Security setup for CentOS – Acme Corporation

The purpose of this document is to guide you through the process of adding a few scripts to your CentOS VM. These scripts are intended to enhance the security and network monitoring for your CentOS machine.

1. First, if not already installed you will need to install inotify-tools.

# yum install inotify-tools

1. Add script “detect\_ip” to your machine. The file should be attached to your email. If not, it is copied below. Note, the script should be placed in the /root/class/test/ directory. Ensure the file permissions are set to 755, use “chmod 755 filename” to change the permissions if needed.

#!/bin/sh

# Log the date of the collection or scan.

date >> /root/class/test/network\_scan.txt

# scan for IP addresses on my network and redirect the output to a text file.

nmap -sT -0 192.169.0.0/24 >> /root/class/test/network\_scan.txt

1. Add script “detect\_dir\_change” to your machine. The file should be attached to your email. If not, it is copied below. Note, the script should be placed in the /root/class/test/ directory. Ensure the file permissions are set to 755, use “chmod 755 filename” to change the permissions if needed.

#!/bin/sh

# Generate timestamp, hash, and watch for changes in /etc/directory, redirect output to text file.

date >> /root/class/test/etc\_monitoring\_log.txt

sha1sum /etc/\* | sha1sum >> /root/class/test/etc\_monitoring\_log.txt

inotifywait -m /etc >> /root/class/test/etc\_monitoring\_log.txt

# Generate timestamp, hash, and watch for changes in /var/log directory, redirect output to text file.

sha1sum /var/log/\* | sha1sum >> /root/class/test/var\_log\_monitoring.txt

inotifywait -m /var/log >> /root/class/test/var\_log\_monitoring.txt

1. Add script “monitor\_hidden” to your machine. The file should be attached to your email. If not, it is copied below. Note, the script should be placed in the /root/class/test/ directory. Ensure the file permissions are set to 755, use “chmod 755 filename” to change the permissions if needed.

#!/bin/sh

# Append log file with date of collection.

date >> /root/class/test/monitor\_hidden\_log.txt

# List only the hidden files in root.

ls -ld /root/.?\* >> /root/class/test/monitor\_hidden\_log.txt

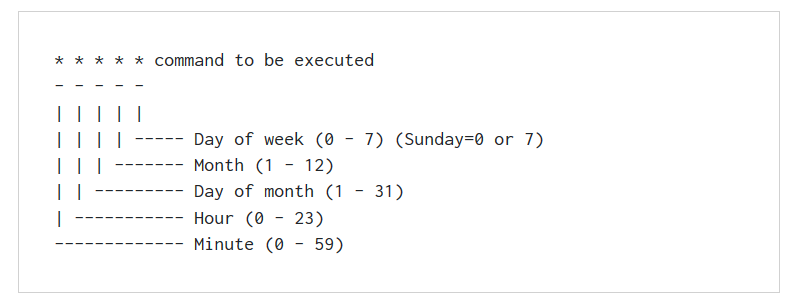
# List the statistics on the hidden files such as last modification date etc..

stat /root/.?\* >> /root/class/test/monitor\_hidden\_log.txt

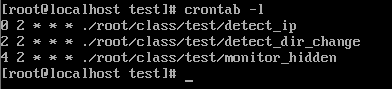
1. Lastly, we will schedule these scripts to run as cronjobs. To open the crontab file for editing, issue the following:

# crontab –e

This will open the crontab configuration file in VI. To schedule jobs we select the time, and the command or script that we want to execute. The format looks like this:



1. Edit your crontab file so it matches the image below, exit the VI file and commit the changes by pressing the ESC key twice, followed by wq! You can confirm the contents have been added by issuing the “crontab –l” command as shown in the image.



1. This concludes the security setup for CentOS.