Lynis for Ubuntu

Lynis is an audit tool that allows you to scan your system and its security defenses. The first thing I did was install Lynis, to do so I switched into root by using **su – root.** Once I was in root I then used the command **sudo apt-get install lynis** this allowed me to install the Lynis audit tool.Text

Description automatically generated

After the Lynis installation is complete I then ran the Lynis command that allowed me to scan the system. The command that I used was **lynis audit system,** this command allows me to scan the system and its security defenses.Text

Description automatically generated

While running the command I found interesting things about my ubuntu server. One thing that I found was the boot and services, I noticed that most of these services are not secured, and some are exposed. I also found the software firewall such as iptables kernel module and other firewall rules. I noticed I had an empty ruleset warning meaning I have no rules active for the firewall. I then found logging and files status. In the logging and files, I noticed that it checks for deleted files and looking at my status it had found some deleted files. I also looked at the Networking and the ssh support and everything seemed to be okay. Lastly, I looked at my warning section, in the warning section I only had to issue which was the iptables modules loaded, but no rules active and the other issue was that I didn’t have a set password for root in MYSQL server. Moving forward with this server I plan on improving by making sure I take care of the two warning that I have which is making sure root has a password on MYSQL and also having set some rules for the firewall and I also plan on making sure that most of these services are secured instead of being exposed.

Text

Description automatically generatedText

Description automatically generatedText

Description automatically generatedText

Description automatically generatedText

Description automatically generatedText

Description automatically generated