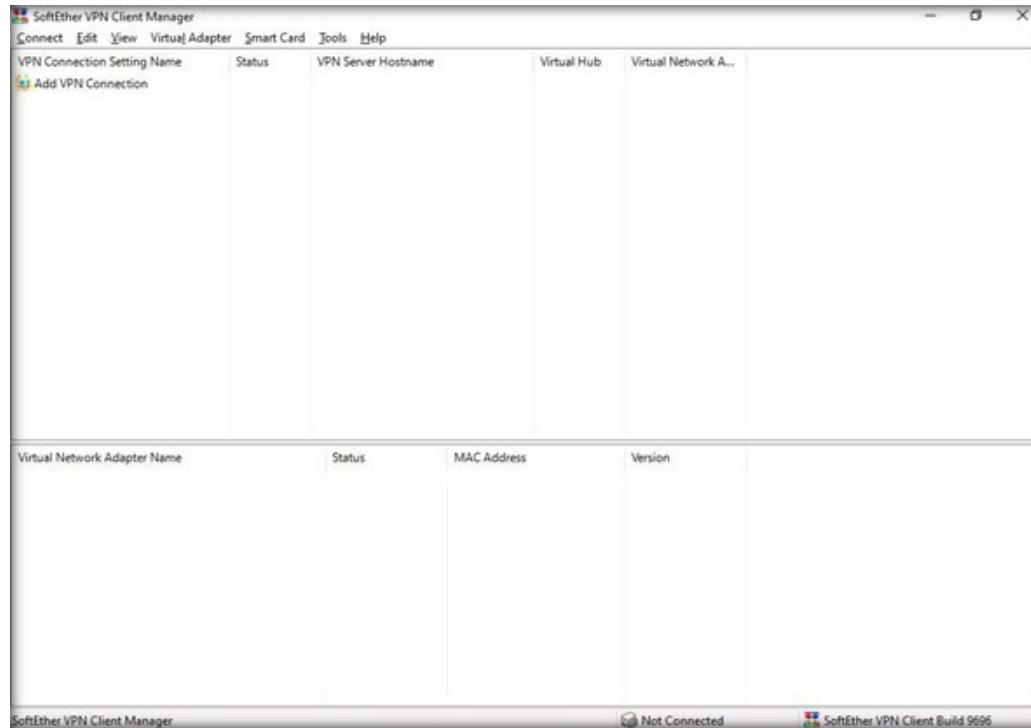


Note: Alternatively, you can also launch the application by double-clicking the shortcut icon on the desktop or from the Start menu installed apps.

30. The **SoftEther VPN Client Manager** window appears.

Note: If an **Update Available** pop-up appears, click on **Do Not Show this Message Again**.

EXERCISE 8:
ESTABLISH VIRTUAL PRIVATE NETWORK CONNECTION USING SOFTETHER VPN



31. Double-click **Add VPN Connection** to add a system to the VPN network.

32. Before creating a VPN Connection Setting, we need to create a Virtual Network Adapter. When the **SoftEther VPN Client Manager** prompts to create a Virtual Network Adapter, click **Yes**.



EXERCISE 8: ESTABLISH VIRTUAL PRIVATE NETWORK CONNECTION USING SOFTETHER VPN

33. The **Create New Virtual Network Adapter** pop-up appears. Type the name in the **Virtual Network Adapter Name** field. Click **OK**. Retain the default settings.

Note: The Virtual Network Adapter Name should be VPN or should range from VPN2 to VPN127 as shown in the pop-up (you can create a maximum of 127 Virtual Network Adapters).

EXERCISE 8:
ESTABLISH VIRTUAL
PRIVATE NETWORK
CONNECTION USING
SOFTETHER VPN

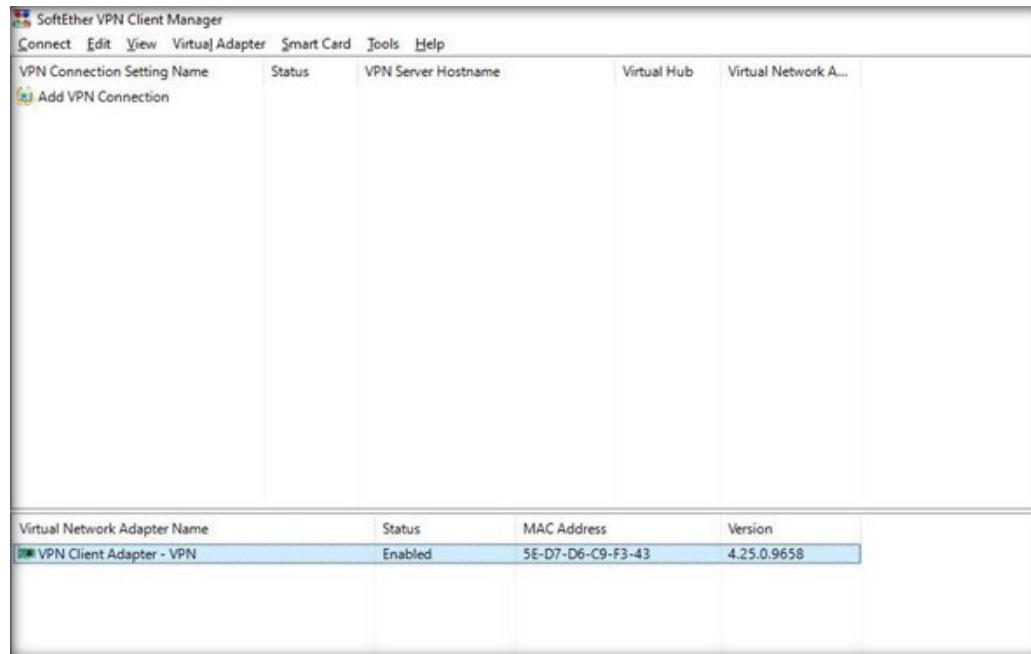


34. The SoftEther VPN client will create a new **Virtual Network Adapter**. Wait until the process is completed.

35. The newly created **Virtual Network Adapter** can be seen in the lower pane of the **SoftEther VPN Client Manager** window with the assigned **Status, MAC Address, and Version**. In this exercise, the newly created Virtual Network Adapter is **VPN Client Adapter - VPN**.

