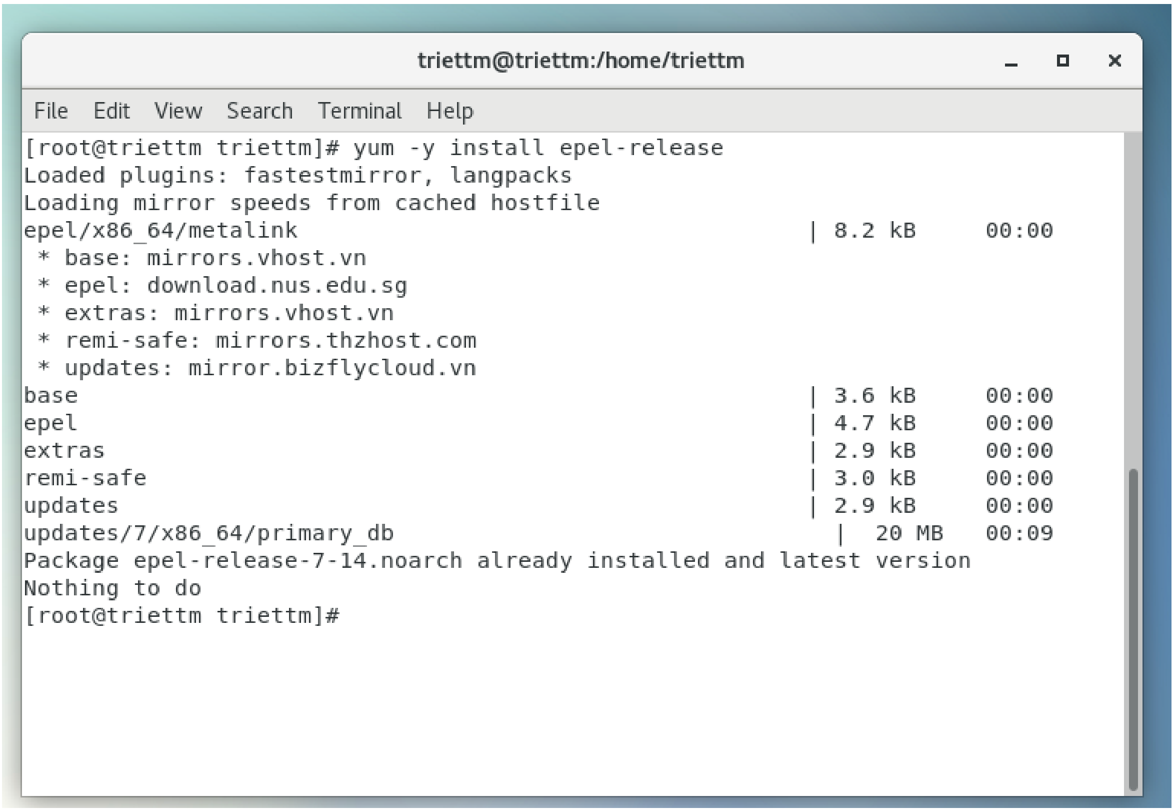
Install Clamav and maldet

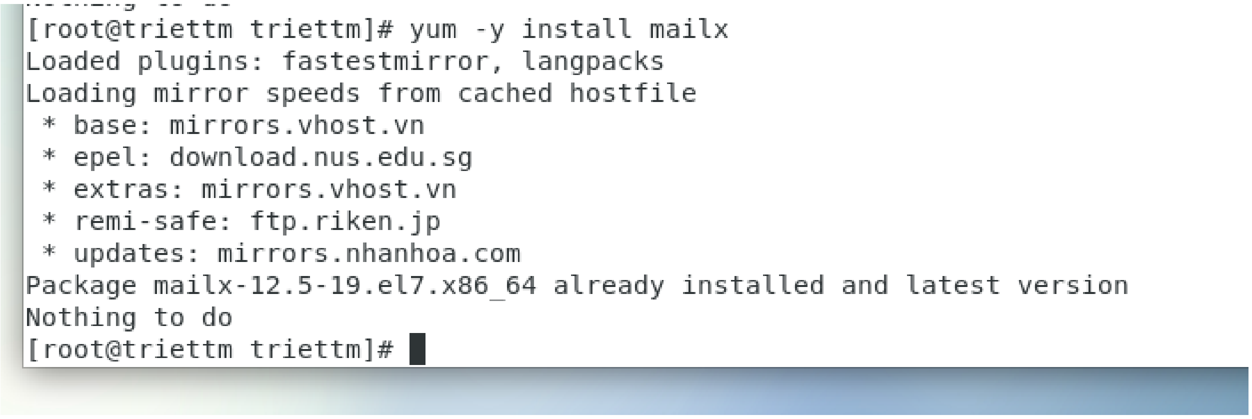
Step 1 - Install Epel repository and Mailx

Install the Epel (Extra Packages for Enterprise Linux) repository and the mailx command with yum. We need mailx installed on the system so that LMD can send the scan reports to your email address.


triettm@triettm:/home/triettm
File Edit View Search Terminal Help

```
[root@triettm triettm]# yum -y install epel-release
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
epel/x86_64/metalink                                     | 8.2 kB     00:00
 * base: mirrors.vhost.vn
 * epel: download.nus.edu.sg
 * extras: mirrors.vhost.vn
 * remi-safe: mirrors.thzhost.com
 * updates: mirror.bizflycloud.vn
base                                                     | 3.6 kB     00:00
epel                                                     | 4.7 kB     00:00
extras                                                   | 2.9 kB     00:00
remi-safe                                                | 3.0 kB     00:00
updates                                                  | 2.9 kB     00:00
updates/7/x86_64/primary_db                                |  20 MB   00:09
Package epel-release-7-14.noarch already installed and latest version
Nothing to do
[root@triettm triettm]#
```

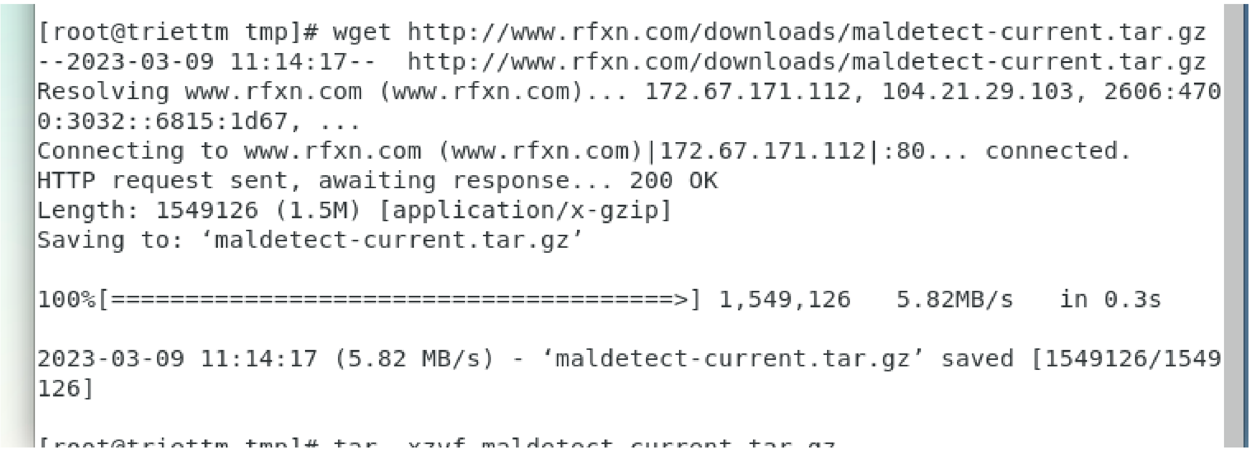
Install mailx so we can use the mail command on CentOS 7:



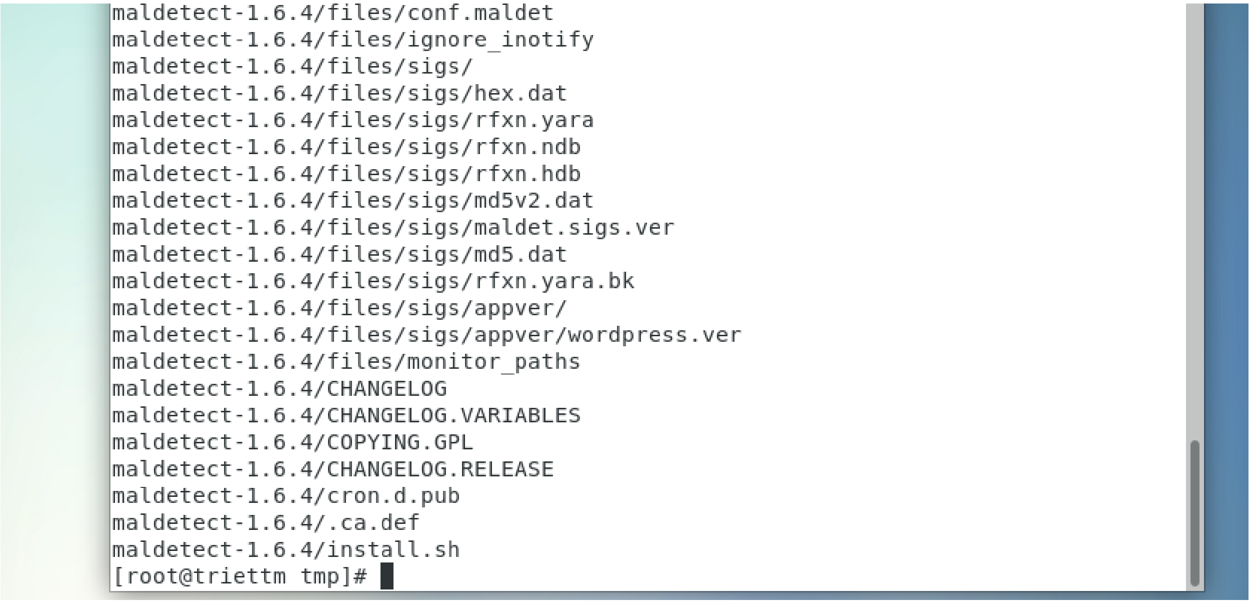
```
[root@triettm triettm]# yum -y install mailx
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirrors.vhost.vn
 * epel: download.nus.edu.sg
 * extras: mirrors.vhost.vn
 * remi-safe: ftp.riken.jp
 * updates: mirrors.nhanhoa.com
Package mailx-12.5-19.el7.x86_64 already installed and latest version
Nothing to do
[root@triettm triettm]# 
```

Step 2 - Install Linux Malware Detect (LMD)

Linux Malware Detect is not available in CentOS or Epel repository, we need to install it manually from source.

