

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

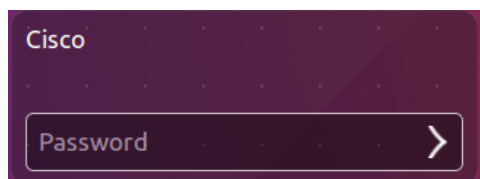
- PC with Ubuntu 16.04 Desktop LTS installed in a VirtualBox or VMware virtual machine.

Step 1: Open a terminal window in Ubuntu.

- Log in to Ubuntu using the following credentials:

User: **cisco**

Password: **password**



- Click the terminal icon to open a terminal window.



Step 2: The Lynis Tool

- 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:~/Downloads/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)... [ NO UPDATE ]
- Program update status...

[+] 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
```

```
cisco@ubuntu: ~/Downloads/lynis
Result: found 45 enabled services
- Check startup files (permissions) [ OK ]

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

[+] Kernel
-----
- Checking default run level [ RUNLEVEL 5 ]
- Checking CPU support (NX/PAE)
  CPU support: PAE and/or NoeXecute supported [ FOUND ]
- Checking kernel version and release [ DONE ]
- Checking kernel type [ DONE ]
- Checking loaded kernel modules [ DONE ]
  Found 48 active modules
- Checking Linux kernel configuration file [ FOUND ]
- Checking default I/O kernel scheduler [ FOUND ]
- Checking for available kernel update [ OK ]
- Checking core dumps configuration [ DISABLED ]
  - Checking setuid core dumps configuration [ PROTECTED ]
- Check if reboot is needed [ NO ]

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

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

```
[+] Plugins (phase 1)
-----
Note: plugins have more extensive tests, which may take a few minutes to complete

- Plugins enabled [ NONE ]

[+] 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 26 running services
- Check enabled services at boot (systemctl) [ DONE ]
  Result: found 45 enabled services
- Check startup files (permissions) [ OK ]

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

[+] Kernel
-----
- Checking default run level [ RUNLEVEL 5 ]
- Checking CPU support (NX/PAE) [ FOUND ]
  CPU support: PAE and/or NoeXecute supported
- Checking kernel version and release [ DONE ]
- Checking kernel type [ DONE ]
- Checking loaded kernel modules [ DONE ]
  Found 49 active modules
- Checking Linux kernel configuration file [ FOUND ]
- Checking default I/O kernel scheduler [ FOUND ]
- Checking for available kernel update [ OK ]
- Checking core dumps configuration [ DISABLED ]
  - Checking setuid core dumps configuration [ PROTECTED ]
- Check if reboot is needed [ NO ]

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

[+] Memory and processes
-----
- Checking /proc/meminfo [ FOUND ]
- Searching for dead/zombie processes [ OK ]
- Searching for IO waiting processes [ OK ]

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

[+] 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 ]
```

```

ubuntu: ~/Downloads/lynis
- Checking Locate database [ FOUND ]

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

+) Storage
-----
- Checking usb-storage driver (modprobe config) [ NOT DISABLED ]
- Checking USB devices authorization [ DISABLED ]
- Checking firewire ohci driver (modprobe config) [ DISABLED ]

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

+) NFS
-----
- Check running NFS daemon [ NOT FOUND ]

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

+) Name services
-----
- Checking default DNS search domain [ NONE ]
- Checking search domains [ FOUND ]
- Checking /etc/resolv.conf options [ NONE ]
- Searching DNS domain name [ FOUND ]
  Domain name: ubuntu
- Checking nsd status [ NOT FOUND ]
- Checking Unbound status [ NOT FOUND ]
- Checking BIND status [ NOT FOUND ]
- Checking PowerDNS status [ NOT FOUND ]
- Checking ypbind status [ NOT FOUND ]
- Checking /etc/hosts
  - Checking /etc/hosts (duplicates) [ OK ]
  - Checking /etc/hosts (hostname) [ OK ]
  - Checking /etc/hosts (localhost) [ OK ]

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

+) Ports and packages
-----
- Searching package managers
  - Searching dpkg package manager [ FOUND ]
  - Querying package manager
  - Query unpurged packages [ FOUND ]
- Checking security repository in sources.list file [ OK ]
- Checking APT package database [ OK ]

- Checking vulnerable packages [ WARNING ]
- Checking upgradeable packages [ SKIPPED ]
- Checking package audit tool [ INSTALLED ]

