Exploring the Lab Environment

Scenario

In this activity, you will familiarize yourself with the systems you will be using in the course activities as well as the Lab engine Apporto Modular Cyberlab (AMC).

Task 1

Using the Lab Interface

To complete most of the labs in this course, you will use one or more Virtual Machines (VMs) hosted on a cloud platform. Each VM works very much like a physical computer, but you access them via your browser. The main thing to remember is that your WINDOWS/START key will work on your own computer not the VM. Take a few moments to familiarize yourself with some other features of the lab browser controls.

1. To open the Lab environment for the CompTIA Security+ Practice labs, click on the left Dock sidebar the **Modular Cyberlab** Icon to open the Apporto Modular Cyberlab (AMC) Graphical User Interface (GUI).

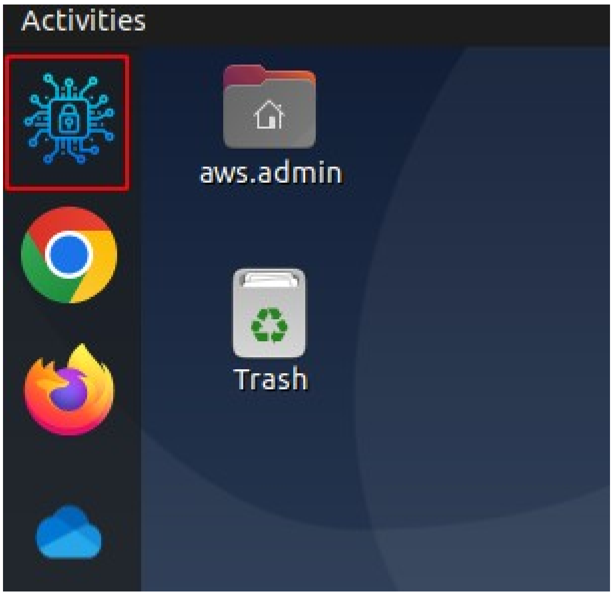
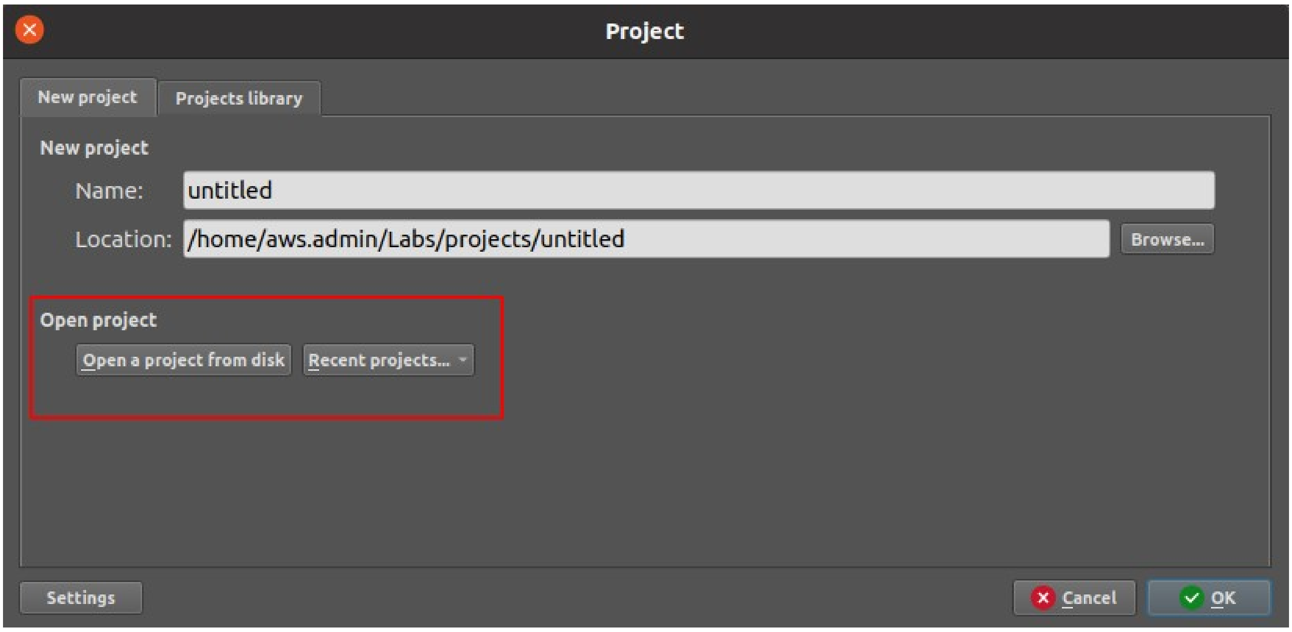


Figure 1.1 – Selecting the Modular Cyberlab favorite shortcut from the Dock sidebar.

2. When the program launches it will ask to name a new project or to open a previously saved project. Select the **Recent projects** drop down under **Open project** section.



Name: untitled

Location: /home/aws.admin/Labs/projects/untitled

Figure 1.2 – Opening a Recent Project.

3. Select from the list **Practice_Labs**.

These steps will open the project and the related Security+ topology view of the Lab VMs.