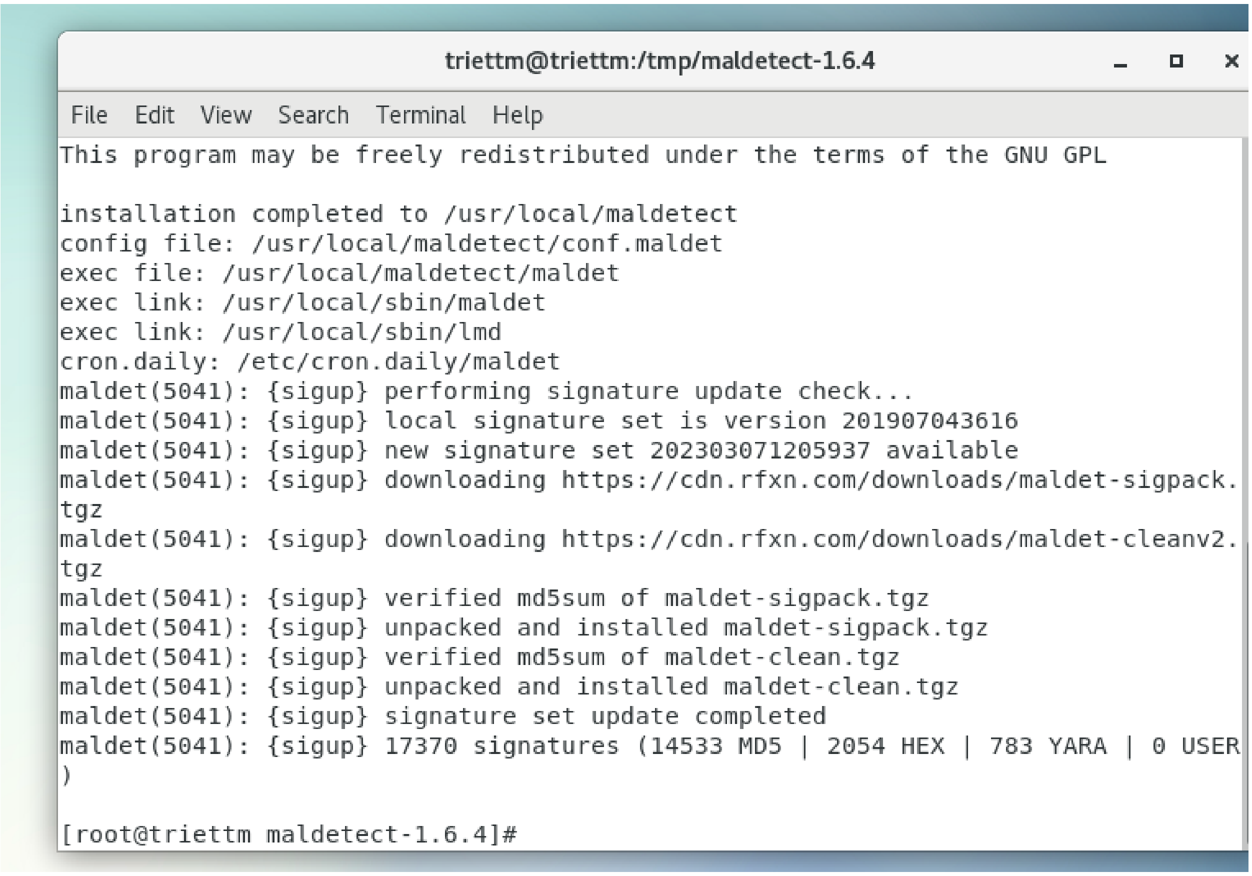


```
[root@triettm tmp]# wget http://www.rfxn.com/downloads/maldetect-current.tar.gz
--2023-03-09 11:14:17--  http://www.rfxn.com/downloads/maldetect-current.tar.gz
Resolving www.rfxn.com (www.rfxn.com)... 172.67.171.112, 104.21.29.103, 2606:470
0:3032::6815:1d67, ...
Connecting to www.rfxn.com (www.rfxn.com)|172.67.171.112|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1549126 (1.5M) [application/x-gzip]
Saving to: ‘maldetect-current.tar.gz’

100%[======================================>] 1,549,126   5.82MB/s   in 0.3s

2023-03-09 11:14:17 (5.82 MB/s) - ‘maldetect-current.tar.gz’ saved [1549126/1549
126]

[root@triettm tmp]# tar -xzvf maldetect-current.tar.gz
```



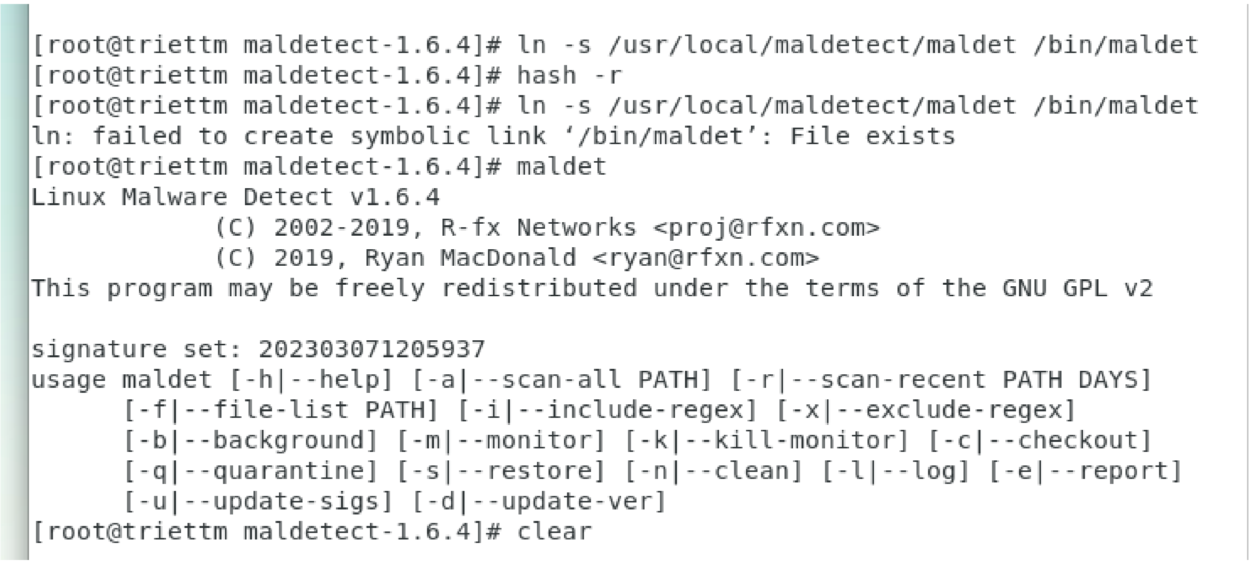
```
maldetect-1.6.4/files/conf.maldet
maldetect-1.6.4/files/ignore_inotify
maldetect-1.6.4/files/sigs/
maldetect-1.6.4/files/sigs/hex.dat
maldetect-1.6.4/files/sigs/rfxn.yara
maldetect-1.6.4/files/sigs/rfxn.ndb
maldetect-1.6.4/files/sigs/rfxn.hdb
maldetect-1.6.4/files/sigs/md5v2.dat
maldetect-1.6.4/files/sigs/maldet.sigs.ver
maldetect-1.6.4/files/sigs/md5.dat
maldetect-1.6.4/files/sigs/rfxn.yara.bk
maldetect-1.6.4/files/sigs/appver/
maldetect-1.6.4/files/sigs/appver/wordpress.ver
maldetect-1.6.4/files/monitor_paths
maldetect-1.6.4/CHANGELOG
maldetect-1.6.4/CHANGELOG.VARIABLES
maldetect-1.6.4/COPYING.GPL
maldetect-1.6.4/CHANGELOG.RELEASE
maldetect-1.6.4/cron.d.pub
maldetect-1.6.4/.ca.def
maldetect-1.6.4/install.sh
[root@triettm tmp]# █
```

Go to the maldetect directory and run the installer script 'install.sh' as root:


triettm@triettm:/tmp/maldetect-1.6.4
File Edit View Search Terminal Help

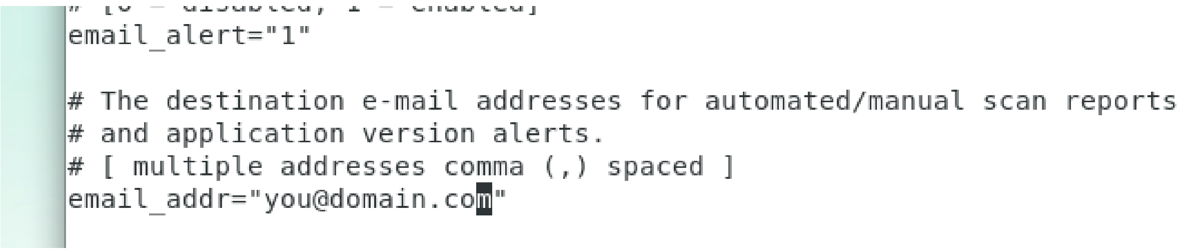
```
This program may be freely redistributed under the terms of the GNU GPL

installation completed to /usr/local/maldetect
config file: /usr/local/maldetect/conf.maldet
exec file: /usr/local/maldetect/maldet
exec link: /usr/local/sbin/maldet
exec link: /usr/local/sbin/lmd
cron.daily: /etc/cron.daily/maldet
maldet(5041): {sigup} performing signature update check...
maldet(5041): {sigup} local signature set is version 201907043616
maldet(5041): {sigup} new signature set 202303071205937 available
maldet(5041): {sigup} downloading https://cdn.rfxn.com/downloads/maldet-sigpack.
tgz
maldet(5041): {sigup} downloading https://cdn.rfxn.com/downloads/maldet-cleanv2.
tgz
maldet(5041): {sigup} verified md5sum of maldet-sigpack.tgz
maldet(5041): {sigup} unpacked and installed maldet-sigpack.tgz
maldet(5041): {sigup} verified md5sum of maldet-clean.tgz
maldet(5041): {sigup} unpacked and installed maldet-clean.tgz
maldet(5041): {sigup} signature set update completed
maldet(5041): {sigup} 17370 signatures (14533 MD5 | 2054 HEX | 783 YARA | 0 USER
)

[root@triettm maldetect-1.6.4]#
```

Next, make a symlink to the maldet command in the /bin/ directory:

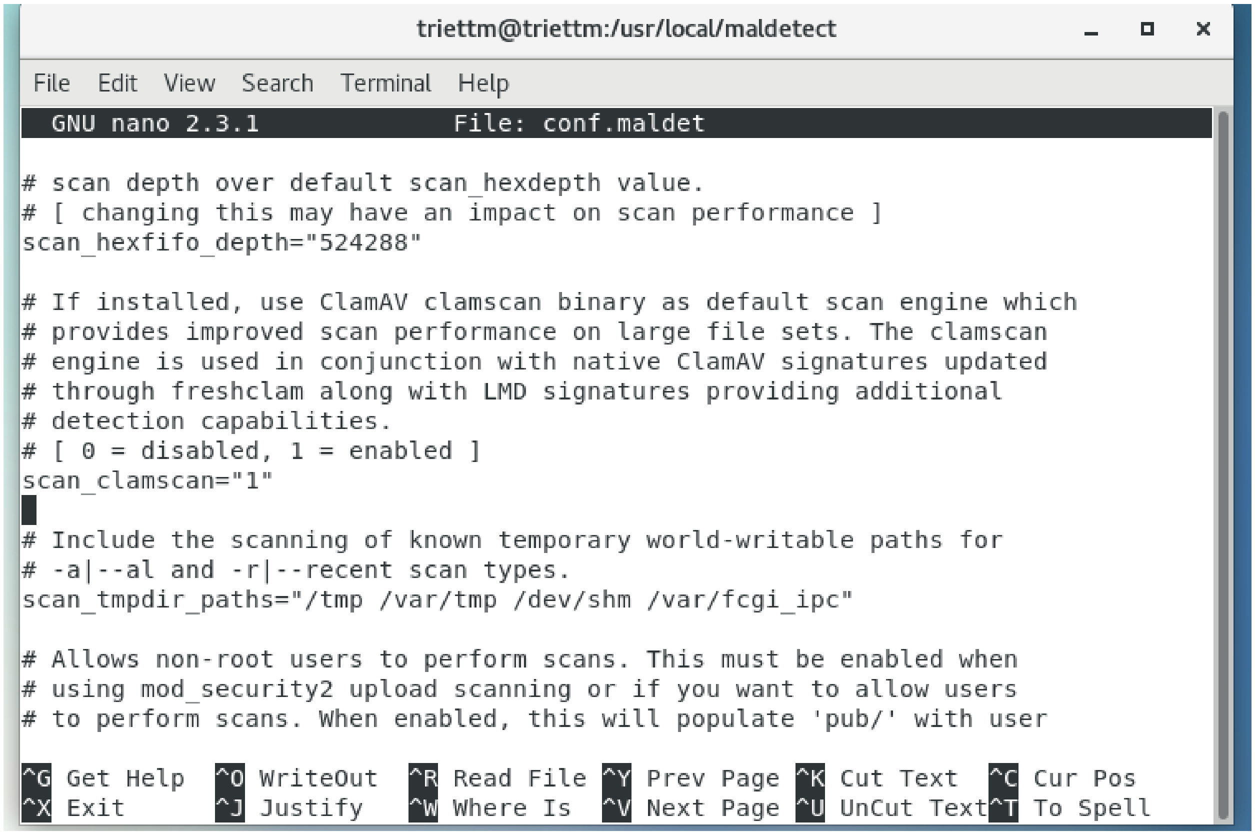


```
[root@triettm maldetect-1.6.4]# ln -s /usr/local/maldetect/maldet /bin/maldet
[root@triettm maldetect-1.6.4]# hash -r
[root@triettm maldetect-1.6.4]# ln -s /usr/local/maldetect/maldet /bin/maldet
ln: failed to create symbolic link ‘/bin/maldet’: File exists
[root@triettm maldetect-1.6.4]# maldet
Linux Malware Detect v1.6.4
            (C) 2002-2019, R-fx Networks <proj@rfxn.com>
            (C) 2019, Ryan MacDonald <ryan@rfxn.com>
This program may be freely redistributed under the terms of the GNU GPL v2

signature set: 202303071205937
usage maldet [-h|--help] [-a|--scan-all PATH] [-r|--scan-recent PATH DAYS]
      [-f|--file-list PATH] [-i|--include-regex] [-x|--exclude-regex]
      [-b|--background] [-m|--monitor] [-k|--kill-monitor] [-c|--checkout]
      [-q|--quarantine] [-s|--restore] [-n|--clean] [-l|--log] [-e|--report]
      [-u|--update-sigs] [-d|--update-ver]
[root@triettm maldetect-1.6.4]# clear
```