Note: The MAC Address might differ in your lab environment.

EXERCISE 8:
ESTABLISH VIRTUAL
PRIVATE NETWORK
CONNECTION USING
SOFTETHER VPN

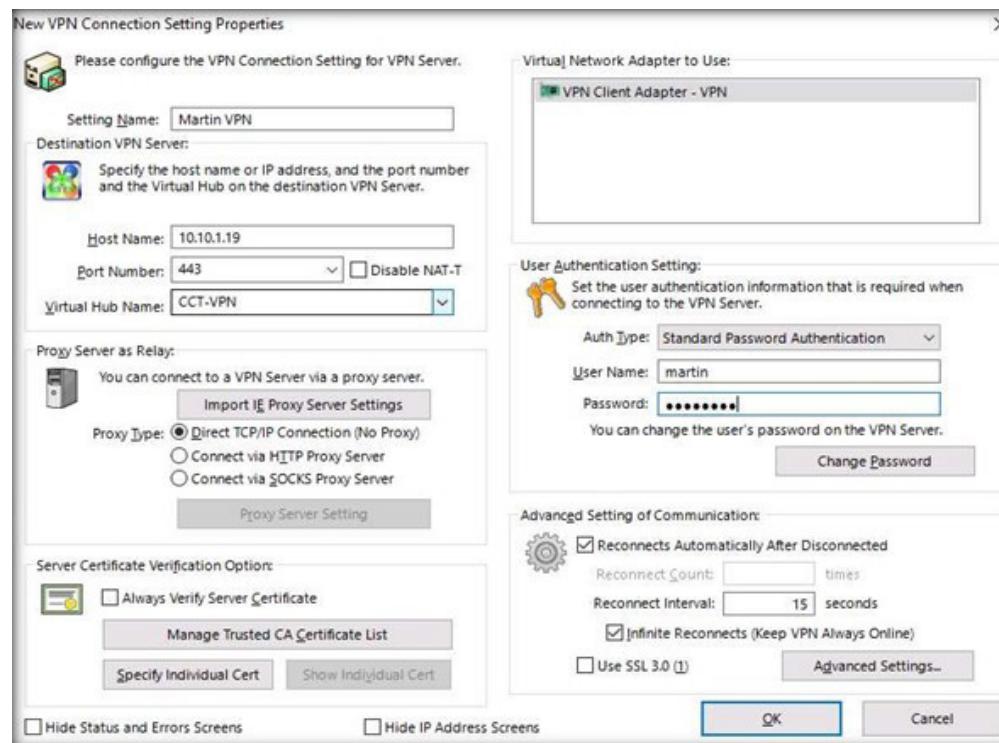


36. Next, we need to configure the adapter. Double-click on the newly created **Virtual Network Adapter**.

37. The **New VPN Connection Setting Properties** wizard appears.

38. In the **Setting Name** field, provide a name for the VPN Connection [**Martin VPN**]. Under the **Destination VPN Server** section, type your public IP in the **Host Name** field [**10.10.1.19**]. You can choose any port from the **Port Number** dropdown [**443**]. In the **Virtual Hub Name** field, choose the appropriate name. In this exercise, we have created a virtual hub name **CCT-VPN** in **Step 14**. If you have created multiple virtual hubs, choose the appropriate one. Retain the other default settings.

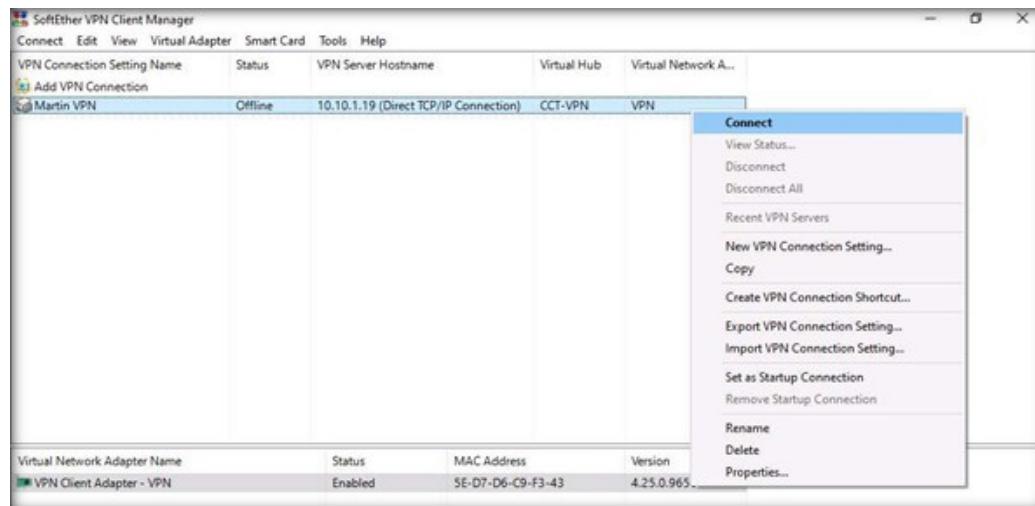
39. On the right side in the **User Authentication Setting**: type the username and password of the user that you have created in **Step 19**. In this exercise, the username is **martin** and the password is **user@123**. Click **OK** and retain the other default settings.