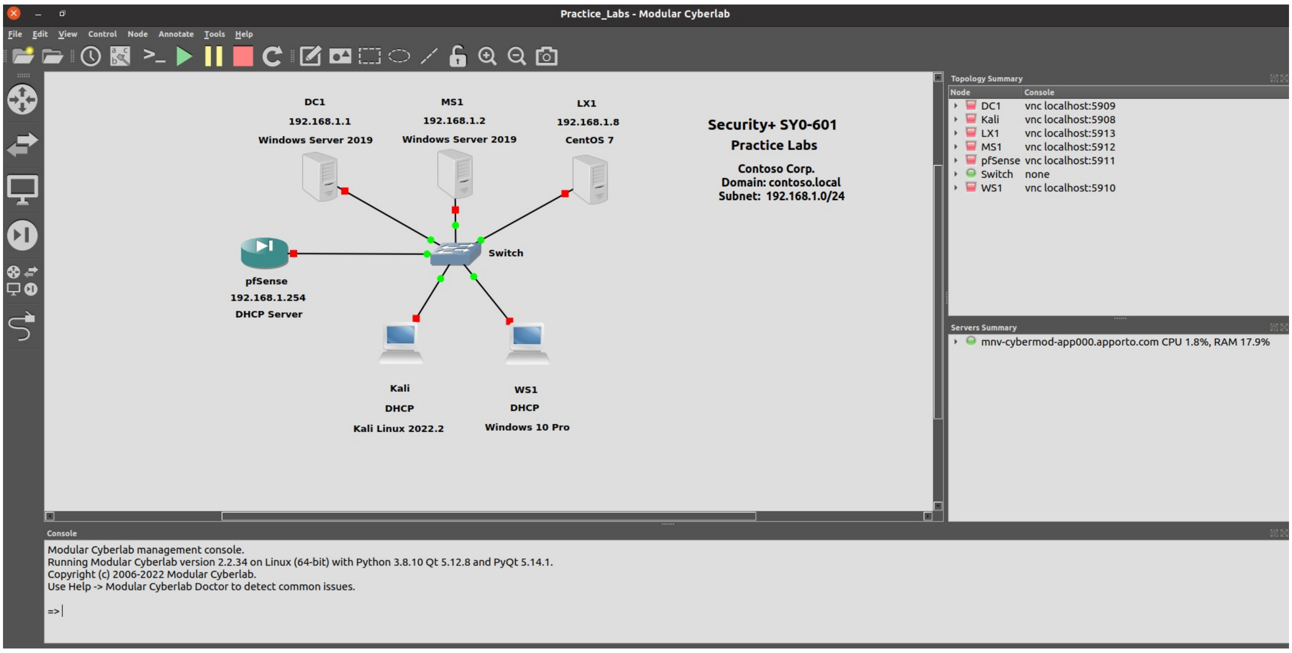
Task 2

Exploring the Lab Environment

This section explains various options in the AMC GUI which helps you manage the Security+ VMs.

Screen Layout

The screen layout of the lab environment is subdivided into several sections: The Workspace, Toolbar, Devices Toolbar, Topology Summary, and the Console.



Topology Summary

Node	Console
DC1	vnc localhost:5909
Kali	vnc localhost:5908
LX1	vnc localhost:5913
MS1	vnc localhost:5912
pfSense	vnc localhost:5911
Switch	none
WS1	vnc localhost:5910

Servers Summary

mnv-cybermod-app000.apporto.com CPU 1.8%, RAM 17.9%

Console

```
Modular Cyberlab management console.
Running Modular Cyberlab version 2.2.34 on Linux (64-bit) with Python 3.8.10 Qt 5.12.8 and PyQt 5.14.1.
Copyright (c) 2006-2022 Modular Cyberlab.
Use Help -> Modular Cyberlab Doctor to detect common issues.

=>|
```

Figure 2.1 – The CompTIA Security+ AMC project.

Next, We will describe the areas which pertain to the Security+ labs.

CompTIA Security+ AMC Workspace

The Workspace is where devices are located in a topology view to represent an internal LAN network.

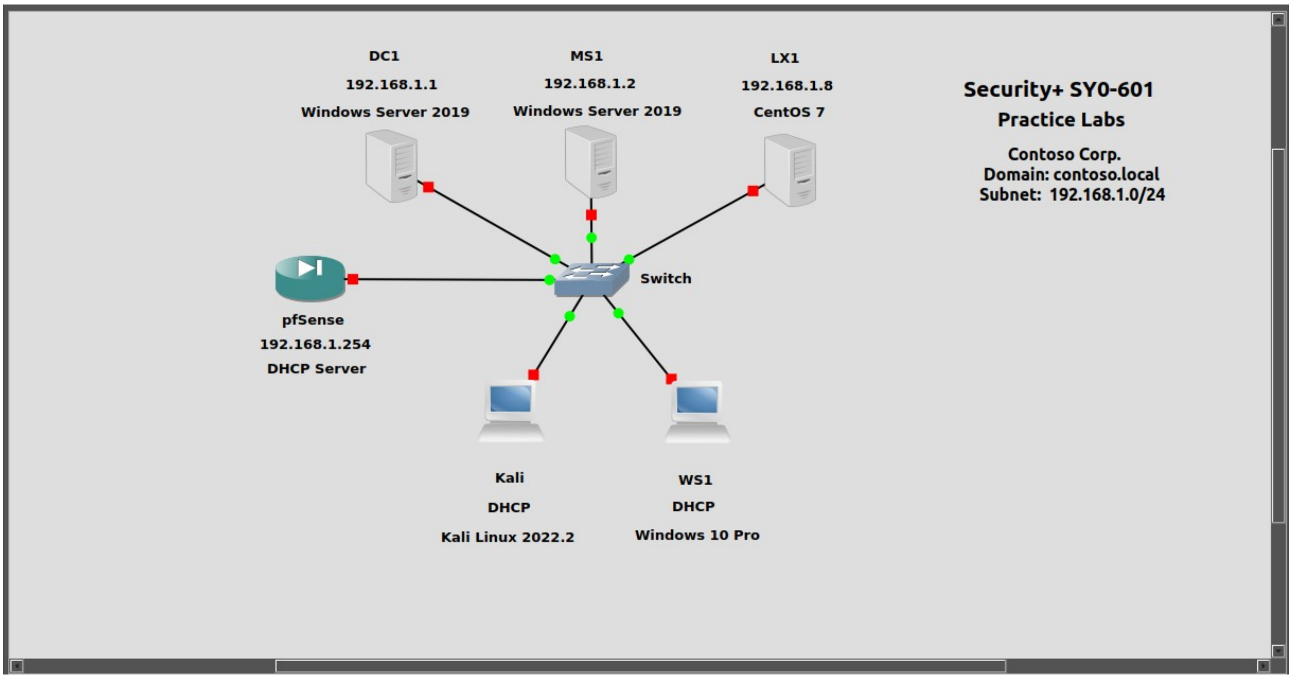
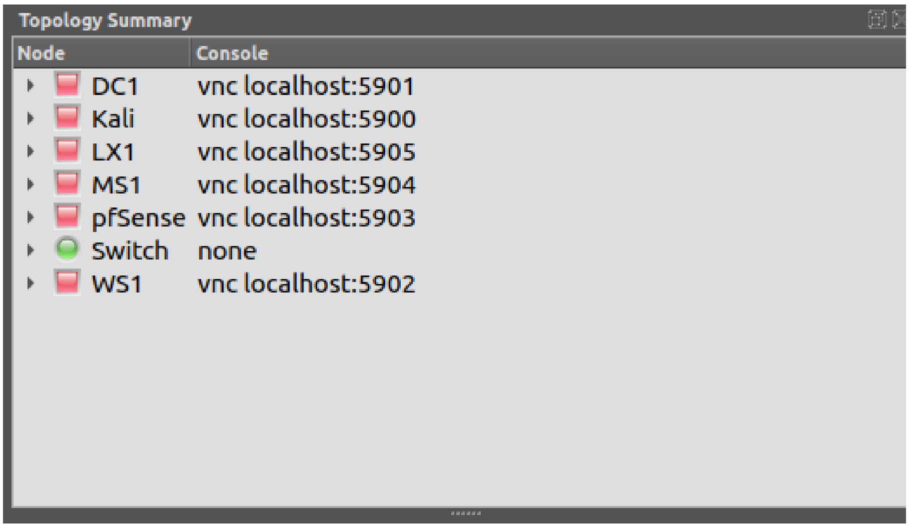


Figure 2.2 – The CompTIA Security+ Workspace pane.

