Lab – Hardening a Linux System

Objectives

Demonstrate the use of a security auditing tool to harden a Linux 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.

Required Resources

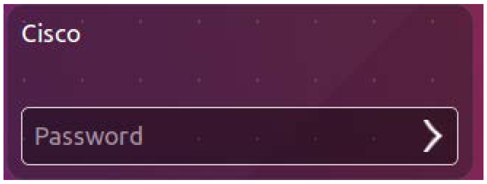
- PC with Ubuntu 16.04 Desktop LTS installed in a VirtualBox or VMware virtual machine.

Step 1: Open a terminal window in Ubuntu.

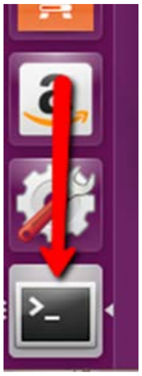
a. Log in to Ubuntu using the following credentials:

User: **cisco**

Password: **password**



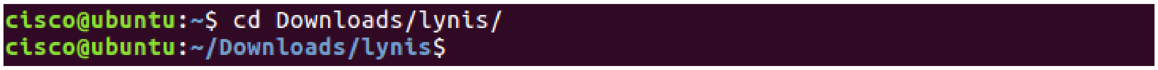
b. Click the terminal icon to open a terminal window.



Step 2: The Lynis Tool

a. At the command prompt, enter the following command to change to the lynis directory:

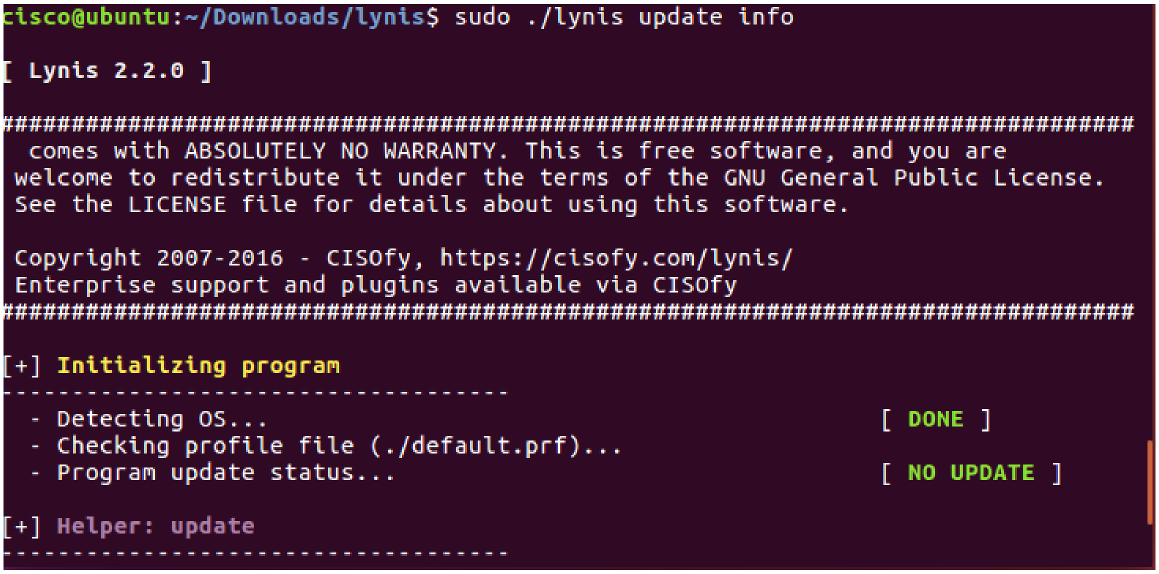
```
cisco@ubuntu:~$ cd Downloads/lynis/
```



```
cisco@ubuntu:~$ cd Downloads/lynis/
cisco@ubuntu:~/Downloads/lynis$
```

b. At the command prompt, enter the following command and enter the password **password** when prompted:

