Install Lynis

Lynis might be available in your Linux software repository. If so, you can install it using:

```
dnf install lynis
```

or

```
apt install lynis
```

However, if the version in your repo isn't the latest one, you are better off installing it from GitHub. (I am using a Red Hat Linux system, but you can run it on any Linux distribution.) As with all tools, it makes sense to try it out on a virtual machine first. To install it from GitHub:

```
$ cat /etc/redhat-release

Red Hat Enterprise Linux Server release 7.8 (Maipo)

$

$ uname  -r

3.10.0-1127.el7.x86_64

$

$ git clone https://github.com/CISOfy/lynis.git

Cloning into 'lynis'...

remote: Enumerating objects: 30, done.

remote: Counting objects: 100% (30/30), done.

remote: Compressing objects: 100% (30/30), done.

remote: Total 12566 (delta 15), reused 8 (delta 0), pack-reused 12536

Receiving objects: 100% (12566/12566), 6.36 MiB | 911.00 KiB/s, done.

Resolving deltas: 100% (9264/9264), done.

$
```

Once you have cloned the repository, move into it and see what is available. The main tool is in a file called **lynis**. It's actually a shell script, so you can open it and read what it is doing. In fact, Lynis is mainly implemented using shell scripts:

```
$ cd lynis/

$ ls

CHANGELOG.md        CONTRIBUTING.md  db           developer.prf  FAQ
         include  LICENSE  lynis.8  README     SECURITY.md
```

```
CODE_OF_CONDUCT.md  CONTRIBUTORS.md  default.prf  extras         HAPPY_USER
S.md  INSTALL  lynis    plugins  README.md

$

$ file lynis

lynis: POSIX shell script, ASCII text executable, with very long lines

$
```

Run Lynis

Take Lynis out for a spin by giving it a **-h** option to see the Help section:

```
$ ./lynis -h
```

You'll see a short information screen followed by all the commands that Lynis supports.

Next, try out some test commands to get a feel for things and get comfortable. To see which version of Lynis you are working with, run:

```
$ ./lynis show version

3.0.0

$
```

To see all the commands available in Lynis:

```
$ ./lynis show commands


Commands:

lynis audit

lynis configure

lynis generate

lynis show

lynis update

lynis upload-only


$
```

Audit a Linux system

To audit your system's security posture, run the following command:

```
$ ./lynis audit system
```

This runs quickly and returns a detailed report—the output might seem intimidating at first, but I'll walk you through it below. The command's output is also saved to a log file, so you can always go back later and check anything that might be of interest.

Lynis saves the logs here:

```
  Files:

  - Test and debug information      : /var/log/lynis.log

  - Report data                     : /var/log/lynis-report.dat
```

You can verify whether the log files were created, and indeed they were:

```
$ ls -l /var/log/lynis.log

-rw-r-----. 1 root root 341489 Apr 30 05:52 /var/log/lynis.log

$

$ ls -l /var/log/lynis-report.dat

-rw-r-----. 1 root root 638 Apr 30 05:55 /var/log/lynis-report.dat

$
```

Explore the reports

Lynis provides pretty comprehensive reports, so I will cover some of the important sections. The very first thing that Lynis does as part of initialization is to find out complete information about the operating system running on the machine. This is followed by checks to see what system tools and plugins are installed:

```
[+] Initializing program

------------------------------------

  - Detecting OS...                                           [ DONE ]

  - Checking profiles...                                      [ DONE ]


  ---------------------------------------------------

  Program version:           3.0.0

  Operating system:          Linux

  Operating system name:     Red Hat Enterprise Linux Server 7.8 (Maipo)

  Operating system version:  7.8
```

```
  Kernel version:            3.10.0

  Hardware platform:         x86_64

  Hostname:                  example

  ------------------------------------------------------

<<snip>>


[+] System Tools

------------------------------------

  - Scanning available tools...

  - Checking system binaries...


[+] Plugins (phase 1)

------------------------------------

 Note: plugins have more extensive tests and may take several minutes to
complete


  - Plugin: pam

    [..]

  - Plugin: systemd

    [.............]
```

