ETHICAL HACKING
LAB SERIES

Lab 19: Auditing Linux Systems

Material in this Lab Aligns to the Following Certification Domains/Objectives
SANS GPEN Objective
13: Pentesting via the Command Line

Document Version: 2016-03-09

Contents

Introduction

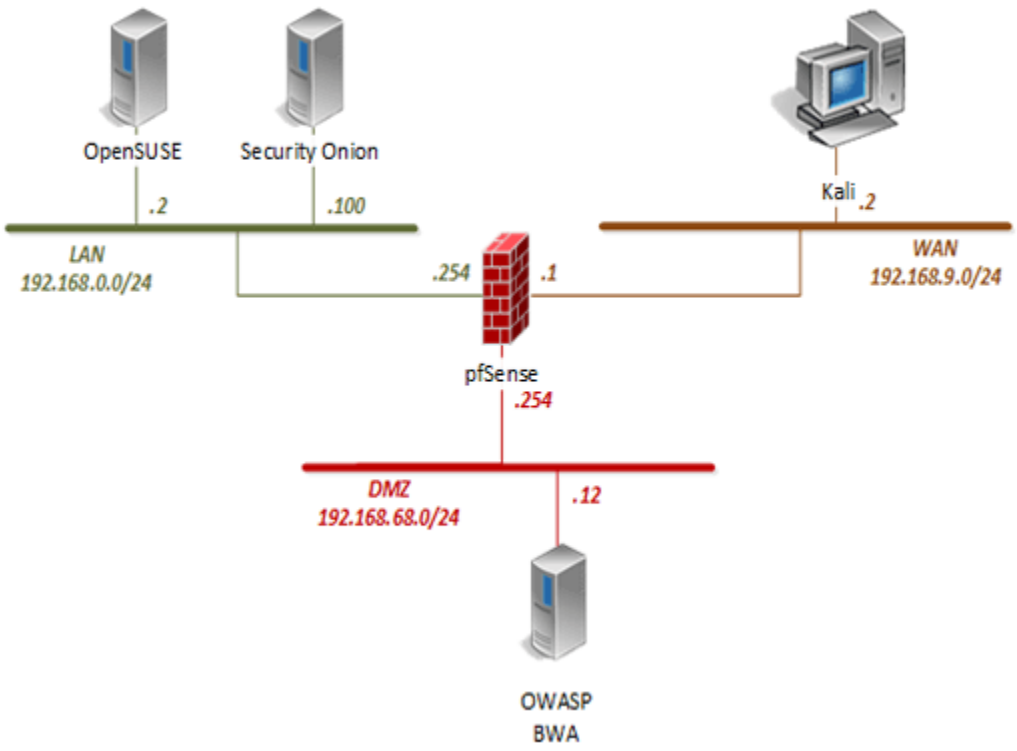
Testing a system for security issues is part of a security assessment. Using the open source tool Lynis in this lab demonstrates how to assess a Linux system and evaluate what vulnerabilities exist in its configuration.

Objective

In this lab, you will be conducting ethical hacking practices using various tools. You will be performing the following tasks:

1. Getting Familiarized with Lynis
2. Auditing with Lynis

Pod Topology



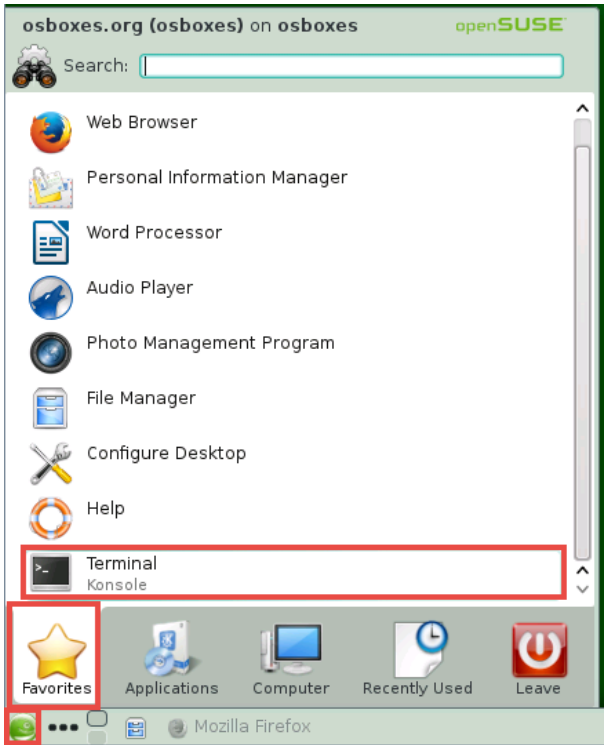
Lab Settings

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

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Kali Linux	192.168.9.2	root	toor
pfSense	192.168.0.254	admin	pfsense
OWASP Broken Web App	192.168.68.12	root	owaspbwa
OpenSUSE	192.168.0.2	osboxes	osboxes.org
Security Onion	n/a	ndg	password123

1 Getting Familiarized with Lynis

1. Click on the **OpenSUSE** graphic on the *topology page*.
2. Enter **osboxes** as the *username*. Click **Next**.
3. Enter **osboxes.org** as the *password*. Press **Enter**.
4. Open the *Terminal* by clicking on the **Application Launcher** and then clicking on the **Terminal** icon.



5. In the *terminal* window, change to the **/home/osboxes/Downloads/lynis** directory. Type the command below followed by pressing the **Enter** key.

```
cd Downloads/lynis
```

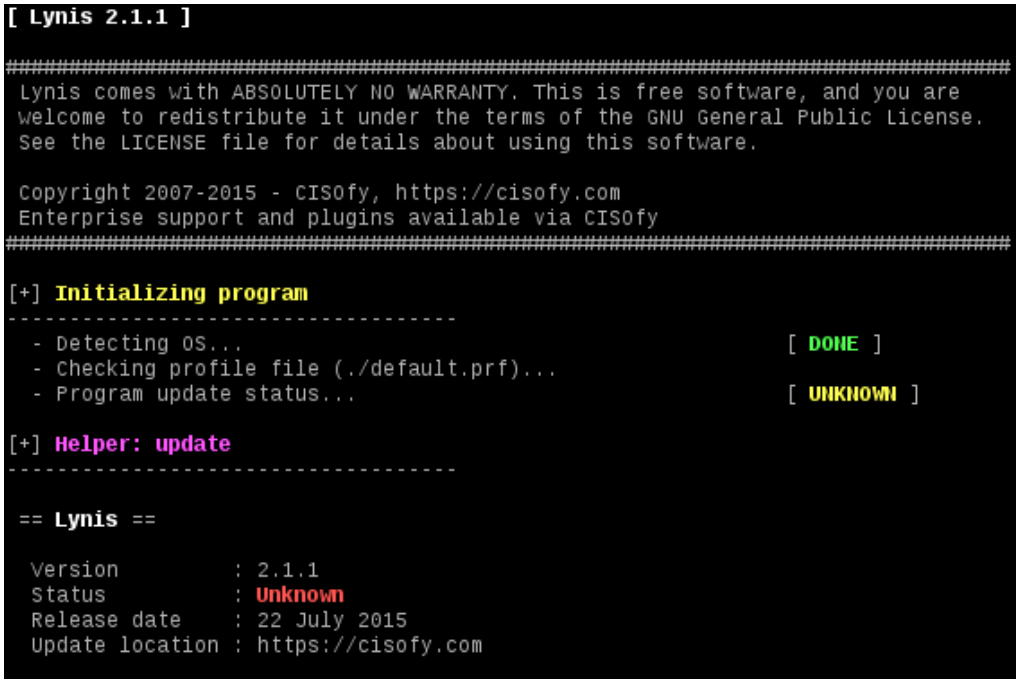
6. Enter the command below to start the **Lynis** application with root privileges.

```
sudo ./lynis
```

7. When prompted for *root's password*, type **osboxes.org** and press **Enter**.
8. Notice the program exits with an error stating that no scanning mode has been specified, this is okay. For the purpose of this step is to observe the available options for the *Lynis* application.