Step 3 - Configure Linux Malware Detect (LMD)

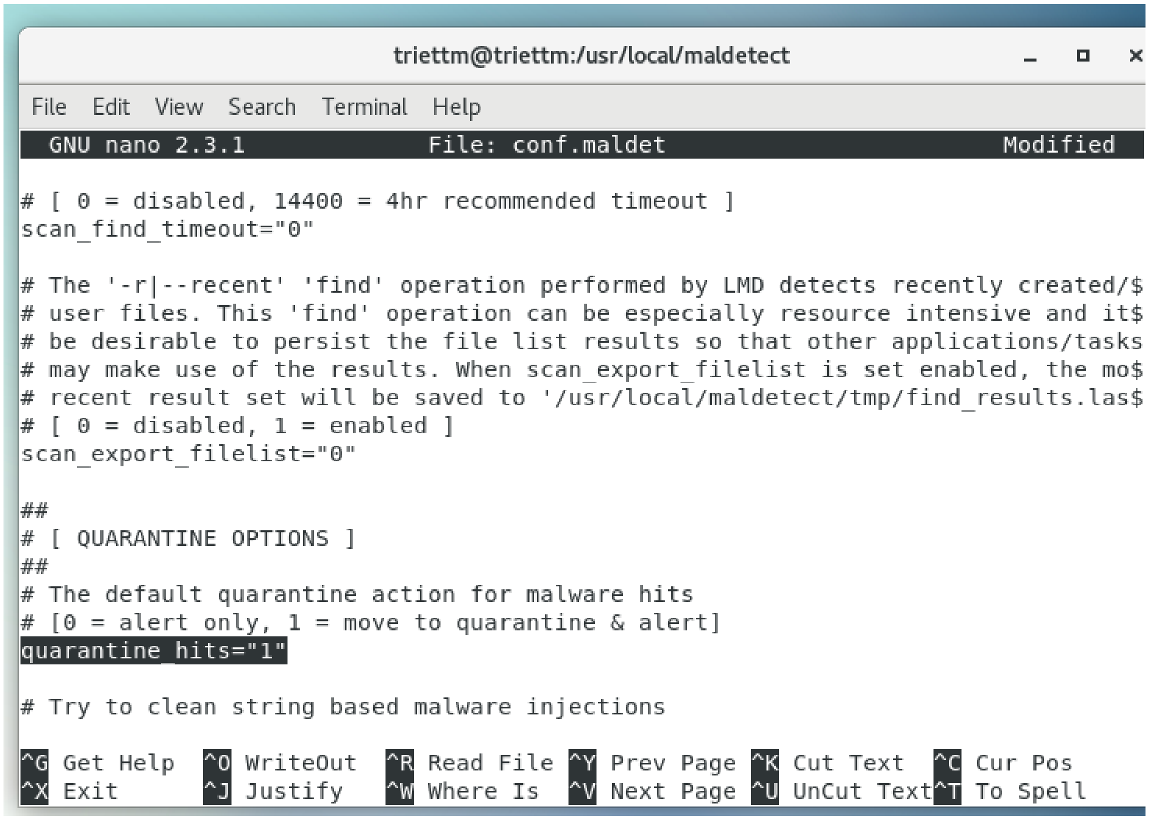


```
# [ 0 = disabled, 1 = enabled ]
email_alert="1"

# The destination e-mail addresses for automated/manual scan reports
# and application version alerts.
# [ multiple addresses comma (,) spaced ]
email_addr="you@domain.com"
```



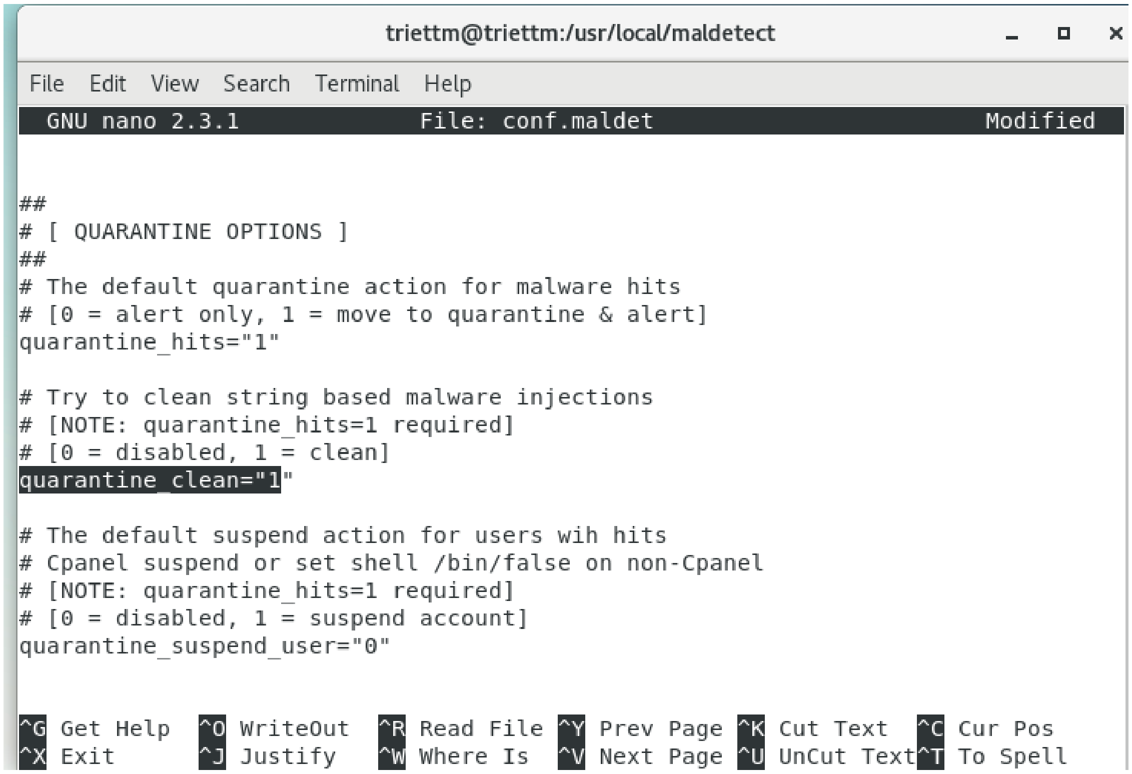
```
  GNU nano 2.3.1             File: conf.maldet

# scan depth over default scan_hexdepth value.
# [ changing this may have an impact on scan performance ]
scan_hexfifo_depth="524288"

# If installed, use ClamAV clamscan binary as default scan engine which
# provides improved scan performance on large file sets. The clamscan
# engine is used in conjunction with native ClamAV signatures updated
# through freshclam along with LMD signatures providing additional
# detection capabilities.
# [ 0 = disabled, 1 = enabled ]
scan_clamscan="1"

# Include the scanning of known temporary world-writable paths for
# -a|--al and -r|--recent scan types.
scan_tmpdir_paths="/tmp /var/tmp /dev/shm /var/fcgi_ipc"

# Allows non-root users to perform scans. This must be enabled when
# using mod_security2 upload scanning or if you want to allow users
# to perform scans. When enabled, this will populate 'pub/' with user

^G Get Help   ^O WriteOut   ^R Read File ^Y Prev Page ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

Next, enable quarantining to move malware to the quarantine automatically during the scan process.


triettm@triettm:/usr/local/maldetect
File Edit View Search Terminal Help

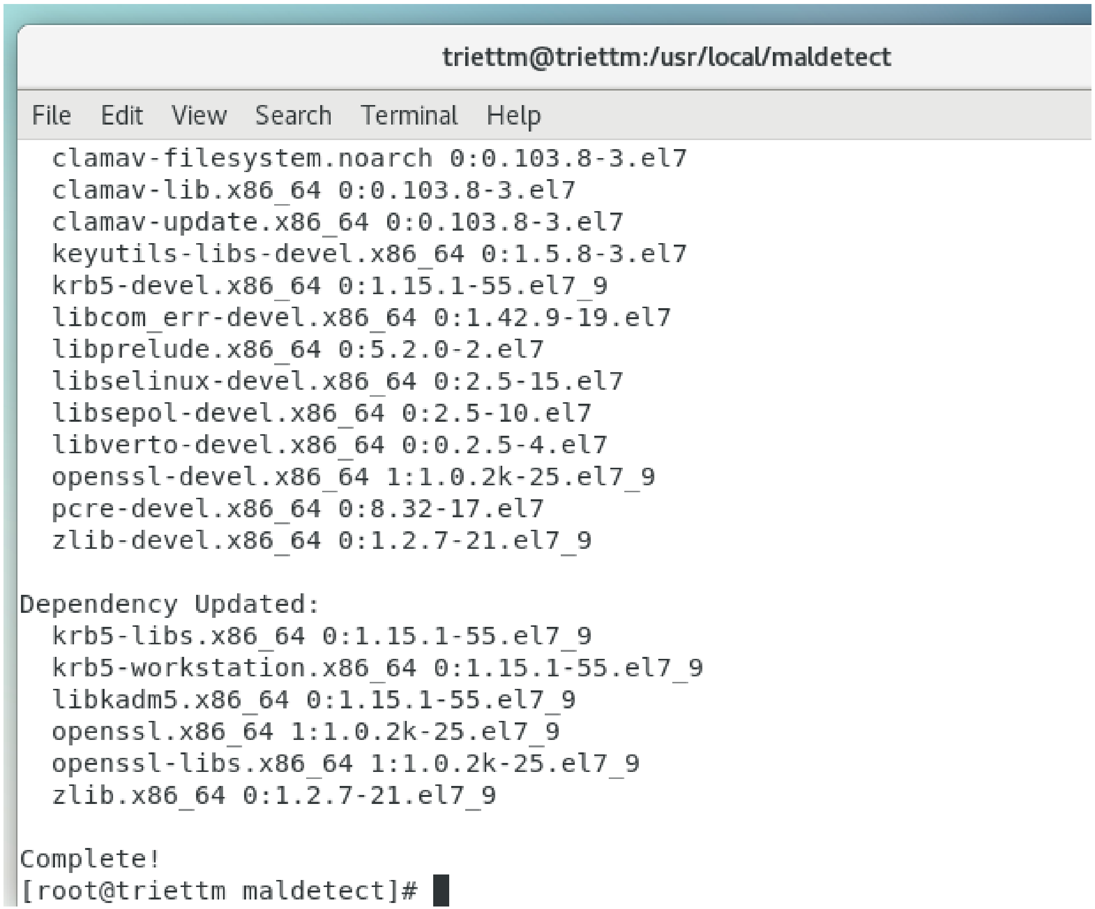
```
  GNU nano 2.3.1             File: conf.maldet                          Modified