   ```
   cisco@ubuntu:~/Dowloads/lynis$ sudo ./lynis update info
   ```



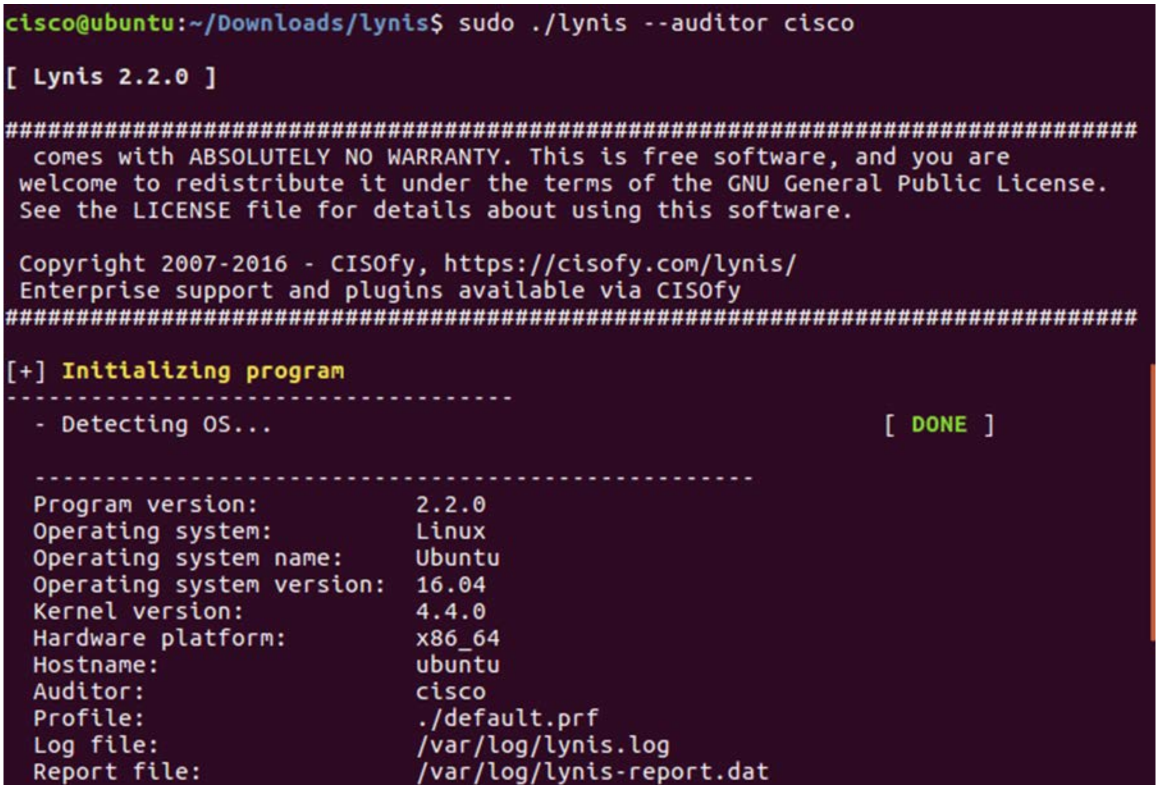
```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis update info

[ Lynis 2.2.0 ]

################################################################################
  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.

 Copyright 2007-2016 - CISOfy, https://cisofy.com/lynis/
 Enterprise support and plugins available via CISOfy
################################################################################

[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profile file (./default.prf)...
  - Program update status...                                  [ NO UPDATE ]

[+] Helper: update
------------------------------------
```

This command verifies that this is the latest version and updates for the tool at the time of writing of this lab.

Step 3: Run the Tool

a. Type the following command in terminal and press **Enter**:

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

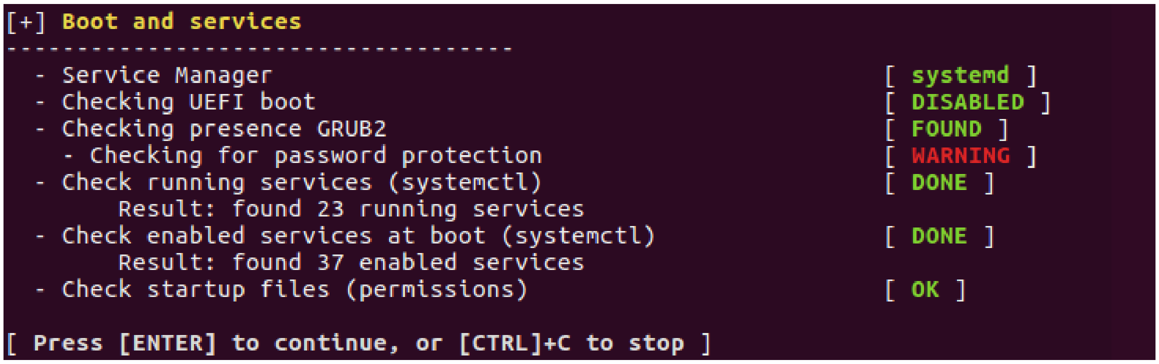


```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis --auditor cisco

[ Lynis 2.2.0 ]

################################################################################
  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.

 Copyright 2007-2016 - CISOfy, https://cisofy.com/lynis/
 Enterprise support and plugins available via CISOfy
################################################################################

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

  ---------------------------------------------------
  Program version:           2.2.0
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  16.04
  Kernel version:            4.4.0
  Hardware platform:         x86_64
  Hostname:                  ubuntu
  Auditor:                   cisco
  Profile:                   ./default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
```

As displayed above, the tool will begin auditing using the user **cisco** as the auditor.