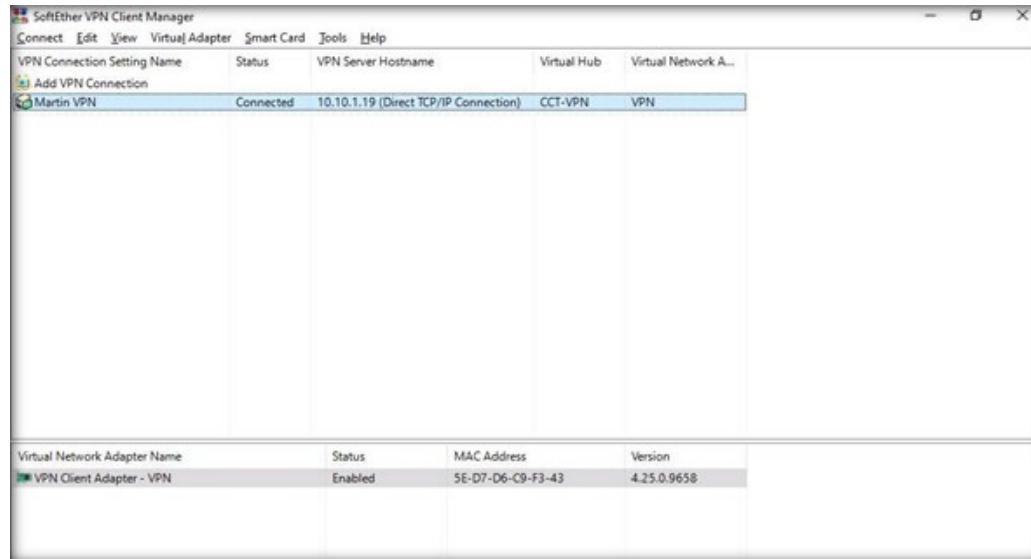
40. A newly created VPN connection appears in the **SoftEther VPN Client Manager** window with the status showing as **Offline**.

41. Right-click **Martin VPN** and select **Connect** from the context menu to connect the organization network through the VPN.

EXERCISE 8:
ESTABLISH VIRTUAL PRIVATE NETWORK CONNECTION USING SOFTEther VPN

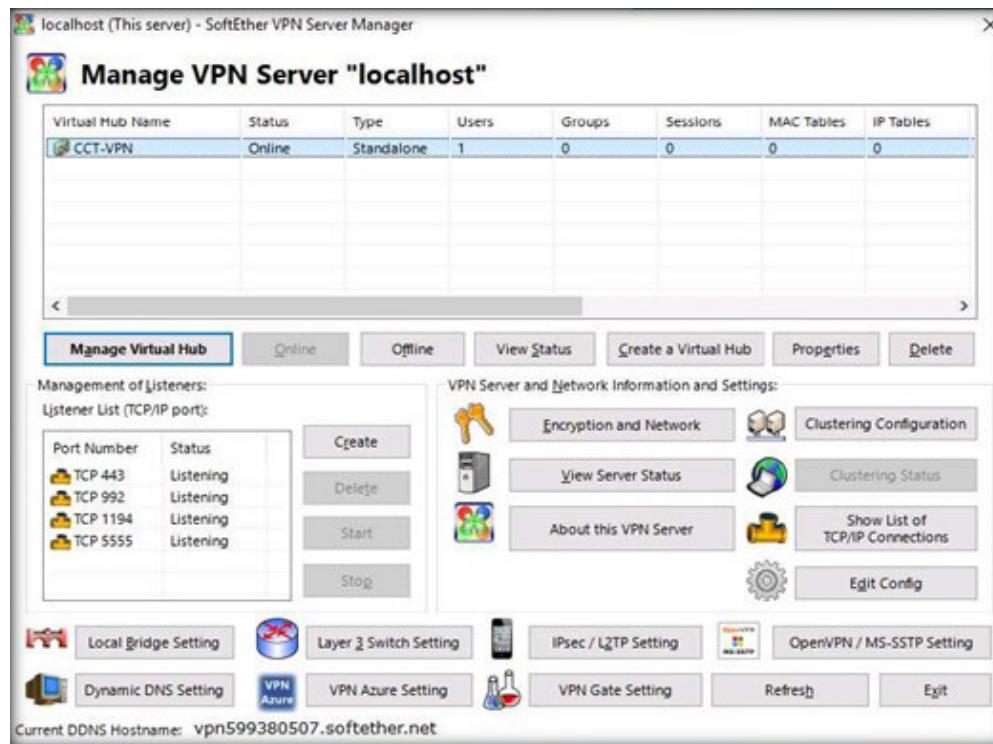


EXERCISE 8:
ESTABLISH VIRTUAL
PRIVATE NETWORK
CONNECTION USING
SOFTETHER VPN



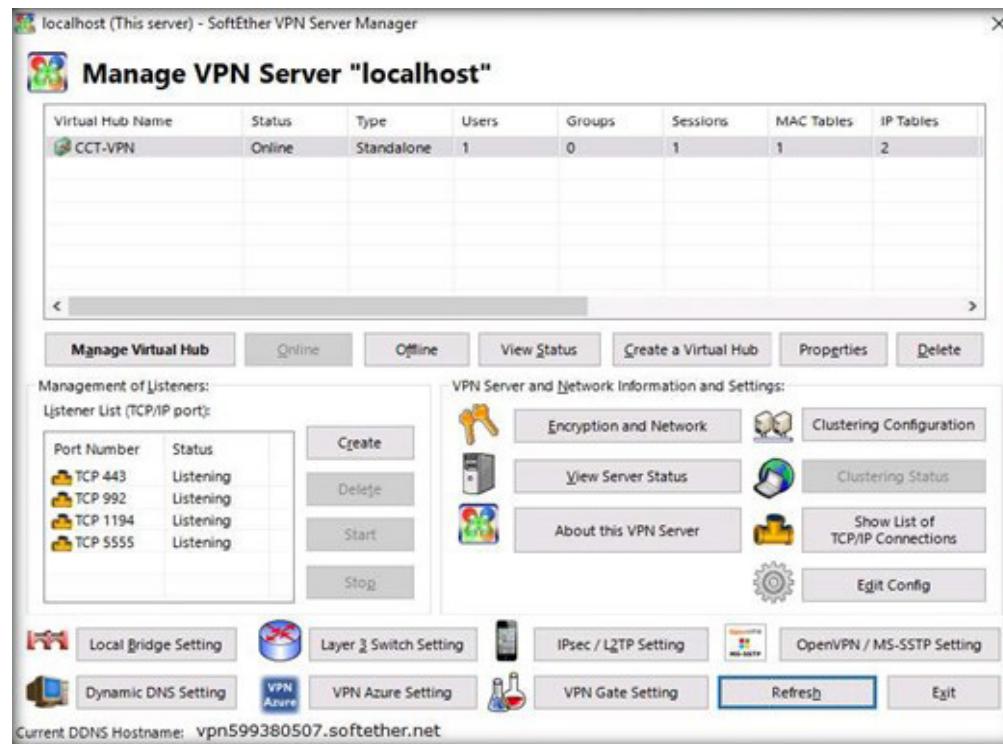
44. Switch back to the **AD Domain Controller** virtual machine, where the **SoftEther VPN Server** is installed. See the active sessions using the VPN. You can see **0 Sessions**.

