**CentOS Security Scripts**

**Scripts**

All scripts I had to change permission **u+x** then the script name in order to execute

**Comp 1 and 2**

The following scripts are for the second portion asking to detect changes in a directory I did **/var/log** and I decided to detect changes in that file I did it in two scripts **compOne.sh** and **compTwo.sh** the first portion of the code is relatively simple and consists of a command an simple command as shown in this screenshot

A computer screen shot of white text

Description automatically generated

This takes the hash of all files in **/var/log** using an asterisk for a wild card and appends and overwrites to a file in **/home/dlara/reports/base.txt** (reports directory is made in the security script see more below)

Next we go to the second part in **compTwo.sh** of the script where I do the same in **compOne.sh** but then compare the file made in **compOne.sh** two the file **compTwo.sh** to compare differences in hash it then appends the output of the command to **/home/reports/changes.txt** the if statement checks if there is anything in that file as if the contents are the same the diff command will output nothing if there something in the **changes.txt file** it will echo that changes were detected else it will echo that there were no changes detected

A screen shot of a computer code

Description automatically generated

Scripts in action:

A computer screen shot of a program

Description automatically generated

A computer screen with numbers

Description automatically generated

(Contents of changes.txt)

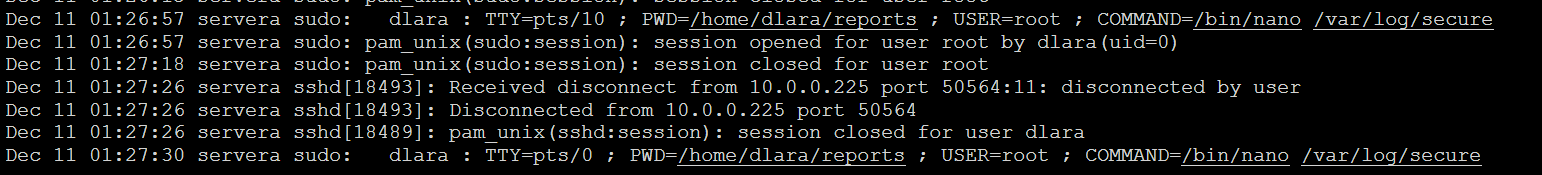
**Security Script**

The next script is the main security script detecting red flag behavior as seen below

A screenshot of a computer program

Description automatically generated

The following sed commands are used to filter out any line that detects commands being used in the log files as that is something that is captured in stored in the log files



The first thing this script does is see if the directory **reports** exists this where the files that will be detecting different portions of the code will be stored the if statement checks if the directory exists it will echo a message saying that the script will begin or else it will make the directory and echo a message saying so assuming it is for first time use it will then do the following procedures make sure you have sudo privileges.

**sudo grep -E "0[0-6]:[0-9]{2}:[0-9]{2}" /var/log/secure >> "$DIR/12to6.txt/**

This command uses searches for the pattern of characters in the quotes which is a regular expression to find the time between 12 AM to 6 AM in the file **/var/log/secure** which is where authentication related activity is stored this is concerning because ideally speaking I should and other users should be using it during the day time so there is no reason for anyone to be using this server during that time anything the command finds will be output to **reports/12to6.txt**

A screen shot of a computer screen

Description automatically generated

(Contents from 12to6.txt)

**sudo last -f /var/log/btmp | grep -v -e "serverb" -e "10.0.0.225" >> "$DIR/unknownusers.txt"**

This command uses **last -f** in the file **/var/log/btmp** which is where failed logins are stored I then pipe and use a grep commands to not get outputs from **serverb** which is a hostname for the **10.0.0.83** which is my ubuntu server address which I trust and and my **10.0.0.225** address which is my host address. This portion is meant to detect attempts from unknown ip addresses who could be attempting to access for malicious reasons. to test the effectiveness of this script I made another ubuntu server called serverc and have made a login attempt this command will outputs failed login attempts from that servers ip and not the others and append the output to **unkownusers.txt**

A screenshot of a computer

Description automatically generated

(Results from unknownusers.txt)

