Joel Lantigua

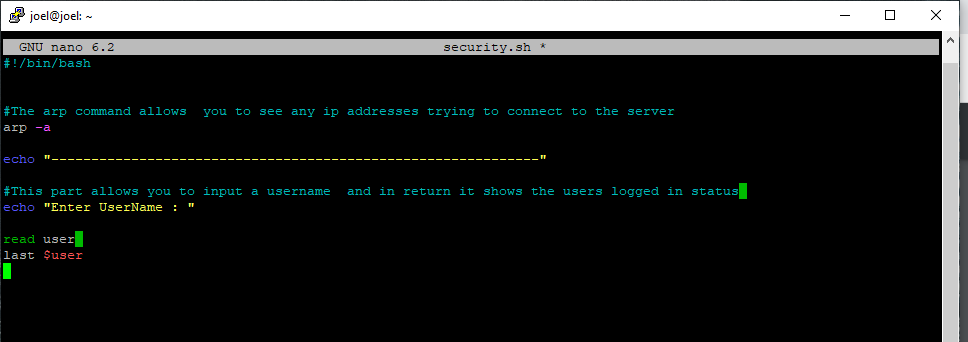
Linux Administrator

Scripts for security 1

11/12/22

Ubuntu Scripts For Security part 1

On my ubuntu server the first thing I did was use the nano command followed by the name of my script, in this case it’s **security.sh**. After the nano opens, I started with **# !/bin/bash** at the very top. After I inserted an **arp-a** command allowing the script to show any local addresses my server has communicated with. Next, I inserted a command that checks a user’s login. I used the command **echo “Enter UserName : ”** followed by  **read user**  & **last $user.** This command asks for an input which is a username that has been already created on the server, I inserted **joel** as you can see in the screenshots below



This Screenshot below shows the command that I used to run the script which was **./security.sh**. once I hit enter you can see the **arp -a** command work. Next the script asks for a username input in my case I entered joel.

Text

Description automatically generated

In this screenshot below you can see the user **Joel**’s login dates Graphical user interface, text

Description automatically generated

Next, I created a script that detects changes to **/var/log** and **/etc/**  The script also monitors hidden files changes. First thing I used was the nano command followed by a new script name called **changes.sh.** Once the nano opened the file, I started with **#!/bin/bash** at the top. I then used the command **find /var/log -type f -mtime +7**  to search for any **/var/log** changes in the last 7 days. The **-type f**  means file. Next the **-mtime +7** means to find anything that was modified in the last 7 days. The next command that I used in this script was **sudo find / -type f -name “.\*” -mtime +7** to find hidden files changes in the last 7 days. In this command since we are looking for hidden files i used  **-name** followed by **“.\*”** allowing me to search by name. hidden files are named **“.\*”.** next I added the **-mtime +7** to show any changes in the last 7 days. The last command I used in this script was **find /etc/ -type f -mtime +7** this allows me to seach for any changes in the last 7 days on **/etc/** files.

Text

Description automatically generated

This screen shot below shows changes in **/var/log** files in the last 7 daysText

Description automatically generated

This screenshot below shows any changes to any hidden files in the last 7 days Text

Description automatically generated

This screenshot below shows any changes to **/etc/** files in the last 7 days Text

Description automatically generated

Next I sent both scripts to my CentOS server by using the command **scp/home/joel/scurity.sh** [**joel@192.168.241.146:home/joel**](mailto:joel@192.168.241.146:home/joel)this command allowed me to send this script to my CentOS server

****

Next to send my other script to my CentOS server I used the same command but just changed the script name. **scp/home/joel/changes.sh** [**joel@192.168.241.146:home/joel**](mailto:joel@192.168.241.146:home/joel)

Text

Description automatically generated

**Work Cited**

<https://quickref.me/find>

<https://www.cyberciti.biz/faq/unix-linux-check-last-time-user-loggedin-command/>