EXERCISE 8: ESTABLISH VIRTUAL PRIVATE NETWORK CONNECTION USING SOFTETHER VPN



45. Click the **Refresh** button. You can see the active sessions that are accessed by the users.

EXERCISE 8: ESTABLISH VIRTUAL PRIVATE NETWORK CONNECTION USING SOFTETHER VPN

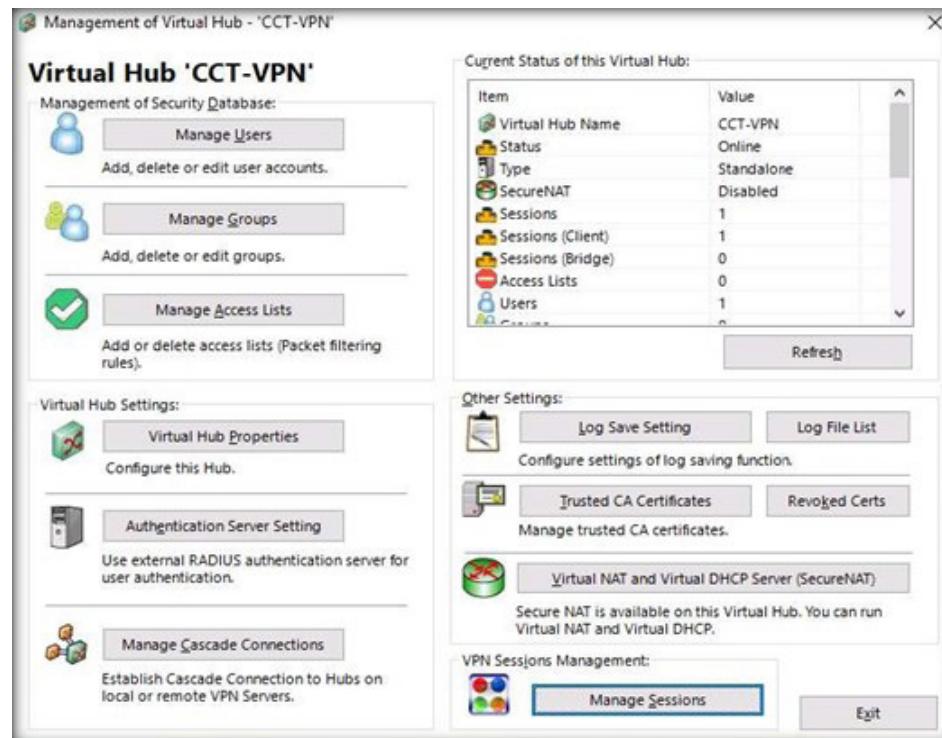


46. To view and manage the sessions; click **Manage Virtual Hub** button or double-click the available VPN Hub in the dashboard. The **Management of Virtual Hub - (Virtual Hub Name)** window appears.

47. Traverse through all the required options available in the wizard. You can manage the sessions and settings of the VPN Network.

48. For instance, to access the **Manage Sessions** option, click the **Manage Sessions** button.

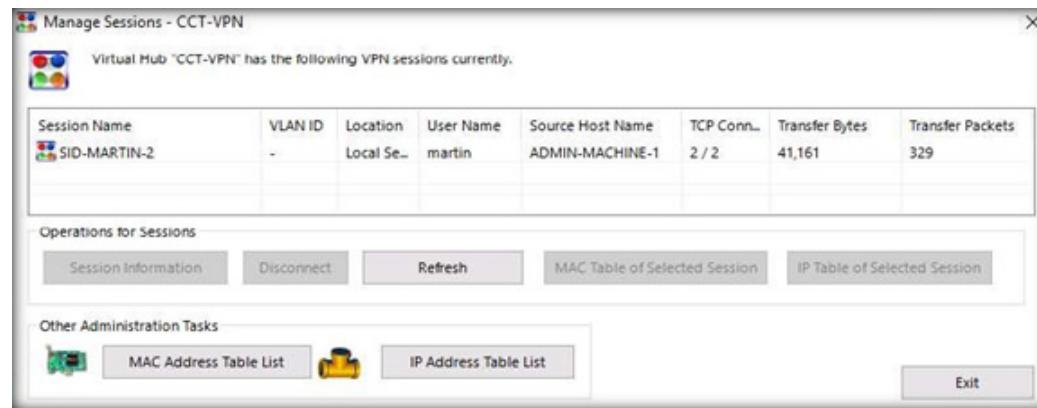
EXERCISE 8 ESTABLISH VIRTUAL PRIVATE NETWORK CONNECTION USING SOFTETHER VPN



49. The **Manage Sessions** window appears, where you can see connected users through the VPN Network. You can use different options to manage the VPN users.