9. Check to see if *Lynis* is up to date by entering the command below.

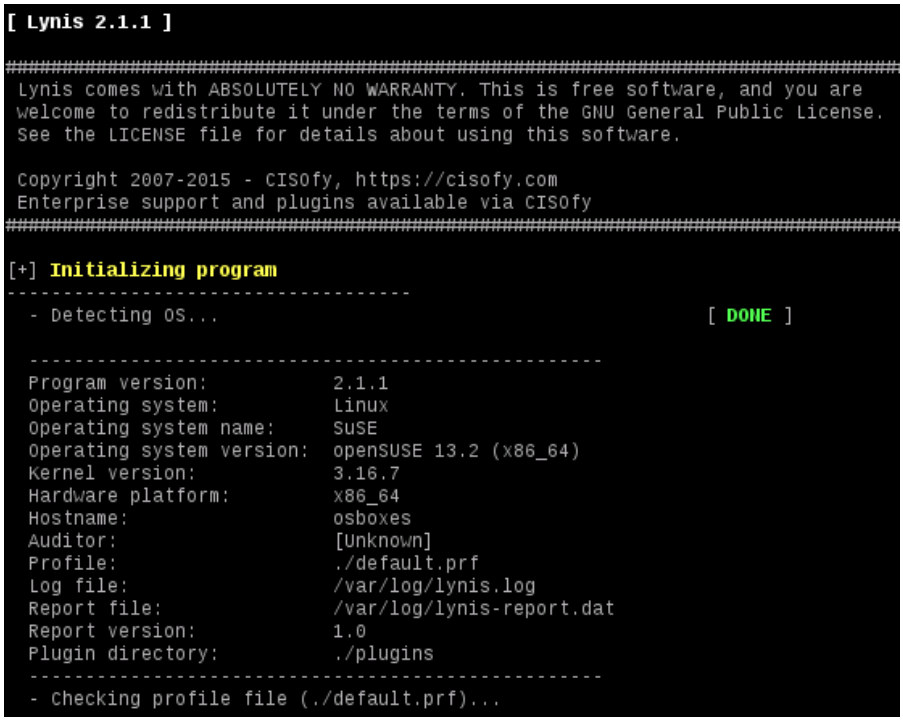
```
sudo ./lynis update info
```



Notice the status is unknown because the VM cannot access the Internet in this environment to check, but do notice the version number is given. At the time of writing this lab module, *Lynis* is up-to-date.

10. Enter the command below to check the tests available.

```
sudo ./lynis --tests "Test-IDs"
```



To navigate, use the **Enter** key when prompted *Press [ENTER] to continue, or [CTRL]+C to stop*. To quit at any given point, press **CTRL+C**.

2 Auditing with Lynis

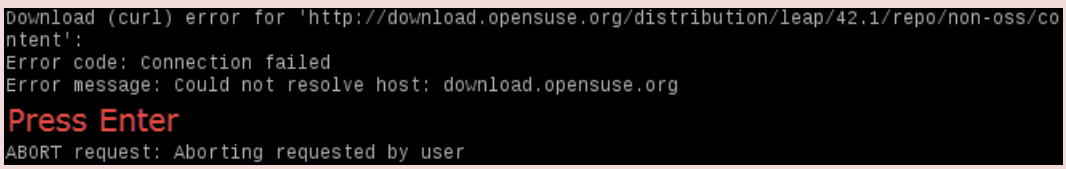
1. Enter the command below to add an auditor.

```
sudo ./lynis -c --auditor "Joe"
```

If prompted for *root's password*, type **osboxes.org**. Press **Enter**.

2. Navigate through the audit using the **Enter** key when prompted *Press [ENTER] to continue, or [CTRL]+C to stop*. When the prompt is not shown, wait for a couple seconds for the program to run its tests. Once completed, a log is created.

Notice that during the audit process, there are a few processes that will attempt to connect to the internet. During these processes, a message will appear (see below). When these error messages appear, press the **Enter** key to signal an "abort request" and to move on with the audit.



3. Enter the command below to pull out the suggestions from the log.

```
sudo cat /var/log/lynis.log | grep Suggestion
```

If prompted for *root's password*, type **osboxes.org**. Press **Enter**.

Notice the suggested recommendations listed to harden the machine.

4. Close the **OpenSUSE** PC viewer.