CompTIA Security+ Topology Summary

This pane will display devices currently in the Workspace, their status (on/off/suspended), as well as which devices are connected to one another.

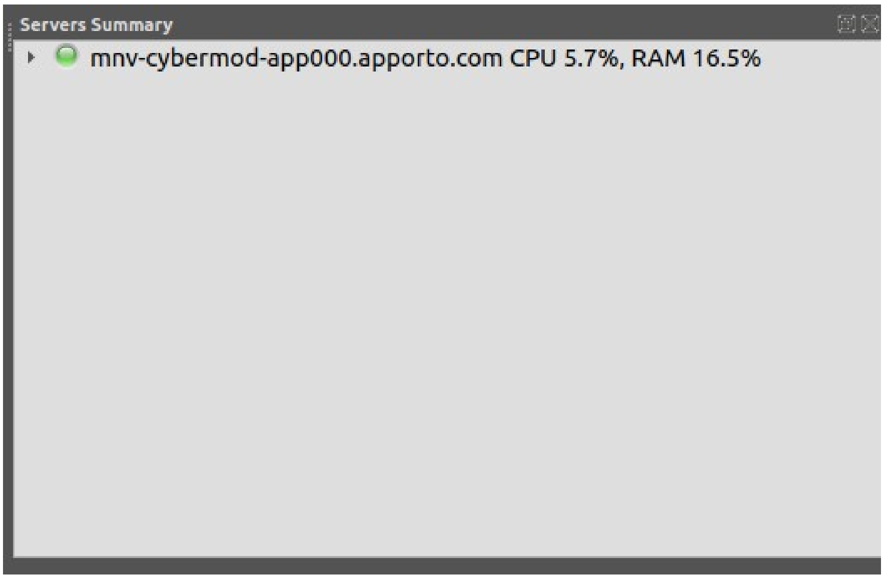


Node	Console
🟥 DC1	vnc localhost:5901
🟥 Kali	vnc localhost:5900
🟥 LX1	vnc localhost:5905
🟥 MS1	vnc localhost:5904
🟥 pfSense	vnc localhost:5903
🟢 Switch	none
🟥 WS1	vnc localhost:5902

Figure 2.3 – Topology Summary pane.

Servers Summary

This pane will display the server in use and the current resource usage. In case you have multiple VMs open at the same time you can check this pane to check the current resource usage.



🟢 mnv-cybermod-app000.apporto.com CPU 5.7%, RAM 16.5%

Figure 2.4 – Servers Summary pane.

Task 3

Managing the VMs

In order to interact with the VMs we need to turn them ON and connect to the machine using the console. We will turn ON a Machine and explore the context menu options.

1. Right-click **DC1** VM. From the **context menu** notice all the options we can use. Select **Start** to **Power ON** this Virtual Machine.

TIP: Note that when the Virtual Machine is Powered OFF it has a red dot next to it. When the Virtual Machine Powers ON it will show a green dot instead.

NOTE: You will perform the same steps to Power ON the VMs in the topology when needed.

WARNING: Just Power ON the VMs needed to perform each of the Lab activities. Turning all the VMs at the same time can cause some VMs to have poor performance. Keep an eye on the **Servers Summary** Pane in the Modular Cyberlab.

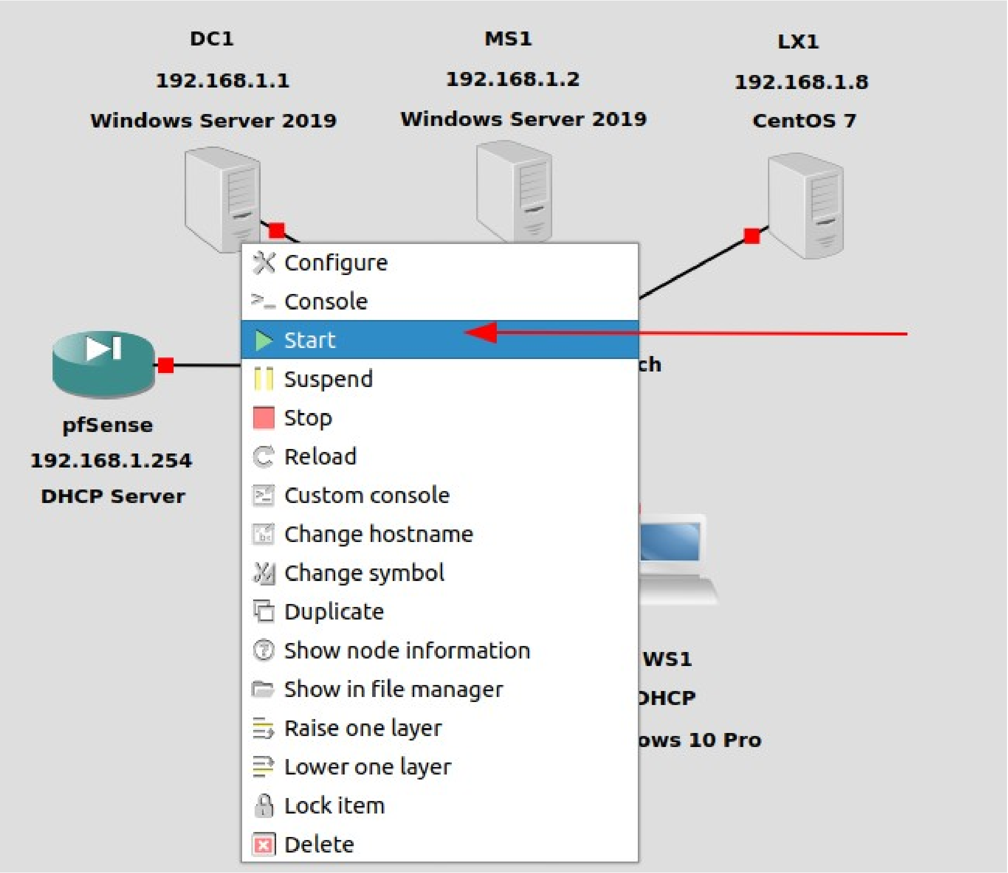


Figure 3.1 – Virtual machine context menu.