Next, the report is divided into various sections, and each section starts with a **[+]** symbol. Some of the sections can be seen below. (Wow, there are so many areas to audit, and Lynis is the right tool for the job!)

```
[+] Boot and services

[+] Kernel

[+] Memory and Processes

[+] Users, Groups and Authentication

[+] Shells

[+] File systems

[+] USB Devices

[+] Storage
```

[+] NFS

[+] Name services

[+] Ports and packages

[+] Networking

[+] Printers and Spools

[+] Software: e-mail and messaging

[+] Software: firewalls

[+] Software: webserver

[+] SSH Support

[+] SNMP Support

[+] Databases

[+] LDAP Services

[+] PHP

[+] Squid Support

[+] Logging and files

[+] Insecure services

[+] Banners and identification

[+] Scheduled tasks

[+] Accounting

[+] Time and Synchronization

[+] Cryptography

[+] Virtualization

[+] Containers

[+] Security frameworks

[+] Software: file integrity

[+] Software: System tooling

[+] Software: Malware

[+] File Permissions

[+] Home directories

[+] Kernel Hardening

```
[+] Hardening

[+] Custom tests
```

Lynis uses color-coding to make the report easier to parse:

- Green: All good
- Yellow: Skipped, not found, or it may have a suggestion
- Red: You might need to give this a closer look

In my case, most of the red marks were found in the Kernel Hardening section. The kernel has various tunable settings that define how the kernel functions, and some of these tunables may have a security context. The distro may not be setting these by default for various reasons, but you should examine each and see if you need to change its value based on your security posture:

```
[+] Kernel Hardening

------------------------------------

  - Comparing sysctl key pairs with scan profile

    - fs.protected_hardlinks (exp: 1)                           [ OK ]

    - fs.protected_symlinks (exp: 1)                            [ OK ]

    - fs.suid_dumpable (exp: 0)                                 [ OK ]

    - kernel.core_uses_pid (exp: 1)                             [ OK ]

    - kernel.ctrl-alt-del (exp: 0)                              [ OK ]

    - kernel.dmesg_restrict (exp: 1)                            [ DIFFERENT ]

    - kernel.kptr_restrict (exp: 2)                             [ DIFFERENT ]

    - kernel.randomize_va_space (exp: 2)                        [ OK ]

    - kernel.sysrq (exp: 0)                                     [ DIFFERENT ]

    - kernel.yama.ptrace_scope (exp: 1 2 3)                     [ 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)      [ OK ]
    - 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 1)                      [ OK ]
    - net.ipv6.conf.all.accept_redirects (exp: 0)             [ DIFFERENT ]
    - net.ipv6.conf.all.accept_source_route (exp: 0)          [ OK ]
    - net.ipv6.conf.default.accept_redirects (exp: 0)         [ DIFFERENT ]
    - net.ipv6.conf.default.accept_source_route (exp: 0)      [ OK ]
```

Look at SSH, an example, since it is a key area and needs to be secured. There's nothing in red here, but Lynis has a lot of suggestions about hardening the SSH service on my setup:

```
[+] SSH Support
------------------------------------
  - Checking running SSH daemon                               [ FOUND ]
    - Searching SSH configuration                             [ FOUND ]
    - OpenSSH option: AllowTcpForwarding                      [ SUGGESTION
]
    - OpenSSH option: ClientAliveCountMax                     [ SUGGESTION
]
    - OpenSSH option: ClientAliveInterval                     [ OK ]
    - OpenSSH option: Compression                             [ SUGGESTION
]
    - OpenSSH option: FingerprintHash                         [ OK ]
    - OpenSSH option: GatewayPorts                            [ OK ]
    - OpenSSH option: IgnoreRhosts                            [ OK ]
    - OpenSSH option: LoginGraceTime                          [ OK ]
    - OpenSSH option: LogLevel                                [ SUGGESTION
]
    - OpenSSH option: MaxAuthTries                            [ SUGGESTION
]
```

```
    - OpenSSH option: MaxSessions                                [ SUGGESTION
]

    - OpenSSH option: PermitRootLogin                            [ SUGGESTION
]

    - OpenSSH option: PermitUserEnvironment                      [ OK ]

    - OpenSSH option: PermitTunnel                               [ OK ]

    - OpenSSH option: Port                                       [ SUGGESTION
]

    - OpenSSH option: PrintLastLog                               [ OK ]

    - OpenSSH option: StrictModes                                [ OK ]

    - OpenSSH option: TCPKeepAlive                               [ SUGGESTION
]

    - OpenSSH option: UseDNS                                     [ SUGGESTION
]

    - OpenSSH option: X11Forwarding                              [ SUGGESTION
]

    - OpenSSH option: AllowAgentForwarding                       [ SUGGESTION
]

    - OpenSSH option: UsePrivilegeSeparation                     [ OK ]

    - OpenSSH option: AllowUsers                                 [ NOT FOUND ]

    - OpenSSH option: AllowGroups                                [ NOT FOUND ]
```