```



```

buntu: ~/Downloads/lynis
[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] Networking
-----
- Checking IPv6 configuration [ ENABLED ]
  Configuration method [ AUTO ]
  IPv6 only [ NO ]
- Checking configured nameservers
  - Testing nameservers
    Nameserver: 127.0.1.1 [ OK ]
  - Minimal of 2 responsive nameservers [ WARNING ]
- Checking default gateway [ DONE ]
- Getting listening ports (TCP/UDP) [ DONE ]
  * Found 13 ports
- Checking promiscuous interfaces [ OK ]
- Checking waiting connections [ OK ]
- Checking status DHCP client [ RUNNING ]
- Checking for ARP monitoring software [ NOT FOUND ]

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

[+] Printers and Spools
-----
- Checking cups daemon [ RUNNING ]
- Checking CUPS configuration file [ OK ]
  - File permissions [ WARNING ]
- Checking CUPS addresses/sockets [ FOUND ]
- Checking lp daemon [ NOT RUNNING ]

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

[+] Software: e-mail and messaging
-----
- Checking Exim status [ NOT FOUND ]
- Checking Postfix status [ NOT FOUND ]
- Checking Dovecot status [ NOT FOUND ]
- Checking Qmail status [ NOT FOUND ]
- Checking Sendmail status [ NOT FOUND ]

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

[+] Software: firewalls
-----
- Checking iptables kernel module [ NOT FOUND ]
- Checking host based firewall [ NOT ACTIVE ]

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

[+] Software: webserver
-----

```



```

buntu: ~/Downloads/lynis
[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] Software: webserver
-----
- Checking Apache [ NOT FOUND ]
- Checking nginx [ NOT FOUND ]

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

[+] SSH Support
-----
- Checking running SSH daemon [ FOUND ]
- Searching SSH configuration [ FOUND ]
- SSH option: AllowTcpForwarding [ NOT FOUND ]
- SSH option: ClientAliveCountMax [ NOT FOUND ]
- SSH option: ClientAliveInterval [ NOT FOUND ]
- SSH option: Compression [ NOT FOUND ]
- SSH option: FingerprintHash [ NOT FOUND ]
- SSH option: GatewayPorts [ NOT FOUND ]
- SSH option: IgnoreRhosts [ OK ]
- SSH option: LoginGraceTime [ OK ]
- SSH option: LogLevel [ MEDIUM ]
- SSH option: MaxAuthTries [ NOT FOUND ]
- SSH option: MaxStartups [ NOT FOUND ]
- SSH option: MaxSessions [ NOT FOUND ]
- SSH option: PermitRootLogin [ DEFAULT ]
- SSH option: PermitUserEnvironment [ NOT FOUND ]
- SSH option: PermitTunnel [ NOT FOUND ]
- SSH option: Port [ WARNING ]
- SSH option: PrintLastLog [ OK ]
- SSH option: Protocol [ OK ]
- SSH option: StrictModes [ OK ]
- SSH option: TCPKeepAlive [ WARNING ]
- SSH option: UseDNS [ NOT FOUND ]
- SSH option: UsePrivilegeSeparation [ MEDIUM ]
- SSH option: VerifyReverseMapping [ NOT FOUND ]
- SSH option: X11Forwarding [ WARNING ]
- SSH option: AllowUsers [ NOT FOUND ]
- SSH option: AllowGroups [ NOT FOUND ]

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

[+] SNMP Support
-----
- Checking running SNMP daemon [ NOT FOUND ]

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

[+] Databases

```

```
[+] Databases
-----
- MySQL process status [ NOT FOUND ]
- PostgreSQL processes status [ NOT FOUND ]
- Oracle processes status [ NOT FOUND ]

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

[+] LDAP Services
-----
- Checking OpenLDAP instance [ NOT FOUND ]

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

[+] PHP
-----
- Checking PHP [ NOT FOUND ]

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

[+] Squid Support
-----
- Checking running Squid daemon [ NOT FOUND ]

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

[+] Logging and files
-----
- Checking for a running log daemon [ OK ]
- Checking Syslog-NG status [ NOT FOUND ]
- Checking systemd journal status [ FOUND ]
- Checking Metalog status [ NOT FOUND ]
- Checking RSyslog status [ FOUND ]
- Checking RFC 3195 daemon status [ NOT FOUND ]
- Checking minilogd instances [ NOT FOUND ]
- Checking logrotate presence [ OK ]
- Checking log directories (static list) [ DONE ]
- Checking open log files [ DONE ]
- Checking deleted files in use [ FILES FOUND ]

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

[+] Insecure services
-----
```



```
buntu: ~/Downloads/lynis
[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] Insecure services
-----
- Checking inetd status           [ ACTIVE ]
- Checking inetd.conf           [ FOUND ]
- Checking inetd (telnet)       [ WARNING ]

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

[+] 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 ]

[+] Scheduled tasks
-----
- Checking crontab/cronjob       [ DONE ]
- Checking atd status           [ NOT RUNNING ]

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

[+] Accounting
-----
- Checking accounting information [ NOT FOUND ]
- Checking sysstat accounting data [ NOT FOUND ]
- Checking auditd                [ NOT FOUND ]

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

[+] Time and Synchronization
-----

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

[+] Cryptography
-----
- Checking for expired SSL certificates [ NONE ]

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

