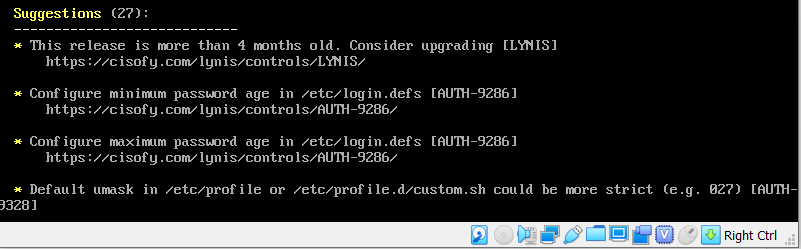
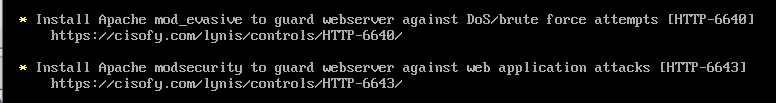
Security, Hardening, and Compliance

Installing and executing Lynis was easy and gave me no issues. I used Lynis to run an audit of my system, I also used the quick scan so I could compare the outputs and see what might be different. Running both ways provided me with similar results. There were a total of 27 suggestions offered for my CentOS VM, while several more were listed for my Ubuntu. I suspect it is because I do most of my work in the CentOS system…



Some of these suggestions could be discarded, such as the first one. Which states the release is more than for months old. If I scrolled up a bit from this screen, it also showed me the latest release which matched the version I have installed. Other suggestions included placing /var/tmp, and /home in a separate partition to prevent exceeding file system capacity and setting minimum and maximum password ages.

Suggestions that I found most useful and decided to implement were to further protect Apache from Dos/DDos attacks, and to use some sort of ARP monitoring tool, like arpwatch.



Dos/DDos are some of the most common attacks and your site going down for any amount of time can have a negative impact. The more you can do to safeguard from these attacks the better. The ARP monitoring tool is another way to keep track of who is on or trying to access your network. The sooner you can identify malicious behavior the better. For the Ubuntu server I will also work to implement other suggestions to try and get it to match a bit more closely to my CentOS VM. Another suggestion I would look into is that of a malware scanner.