I do not have virtual machines or containers running on my system, so they show empty results:

```
[+] Virtualization

------------------------------------


[+] Containers

------------------------------------
```

Lynis checks file permissions on some files that are important from a security standpoint:

```
[+] File Permissions

------------------------------------

  - Starting file permissions check

    File: /boot/grub2/grub.cfg                                   [ SUGGESTION
]
```

```
    File: /etc/cron.deny                                        [ OK ]

    File: /etc/crontab                                          [ SUGGESTION
]

    File: /etc/group                                            [ OK ]

    File: /etc/group-                                           [ OK ]

    File: /etc/hosts.allow                                      [ OK ]

    File: /etc/hosts.deny                                       [ OK ]

    File: /etc/issue                                            [ OK ]

    File: /etc/issue.net                                        [ OK ]

    File: /etc/motd                                             [ OK ]

    File: /etc/passwd                                           [ OK ]

    File: /etc/passwd-                                          [ OK ]

    File: /etc/ssh/sshd_config                                  [ OK ]

    Directory: /root/.ssh                                       [ SUGGESTION
]

    Directory: /etc/cron.d                                      [ SUGGESTION
]

    Directory: /etc/cron.daily                                  [ SUGGESTION
]

    Directory: /etc/cron.hourly                                 [ SUGGESTION
]

    Directory: /etc/cron.weekly                                 [ SUGGESTION
]

    Directory: /etc/cron.monthly                                [ SUGGESTION
]
```

Towards the bottom of the report, Lynis offers suggestions based on the report's findings. Each suggestion is followed by a **TEST-ID** (keep this handy for the next part):

```
 Suggestions (47):

  ----------------------------

  * If not required, consider explicit disabling of core dump in
/etc/security/limits.conf file [KRNL-5820]

      https://cisofy.com/lynis/controls/KRNL-5820/



  * Check PAM configuration, add rounds if applicable and expire passwords
to encrypt with new values [AUTH-9229]
```

```
      https://cisofy.com/lynis/controls/AUTH-9229/
```

Lynis provides an option to find more information about each suggestion, which you can access using the **show details** command followed by the test ID number:

```
./lynis show details TEST-ID
```

This will show additional information about that test. For example, I checked the details of SSH-7408:

```
$ ./lynis show details SSH-7408

2020-04-30 05:52:23 Performing test ID SSH-7408 (Check SSH specific defined
options)

2020-04-30 05:52:23 Test: Checking specific defined options in
/tmp/lynis.k8JwazmKc6

2020-04-30 05:52:23 Result: added additional options for OpenSSH < 7.5

2020-04-30 05:52:23 Test: Checking AllowTcpForwarding in
/tmp/lynis.k8JwazmKc6

2020-04-30 05:52:23 Result: Option AllowTcpForwarding found

2020-04-30 05:52:23 Result: Option AllowTcpForwarding value is YES

2020-04-30 05:52:23 Result: OpenSSH option AllowTcpForwarding is in a weak
configuration state and should be fixed

2020-04-30 05:52:23 Suggestion: Consider hardening SSH configuration
[test:SSH-7408] [de
```