```
buntu: ~/Downloads/lynis

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

[+] Cryptography
-----
- Checking for expired SSL certificates [ NONE ]

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

[+] Virtualization
-----

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

[+] Containers
-----

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

[+] Security frameworks
-----
- Checking presence AppArmor [ FOUND ]
- Checking AppArmor status [ ENABLED ]
- Checking presence SELinux [ NOT FOUND ]
- Checking presence grsecurity [ NOT FOUND ]
- Checking for implemented MAC framework [ OK ]

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

[+] Software: file integrity
-----
- Checking file integrity tools
- Checking presence integrity tool [ NOT FOUND ]

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

[+] Software: System tooling
-----
- Checking automation tooling
- Automation tooling [ NOT FOUND ]

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

[+] Software: Malware scanners
-----
```

```

buntu: ~/Downloads/lynis
[+] Software: System tooling
-----
- Checking automation tooling
- Automation tooling [ NOT FOUND ]

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

[+] Software: Malware scanners
-----

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

[+] File Permissions
-----
- Starting file permissions check
  /etc/lilo.conf [ NOT FOUND ]
  /root/.ssh [ NOT FOUND ]

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

[+] Home directories
-----
- Checking shell history files [ OK ]

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

[+] Kernel Hardening
-----
- Comparing sysctl key pairs with scan profile
  - kernel.core_uses_pid (exp: 1) [ DIFFERENT ]
  - kernel.ctrl-alt-del (exp: 0) [ OK ]
  - kernel.kptr_restrict (exp: 1) [ OK ]
  - kernel.sysrq (exp: 0) [ DIFFERENT ]
  - net.ipv4.conf.all.accept_redirects (exp: 0) [ DIFFERENT ]
  - net.ipv4.conf.all.accept_source_route (exp: 0) [ OK ]
  - net.ipv4.conf.all.bootp_relay (exp: 0) [ OK ]
  - net.ipv4.conf.all.forwarding (exp: 0) [ OK ]
  - net.ipv4.conf.all.log_martians (exp: 1) [ DIFFERENT ]
  - net.ipv4.conf.all.mc_forwarding (exp: 0) [ OK ]
  - net.ipv4.conf.all.proxy_arp (exp: 0) [ OK ]
  - net.ipv4.conf.all.rp_filter (exp: 1) [ OK ]
  - net.ipv4.conf.all.send_redirects (exp: 0) [ DIFFERENT ]
  - net.ipv4.conf.default.accept_redirects (exp: 0) [ DIFFERENT ]
  - net.ipv4.conf.default.accept_source_route (exp: 0) [ DIFFERENT ]
  - net.ipv4.conf.default.log_martians (exp: 1) [ DIFFERENT ]
  - net.ipv4.icmp_echo_ignore_broadcasts (exp: 1) [ OK ]
  - net.ipv4.icmp_ignore_bogus_error_responses (exp: 1) [ OK ]
  - net.ipv4.tcp_syncookies (exp: 1) [ OK ]
  - net.ipv4.tcp_timestamps (exp: 0) [ DIFFERENT ]
  
```

```

ubuntu: ~/Downloads/lynis
[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] Hardening
-----
- Installed compiler(s) [ FOUND ]
- Installed malware scanner [ NOT FOUND ]

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

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

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

=====

-[ Lynis 2.2.0 Results ]-

Warnings (3):
-----
- Version of Lynis is very old and should be updated [LYNIS]
  https://cisofy.com/controls/LYNIS/

- Found one or more vulnerable packages. [PKGS-7392]
  https://cisofy.com/controls/PKGS-7392/

- Couldn't find 2 responsive nameservers [NETW-2705]
  https://cisofy.com/controls/NETW-2705/

Suggestions (35):
-----
- Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot in single
user mode without password) [BOOT-5122]
  https://cisofy.com/controls/BOOT-5122/
- Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-92
62]
  https://cisofy.com/controls/AUTH-9262/
- Configure minimum password age in /etc/login.defs [AUTH-9286]
  https://cisofy.com/controls/AUTH-9286/
- Configure maximum password age in /etc/login.defs [AUTH-9286]
  https://cisofy.com/controls/AUTH-9286/
- Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
  https://cisofy.com/controls/AUTH-9328/
- Default umask in /etc/init.d/rc could be more strict like 027 [AUTH-9328]
  https://cisofy.com/controls/AUTH-9328/
- To decrease the impact of a full /home file system, place /home on a separated partition [FIL
E-6310]
  https://cisofy.com/controls/FILE-6310/
- To decrease the impact of a full /tmp file system, place /tmp on a separated partition [FILE-

```

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

How many Warnings did you receive? **8**

How many Suggestions did you receive? 35

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?

AUTH-9262

What is your suggested solution?

El sistema necesita comprobar la seguridad de las contraseñas para mantener su robustez, se soluciona implementando un módulo PAM como passwdqc o cracklib.

References

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