2. To connect to the Virtual Machine, right-click and select Console (refer to Figure 3.1 for context menu options).

3. Once the Console opens, you will see a window representing the Virtual Machine Desktop.

You can interact with the Desktop like if you were sitting in front of the monitor of the computer you are working with.

NOTE: On GUI type operating systems you will see the Desktop. On Terminal type operating systems you will see the console Terminal window.

Most of the Virtual Machines will need some sort of key combinations like CTRL+ALT+DELETE. In order to send those commands to the Virtual Machine press the **F8** key on your keyboard and a new context menu will be displayed with key combination options, one of them being CTRL+ALT+DEL.

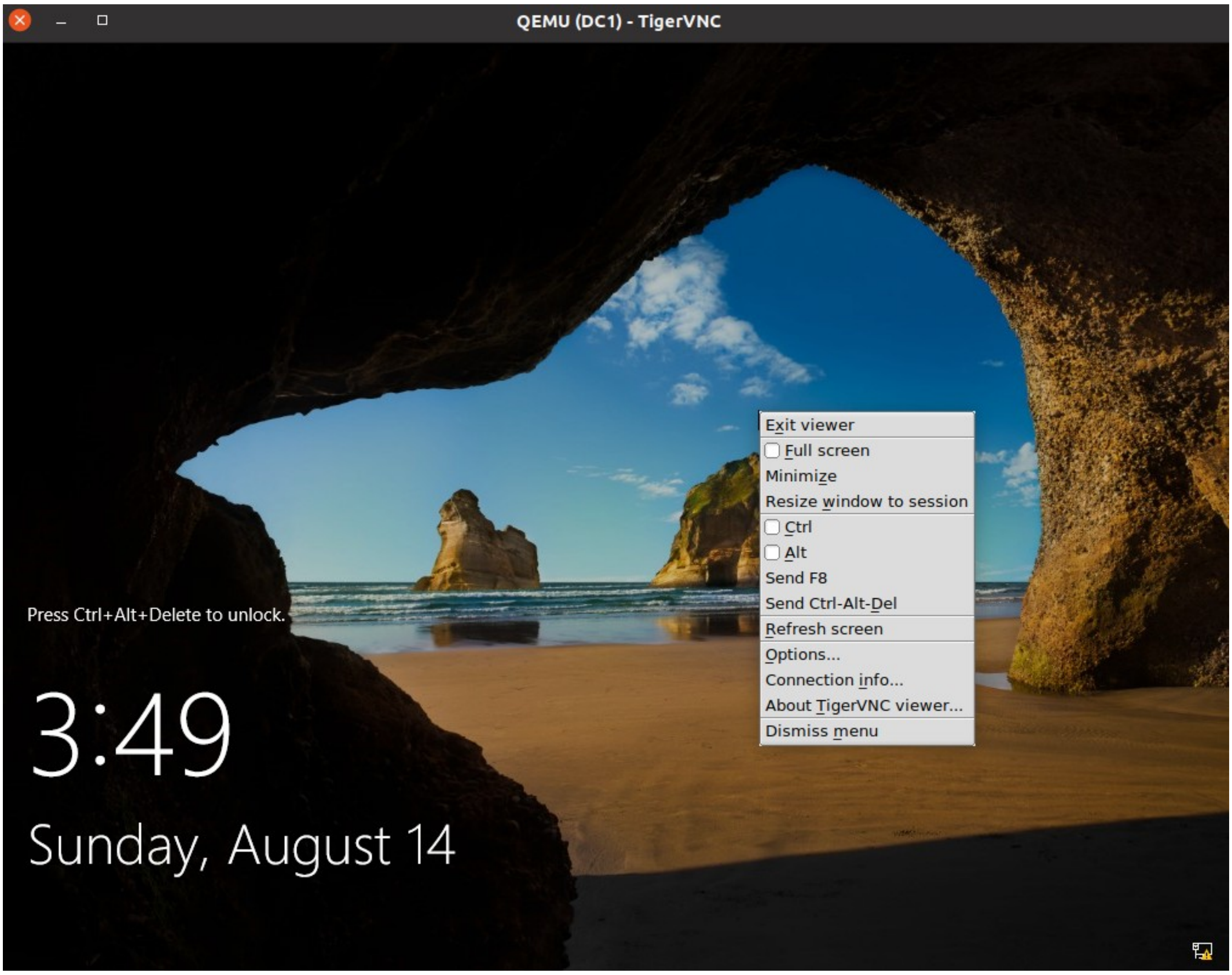


Figure 3.2 – The Console screen of DC1 showing the F8 context menu options.

Task 4

Explore Windows VMs

The Windows network contains a domain controller, a member server, and a client workstation. Both servers are running Windows Server 2019. The client workstation VM is running Windows 10 Pro.

DC1 VM is configured as the network's domain controller (DC). Normally the DC role should not be combined with other roles, but to minimize the number of VMs you have to run, this machine is also configured as a DNS server , CA (certificate Authority) server, IIS, and will be used for a number of other services and configurations. This VM is configured with a static IP address (192.168.1.1).

MS1 VM is configured as a member server for running applications. It runs a DHCP service to perform auto addressing for clients connecting as part of the lab activities. The DHCP service is turned off. It has the web server (IIS) role installed. This VM is also configured with a static IP address (192.168.1.2).

WS1 VM is configured as a domain joined Windows client. It is used as part of the lab activities and can use the domain administrator and a user account. Both user accounts are managed at the domain controller.

You will usually use the username **CONTOSO\Administrator** to log on to the Windows VMs. Each user account in this lab environment uses the same password of **Pa$$w0rd** (awful security practice, but it makes the the activities simpler for you to complete).

