Miles Ogrady

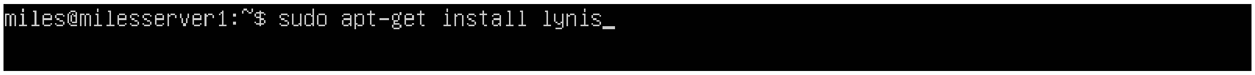
Server Hardening

Github link:

https://github.com/miles5k/healthreport

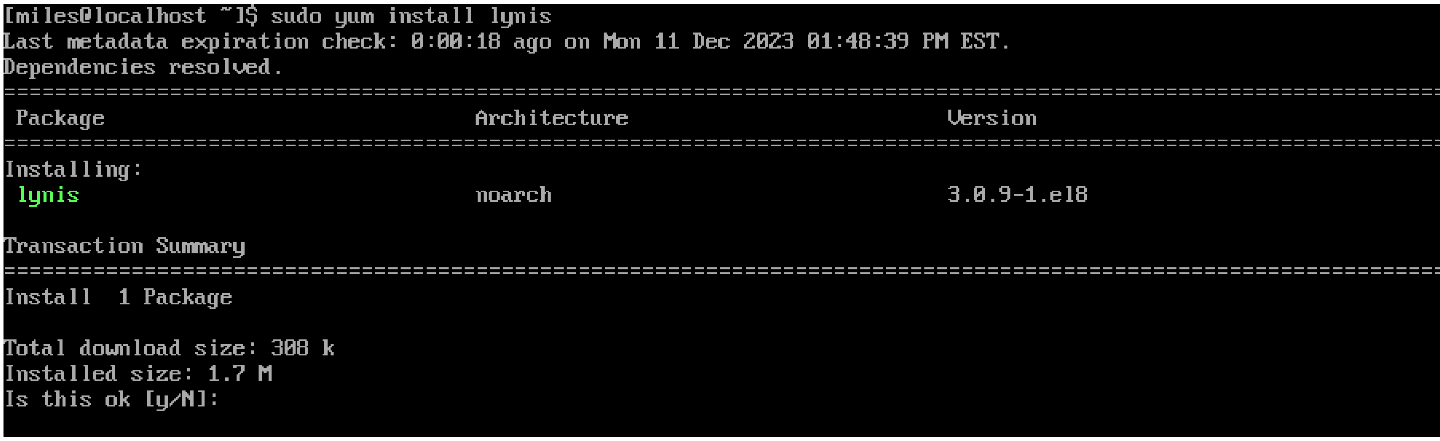
The only changes Iv'e made before doing the report were installing Lynis. I Installed it with the commands (sudo apt-get install lynis) on ubuntu and (sudo yum install lynis -y) on centos

Lynis Installation in ubuntu



```
miles@milesserver1:~$ sudo apt-get install lynis_
```

Lynis Installation in centOS server



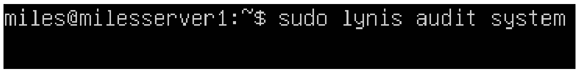
```
[miles@localhost ~]$ sudo yum install lynis
Last metadata expiration check: 0:00:18 ago on Mon 11 Dec 2023 01:48:39 PM EST.
Dependencies resolved.
==========================================================================================================
 Package                            Architecture                       Version
==========================================================================================================
Installing:
 lynis                              noarch                             3.0.9-1.el8

Transaction Summary
==========================================================================================================
Install  1 Package

Total download size: 308 k
Installed size: 1.7 M
Is this ok [y/N]:
```

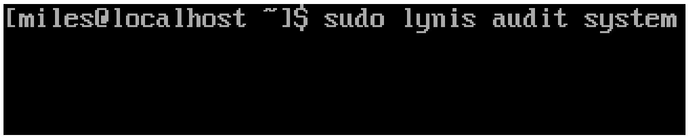
To make a lynis report for your system use the command (sudo lynis audit system)

Report command In ubuntu server



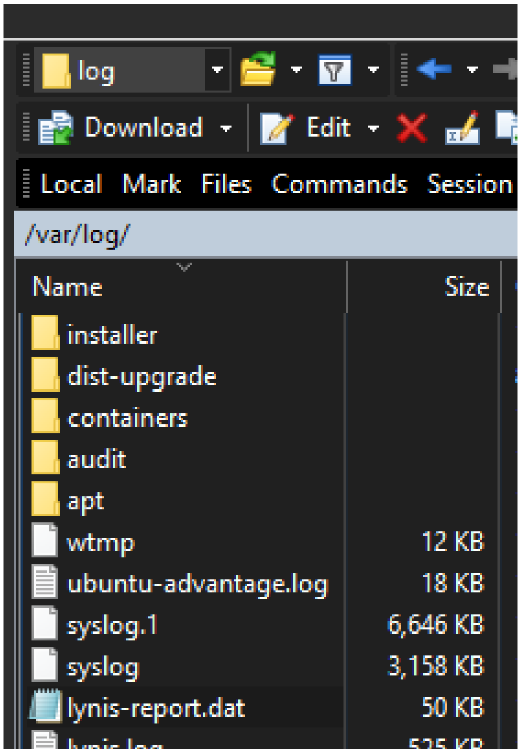
```
miles@milesserver1:~$ sudo lynis audit system
```