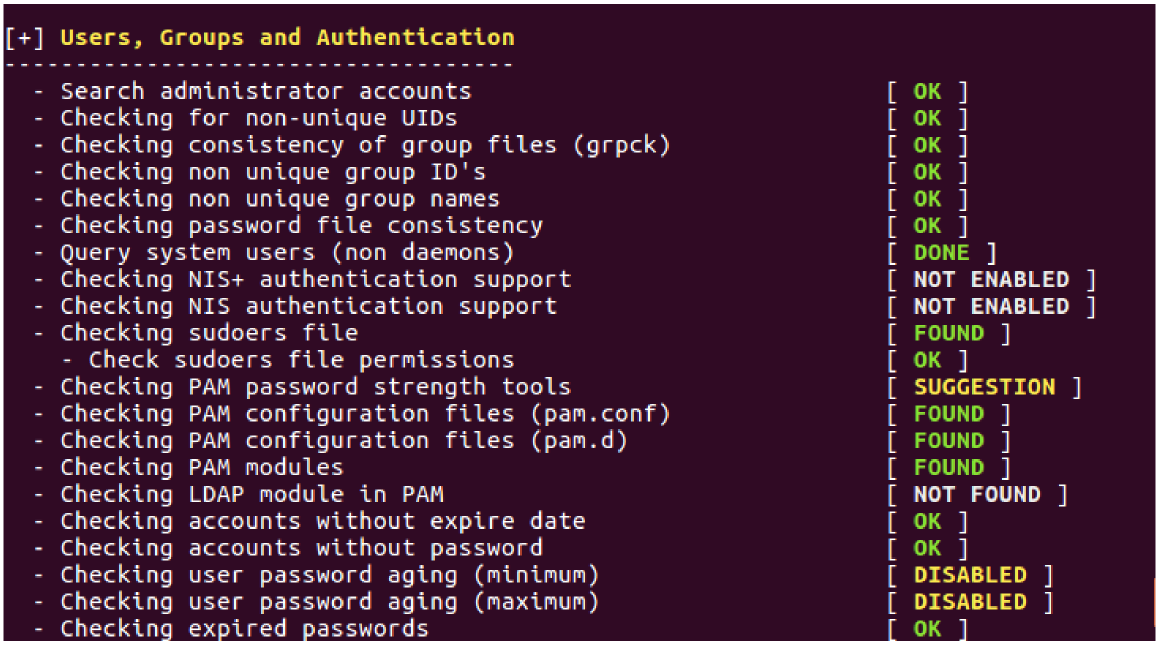
Notice: You will receive **warnings**.

b. To continue with each stage of the audit press **Enter**. You will receive warnings as shown below.



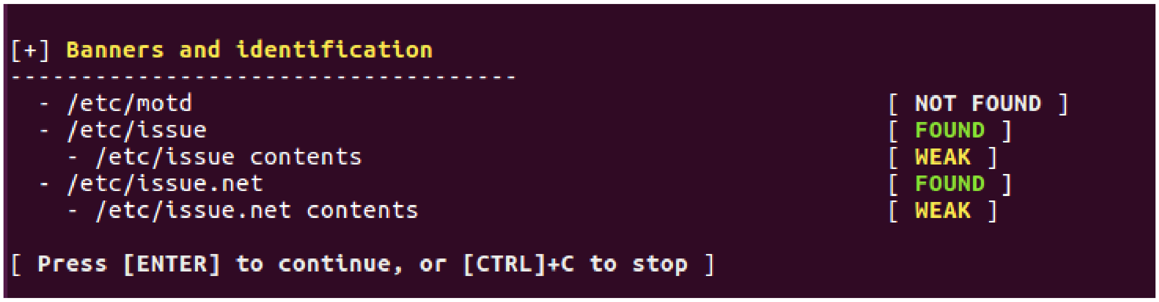
```
[+] Boot and services
------------------------------------
  - Service Manager                                           [ systemd ]
  - Checking UEFI boot                                        [ DISABLED ]
  - Checking presence GRUB2                                   [ FOUND ]
    - Checking for password protection                        [ WARNING ]
  - Check running services (systemctl)                        [ DONE ]
        Result: found 23 running services
  - Check enabled services at boot (systemctl)                [ DONE ]
        Result: found 37 enabled services
  - Check startup files (permissions)                         [ OK ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]
```

c. You will receive suggestions, as shown below.



