Nathan Christensen-Padilla

Adrianna Holden-Gouveia

Linux Administration

12/13/2021

Security Scripts pt.1 CentOS

I installed inotify-tools so I could monitor hidden files and root executables and see what changes were made to them. I did this by using the command sudo yum install inotify-tools and then entering y to confirm the download. That’s all you need to install it.

Text

Description automatically generated

1. My first command in my security scripts is used to see activity that occurred from midnight to 9am since that’s usually when I’m asleep.

Text

Description automatically generatedA screen shot of a computer

Description automatically generated with medium confidence

My Next command is used to look at logins not from myself.

Text

Description automatically generated

Graphical user interface

Description automatically generated with medium confidence

My Third command is used to see failed login attempts not from my IP address. Text

Description automatically generated

Text

Description automatically generated

1. This command detects changes to the /etc directory by using the hash

Text

Description automatically generated

I added these three commands so I could capture the output of the file and direct it to a log file.

Text

Description automatically generated

Output of script:

Graphical user interface

Description automatically generated with medium confidence

A picture containing text

Description automatically generatedText

Description automatically generated

Also if you haven’t done so already use the command chmod +x ./SecurityScript on the file so it can be executable.



1. To monitor files and my root executables I used the inotifywait command to constantly monitor the directory, and so this doesn’t hinder my work on the server I use the commands ctrl + alt + f2 to open up a new terminal window and then I login and execute the script.

Text

Description automatically generated

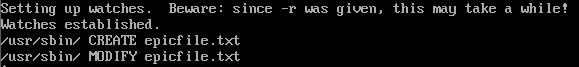


Then I create a new file in the /usr/sbin directory name epicfile.txt to make sure the script is working.



A picture containing text

Description automatically generated



After that I can use the stat command on the file to see who made changes to the file and when.Text

Description automatically generated

Also if you haven’t done so already use the command chmod +x ./MonitorScript.sh on the file so it can be executable.



A security script that could be useful for someone’s server is one that is used in case of emergencies, like a DDOS attack is happening so you limit the amount of traffic allowed and make sure all unused ports are close. This would be a good combo with a cron job that is monitoring the network every few minutes for suspicious activity like a bunch of attempted connections from one host in a short amount of time. Overall, there are a lot of scripts you could make using cron jobs not only for security but for also keeping backups of important information, which could technically fall under security depending on what you are saving.

Sources:

<https://linuxhandbook.com/linux-login-history/>

[Reviewing logins on Linux | Network World](https://www.networkworld.com/article/3263752/reviewing-logins-on-linux.html)

[Linux audit files to see who made changes to a file - nixCraft (cyberciti.biz)](https://www.cyberciti.biz/tips/linux-audit-files-to-see-who-made-changes-to-a-file.html)

[Linux Filesystem Events with inotify | Linux Journal](https://www.linuxjournal.com/content/linux-filesystem-events-inotify)