Matt Favazza

Security Part 1 CentOS

For this part of the assignment I’ve uploaded the same scripts I made on the ubuntu server to the CentOS server and ran them to test. We will use this as a base. If we run the script as is we get this as an output.

Text

Description automatically generated

Already we can see that the ACCESSATTMPTS and HIDDENFILES scripts need to be altered to better suite this machine.

In CentOS failed log in from SSH are stored in /var/log/secure so well need to modify the script to work.

A screenshot of a computer

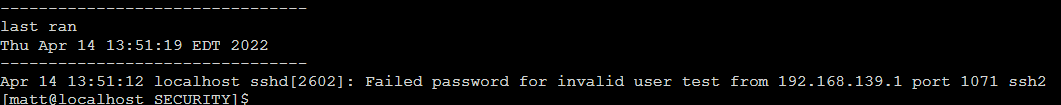
Description automatically generated with medium confidence

And a quick test,

Text

Description automatically generated

The last entry is from after we changed the script, and we can see there have been no failed attempts to log in. But now if we fail to log in,



The access attempts script works by scanning the **/var/log/secure** file and uses **grep** to search for two keywords “Failed password” and “from”. This filters out failed password attempts from an IP address that tried to connect to the server.

The directory change script does not need to be modified, but works in the same way as the Ubuntu script. It creates a temporary file and runs a checksum using the sha1sum command, and filters out the output using sed.

The next script we need to modify is the hidden files script.

CentOS has the same files we want to examine except the ‘lost+found’ directory. So we can just delete that line from the script.



Now when we run we don’t have any errors.

This script works by using the **find** command which searches for filenames that start with “.” and lists them out. We use this command on every main directory in the system.

To automate these tasks, we can still use cronjobs. This time I want to have all three scripts automated. The access attempts, and directory changes running weekly and the hidden files monthly.

All three scripts are going to need to be copied to the /usr/local/bin directory.

Graphical user interface, text

Description automatically generated

Now we can set up the cronjobs. Type **crontab -e** and you’ll be presented with a blank editor.

Here I put the same guide in as the Ubuntu Server

A computer screen capture

Description automatically generated with medium confidence

Then we can add our scripts to be ran

Text

Description automatically generated

To save and exit this file, press ‘esc’ on the keyboard and type **:wq**