# [ 0 = disabled, 14400 = 4hr recommended timeout ]
scan_find_timeout="0"

# The '-r|--recent' 'find' operation performed by LMD detects recently created/$
# user files. This 'find' operation can be especially resource intensive and it$
# be desirable to persist the file list results so that other applications/tasks
# may make use of the results. When scan_export_filelist is set enabled, the mo$
# recent result set will be saved to '/usr/local/maldetect/tmp/find_results.las$
# [ 0 = disabled, 1 = enabled ]
scan_export_filelist="0"

##
# [ QUARANTINE OPTIONS ]
##
# The default quarantine action for malware hits
# [0 = alert only, 1 = move to quarantine & alert]
quarantine_hits="1"

# Try to clean string based malware injections

^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text^T To Spell
```

Enable clean based malware injections.


triettm@triettm:/usr/local/maldetect
File Edit View Search Terminal Help

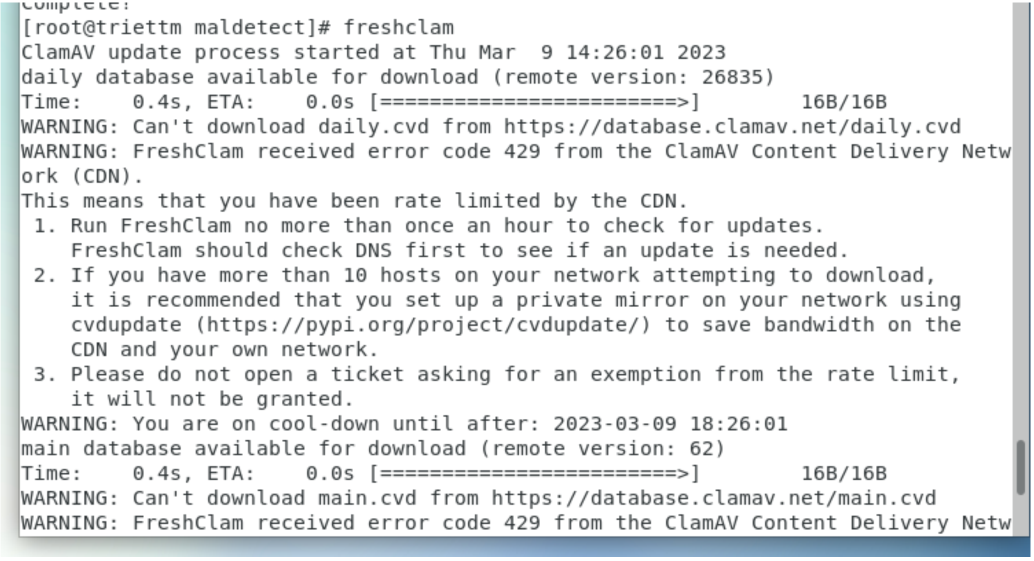
```
  GNU nano 2.3.1             File: conf.maldet                          Modified


##
# [ QUARANTINE OPTIONS ]
##
# The default quarantine action for malware hits
# [0 = alert only, 1 = move to quarantine & alert]
quarantine_hits="1"

# Try to clean string based malware injections
# [NOTE: quarantine_hits=1 required]
# [0 = disabled, 1 = clean]
quarantine_clean="1"

# The default suspend action for users wih hits
# Cpanel suspend or set shell /bin/false on non-Cpanel
# [NOTE: quarantine_hits=1 required]
# [0 = disabled, 1 = suspend account]
quarantine_suspend_user="0"


^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text^T To Spell
```

Step 4 - Install ClamAV



triettm@triettm:/usr/local/maldetect
File Edit View Search Terminal Help

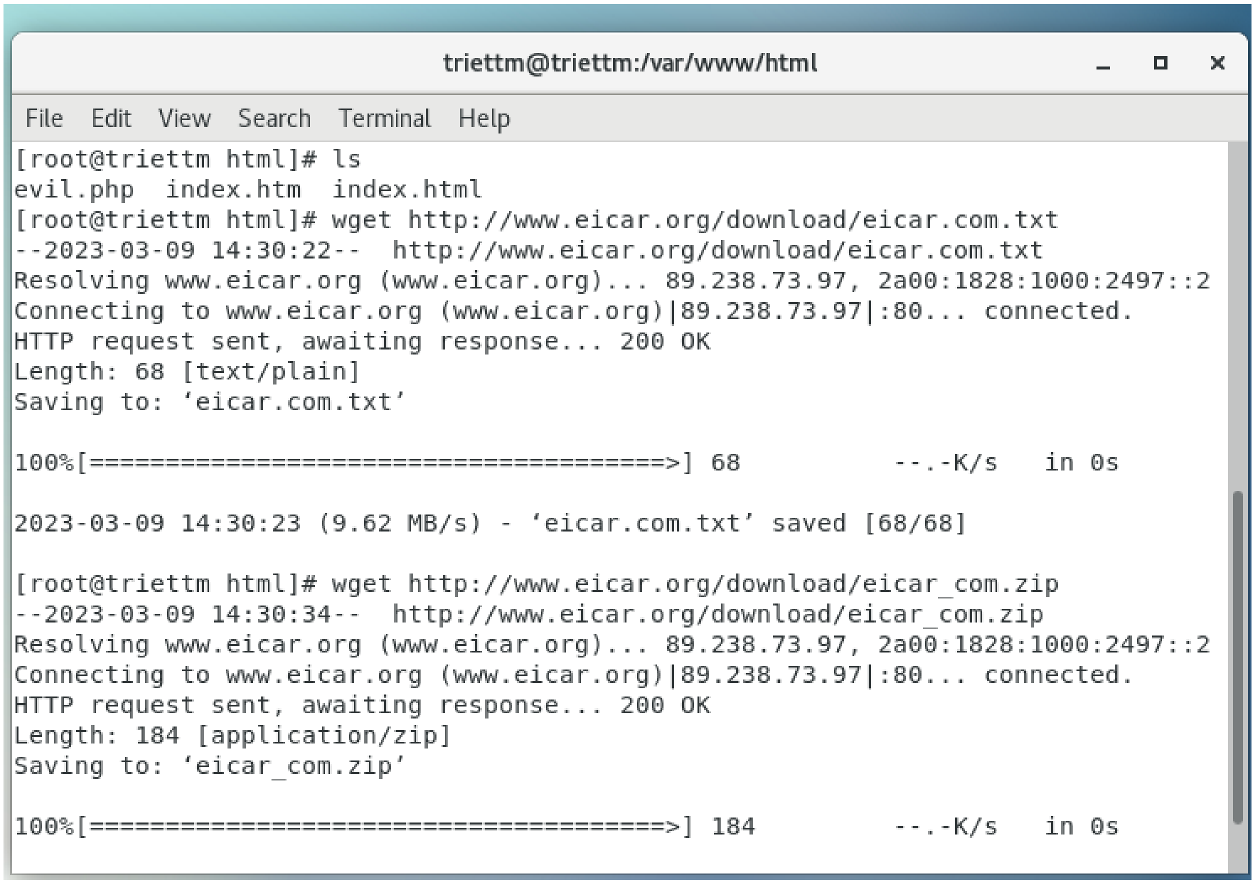
```
  clamav-filesystem.noarch 0:0.103.8-3.el7
  clamav-lib.x86_64 0:0.103.8-3.el7
  clamav-update.x86_64 0:0.103.8-3.el7
  keyutils-libs-devel.x86_64 0:1.5.8-3.el7
  krb5-devel.x86_64 0:1.15.1-55.el7_9
  libcom_err-devel.x86_64 0:1.42.9-19.el7
  libprelude.x86_64 0:5.2.0-2.el7
  libselinux-devel.x86_64 0:2.5-15.el7
  libsepol-devel.x86_64 0:2.5-10.el7
  libverto-devel.x86_64 0:0.2.5-4.el7
  openssl-devel.x86_64 1:1.0.2k-25.el7_9
  pcre-devel.x86_64 0:8.32-17.el7
  zlib-devel.x86_64 0:1.2.7-21.el7_9

Dependency Updated:
  krb5-libs.x86_64 0:1.15.1-55.el7_9
  krb5-workstation.x86_64 0:1.15.1-55.el7_9
  libkadm5.x86_64 0:1.15.1-55.el7_9
  openssl.x86_64 1:1.0.2k-25.el7_9
  openssl-libs.x86_64 1:1.0.2k-25.el7_9
  zlib.x86_64 0:1.2.7-21.el7_9