50. Click on **Exit** to close the **Manage Sessions** window.

EXERCISE 8:
ESTABLISH VIRTUAL PRIVATE NETWORK CONNECTION USING SOFTETHER VPN



51. Now in the **Management of Virtual Hub – (Virtual Hub Name)** window, click the **Manage Users** button.

EXERCISE 8: ESTABLISH VIRTUAL PRIVATE NETWORK CONNECTION USING SOFTETHER VPN



52. The **Manage Users** window appears, where you can see the details of the users.

53. Click on **Exit** to close the **Manage Users** window to return to Management of **Virtual Hub – (Virtual Hub Name)** window.



EXERCISE 8:
**ESTABLISH VIRTUAL
PRIVATE NETWORK
CONNECTION USING
SOFTETHER VPN**

54. In the same way you can explore different options in the **Management of Virtual Hub – (Virtual Hub Name)** window like **Manage Groups**, **Manage Access** lists etc.

55. Close all the open windows in both machines.

56. Turn off the **AD Domain Controller** virtual machine.

EXERCISE 9: SCAN SYSTEM FOR VIRUSES USING KASPERSKY INTERNET SECURITY

Anti-virus software is a tool or program that is designed to identify and prevent malicious Trojans or malware from infecting computer systems or electronic devices.

LAB SCENARIO

An attacker uses malware to commit online fraud or theft. Thus, the use of antivirus or anti-malware software is recommended to help detect malware, remove it, and repair any damage it might cause.

A security professional must have the required knowledge to scan the systems in the network with Antivirus or Anti-malware software to remove any unwanted or malicious files which can be harmful to the system and overall network security.

LAB OBJECTIVE

This lab will demonstrate how to perform a scan on a system using Kaspersky Internet Security.

OVERVIEW OF ANTI-VIRUS

Anti-virus systems and threat intelligence platforms use Indicators of Compromise (IoCs) to spot and stop malicious activities at an initial stage. Examples for IoCs include using specific registry entries, domain names of botnet command-and-control (C&C) servers, hashes of malware files, virus signatures, and Internet Protocol (IP) addresses.

LAB TASKS

Note: Ensure that **Admin Machine-1**, **Web Server** and **PfSense Firewall** virtual machines are running.

1. Switch to the **Admin Machine-1** virtual machine.

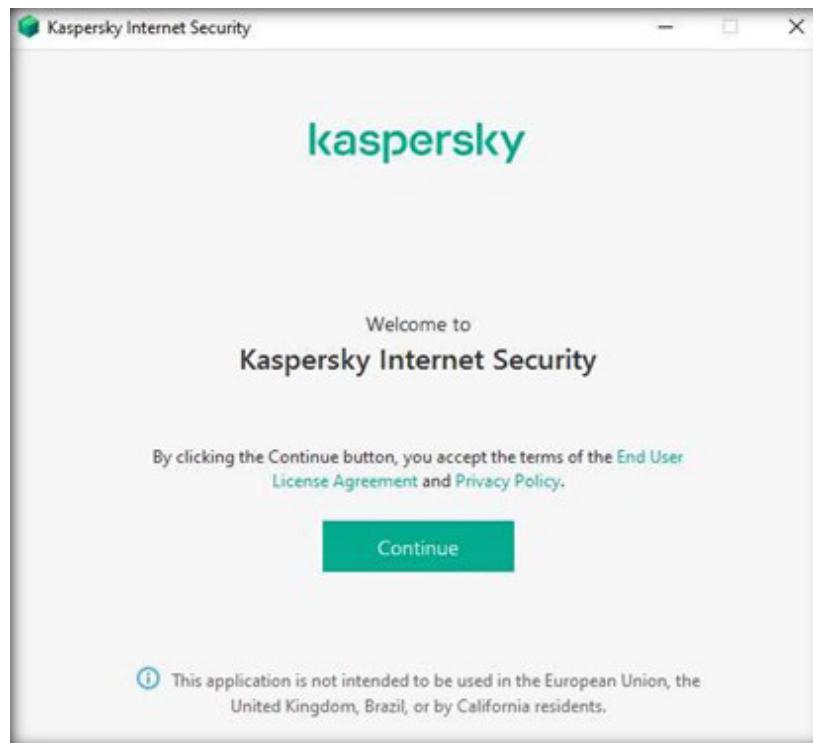
2. To install the **Kaspersky Internet Security**, navigate to **Z:\CCT-Tools\CCT Module 07 Network Security Controls - Technical Controls\Kaspersky Internet Security**.

3. Double-click **Kis21.3.10.391en_26096.exe**.

Note: You can download the latest version of **Kaspersky Internet Security** from <https://www.kaspersky.com>. If you use the downloaded file, the screenshots in the lab may vary.

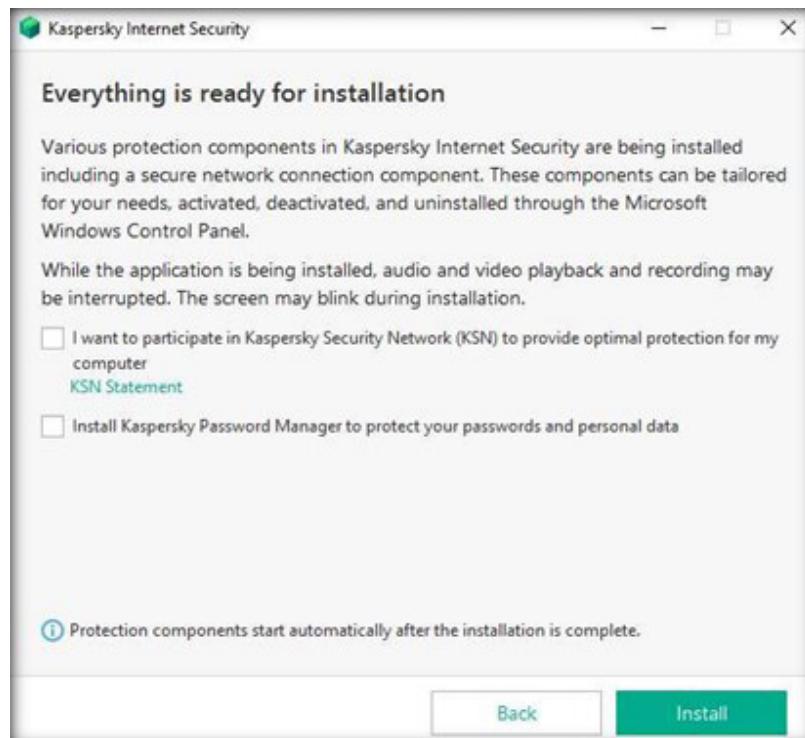
4. The **Kaspersky Internet Security** window appears. After the connection to the server has been established, the **Continue** button appears, click on it.

