Lab - Harden a Linux System

Objectives

- Use a security auditing tool to discover system vulnerabilities.
- Implement recommended solutions to harden the system.

Background / Scenario

Auditing a system for potential misconfigurations or unprotected services is an important aspect of system hardening. Lynis is an open source security auditing tool with an automated set of scripts developed to test a Linux system. Lynis performs an extensive health scan of your system. It includes a detailed report of vulnerabilities and recommended actions. In this lab, you will use Lynis to scan your VM and then implement solutions to harden your system.

Required Resources

PC with the **CSE-LABVM** installed in VirtualBox

Instructions

Step 1: Open a terminal window in the CSE-LABVM.

a. Launch the **CSE-LABVM**.

b. Double-click the **Terminal** icon to open a terminal.

Step 2: Examine the current version of Lynis.

Change to the Lynis directory, and then enter the **sudo ./lynis update info** command to check the update information for Lynis. Enter **password** for the sudo password. This command verifies that this is the latest version and updates for the tool at the time of writing of this lab.

```
cisco@labvm:~$ cd Downloads/lynis/
cisco@labvm:~/Downloads/lynis$ sudo ./lynis update info
[sudo] password for cisco: password

 == Lynis ==

  Version            : 3.0.3
  Status             : Up-to-date
  Release date       : 2021-01-07
  Project page       : https://cisofy.com/lynis/
  Source code        : https://github.com/CISOfy/lynis
  Latest package     : https://packages.cisofy.com/


2007-2021, CISOfy - https://cisofy.com/lynis/

cisco@labvm:~/Downloads/lynis$
```

Step 3: Run the Lynis tool.

a. Enter the **sudo ./lynis --auditor cisco** command. You may or may not need to enter **password** as the password again. The scan will take about a minute to run.

```
cisco@labvm:~/Downloads/lynis$ sudo ./lynis --auditor cisco
```

b. You should receive output for a variety of system features starting with **Boot and services** and ending with **Hardening**, **Custom tests**, and **Plugins (phase 2)**. The next section is the **Lynis 3.0.3 Results**. Your results most likely include the two **Warnings** shown below. You may also receive other warnings. In addition, there will be a section with a listing of **Suggestions**, which lists 51 in the example output below. Only the first suggestion is shown.

```
[ Lynis 3.0.3 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]

<output omitted>
[+] Boot and services
------------------------------------
  - Service Manager                                           [ systemd ]
  - Checking UEFI boot                                        [ DISABLED ]
  - Checking presence GRUB2                                   [ FOUND ]
<output omitted>
[+] Hardening
------------------------------------
    - Installed compiler(s)                                   [ FOUND ]
    - Installed malware scanner                               [ NOT FOUND ]
    - Non-native binary formats                               [ NOT FOUND ]

[+] Custom tests
------------------------------------
  - Running custom tests...                                   [ NONE ]

[+] Plugins (phase 2)
------------------------------------

================================================================================
```

```
  -[ Lynis 3.0.3 Results ]-

  Warnings (2):
  ----------------------------
  ! Found one or more vulnerable packages. [PKGS-7392]
      https://cisofy.com/lynis/controls/PKGS-7392/

  ! iptables module(s) loaded, but no rules active [FIRE-4512]
      https://cisofy.com/lynis/controls/FIRE-4512/

  Suggestions (51):
  ----------------------------
  * Set a password on GRUB boot loader to prevent altering boot configuration (e.g.
boot in single user mode without password) [BOOT-5122]
      https://cisofy.com/lynis/controls/BOOT-5122/
<output omitted>
================================================================================

  Lynis 3.0.3

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)

================================================================================

  [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see
/home/cisco/Downloads/lynis/default.prf for all settings)

cisco@labvm:~/Downloads/lynis$
```

Step 4: Review the results of your scan and address any warnings.

a. Scroll to the **Results** section in the output for your scan.

How many Warnings did you receive?

How many Suggestions did you receive?

b. You should address the warnings. Pick at least one warning and research how to fix that problem. You can use the link provided in the warning output as a starting point for addressing a warning. But you may also need to use your internet research skills to track down additional information.

Which warning are you addressing?

What is your solution?

c. Implement your solution and run the **sudo ./lynis --auditor cisco** command again. If your chosen warning is no longer listed in the **Results** section, then congratulations! You just increased the hardening of your Ubuntu VM. If the warning is still listed, see if you can discover more information to help you get a clean report from Lynis in which the warning is no longer reported.

