

Miles Ogrady

Server Hardening

1. Download and install Lynis (<https://cisofy.com/lynis/>) on both your servers and run it.

Lynis download on Ubuntu server

```
[miles@localhost ~]$ sudo yum install lynis -y
Extra Packages for Enterprise Linux 8 - Next - x86_64      147 kB/s | 179 kB      00:01
Dependencies resolved.
=====
Package                Architecture      Version           Repository         Size
=====
Installing:
  lynis                 noarch            3.0.8-1.el8      epel                307 k
=====
Transaction Summary
=====
Install 1 Package

Total download size: 307 k
Installed size: 1.7 M
Downloading Packages:
lynis-3.0.8-1.el8.noarch.rpm                                939 kB/s | 307 kB      00:00
=====
Total                                                    353 kB/s | 307 kB      00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :                                1/1
  Installing     : lynis-3.0.8-1.el8.noarch        1/1
  Running scriptlet: lynis-3.0.8-1.el8.noarch        1/1
  Verifying      : lynis-3.0.8-1.el8.noarch        1/1

Installed:
  lynis-3.0.8-1.el8.noarch

Complete!
[miles@localhost ~]$
```

Lynis download on centos

```

[miles@localhost ~]$ sudo yum install lynis -y
Extra Packages for Enterprise Linux 8 - Next - x86_64      147 kB/s | 179 kB      00:01
Dependencies resolved.
=====
Package                Architecture      Version           Repository        Size
=====
Installing:
  lynis                 noarch            3.0.8-1.el8       epel               307 k
Transaction Summary
=====
Install 1 Package

Total download size: 307 k
Installed size: 1.7 M
Downloading Packages:
lynis-3.0.8-1.el8.noarch.rpm                               939 kB/s | 307 kB      00:00
-----
Total                                                       353 kB/s | 307 kB      00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :                                1/1
  Installing     : lynis-3.0.8-1.el8.noarch       1/1
  Running scriptlet: lynis-3.0.8-1.el8.noarch     1/1
  Verifying      : lynis-3.0.8-1.el8.noarch       1/1

Installed:
  lynis-3.0.8-1.el8.noarch

Complete!
[miles@localhost ~]$

```

2. Create a short report on the findings (one report for each server) and what you'll do to improve your server setup.

To do a report you want to use `sudo lynis audit system`
 I appended the report to a file and have attached both files

3. Write a script to monitor the health of your server using the commands from the PowerPoints on Security, DFIR and Backups as your base. Think about what info you care about, and how to make it easier for you to read or upload to your dashboard. Data is only good if you're using it for something.

For my health monitor I chose to include **free -m** to show me how much storage is on the server, This is important because it will let me know how much storage is on the server so I can download things. I also backed up a file with `cp`, I backed up my high score file from `bastet(tetris)` and sent it to a new file called `scorebackup.txt`.

To run the script first change the permissions for it to be executable with `chmod 755` then open the shell and type `./health.sh` and a file called `healthreport.txt` and a backup bastet scores will be created.

D) Answer the following: Are they different for each server? the same for both? Are the running instructions any different?

No you can run all of this on both servers with the same commands