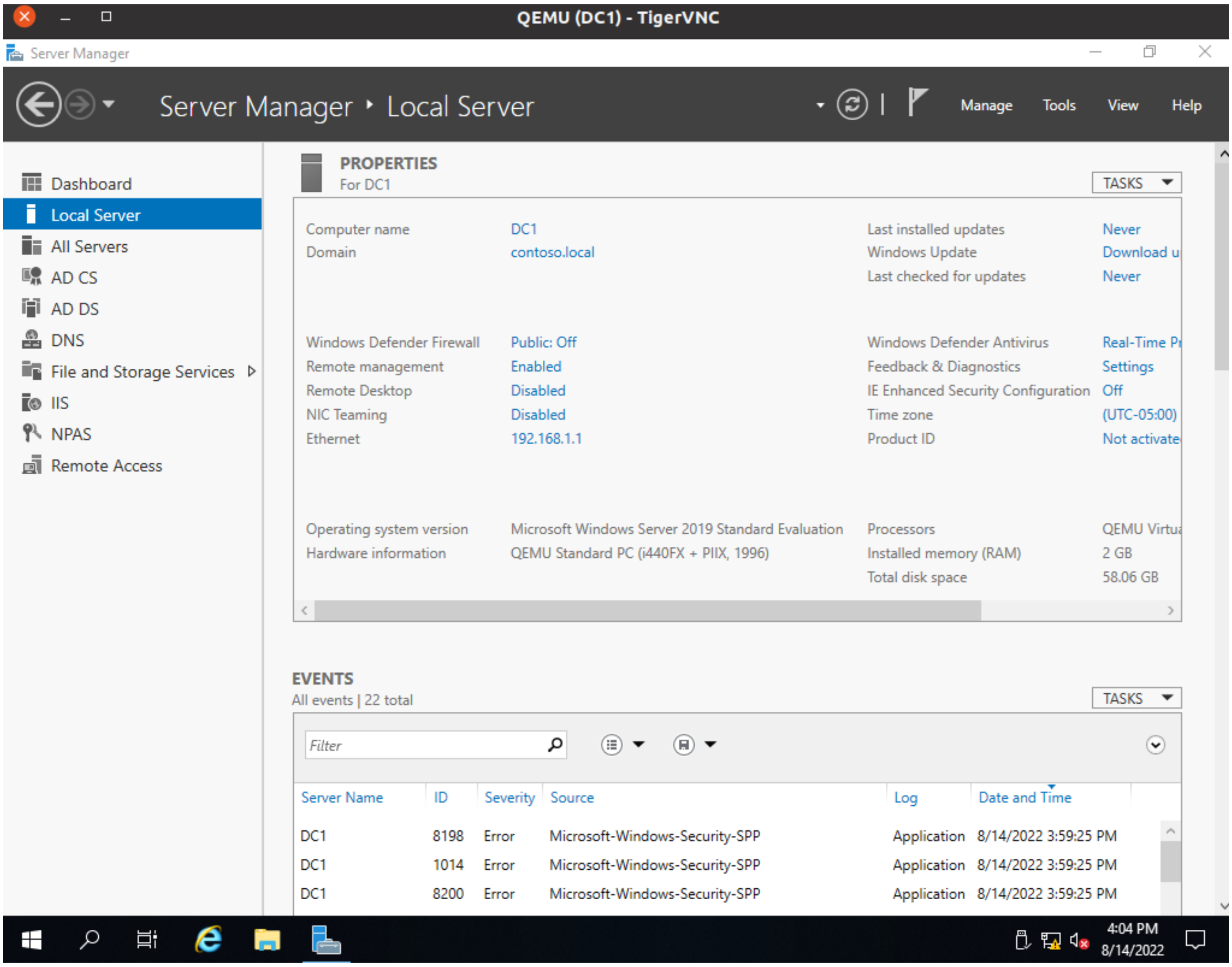
1. At each point in an activity, you should ensure that you are working within the correct virtual machine. The correct VM may usually accessed by selecting the VM in the topology view and right-clicking it choosing **Console** to open a remote screen viewer window.

2. Select the **DC1** VM, right-click and select **Start**, send **CTRL+ALT+DEL** and then select the password box. Type the password **Pa$$w0rd**.

3. Press **ENTER** or select the **arrow button** to submit the password and log on.

4. You can explore **Server Manager** to see the roles installed. Server Manager will start with each session.

5. Click on **Local Server** to see a preview of the server configuration.



PROPERTIES
For DC1

Computer name	DC1	Last installed updates	Never
Domain	contoso.local	Windows Update	Download u
		Last checked for updates	Never
Windows Defender Firewall	Public: Off	Windows Defender Antivirus	Real-Time Pr
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	Off
NIC Teaming	Disabled	Time zone	(UTC-05:00)
Ethernet	192.168.1.1	Product ID	Not activate
Operating system version	Microsoft Windows Server 2019 Standard Evaluation	Processors	QEMU Virtu
Hardware information	QEMU Standard PC (i440FX + PIIX, 1996)	Installed memory (RAM)	2 GB
		Total disk space	58.06 GB

EVENTS
All events | 22 total

Server Name	ID	Severity	Source	Log	Date and Time
DC1	8198	Error	Microsoft-Windows-Security-SPP	Application	8/14/2022 3:59:25 PM
DC1	1014	Error	Microsoft-Windows-Security-SPP	Application	8/14/2022 3:59:25 PM
DC1	8200	Error	Microsoft-Windows-Security-SPP	Application	8/14/2022 3:59:25 PM

Figure 4.1 – Windows Server – Server Manager – Local Server view.

NOTE: To shutdown any of the Windows Virtual Machines you will do it from the Start Windows Button > Power > Shutdown.

Task 5

Explore Kali Linux VM

The Kali VM is running the Kali pentesting/forensics Linux distribution, created and maintained by Offensive Security (kali.org). You will be using this VM for some security posture assessment and pentesting activities, as well as general Linux configuration management. Kali is based on the Debian Linux distribution with the XFCE desktop environment.

1. Select the **Kali** VM. Note that this VM has not been started automatically. Right-click and select **Start**.

2. When the VM has started, log on with the username **kali** and the password **Pa$$w0rd**.

NOTE: Kali will screen lock if not used. To restore the screen, click and retype the username and password.

