Having completed this section, you have learned how to set up both versions of Metasploitable 3 within your lab environment. Metasploitable 3 contains newer vulnerabilities than its predecessor and will be fun to exploit in later sections of this book. In the next section, you will learn how to deploy vulnerable web applications for penetration testing purposes.

Setting up vulnerability web application systems

Learning how to simulate real-world cyberattacks using Kali Linux would not be complete without understanding how to discover and exploit vulnerabilities within web applications. The **Open Web Application Security Project** (**OWASP**) is an organization that focuses on improving security through software, including web applications. OWASP is known for its **OWASP Top 10** list of most critical security risks within web applications.

> **Important Note**
>
> At the time of writing this book, the latest version of OWASP Top 10 is 2017. More information can be found at the following URL: `https://owasp.org/www-project-top-ten/2017/`.

As an aspiring penetration tester, it's important to understand how to identify and perform security testing on each category within the OWASP Top 10 list. OWASP created a few projects that allow learners to safely use their offensive security skills and techniques in a safe environment to discover web application vulnerabilities and exploit them.
In this section, we'll be deploying the **OWASP Juice Shop** and **OWASP Broken Web Applications** (**BWA**) projects within our lab.

Let's start deploying OWASP Juice Shop and OWASP BWA!

Part 1 – deploying OWASP Juice Shop

The following steps will ensure the OWASP Juice Shop vulnerable web application has been configured accurately and works seamlessly on your system:

1. Ensure Kali Linux has an internet connection as you will need to download a few components.

2. Within Kali Linux, open the Terminal and use the following commands to download the Docker **Pretty Good Privacy** (**PGP**) key:

```
curl -fsSL https://download.docker.com/linux/debian/gpg
| gpg --dearmor | sudo tee /usr/share/keyrings/docker-
archive-keyring.gpg >/dev/null
```

The following screenshot shows the expected results when executed correctly:

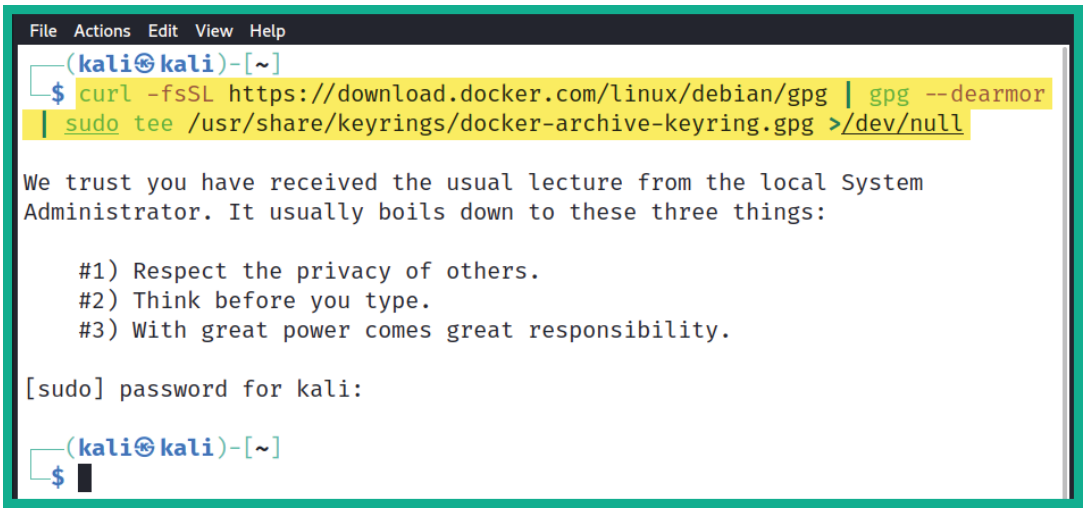

Figure 2.32 – Installing Docker PGP keys

3. Next, use the following commands to configure the Docker APT repository on your Kali Linux system:

```
echo 'deb [arch=amd64 signed-by=/usr/share/keyrings/
docker-archive-keyring.gpg] https://download.docker.com/
linux/debian buster stable' | sudo tee /etc/apt/sources.
list.d/docker.list
```

The following screenshot shows how to execute the commands on the Terminal:

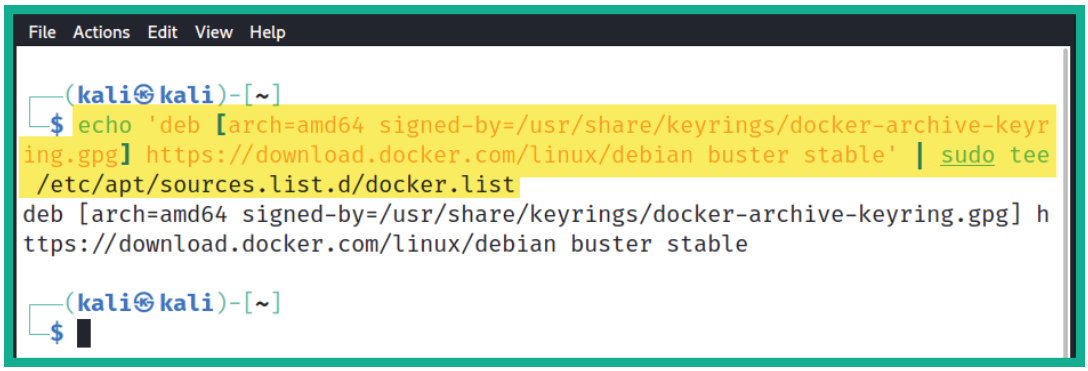

Figure 2.33 – Configuring the Docker repository

4. Next, use the following command to update the repository source list on Kali Linux:

```
sudo apt-get update
```

5. Now, we can install Docker on Kali Linux by using the following command:

```
sudo apt install -y docker-ce docker-ce-cli containerd.io
```

The following screenshot shows the expected results once these commands have been executed correctly:

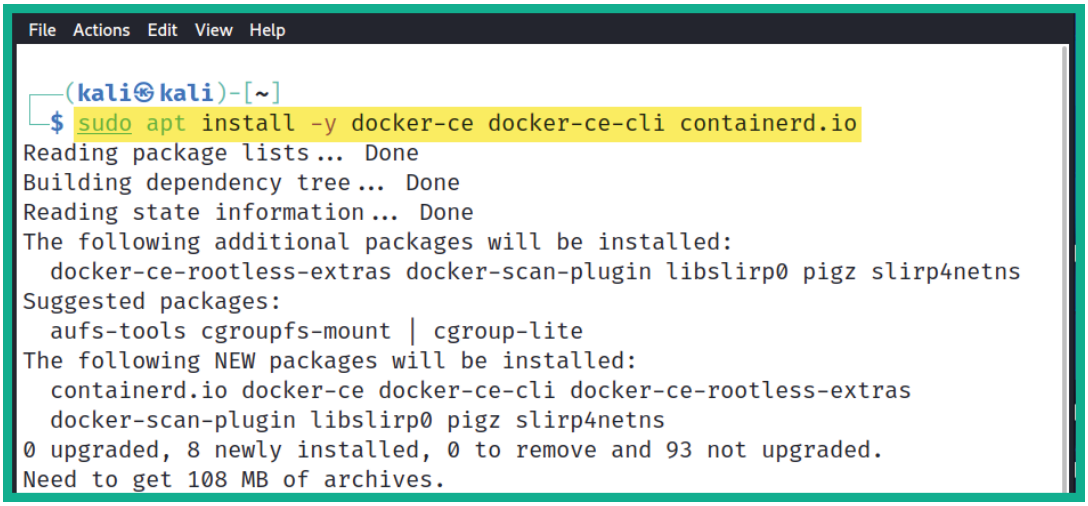

Figure 2.34 – Installing Docker on Kali Linux

6. At this point, Docker has been successfully installed on Kali Linux. To download the OWASP Juice Shop Docker container, use the following command:

```
sudo docker pull bkimminich/juice-shop
```

The following screenshot shows that the OWASP Juice Shop Docker container is being downloaded:

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo docker pull bkimminich/juice-shop
Using default tag: latest
latest: Pulling from bkimminich/juice-shop
ddad3d7c1e96: Pull complete
3a8370f05d5d: Pull complete
71a8563b7fea: Pull complete
119c7e14957d: Pull complete
cc14223d9a87: Pull complete
1b6803f21605: Pull complete
3dbea8a23ca4: Pull complete
4a9468a1f264: Pull complete
Digest: sha256:9dde4f70f060d58dc83a3fa53f4f9ad89cf7a38858ecffdc1d74289a14c61465
Status: Downloaded newer image for bkimminich/juice-shop:latest
docker.io/bkimminich/juice-shop:latest

┌──(kali㉿kali)-[~]
└─$
```

This process may take a couple of minutes to complete.

Figure 2.35 – OWASP Juice Shop Docker container

7. Next, to start OWASP Juice Shop within Docker, use the following command:

```
sudo docker run --rm -p 3000:3000 bkimminich/juice-shop
```

The following screenshot shows that Docker is starting the OWASP Juice Shop container:

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo docker run --rm -p 3000:3000 bkimminich/juice-shop

> juice-shop@12.8.0 start /juice-shop
> node build/app

info: All dependencies in ./package.json are satisfied (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Detected Node.js version v12.22.1 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Required file server.js is present (OK)
info: Required file index.html is present (OK)
info: Required file styles.css is present (OK)
info: Required file main-es2018.js is present (OK)
info: Required file tutorial-es2018.js is present (OK)
info: Required file polyfills-es2018.js is present (OK)
info: Required file runtime-es2018.js is present (OK)
info: Required file vendor-es2018.js is present (OK)
info: Required file main-es5.js is present (OK)
info: Required file tutorial-es5.js is present (OK)
info: Required file polyfills-es5.js is present (OK)
info: Required file runtime-es5.js is present (OK)
info: Required file vendor-es5.js is present (OK)
info: Port 3000 is available (OK)
info: Server listening on port 3000
```

Figure 2.36 – Starting the OWASP Juice Shop Docker container

To stop the container at any time, use *Ctrl* + *Q* or just hit the *Q* keyboard shortcut.

8. Lastly, to access the OWASP Juice Shop interface, open your web browser within Kali Linux and go to `http://localhost:3000/`, as shown here:

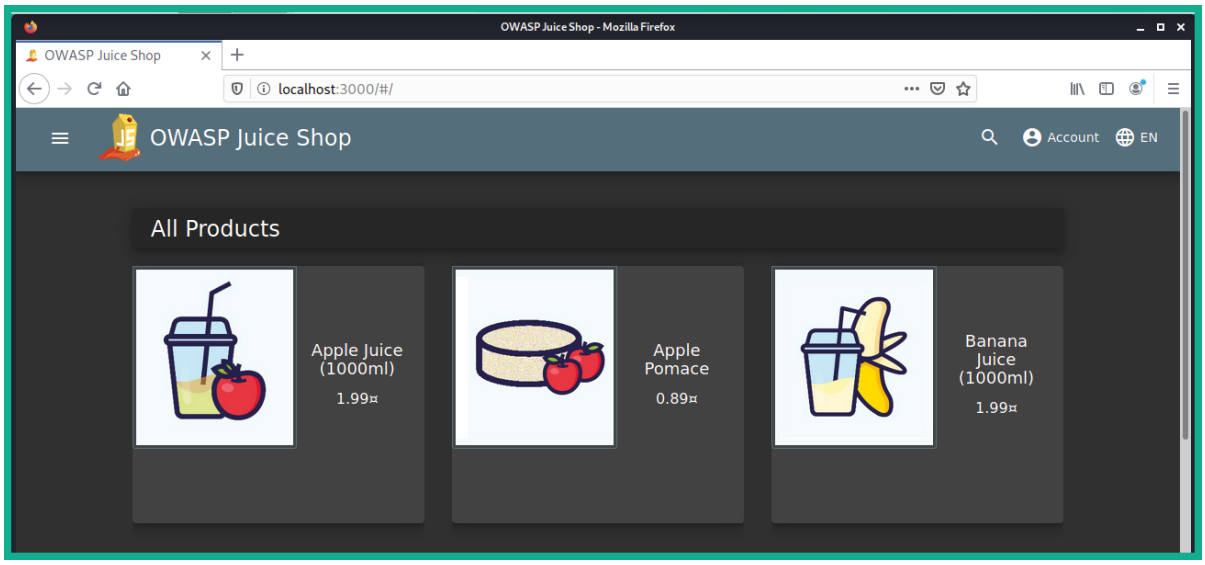

Figure 2.37 – OWASP Juice Shop user interface

Next, let's set up the OWASP Broken Web Applications project as a virtual machine within our penetration testing lab topology.