**sudo grep -E "password check failed" /var/log/secure >> "$DIR/failedlogins.txt"**

**sudo grep "authentication failure" /var/log/secure >> "$DIR/reportsauthfail.txt"**

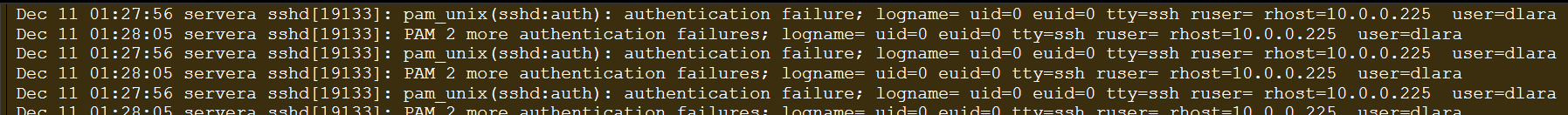
These two commands do similar things but differently the first command on **password check failed** checks for any lines lines in **/var/log/secure** which tracks any login related activity this command is used to append any wrong password attempt and appends to the text file **failedlogins.txt**

A screen shot of a computer

Description automatically generated

(Results from failedlogins.txt)

The next command is also for failed logins but the quotes **“authentication failure”** is for failed logins as after 3 failed login attempts it stops the login and logs in as a failed login after 3 attempts and you have to ssh again in order to attempt to logins. Tracking both of these are important to see if any malicious actors are trying to access the server so keeping tabs on failed passwords and failed authentication could provide insight on any attempt.



(from reportsauthfail.txt)

**sudo grep "closed" /var/log/secure >> "$DIR/closed.txt"**

This command uses grep to search for the pattern **closed**  in **/var/log/secure** this will mainly show any closed sessions but also in the event of a ddos attack show any connections closed the contents of this command is appended to **closed.txt**

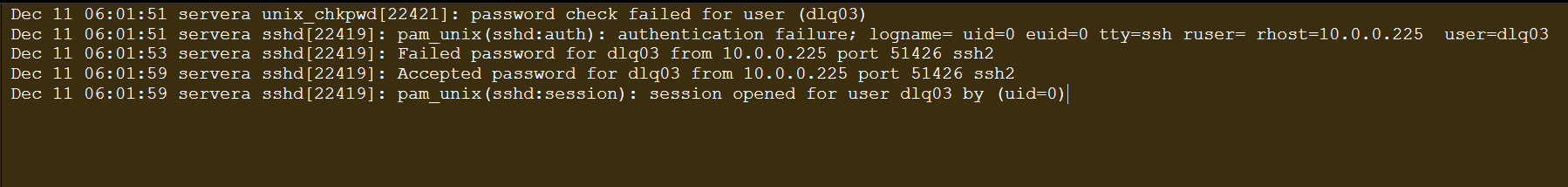
A screen shot of a computer screen

Description automatically generated

(from closed.txt)

**sudo grep "dlq03" /var/log/secure >> "$DIR/dlq03.txt"**

This command appends any login activity for the user dlq03 into the file **dlq03.txt** this account was made for my ubuntu server to connect to but since my centos and ubuntu server do not currently have a reason to connect with each other aside from communication this account is abandoned and not used and as such there should not be much activity coming from such user so it may be worth monitoring activity.



**Conclusion**

Overall while these scripts are serviceable with what they can do I do believe that this is only good for the current setup which is a private local server within my computer. If I want to expand my servers, I definitely need to up my scripts and set up routine cron jobs to monitor my server activity especially for things like web server traffic and for if I want to expand my server and services for Linux administration. Alternatively, I could try to use cron or scripts to utilize my firewalls on both of my servers to detect malicious activity.

<https://www.getastra.com/blog/security-audit/web-server-security/>

<https://www.cisco.com/site/us/en/learn/topics/security/what-is-user-security.html>

<https://www.redhat.com/sysadmin/firewalld-linux-firewall>

**Sources**

<https://askubuntu.com/questions/61826/how-do-i-check-the-sha1-hash-of-a-file>

<https://superuser.com/questions/98825/how-to-check-if-a-directory-exists-in-linux-command-line>

<https://serverfault.com/questions/430895/finding-latest-successful-logins-and-failed-attempts-to-a-centos-server>