3. Take a few moments to familiarize with the desktop.

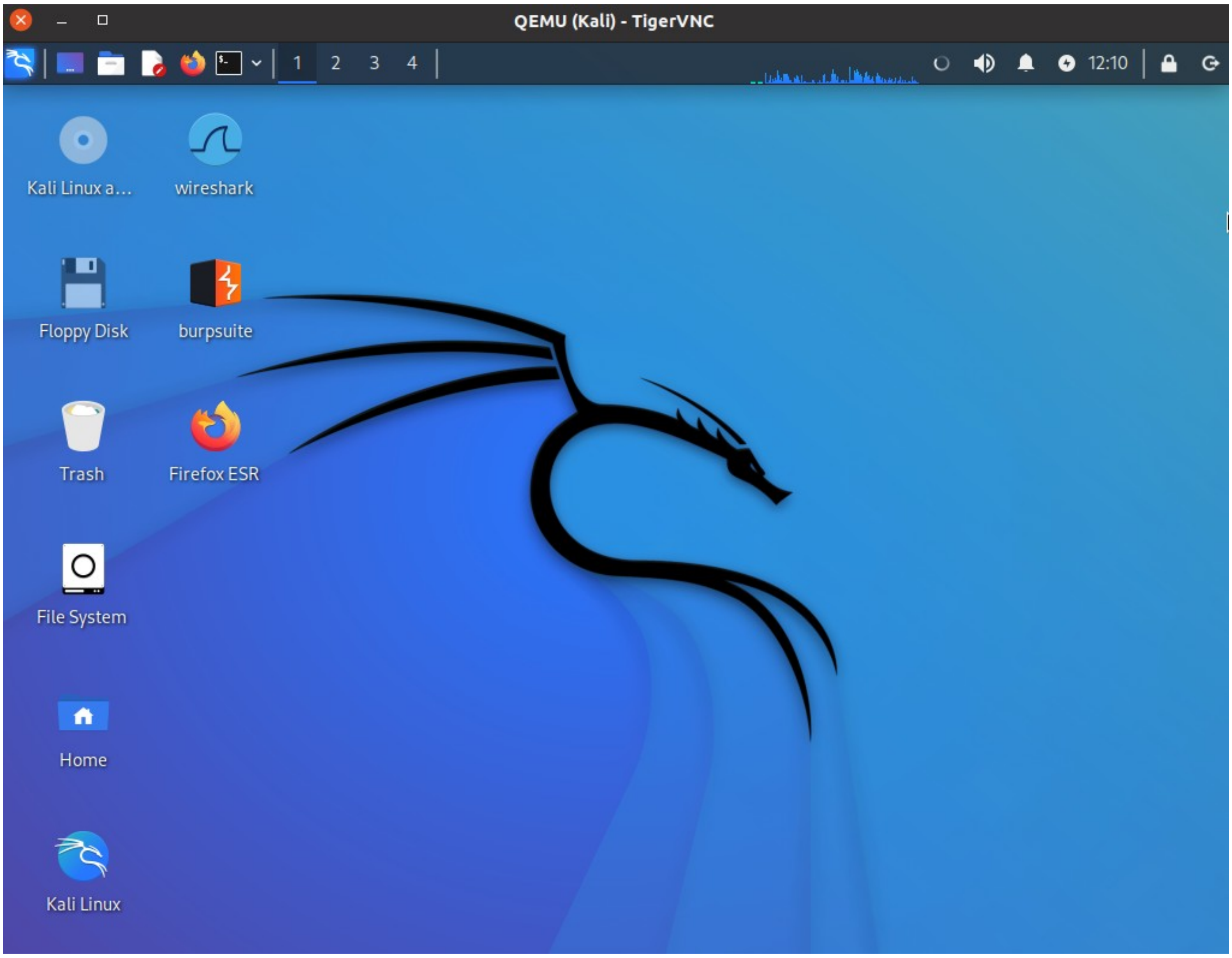


Figure 5.1 – Kali Desktop environment.

4. Right-click the desktop and select **Open Terminal Here**.

5. Run **ifconfig eth0** to check the network adapter configuration.

TIP: Remember that the Linux command-line is case sensitive.

The main eth0 adapter is configured to use DHCP.

6. Run the following commands to start the web server and open the local website in the browser:

```
service apache2 start

firefox http:// localhost &
```

Note the way that the commands are formatted with separate font style. When entering longer commands, ignore any line breaks.

Task 6

Explore CentOS Linux LX1 Server VM

There is also a Linux Server.

LX1 is a CentOS Linux distribution (centos.org) that has been installed with an intentionally vulnerable web application, Mutillidae from OWASP (owasp.org). This VM runs the familiar Linux, Apache, MariaDB, and PHP (LAMP stack). It also has installed Snort.

This VM is usually positioned on the network as a standalone Linux server. It has an static IP address of 192.168.1.8 configured.

1. Select the **LX1** VM. Note that this VM has not been started automatically. Right-click and select **Start**.

2. When the VM has started, log on with the username **User** and the password **Pa$$w0rd**.

NOTE: LX1 will screen lock if not used. To restore the screen, click and retype the username and password.

