Security Part 2 : Cronjobs

This document will explain how to schedule cronjobs. Upon completion you will have scheduled a cronjob to monitor the /etc/passwd file. Monitoring this file is important because it allows us to track users being added to or removed from the server. Knowing who has access to the system is a priority for any admin or security professional.

Crontab is a file that we can edit which allows us to schedule commands or scripts to run at the specific time of our choosing.

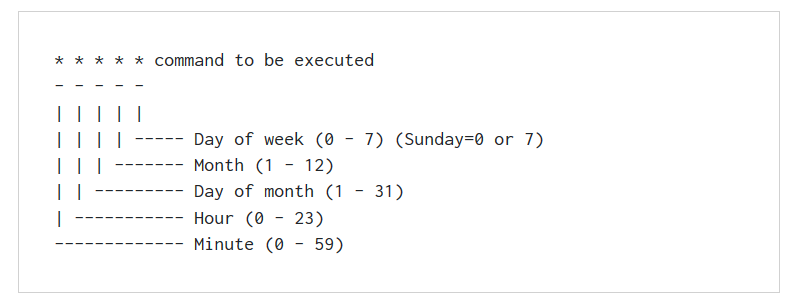
1. To view the contents of crontab issue the following:

#crontab –l

1. To enter the editor which allows you to edit the crontab file, enter the following:

#crontab –e

1. The syntax to flows by first specifying the time the job is to be run, followed by the path to the command or script you wish to execute, and lastly any arguments you wish to pass.
2. The time value is specified in 5 fields. It will look like this:



1. There are several operators available to us as well, \*, -, /, and , These can be used to specify exact times.
2. Now we will schedule two cronjob for our /etc/passwd file. One to run the “sha1sum” command against our /etc/passwd file, and the other to cat the output of /etc/passwd to a file in the event we need to review the usernames. The syntax we will use for this is:

0 \*/2 \* \* \* /etc/passwd >> /root/class/test/user\_hash.txt

0 \*/2 \* \* \* cat /etc/passwd >> /root/class/test/user\_snap.txt

1. Save your changes to the file and quit. You have successfully scheduled a cronjob.

References

I found the following link most helpful for explaining cronjobs and how to edit and list the files. The image I used which explains the time fields was pulled from this site.

https://www.cyberciti.biz/faq/how-do-i-add-jobs-to-cron-under-linux-or-unix-oses/