Almely Ramos

Linux Server Audit Report and Improvements

Linux Admin

11/18/19

When I ran the audit command for my system, I released that I had a lot of red flags, a lot of these flags had to do with my security aspects on the server. Most of the red flags point to passwords and my shh and fail2ban and Ip tables.

Update the Lynis application- it might be an old version. It says its 4 months old; I will proceed to update it to its latest release.

**Passwords Configuration Improvements:**

I have to configure the min and maximum password age in order to make the passwords that I make or the passwords that my users make to be safer.

Add a password expire period- Maybe make it for every 2 months that users have to change their password.

Add passwords requirements (cap letters, specific character number)

**IP Table:**

My IP tables are loaded, but I have to make sure to make changes and put some rules on there to harden my system. Fail2Ban go hand in hand with this, I have to me sure that my jails are activated at all times as that will also harden my server security.

**Security:**

SSH- I have to configure shh to prohibit logging in without a password.

Also have adjust the max tries before someone gets locked out of trying for a certain amount of time.

Change the permit root log in to not accepted.

USB drivers that are not in use should be closed; attackers can gain access through there if they aren’t properly closed.

Make sure users know what is going on for the day with a more detailed