Part 2 – setting up OWASP Broken Web Applications

The following steps will guide you through the process of deploying the OWASP Broken Web Applications virtual machine as an additional vulnerable platform for honing your skills:

1. Go to `https://sourceforge.net/projects/owaspbwa/files/` and download **OWASP Broken Web Applications version 1.2** onto your system.
2. Extract the contents of the `OWASP_Broken_Web_Apps_VM_1.2.7z` file using the 7-Zip application. Copy the extracted contents (virtual hard disk) to the directory of your other virtual machines.
3. Next, let's create a virtual environment where we can deploy the OWASP Broken Web Applications virtual machine. Open **VirtualBox Manager** and click **New**.
4. When the **Create Virtual Machine** window opens, click on **Expert Mode** to change the configuration view.

5. Next, use the following parameters to create the virtual environment:
   - **Name**: `OWASP BWA`
   - **Type**: **Linux**
   - **Version**: **Other Linux (64-bit)**
   - **Memory size**: `1024` MB

   The following screenshot shows these configuration details:

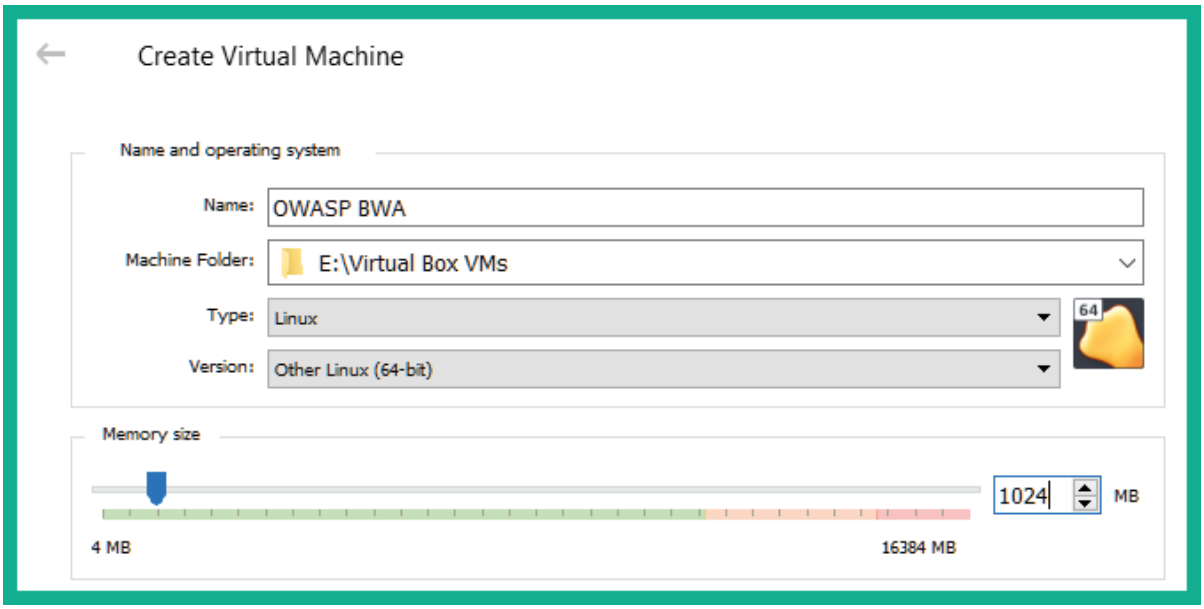

Figure 2.38 – OWASP BWA virtual machine

6. On the same **Create Virtual Machine** window, change the **Hard disk** option to **Use an existing virtual hard disk file** and click the folder icon on the right-hand side to open **Hard Disk Selector**.
7. Next, click **Add** and navigate to the location of the extracted files from *Step 2*. Select the virtual hard disk file called **OWASP Broken Web Apps-cl1** and click **Open**.