Complete!
[root@triettm maldetect]#
```



```
Complete!
[root@triettm maldetect]# freshclam
ClamAV update process started at Thu Mar  9 14:26:01 2023
daily database available for download (remote version: 26835)
Time:    0.4s, ETA:    0.0s [========================>]        16B/16B
WARNING: Can't download daily.cvd from https://database.clamav.net/daily.cvd
WARNING: FreshClam received error code 429 from the ClamAV Content Delivery Netw
ork (CDN).
This means that you have been rate limited by the CDN.
 1. Run FreshClam no more than once an hour to check for updates.
    FreshClam should check DNS first to see if an update is needed.
 2. If you have more than 10 hosts on your network attempting to download,
    it is recommended that you set up a private mirror on your network using
    cvdupdate (https://pypi.org/project/cvdupdate/) to save bandwidth on the
    CDN and your own network.
 3. Please do not open a ticket asking for an exemption from the rate limit,
    it will not be granted.
WARNING: You are on cool-down until after: 2023-03-09 18:26:01
main database available for download (remote version: 62)
Time:    0.4s, ETA:    0.0s [========================>]        16B/16B
WARNING: Can't download main.cvd from https://database.clamav.net/main.cvd
WARNING: FreshClam received error code 429 from the ClamAV Content Delivery Netw
```

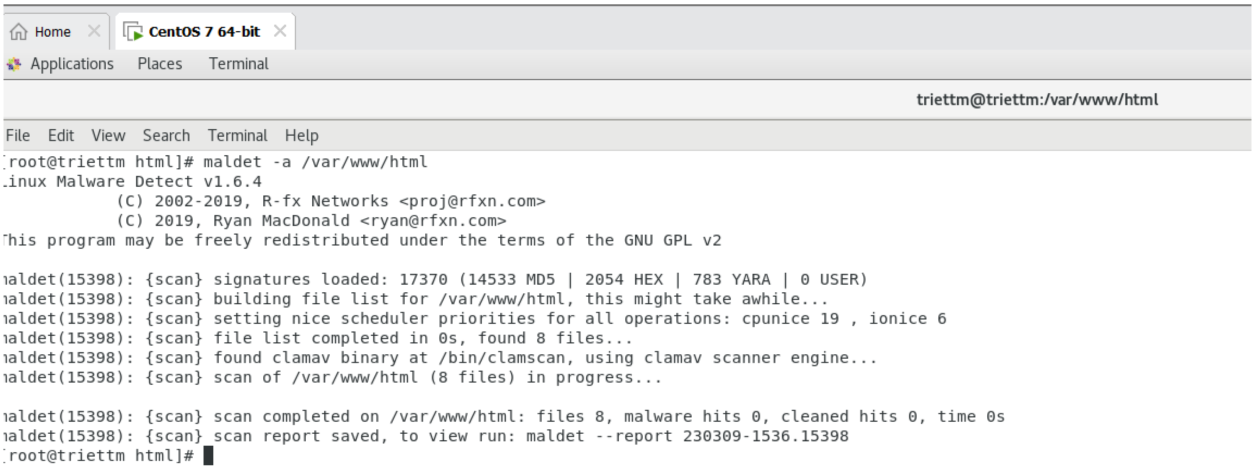
Step 5 - Testing LMD and ClamAV

First we will download some malware for testing purpose


triettm@triettm:/var/www/html
File Edit View Search Terminal Help

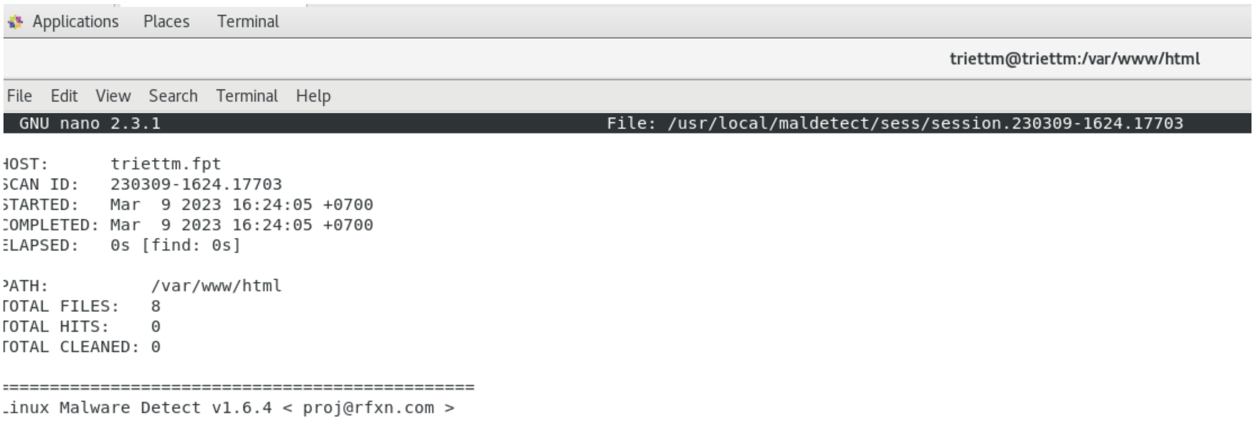
```
[root@triettm html]# ls
evil.php  index.htm  index.html
[root@triettm html]# wget http://www.eicar.org/download/eicar.com.txt
--2023-03-09 14:30:22--  http://www.eicar.org/download/eicar.com.txt
Resolving www.eicar.org (www.eicar.org)... 89.238.73.97, 2a00:1828:1000:2497::2
Connecting to www.eicar.org (www.eicar.org)|89.238.73.97|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 68 [text/plain]
Saving to: ‘eicar.com.txt’

100%[======================================>] 68          --.-K/s   in 0s

2023-03-09 14:30:23 (9.62 MB/s) - ‘eicar.com.txt’ saved [68/68]

[root@triettm html]# wget http://www.eicar.org/download/eicar_com.zip
--2023-03-09 14:30:34--  http://www.eicar.org/download/eicar_com.zip
Resolving www.eicar.org (www.eicar.org)... 89.238.73.97, 2a00:1828:1000:2497::2
Connecting to www.eicar.org (www.eicar.org)|89.238.73.97|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 184 [application/zip]
Saving to: ‘eicar_com.zip’

100%[======================================>] 184         --.-K/s   in 0s
```

Next, scan the web root directory with the maldet command below:


Home
CentOS 7 64-bit
Applications Places Terminal
triettm@triettm:/var/www/html
File Edit View Search Terminal Help

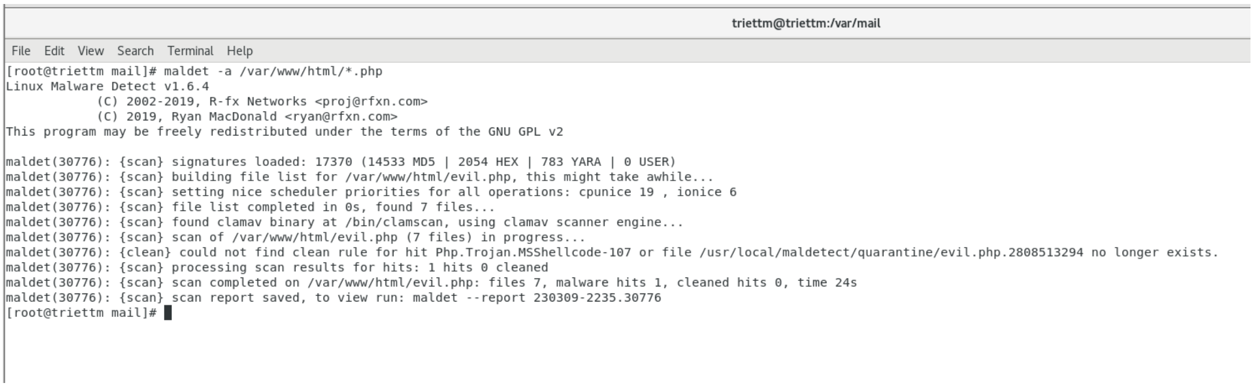
```
root@triettm html]# maldet -a /var/www/html
inux Malware Detect v1.6.4
            (C) 2002-2019, R-fx Networks <proj@rfxn.com>
            (C) 2019, Ryan MacDonald <ryan@rfxn.com>
his program may be freely redistributed under the terms of the GNU GPL v2

aldet(15398): {scan} signatures loaded: 17370 (14533 MD5 | 2054 HEX | 783 YARA | 0 USER)
aldet(15398): {scan} building file list for /var/www/html, this might take awhile...
aldet(15398): {scan} setting nice scheduler priorities for all operations: cpunice 19 , ionice 6
aldet(15398): {scan} file list completed in 0s, found 8 files...
aldet(15398): {scan} found clamav binary at /bin/clamscan, using clamav scanner engine...
aldet(15398): {scan} scan of /var/www/html (8 files) in progress...

aldet(15398): {scan} scan completed on /var/www/html: files 8, malware hits 0, cleaned hits 0, time 0s
aldet(15398): {scan} scan report saved, to view run: maldet --report 230309-1536.15398
root@triettm html]#
```

As we can see maldet does not detect any malware file in the folder



```
 GNU nano 2.3.1                          File: /usr/local/maldetect/sess/session.230309-1624.17703

HOST:      triettm.fpt
SCAN ID:   230309-1624.17703
STARTED:   Mar  9 2023 16:24:05 +0700
COMPLETED: Mar  9 2023 16:24:05 +0700
ELAPSED:   0s [find: 0s]

PATH:          /var/www/html
TOTAL FILES:   8
TOTAL HITS:    0
TOTAL CLEANED: 0

===============================================
Linux Malware Detect v1.6.4 < proj@rfxn.com >
```

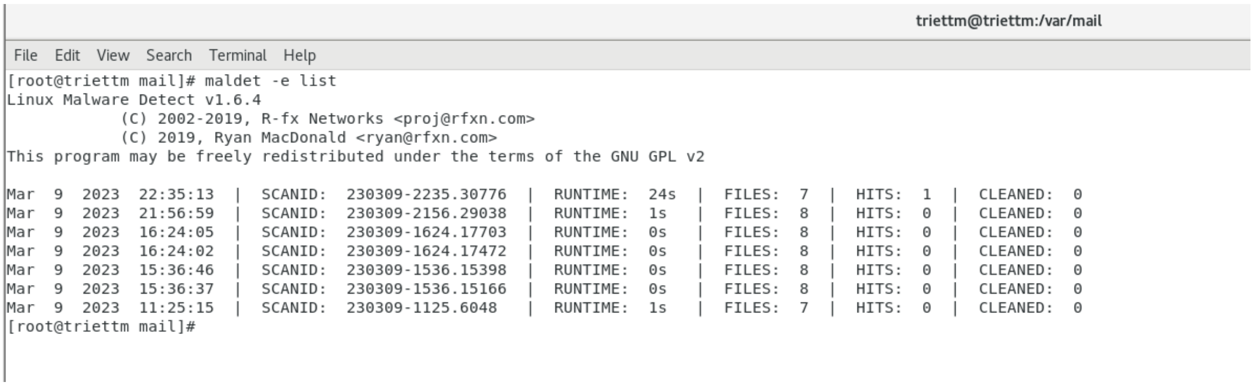
Step 6 - Other LMD Commands



```
[root@triettm mail]# maldet -a /var/www/html/*.php
Linux Malware Detect v1.6.4
            (C) 2002-2019, R-fx Networks <proj@rfxn.com>
            (C) 2019, Ryan MacDonald <ryan@rfxn.com>
This program may be freely redistributed under the terms of the GNU GPL v2