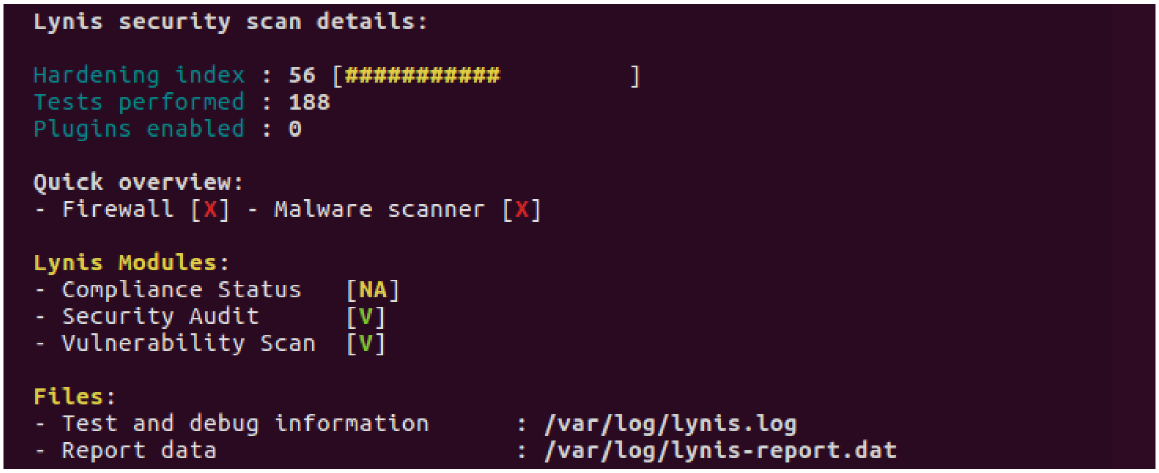
```
[+] Users, Groups and Authentication
------------------------------------
  - Search administrator accounts                             [ OK ]
  - Checking for non-unique UIDs                              [ OK ]
  - Checking consistency of group files (grpck)               [ OK ]
  - Checking non unique group ID's                            [ OK ]
  - Checking non unique group names                           [ OK ]
  - Checking password file consistency                        [ OK ]
  - Query system users (non daemons)                          [ DONE ]
  - Checking NIS+ authentication support                      [ NOT ENABLED ]
  - Checking NIS authentication support                       [ NOT ENABLED ]
  - Checking sudoers file                                     [ FOUND ]
    - Check sudoers file permissions                          [ OK ]
  - Checking PAM password strength tools                      [ SUGGESTION ]
  - Checking PAM configuration files (pam.conf)               [ FOUND ]
  - Checking PAM configuration files (pam.d)                  [ FOUND ]
  - Checking PAM modules                                      [ FOUND ]
  - Checking LDAP module in PAM                               [ NOT FOUND ]
  - Checking accounts without expire date                     [ OK ]
  - Checking accounts without password                        [ OK ]
  - Checking user password aging (minimum)                    [ DISABLED ]
  - Checking user password aging (maximum)                    [ DISABLED ]
  - Checking expired passwords                                [ OK ]
```

d. You will receive a notification for any configuration that is weak as shown below:



```
[+] Banners and identification
------------------------------------
  - /etc/motd                                                 [ NOT FOUND ]
  - /etc/issue                                                [ FOUND ]
    - /etc/issue contents                                     [ WEAK ]
  - /etc/issue.net                                            [ FOUND ]
    - /etc/issue.net contents                                 [ WEAK ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]
```

e. You will receive detailed security enhancement suggestions as well as a final summary which provides the location where you can find the log file.



```
  Lynis security scan details:

  Hardening index : 56 [###########         ]
  Tests performed : 188
  Plugins enabled : 0

  Quick overview:
  - Firewall [X] - Malware scanner [X]

  Lynis Modules:
  - Compliance Status   [NA]
  - Security Audit      [V]
  - Vulnerability Scan  [V]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat
```

Step 4: Review Results

a. Scroll up to the results section after the tool is finished running.

   How many Warnings did you receive?

   How many Suggestions did you receive?

b. Scroll through the suggestions and select one. You will research a suggestion that you can implement to address the issue.

   Which suggestion are you addressing?

   What is your suggested solution?

References

Lynis: https://cisofy.com/lynis/