Answer Key

Step 1: Open a terminal window in the CSE-LABVM.

Step 2: The Lynis Tool

Step 3: Examine the current version of Lynis.

Step 4: Review the results of your scan and address any warnings,

How many Warnings did you receive?

Answers will vary. During testing for this lab, there were 2 warnings.

```
  -[ Lynis 3.0.3 Results ]-

  Warnings (2):
  ----------------------------
  ! Found one or more vulnerable packages. [PKGS-7392]
      https://cisofy.com/lynis/controls/PKGS-7392/

  ! iptables module(s) loaded, but no rules active [FIRE-4512]
      https://cisofy.com/lynis/controls/FIRE-4512/
```

How many Suggestions did you receive?

Answers will vary. There were 51 suggestions in this example.

Which warning are you addressing?

Answers will vary. However, both of the issues shown here can be addressed relatively quickly.

What is your solution?

Answers will vary. However, for the issues listed here visit the recommended link for the first warning, https://cisofy.com/lynis/controls/PKGS-7392/. You will see two commands list: apt-get update and apt-get upgrade. Run these two commands as root to address the vulnerabilities warning. Then run Lynis again to see that the warning is no longer listed.

```
sudo apt-get update
sudo apt-get upgrade
sudo ./lynis --auditor cisco
```

When testing this lab, Firefox needed to be updated with the "apt-get upgrade" command before Lynis would remove the warning.

```
cisco@labvm:~/Downloads/lynis$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
  firefox
1 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 56.4 MB of archives.
After this operation, 953 kB of additional disk space will be used.
```

```
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 firefox amd64
86.0.1+build1-0ubuntu0.20.04.1 [56.4 MB]
Fetched 56.4 MB in 1min 57s (482 kB/s)
(Reading database ... 205661 files and directories currently installed.)
Preparing to unpack .../firefox_86.0.1+build1-0ubuntu0.20.04.1_amd64.deb ...
Unpacking firefox (86.0.1+build1-0ubuntu0.20.04.1) over (86.0+build3-0ubuntu0.20.04.1)
...
Setting up firefox (86.0.1+build1-0ubuntu0.20.04.1) ...
Please restart all running instances of firefox, or you will experience problems.
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for bamfdaemon (0.5.3+18.04.20180207.2-0ubuntu2) ...
Rebuilding /usr/share/applications/bamf-2.index...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
cisco@labvm:~/Downloads/lynis$
```

Note: You may also need to update the Linux distro if you still get a waring. Run the "sudo apt-get dist-upgrade" command to install the latest Linux version. You will need to reboot the system before Lynis will give you a clean report for "vulnerable packages".

To address the second issue about iptables, begin your research by visiting the recommended link for the warning, https://cisofy.com/lynis/controls/FIRE-4512/. Notice that it says to either disable the firewall or populate it with an appropriate firewall. This must mean that iptables has something to do with the VM's firewall. To research further, search for "ubuntu iptables howto". The first link in the search engine results should take you directly to a page at help.ubuntu.com. If you read through the page, you will discover that "Ubuntu comes with ufw - a program for managing the iptables…." This page also has some recommended rules for a basic firewall. The following is a good start on a basic firewall.

```
sudo iptables -A INPUT -i lo -j ACCEPT
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -j DROP
sudo iptables-save
```

However, if you run the "sudo ./lynis --auditor cisco" command again, you will get the same warning. You configured the rules but they are still not active. This is probably because the firewall is not active. Scroll back to the top of the Ubuntu page and click the link for "ufw" or search for "ubuntu ufw". The link will take you to a page that discusses Uncomplicated Firewall (ufw), which is the default firewall configuration tool Ubuntu uses to manage iptables. Read through the page to learn more about ufw. If you check the ufw status, you will see that it is inactive. Might this be why you are still getting a warning from Lynis? Enable the firewall and then run Lynis again. Under Results, you should now see the message, "Great, no warnings".

```
cisco@labvm:~/Downloads/lynis$ sudo ufw status
Status: inactive
cisco@labvm:~/Downloads/lynis$ sudo ufw enable
Firewall is active and enabled on system startup
cisco@labvm:~/Downloads/lynis$ sudo ./lynis --auditor cisco
<output omitted>
```

```
================================================================================

  -[ Lynis 3.0.3 Results ]-

  Great, no warnings
<output omitted>
cisco@labvm:~/Downloads/lynis$
```