maldet(30776): {scan} signatures loaded: 17370 (14533 MD5 | 2054 HEX | 783 YARA | 0 USER)
maldet(30776): {scan} building file list for /var/www/html/evil.php, this might take awhile...
maldet(30776): {scan} setting nice scheduler priorities for all operations: cpunice 19 , ionice 6
maldet(30776): {scan} file list completed in 0s, found 7 files...
maldet(30776): {scan} found clamav binary at /bin/clamscan, using clamav scanner engine...
maldet(30776): {scan} scan of /var/www/html/evil.php (7 files) in progress...
maldet(30776): {clean} could not find clean rule for hit Php.Trojan.MSShellcode-107 or file /usr/local/maldetect/quarantine/evil.php.2808513294 no longer exists.
maldet(30776): {scan} processing scan results for hits: 1 hits 0 cleaned
maldet(30776): {scan} scan completed on /var/www/html/evil.php: files 7, malware hits 1, cleaned hits 0, time 24s
maldet(30776): {scan} scan report saved, to view run: maldet --report 230309-2235.30776
[root@triettm mail]# 
```

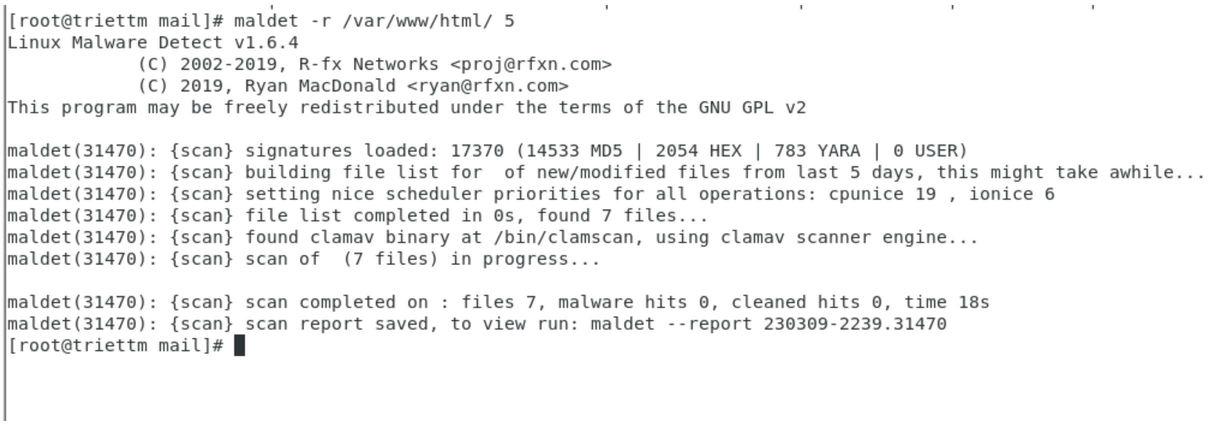
If I specify to detect the php malware file, maldet can detect one of them.

Get a list of all reports:



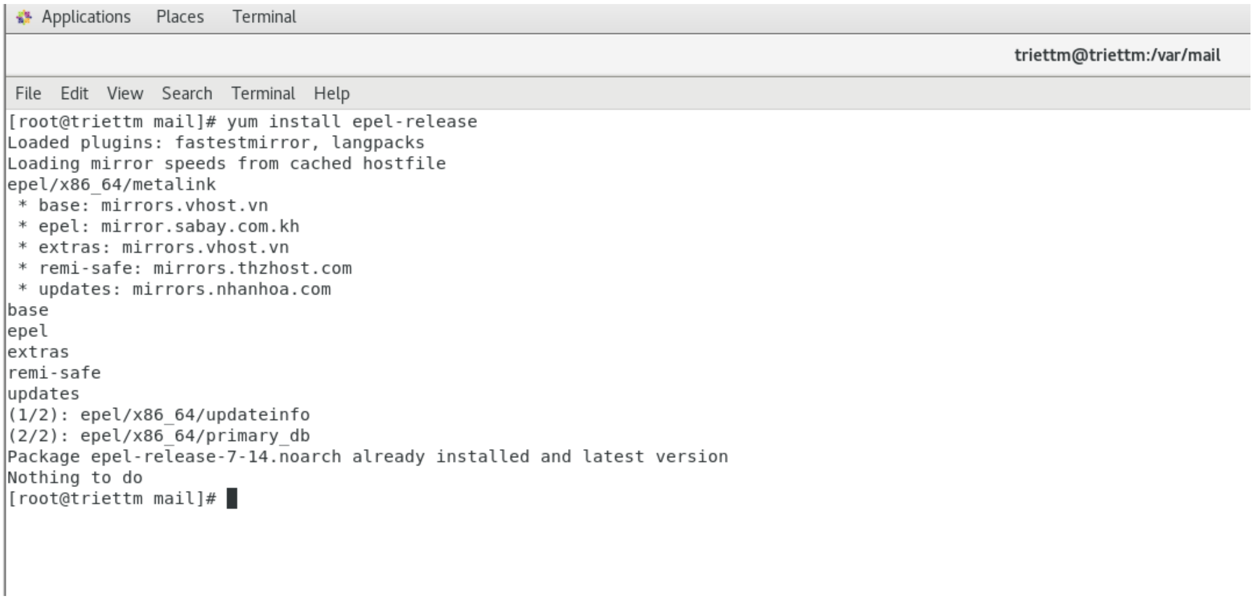
```
[root@triettm mail]# maldet -e list
Linux Malware Detect v1.6.4
            (C) 2002-2019, R-fx Networks <proj@rfxn.com>
            (C) 2019, Ryan MacDonald <ryan@rfxn.com>
This program may be freely redistributed under the terms of the GNU GPL v2

Mar  9  2023  22:35:13  |  SCANID:  230309-2235.30776  |  RUNTIME:  24s  |  FILES:  7  |  HITS:  1  |  CLEANED:  0
Mar  9  2023  21:56:59  |  SCANID:  230309-2156.29038  |  RUNTIME:  1s   |  FILES:  8  |  HITS:  0  |  CLEANED:  0
Mar  9  2023  16:24:05  |  SCANID:  230309-1624.17703  |  RUNTIME:  0s   |  FILES:  8  |  HITS:  0  |  CLEANED:  0
Mar  9  2023  16:24:02  |  SCANID:  230309-1624.17472  |  RUNTIME:  0s   |  FILES:  8  |  HITS:  0  |  CLEANED:  0
Mar  9  2023  15:36:46  |  SCANID:  230309-1536.15398  |  RUNTIME:  0s   |  FILES:  8  |  HITS:  0  |  CLEANED:  0
Mar  9  2023  15:36:37  |  SCANID:  230309-1536.15166  |  RUNTIME:  0s   |  FILES:  8  |  HITS:  0  |  CLEANED:  0
Mar  9  2023  11:25:15  |  SCANID:  230309-1125.6048   |  RUNTIME:  1s   |  FILES:  7  |  HITS:  0  |  CLEANED:  0
[root@triettm mail]#
```

Scan files that have been created/modified in the last X days.

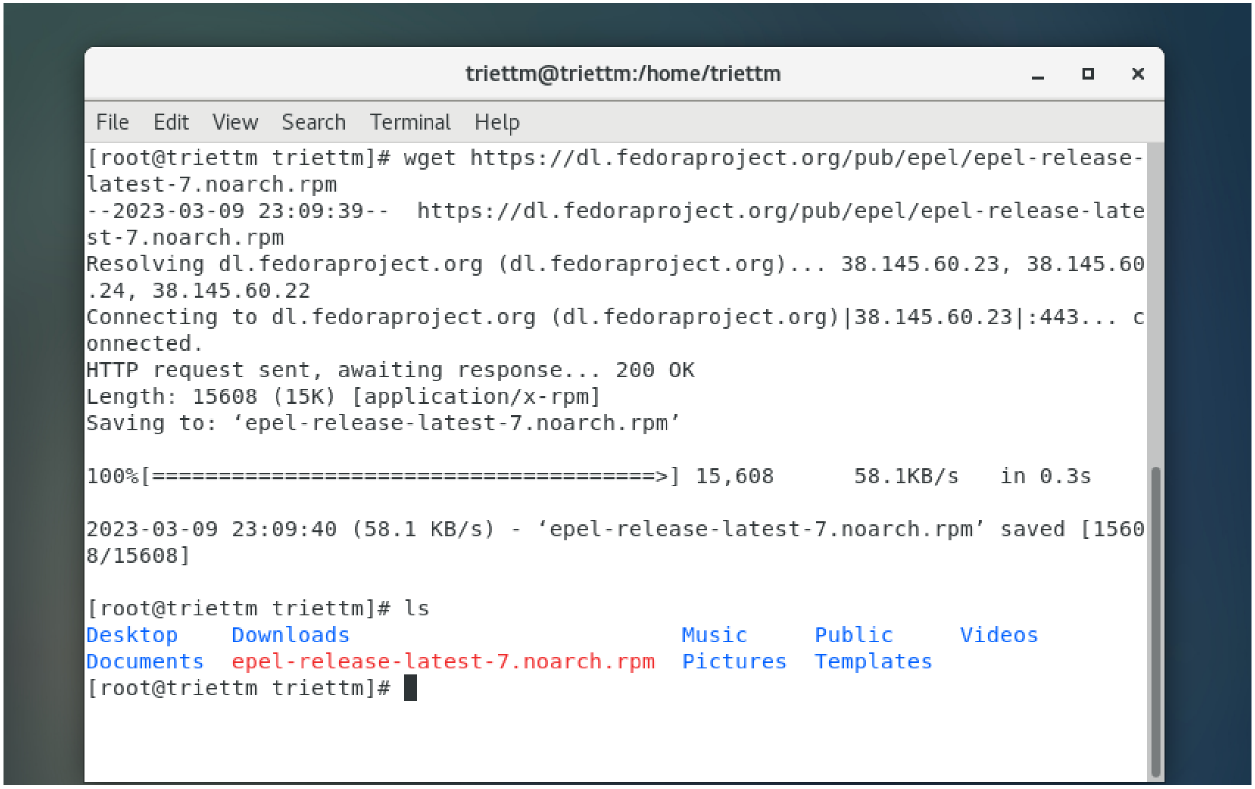


```
[root@triettm mail]# maldet -r /var/www/html/ 5
Linux Malware Detect v1.6.4
            (C) 2002-2019, R-fx Networks <proj@rfxn.com>
            (C) 2019, Ryan MacDonald <ryan@rfxn.com>
This program may be freely redistributed under the terms of the GNU GPL v2

maldet(31470): {scan} signatures loaded: 17370 (14533 MD5 | 2054 HEX | 783 YARA | 0 USER)
maldet(31470): {scan} building file list for  of new/modified files from last 5 days, this might take awhile...
maldet(31470): {scan} setting nice scheduler priorities for all operations: cpunice 19 , ionice 6
maldet(31470): {scan} file list completed in 0s, found 7 files...
maldet(31470): {scan} found clamav binary at /bin/clamscan, using clamav scanner engine...
maldet(31470): {scan} scan of  (7 files) in progress...