EXERCISE 9: SCAN SYSTEM FOR VIRUSES USING KASPERSKY INTERNET SECURITY



5. The **Everything is ready for installation** wizard appears, uncheck both the checkboxes and click Install button.

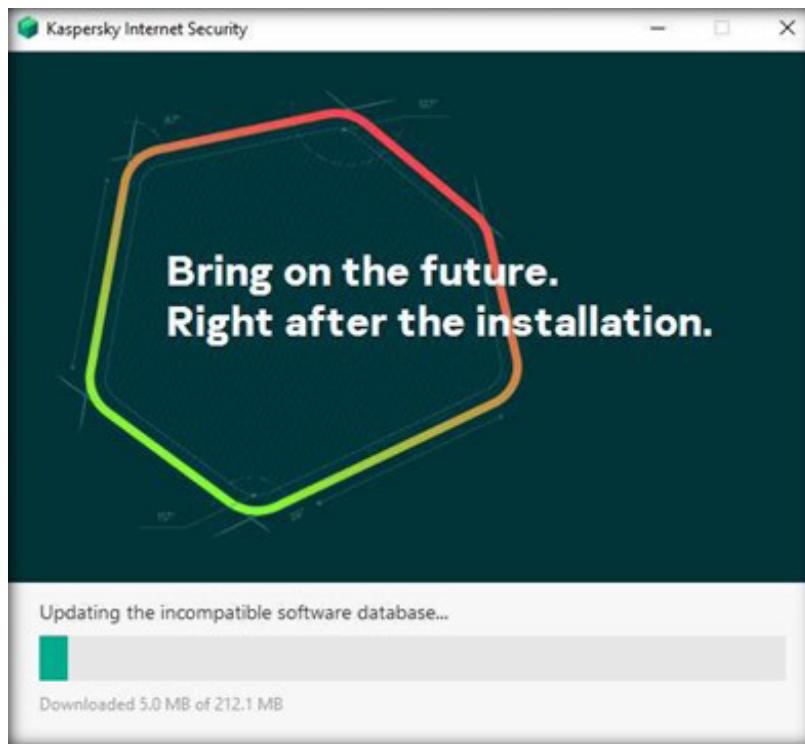
EXERCISE 9: SCAN SYSTEM FOR VIRUSES USING KASPERSKY INTERNET SECURITY



6. The **User Account Control** window appears, click **Yes**.

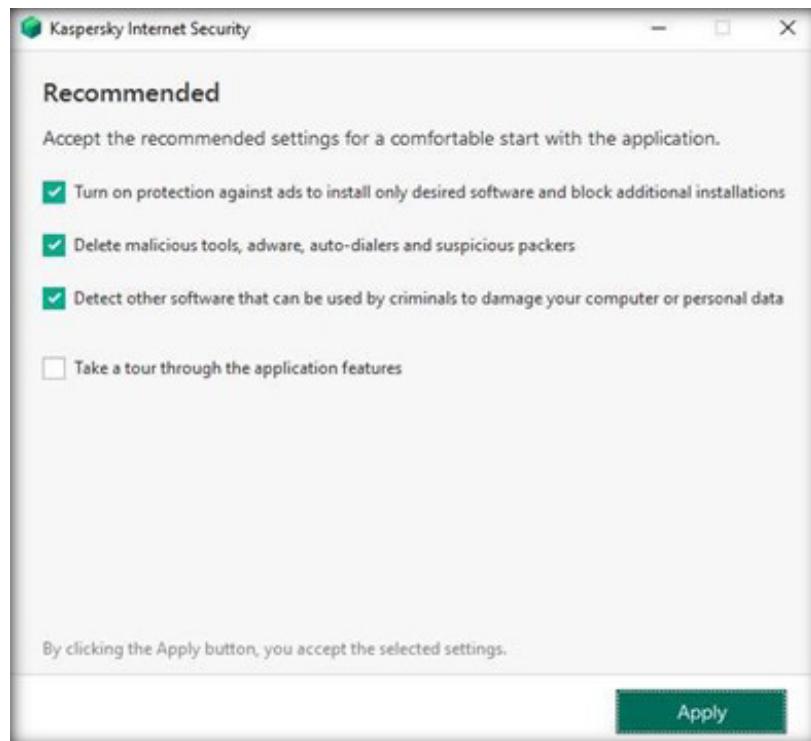
7. Application begins downloading, wait for it to finish. It will take approximately 5 minutes for the download to finish.

EXERCISE 9: SCAN SYSTEM FOR VIRUSES USING KASPERSKY INTERNET SECURITY



8. After the application finishes downloading, the **Recommended** wizard appears. Uncheck **Take a tour through the application features** checkbox and click **Apply**.