8. Select the `OWASP Broken Web Apps-cl1.vmdk` file and click **Choose**, as shown here:

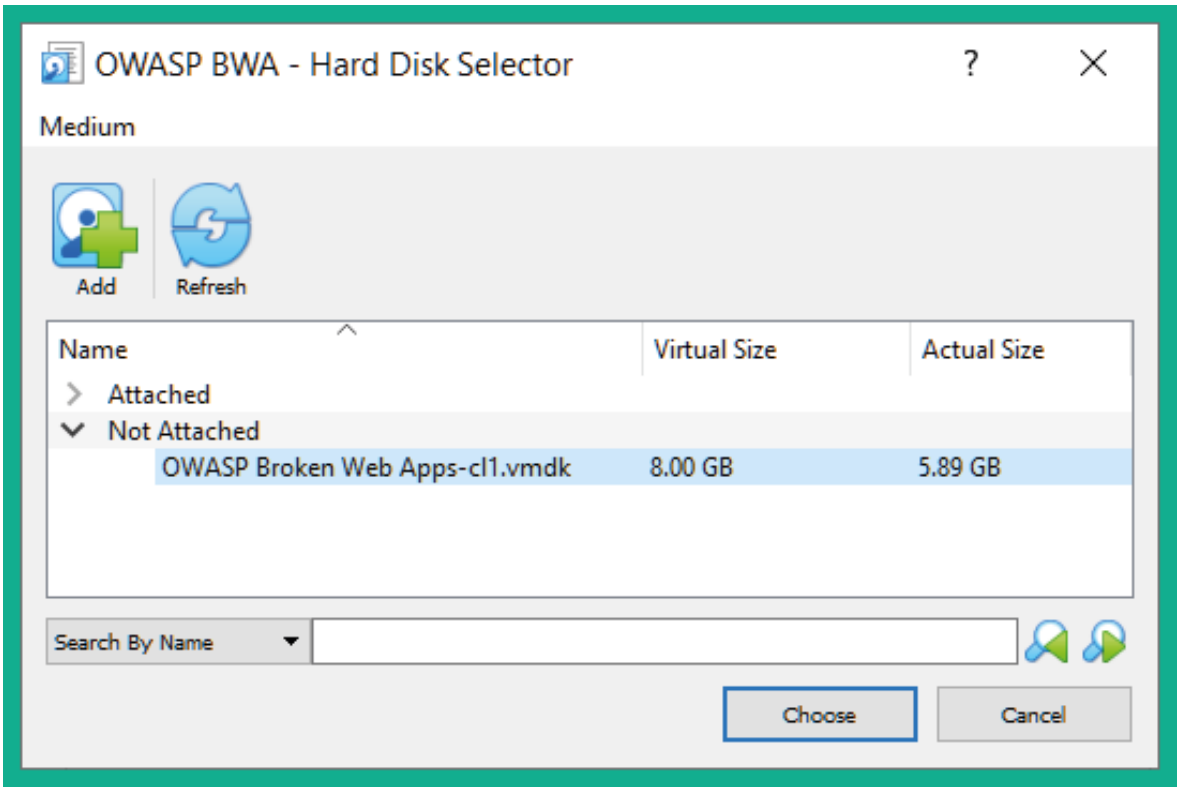

Figure 2.39 – Selecting the virtual disk file

9. At this point, you will be returned to the **Create Virtual Machine** window with the virtual hard disk attached. Simply click on **Create**.
10. Next, select a new OWASP BWA virtual machine within **VirtualBox Manager** and click on **Settings**.
11. Go to the **Network** section, enable **Adapter 1**, and use the following parameters to configure **Adapter 1** so that it's part of the `PentestNet` network of our lab:
    - **Attached to**: **Internal Network**
    - **Name**: `PentestNet`
    - **Promiscuous Mode**: **Allow All**

The following screenshot shows these network configurations:

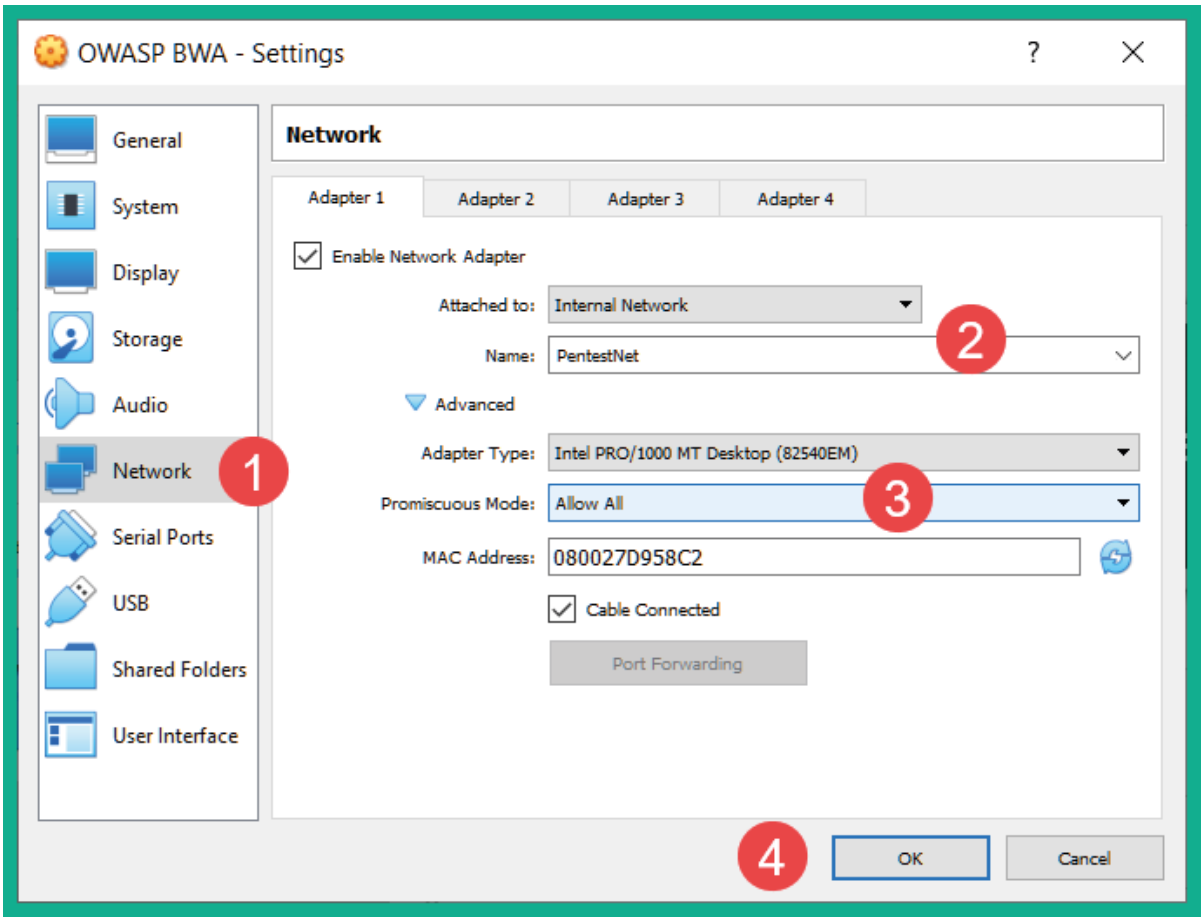

Figure 2.40 – Network adapter configurations

12. Next, power on the OWASP BWA virtual machine; the username for this is `root` and the password is `owaspbwa`. Use the `ip addr` command to verify that the virtual machine is receiving an IP address on the `172.30.1.0/24` network, as shown here:

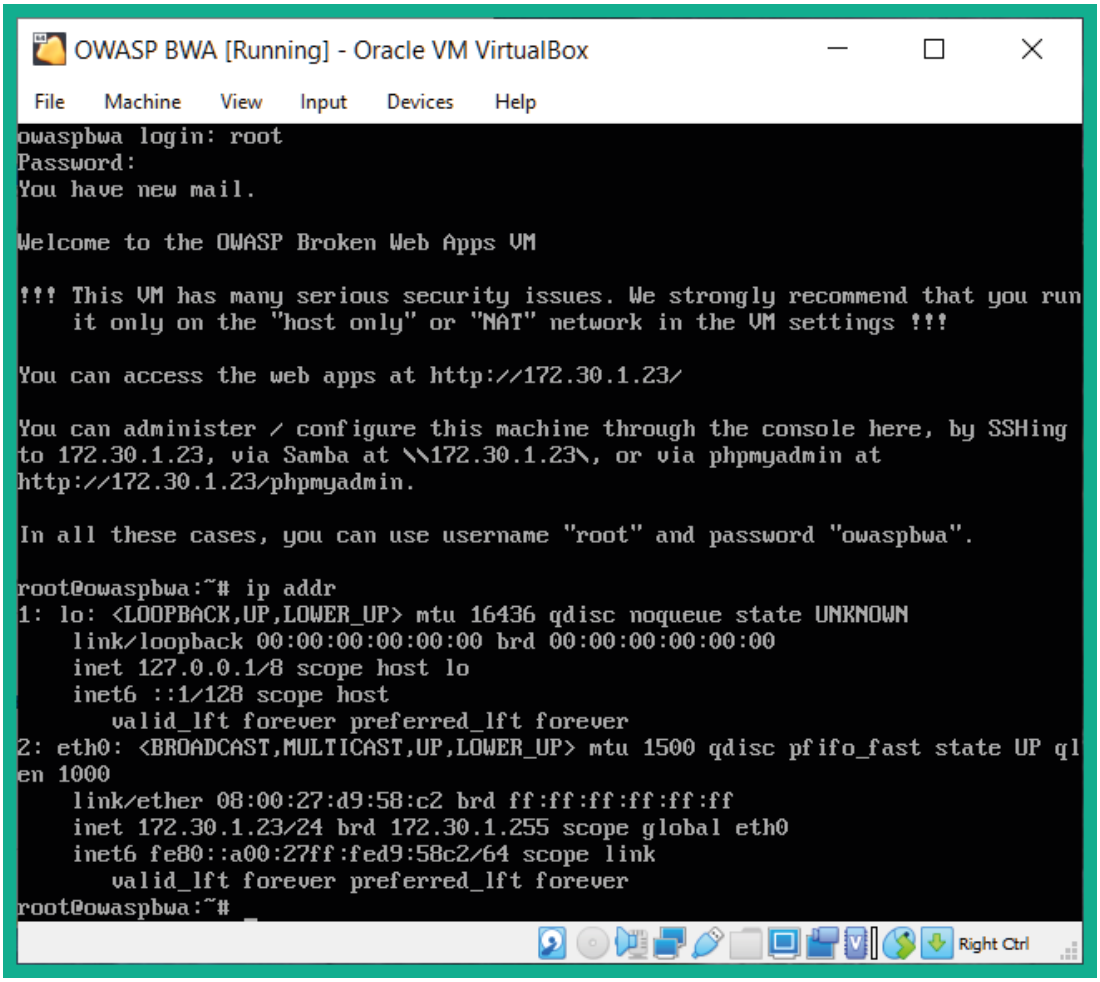

Figure 2.41 – Verifying network connectivity

13. Lastly, to power off the OWASP BWA virtual machine, use the `sudo halt` command.

Having completed this section, you have learned how to set up vulnerable web application environments within our lab to perform web application penetration testing.

Summary

In this chapter, you learned about the importance of building your very own penetration testing lab on your computer. You learned how to use hypervisors to virtualize the hardware resources on a system, which can then be shared with multiple operating systems that are running at the same time on the same system. Furthermore, you have gained the skills needed to set up Kali Linux as a penetration testing virtual machine with vulnerable targets such as Metasploitable 2, as well as with vulnerable web application platforms such as the OWASP Juice Shop and OWASP BWA projects.

I hope this chapter has been informative for you and is helpful in your journey as an aspiring penetration tester, learning how to simulate real-world cyberattacks to discover security vulnerabilities and perform exploitation using Kali Linux. In the next chapter, *Chapter 3*, *Setting Up for Advanced Hacking Techniques*, you will learn how to set up a red team lab environment to perform advanced penetration testing techniques.

Further reading

To learn more on the topics that were covered in this chapter, take a look at the following resources:

- Why secure web-based applications? `https://hub.packtpub.com/why-secure-web-based-applications-with-kali-linux/`
- Kali Linux 2021.2 release information: `https://www.kali.org/blog/kali-linux-2021-2-release/`