maldet(31470): {scan} scan completed on : files 7, malware hits 0, cleaned hits 0, time 18s
maldet(31470): {scan} scan report saved, to view run: maldet --report 230309-2239.31470
[root@triettm mail]# █
```

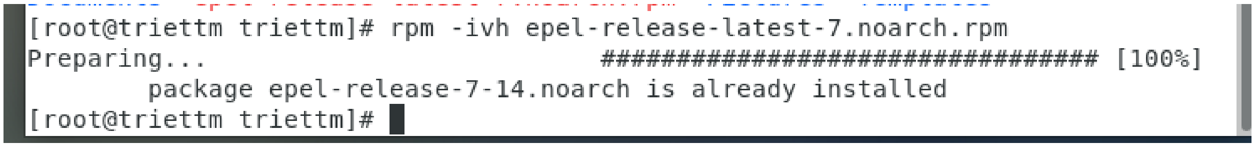
Install rkhunter



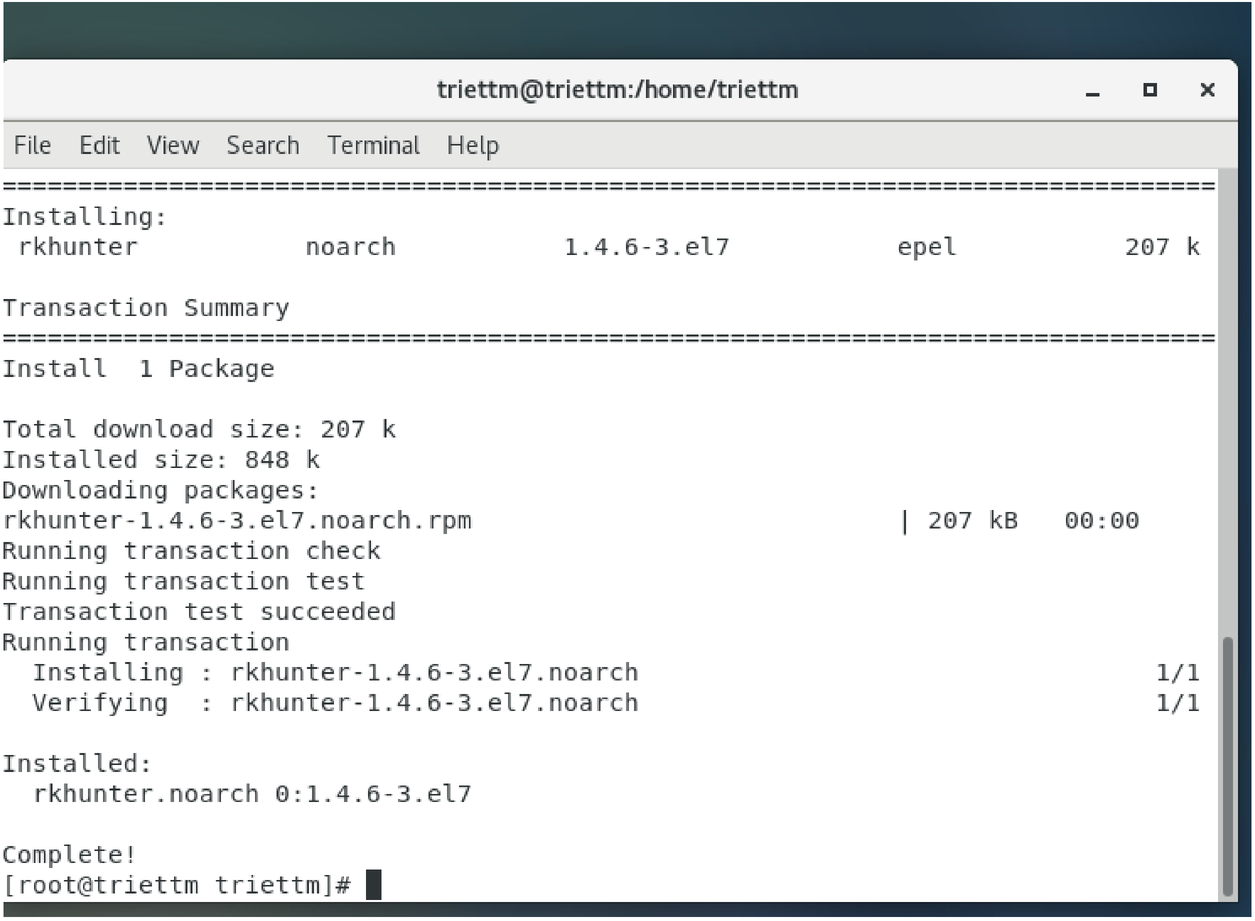
```
[root@triettm mail]# yum install epel-release
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
epel/x86_64/metalink
 * base: mirrors.vhost.vn
 * epel: mirror.sabay.com.kh
 * extras: mirrors.vhost.vn
 * remi-safe: mirrors.thzhost.com
 * updates: mirrors.nhanhoa.com
base
epel
extras
remi-safe
updates
(1/2): epel/x86_64/updateinfo
(2/2): epel/x86_64/primary_db
Package epel-release-7-14.noarch already installed and latest version
Nothing to do
[root@triettm mail]# 
```



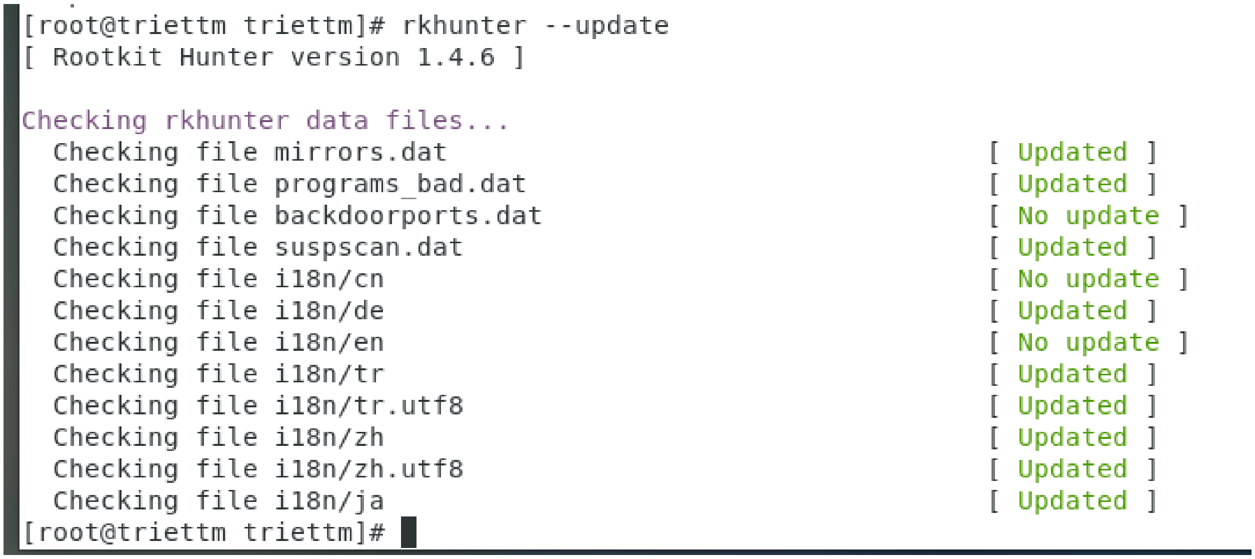
```
[root@triettm triettm]# wget https://dl.fedoraproject.org/pub/epel/epel-release-
latest-7.noarch.rpm
--2023-03-09 23:09:39--  https://dl.fedoraproject.org/pub/epel/epel-release-late
st-7.noarch.rpm
Resolving dl.fedoraproject.org (dl.fedoraproject.org)... 38.145.60.23, 38.145.60
.24, 38.145.60.22
Connecting to dl.fedoraproject.org (dl.fedoraproject.org)|38.145.60.23|:443... c
onnected.
HTTP request sent, awaiting response... 200 OK
Length: 15608 (15K) [application/x-rpm]
Saving to: ‘epel-release-latest-7.noarch.rpm’

100%[======================================>] 15,608      58.1KB/s   in 0.3s

2023-03-09 23:09:40 (58.1 KB/s) - ‘epel-release-latest-7.noarch.rpm’ saved [1560
8/15608]

[root@triettm triettm]# ls
Desktop    Downloads                          Music     Public     Videos
Documents  epel-release-latest-7.noarch.rpm  Pictures  Templates
[root@triettm triettm]# 
```



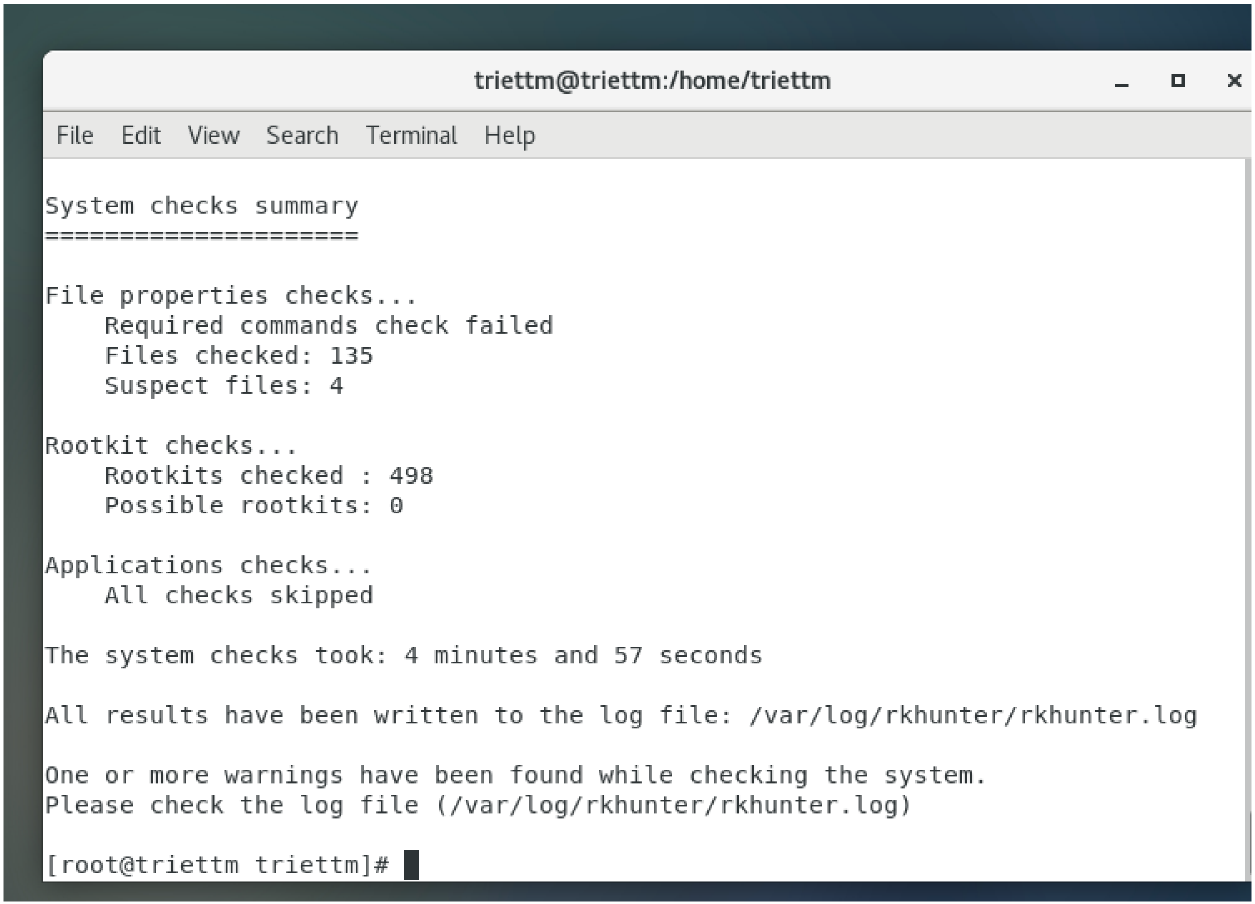
```
[root@triettm triettm]# rpm -ivh epel-release-latest-7.noarch.rpm
Preparing...                          ################################# [100%]
        package epel-release-7-14.noarch is already installed
[root@triettm triettm]# 
```



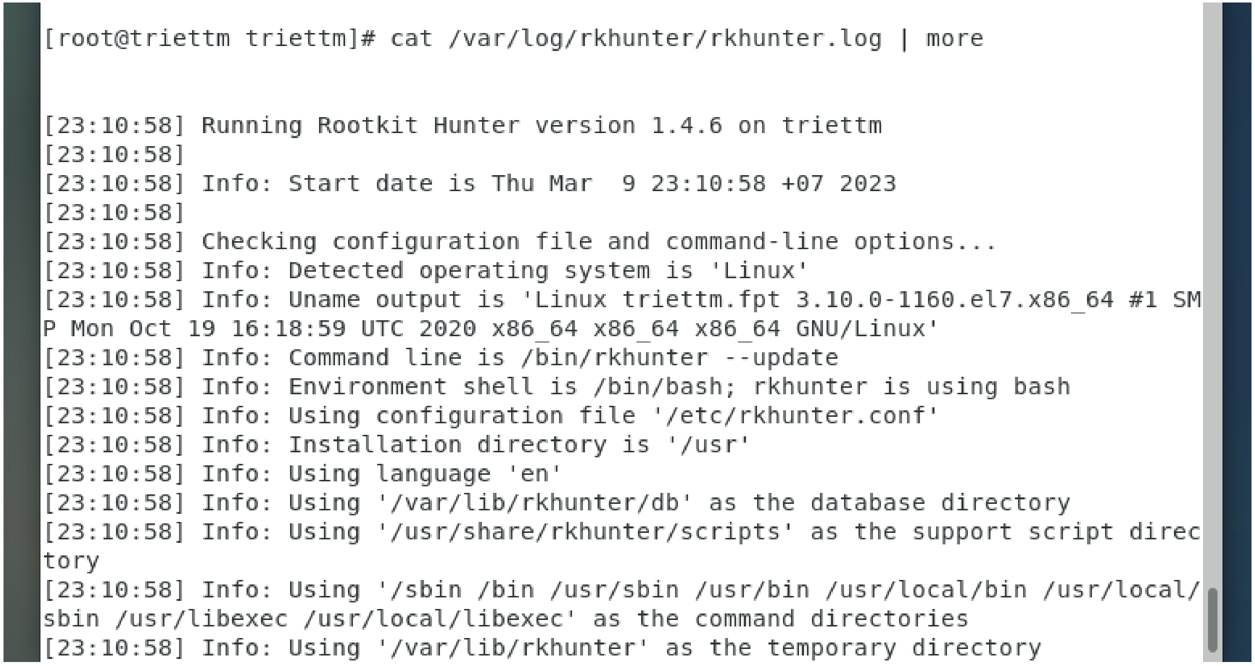
```
================================================================================
Installing:
 rkhunter           noarch           1.4.6-3.el7           epel           207 k