3. Take a few moments to familiarize with the desktop.

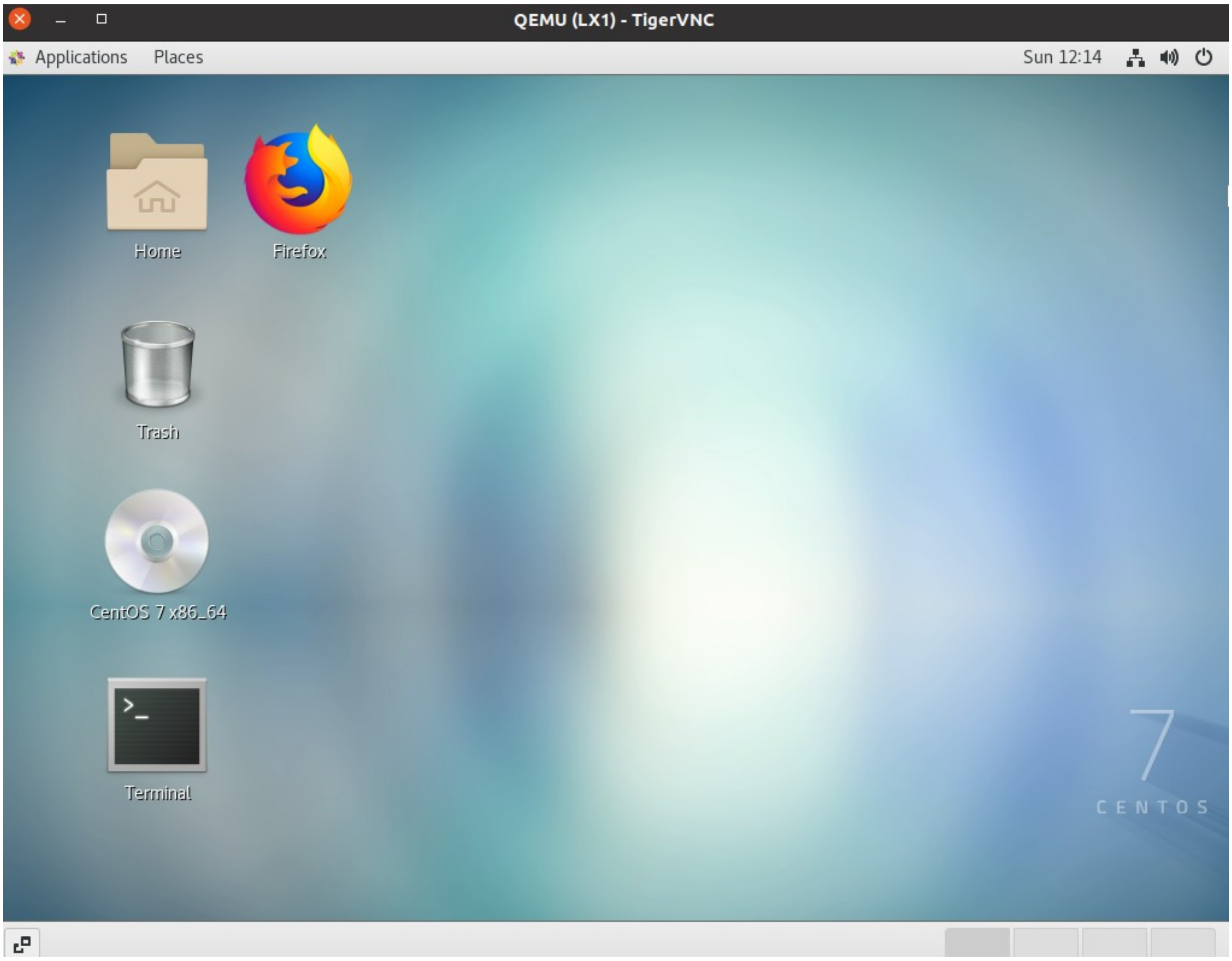


Figure 6.1 – CentOS Desktop environment.

4. Open the **Terminal** double-clicking on the Terminal icon on the **Desktop**.

5. Run **ifconfig** to check the network adapter configuration.

Note that Apache web server is configured to start automatically.

6. Run the following commands to start the web server and open the local website in the browser:

```
firefox http://localhost &
```

Task 7

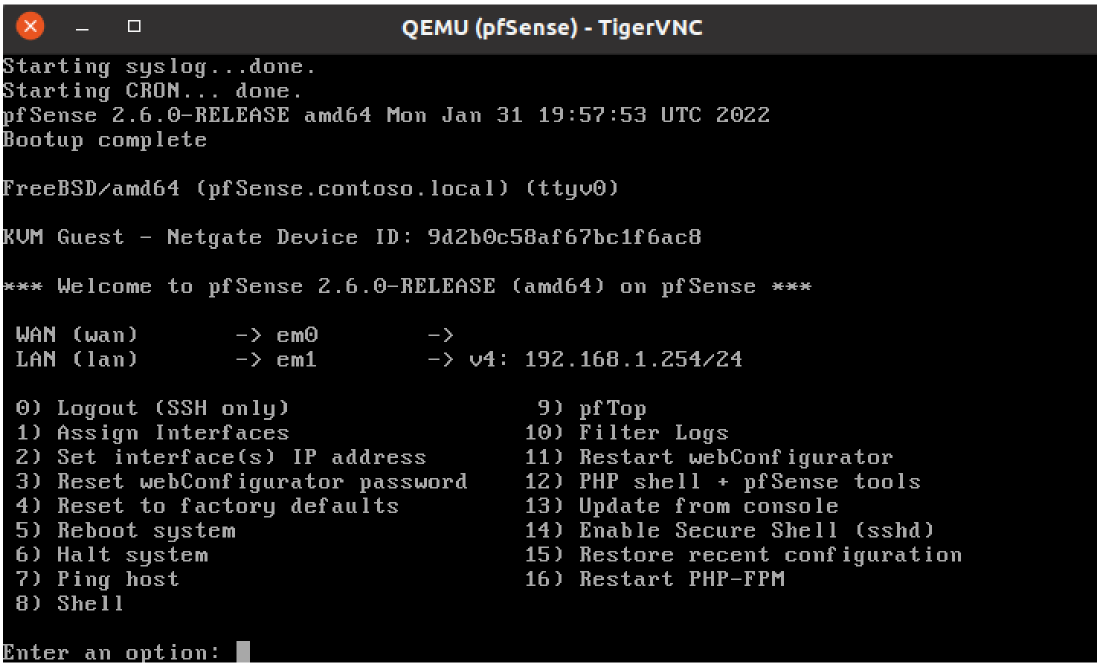
Explore pfSense Appliance VM

In the lab activities, you will use the pfSense security appliance VM to implement network and security functions.

pfSense is created by Netgate (pfsense.org) from the OpenBSD version of UNIX. pfSense is operated using a web GUI (http://192.168.1.254).

1. Select the **pfSense** VM. Note that this VM has not been started automatically. Right-click and select **Start**.

2. Right-click the VM and select **Console**.

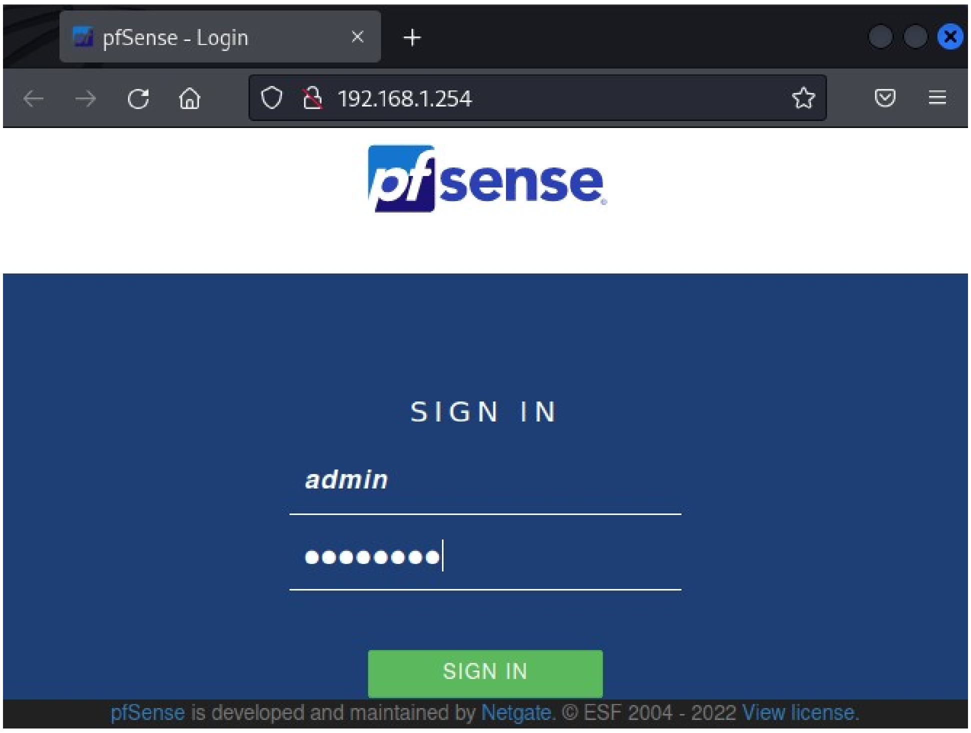


```
Starting syslog...done.
Starting CRON... done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

FreeBSD/amd64 (pfSense.contoso.local) (ttyv0)

KVM Guest - Netgate Device ID: 9d2b0c58af67bc1f6ac8

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        ->
 LAN (lan)       -> em1        -> v4: 192.168.1.254/24

 0) Logout (SSH only)                   9) pfTop
 1) Assign Interfaces                  10) Filter Logs
 2) Set interface(s) IP address        11) Restart webConfigurator
 3) Reset webConfigurator password     12) PHP shell + pfSense tools
 4) Reset to factory defaults          13) Update from console
 5) Reboot system                      14) Enable Secure Shell (sshd)
 6) Halt system                        15) Restore recent configuration
 7) Ping host                          16) Restart PHP-FPM
 8) Shell

Enter an option:
```