EXERCISE 9: SCAN SYSTEM FOR VIRUSES USING KASPERSKY INTERNET SECURITY



9. The application is installed successfully, click **Done** button.

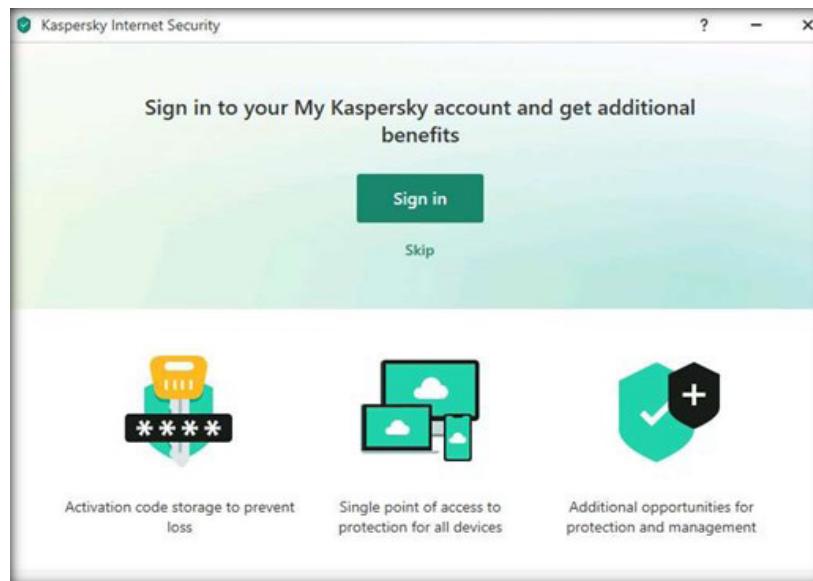
EXERCISE 9: SCAN SYSTEM FOR VIRUSES USING KASPERSKY INTERNET SECURITY



10. Sign in wizard appears, click **Skip** to skip the sign in process.

Note: If Kaspersky VPN window appears, close it.

EXERCISE 9: SCAN SYSTEM FOR VIRUSES USING KASPERSKY INTERNET SECURITY



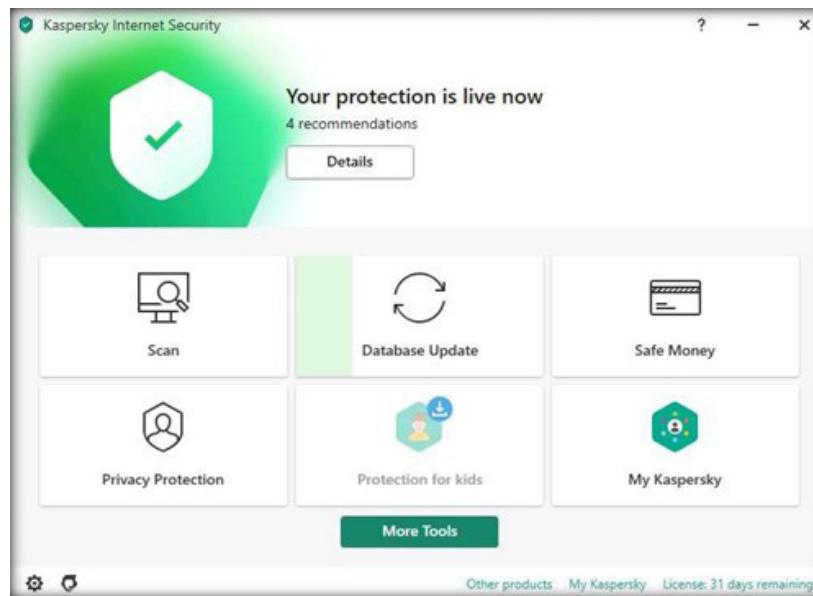
11. The **Activation completed successfully** wizard appears, click **Done**.

12. The **Kaspersky** main window appears, allow **Database Update** to finish installing updates.

Note: If database update is not started automatically, click on **Database Update** and in the next window click on Run update.

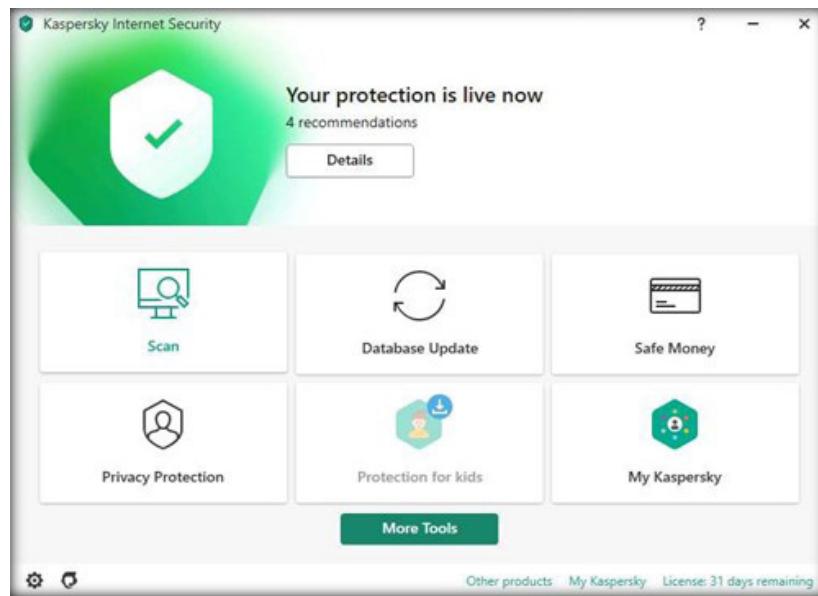
Note: The status will be indicated in green color.

