Lynis for CentOS

Getting started with Lynis in CentOS I first had to change into root by using **su – root.** After I was in root I then went and installed Lynis by using the command **sudo yum install lynis** this allowed me to install the Lynis audit tool on my CentOS server. After Lynis is installed I then used the command **lynis audit system** this allowed me to scan the CentOS system and its security defenses.Text

Description automatically generatedText

Description automatically generated

After running the lynis audit command I found some interesting things about my CentOS server. First thing that I found was the boot and services after reviewing the statuses everything on the boot and services seemed okay. The next thing I found was the Logging and files and everything seemed to be running just fine. As you can see in the logging and files screenshot the scan shows if it found any deleted files and, in the result, it says files found. I also checked the warning section, In the warning section I found 2 warnings. The first one was that the system couldn’t find 2 responsive nameserver. The second one was that all jails in fail2ban were disabled. Moving forward with this CentOS server I will need to improve this server by making sure I fix the two warnings that I have and by also making sure the server is more secured by writing more firewall rules maybe even closing ports that are not needed also making sure I have the iptables rules I need in order for my Centos server to communicate with my ubuntu server only.

Text

Description automatically generatedText

Description automatically generatedText

Description automatically generatedText

Description automatically generated