Figure 7.1 – pfSense console menu view.

3. From any other VM from the lab topology (i.e. Kali VM), open the Web Browser and navigate to **http://192.168.1.254**.

3. From the login page, type the username **admin** and the password is **Pa$$w0rd**.



SIGN IN

admin

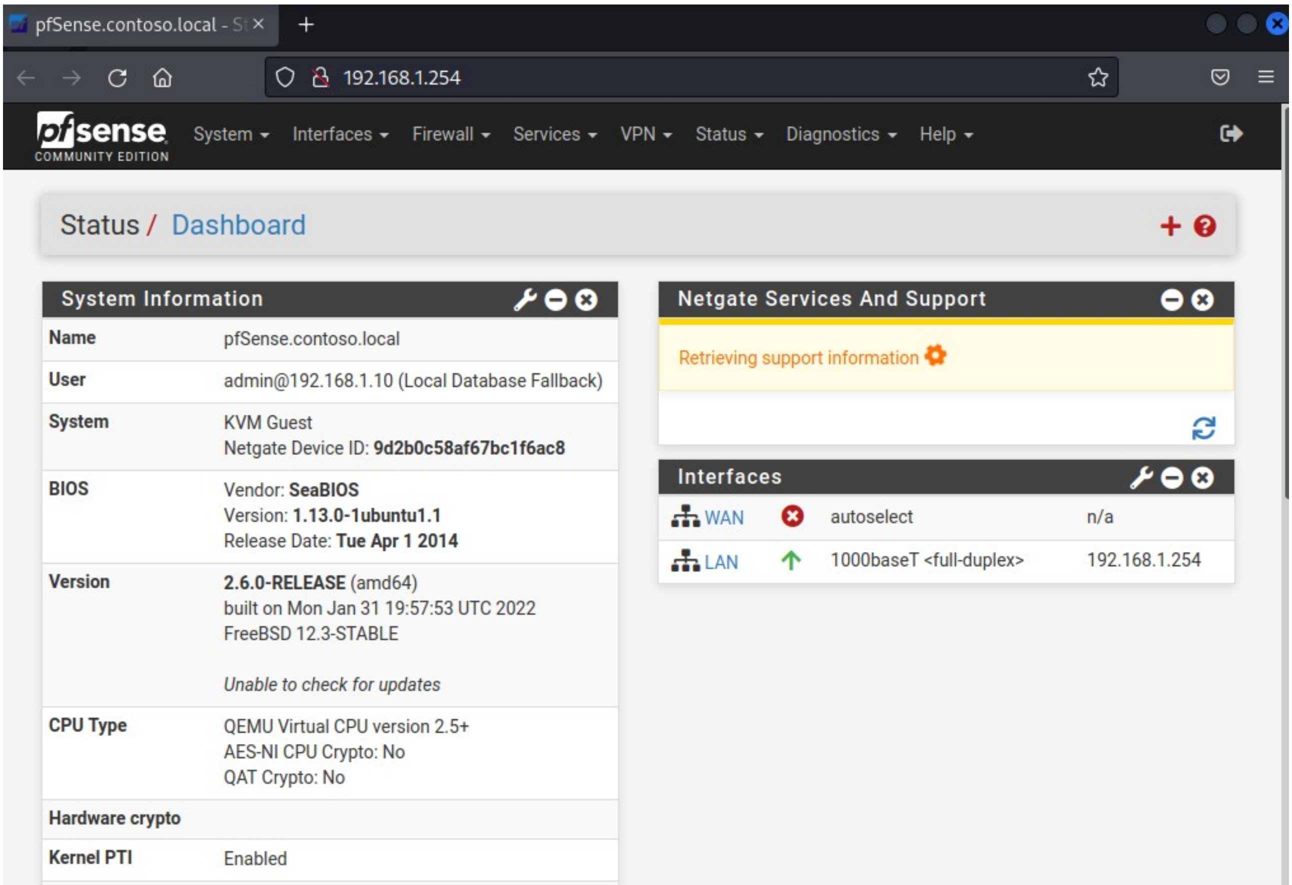
●●●●●●●●

SIGN IN

pfSense is developed and maintained by Netgate. © ESF 2004 - 2022 View license.

Figure 7.2 – pfSense login screen from Kali Linux.

4. Take a moment to explore and browse through the pfSense menu.



Status / Dashboard

System Information

Name	pfSense.contoso.local
User	admin@192.168.1.10 (Local Database Fallback)
System	KVM Guest Netgate Device ID: **9d2b0c58af67bc1f6ac8**
BIOS	Vendor: **SeaBIOS** Version: **1.13.0-1ubuntu1.1** Release Date: **Tue Apr 1 2014**
Version	**2.6.0-RELEASE** (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE *Unable to check for updates*
CPU Type	QEMU Virtual CPU version 2.5+ AES-NI CPU Crypto: No QAT Crypto: No
Hardware crypto	
Kernel PTI	Enabled

Netgate Services And Support

Retrieving support information

Interfaces

WAN	☒	autoselect	n/a
LAN	↑	1000baseT <full-duplex>	192.168.1.254

Figure 7.3 – pfSense Dashboard from the web browser.

Note that pfSense is configured as a DHCP server to lease IP address information to the Kali VM and WS1 VM.

The **Switch** on the topology is an unmanaged network switch that interconnects all the VMs. This device does not need to be turned on/off.