EXERCISE 9: SCAN SYSTEM FOR VIRUSES USING KASPERSKY INTERNET SECURITY



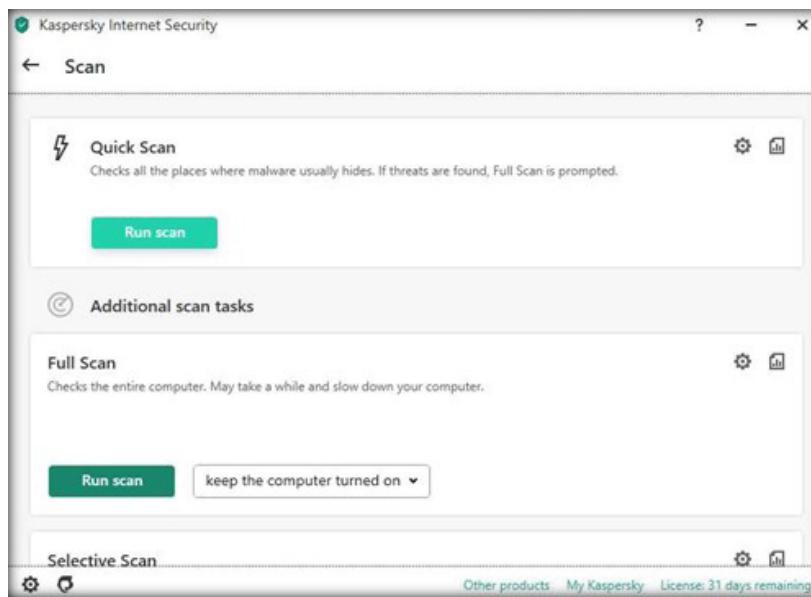
13. Now, click the **Scan** button to scan the system for malicious files.

EXERCISE 9: SCAN SYSTEM FOR VIRUSES USING KASPERSKY INTERNET SECURITY



14. The **Scan** wizard appears. Here, you will perform a quick scan.

15. To do so, click **Run scan** button under the **Quick Scan** section.

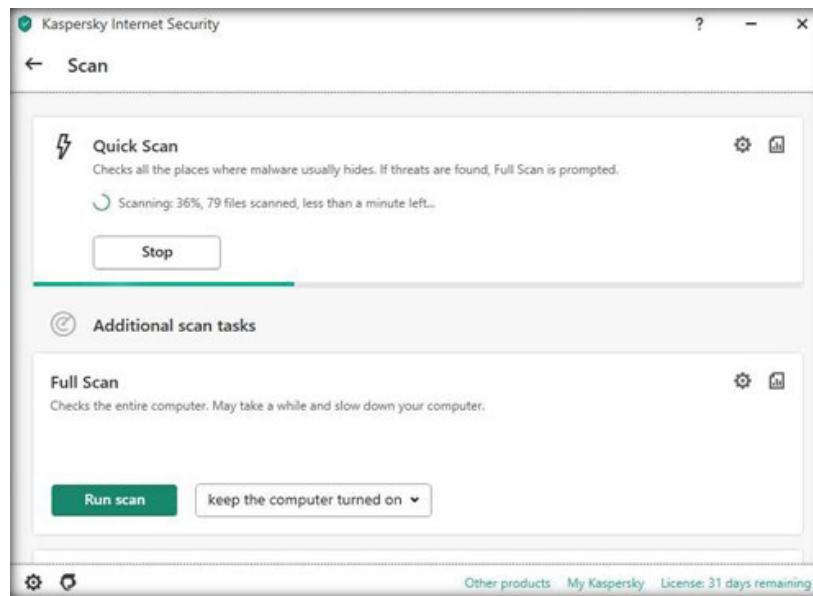


EXERCISE 9: SCAN SYSTEM FOR VIRUSES USING KASPERSKY INTERNET SECURITY

16. The scanning process initializes, the scan status will appear above the **Stop** button, you will have to wait for the status to reach **100%**.

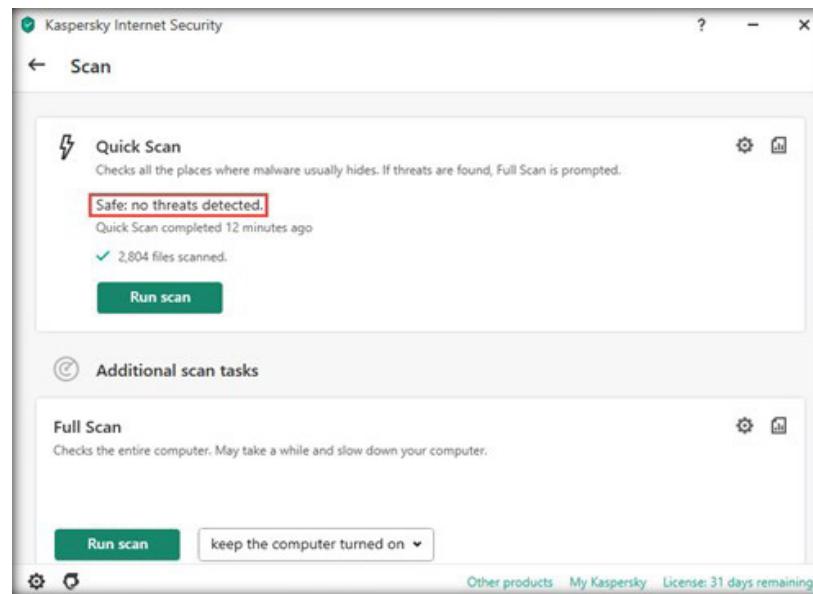
Note: Scanning process will take approximately 5 minutes to finish.

EXERCISE 9: SCAN SYSTEM FOR VIRUSES USING KASPERSKY INTERNET SECURITY



17. After the completion of scan, you can observe the status as **Safe: no threats detected** indicating that the system is free from viruses and malicious files.

EXERCISE 9: SCAN SYSTEM FOR VIRUSES USING KASPERSKY INTERNET SECURITY



18. Scroll-down in the **Scan** wizard. As you so do, you will be able to see different types of scans that can be performed on the system. The scanning may vary depending on the type of scan being performed.
19. Similarly, you can navigate back to the main window of **Kaspersky** and explore the other tools offered by application.
20. This concludes the demonstration of scanning a system using Kaspersky Internet Security.
21. Close all open windows.
22. Turn off **Admin Machine-1** and **PfSense Firewall** virtual machines.

EC-Council

