Matt Favazza

Security Part 2 setup

To monitor users we need to create a script.

Text

Description automatically generated

Here is the base setup for the script. This creates a header for the text file that is created that includes the date.

Linux has built in commands we can use so we don’t have to write two scripts or modify it when we copy it over to the CentOS machine. So, we will only use those built in commands.

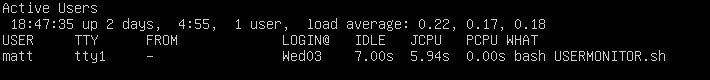
First off, we will list active users, then some of the last login ins, and finally what active users are doing.

We can use the **w**, **last,** and **ps** commands to get this information

Text

Description automatically generated

Here we use **w**, which lists out the uptime of the machine, who is logging in and from where, their impact on the system and what they are doing.



Next we have **last -20**. This goes through the **/var/log/wtmp** file, which is the successful log in file, and lists out logins, where they logged in at what time/date, and if they are logged in still or not.

Text

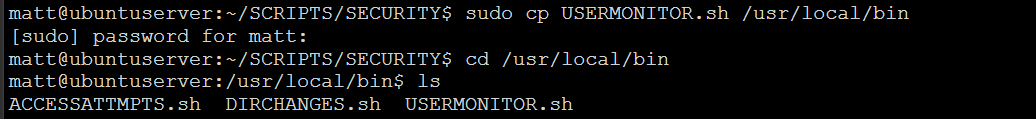
Description automatically generated with low confidence

And finally the **ps -ef** command shows the user, and what process they are running. We have two **sed** command to remove **root** and **www-data** to remove entries related to root and apache operations.

Graphical user interface, text

Description automatically generated

Next we need to move this to the file where the other automated scripts go, which is the **/usr/local/bin** directory.



Now to add it to the **crontab** file. Type **crontab -e** and add it to the list. To have a job run every two hours we can use \*/2. Finally, at the end of the week I want to delete the text file the script makes every Friday night at 5pm, which is the 17th hour in the 24 hour format. We want to delete this file otherwise the file will become enormous very quickly since it can generate a lot of output if there are several users in the system.

Text

Description automatically generated

Now, if we suspect users are being made or removed, we can check the text file, and see with two hour windows, who is logged in and what they are doing. Having the header in the start is especially important because now we can see when the script was exactly ran.

Text

Description automatically generated

Now we can try this out on the CentOS server.

Text

Description automatically generated

And since we only used built in commands, we do not need to modify this script and everything seems to be working as expected.