Report command in centos server



```
[miles@localhost ~]$ sudo lynis audit system
```

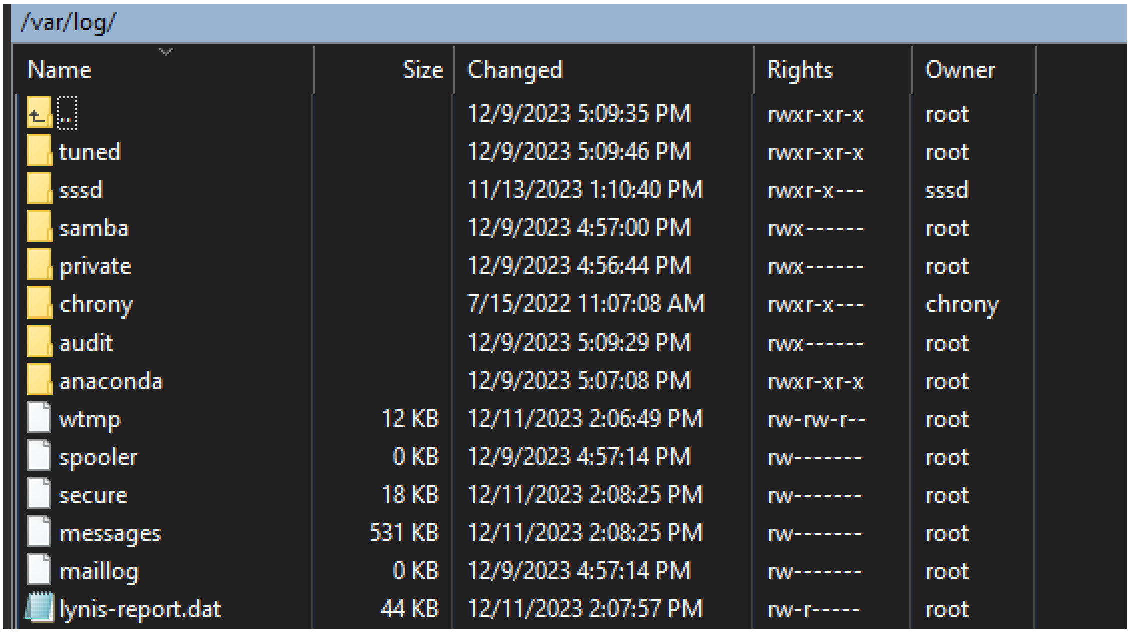
File location in Ubuntu server
The file will be located in /var/log/ and the file will be call lynis-report.dat



/var/log/

Name	Size
installer	
dist-upgrade	
containers	
audit	
apt	
wtmp	12 KB
ubuntu-advantage.log	18 KB
syslog.1	6,646 KB
syslog	3,158 KB
lynis-report.dat	50 KB
lynis.log	525 KB

File location in centos server
The file will be located in /var/log/ and the file will be call lynis-report.dat



/var/log/

Name	Size	Changed	Rights	Owner
..		12/9/2023 5:09:35 PM	rwxr-xr-x	root
tuned		12/9/2023 5:09:46 PM	rwxr-xr-x	root
sssd		11/13/2023 1:10:40 PM	rwxr-x---	sssd
samba		12/9/2023 4:57:00 PM	rwx------	root
private		12/9/2023 4:56:44 PM	rwx------	root
chrony		7/15/2022 11:07:08 AM	rwxr-x---	chrony
audit		12/9/2023 5:09:29 PM	rwx------	root
anaconda		12/9/2023 5:07:08 PM	rwxr-xr-x	root
wtmp	12 KB	12/11/2023 2:06:49 PM	rw-rw-r--	root
spooler	0 KB	12/9/2023 4:57:14 PM	rw-------	root
secure	18 KB	12/11/2023 2:08:25 PM	rw-------	root
messages	531 KB	12/11/2023 2:08:25 PM	rw-------	root
maillog	0 KB	12/9/2023 4:57:14 PM	rw-------	root
lynis-report.dat	44 KB	12/11/2023 2:07:57 PM	rw-r-----	root

1. Health Monitor script.

b.
The health monitor report script is located on my server at home/miles/server_health/health_report.sh

To run the report script use the command sudo ./health_report.sh and will output certain commands in the script to text files.

c. Why I picked the commands I did

I used “logsave mylog who” to show a log of user/date/time

This is important to this script because I want it to show the date/time and the user that runs the script

I used “free -m” to show the storage on the system
This is important to the script because knowing how much free space on a system is important so you know what you can and cannot download.

I used “last miles” to shows logins by this user
This is important in the script because shows when the last time this specif user logged in, so you would know if someone logged in with this user that wasn’t you.

I used “lsmod” to list the modules and shows the status of them so you know everything is Working

I used “dstat -a 2 5” to show sytem stats (to use dstat I hade to use sudo apt-get install dstat, sudo apt-get install pcp) and (sudo yum install dstat, sudo yum install pcp)

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

No, you can run the script on both servers and the instructions are the same. If you are running it on another server you would just change the directory name from “miles” to your own name.