Transaction Summary
================================================================================
Install  1 Package

Total download size: 207 k
Installed size: 848 k
Downloading packages:
rkhunter-1.4.6-3.el7.noarch.rpm                            | 207 kB   00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : rkhunter-1.4.6-3.el7.noarch                                  1/1
  Verifying  : rkhunter-1.4.6-3.el7.noarch                                  1/1

Installed:
  rkhunter.noarch 0:1.4.6-3.el7

Complete!
[root@triettm triettm]# 
```



```
[root@triettm triettm]# rkhunter --update
[ Rootkit Hunter version 1.4.6 ]

Checking rkhunter data files...
  Checking file mirrors.dat                                [ Updated ]
  Checking file programs_bad.dat                           [ Updated ]
  Checking file backdoorports.dat                          [ No update ]
  Checking file suspscan.dat                               [ Updated ]
  Checking file i18n/cn                                    [ No update ]
  Checking file i18n/de                                    [ Updated ]
  Checking file i18n/en                                    [ No update ]
  Checking file i18n/tr                                    [ Updated ]
  Checking file i18n/tr.utf8                               [ Updated ]
  Checking file i18n/zh                                    [ Updated ]
  Checking file i18n/zh.utf8                               [ Updated ]
  Checking file i18n/ja                                    [ Updated ]
[root@triettm triettm]# 
```



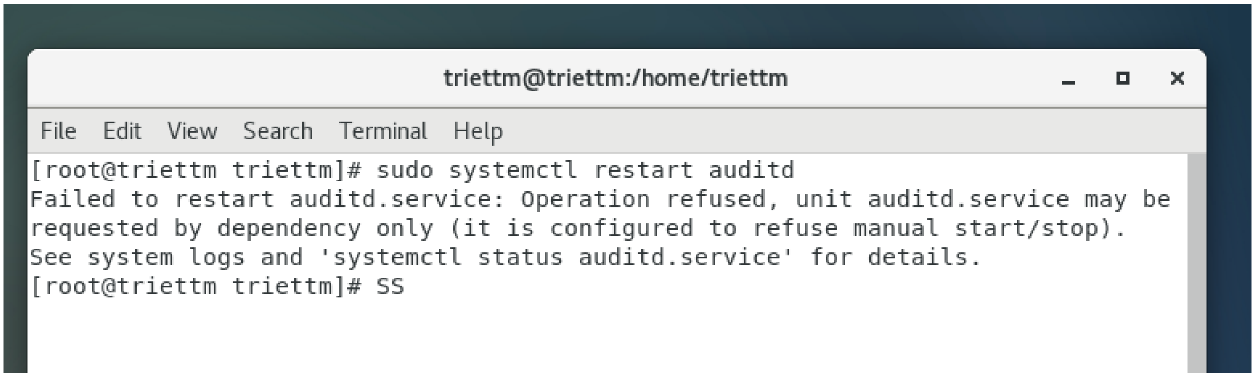
```
System checks summary
=====================

File properties checks...
    Required commands check failed
    Files checked: 135
    Suspect files: 4

Rootkit checks...
    Rootkits checked : 498
    Possible rootkits: 0

Applications checks...
    All checks skipped

The system checks took: 4 minutes and 57 seconds

All results have been written to the log file: /var/log/rkhunter/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter/rkhunter.log)

[root@triettm triettm]# 
```



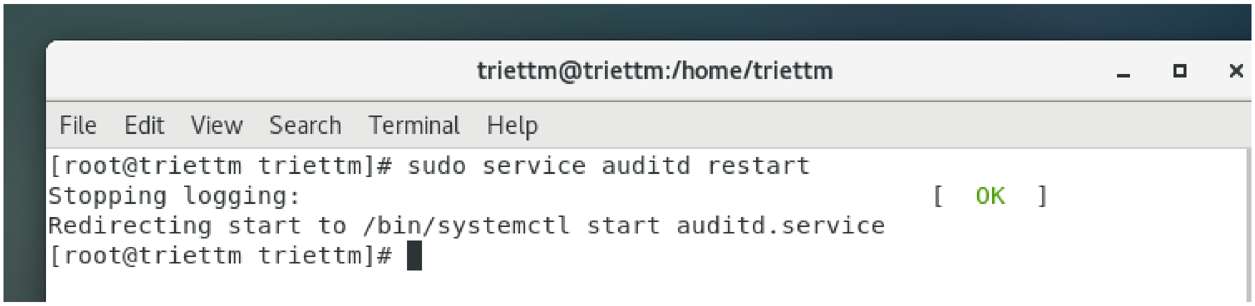
```
[root@triettm triettm]# cat /var/log/rkhunter/rkhunter.log | more


[23:10:58] Running Rootkit Hunter version 1.4.6 on triettm
[23:10:58]
[23:10:58] Info: Start date is Thu Mar  9 23:10:58 +07 2023
[23:10:58]
[23:10:58] Checking configuration file and command-line options...
[23:10:58] Info: Detected operating system is 'Linux'
[23:10:58] Info: Uname output is 'Linux triettm.fpt 3.10.0-1160.el7.x86_64 #1 SM
P Mon Oct 19 16:18:59 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux'
[23:10:58] Info: Command line is /bin/rkhunter --update
[23:10:58] Info: Environment shell is /bin/bash; rkhunter is using bash
[23:10:58] Info: Using configuration file '/etc/rkhunter.conf'
[23:10:58] Info: Installation directory is '/usr'
[23:10:58] Info: Using language 'en'
[23:10:58] Info: Using '/var/lib/rkhunter/db' as the database directory
[23:10:58] Info: Using '/usr/share/rkhunter/scripts' as the support script direc
tory
[23:10:58] Info: Using '/sbin /bin /usr/sbin /usr/bin /usr/local/bin /usr/local/
sbin /usr/libexec /usr/local/libexec' as the command directories
[23:10:58] Info: Using '/var/lib/rkhunter' as the temporary directory
```

Controlling the auditd daemon

On CentOS 7, for some reason that I don't understand, the normal systemctl commands don't work with auditd. (For all other daemons, they do.) So, on your CentOS 7 machine, you'll restart the auditd daemon with the old-fashioned service command, like so:


triettm@triettm:/home/triettm
File Edit View Search Terminal Help

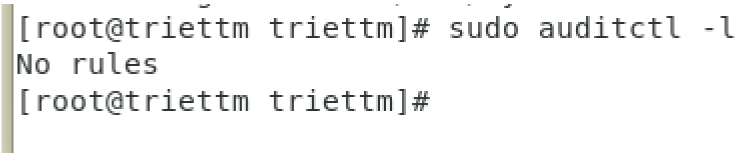
```
[root@triettm triettm]# sudo systemctl restart auditd
Failed to restart auditd.service: Operation refused, unit auditd.service may be
requested by dependency only (it is configured to refuse manual start/stop).
See system logs and 'systemctl status auditd.service' for details.
[root@triettm triettm]# SS
```


triettm@triettm:/home/triettm
File Edit View Search Terminal Help

```
[root@triettm triettm]# sudo service auditd restart
Stopping logging:                                          [  OK  ]
Redirecting start to /bin/systemctl start auditd.service
[root@triettm triettm]#
```

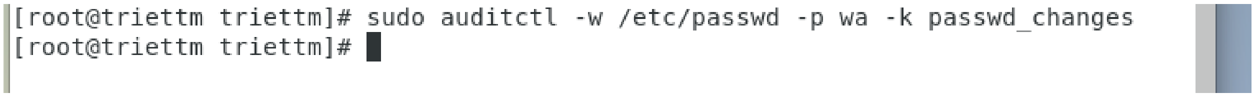
Creating audit rules

Okay, let's start with something simple and work our way up to something awesome. First, let's check to see whether any audit rules are in effect:



```
[root@triettm triettm]# sudo auditctl -l
No rules
[root@triettm triettm]#
```

Auditing a file for changes

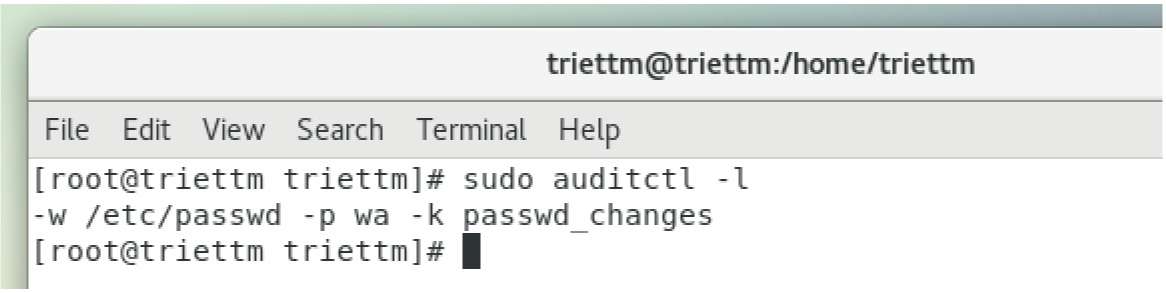


```
[root@triettm triettm]# sudo auditctl -w /etc/passwd -p wa -k passwd_changes
[root@triettm triettm]#
```

As the /etc/passwd have not change anything so the screen print nothing

Here's the breakdown:
-w: This stands for where, and it points to the object that we want to monitor. In this case, it's /etc/passwd.
-p: This indicates the object's permissions that we want to monitor. In this case, we're monitoring to see when anyone either tries to (w)rite to the file, or tries to make (a)ttribute changes. (The other two permissions that we can audit are (r)ead and e(x)ecute.)
-k: The k stands for key, which is just auditd's way of assigning a name to a rule.

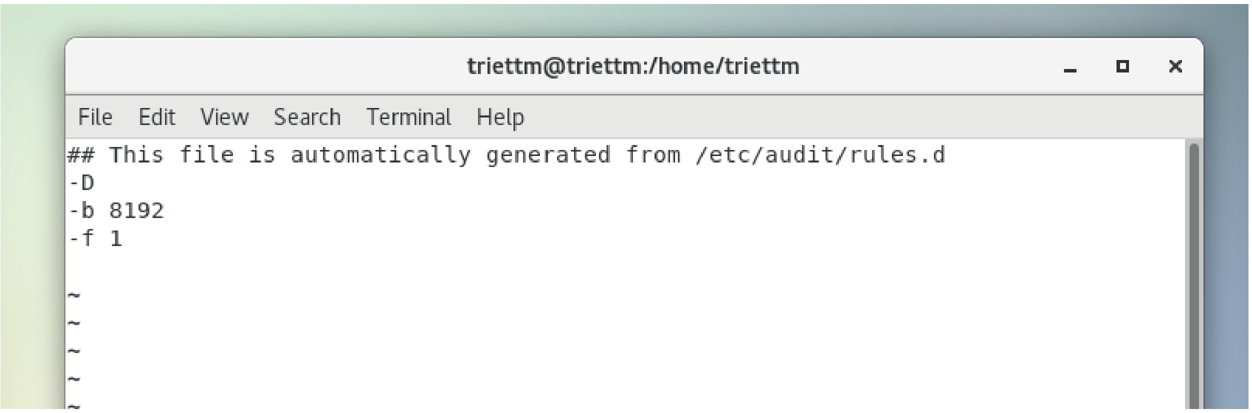
So, passwd_changes is the key, or the name, of the rule that we're creating.



triettm@triettm:/home/triettm
File Edit View Search Terminal Help

```
[root@triettm triettm]# sudo auditctl -l
-w /etc/passwd -p wa -k passwd_changes
[root@triettm triettm]#
```

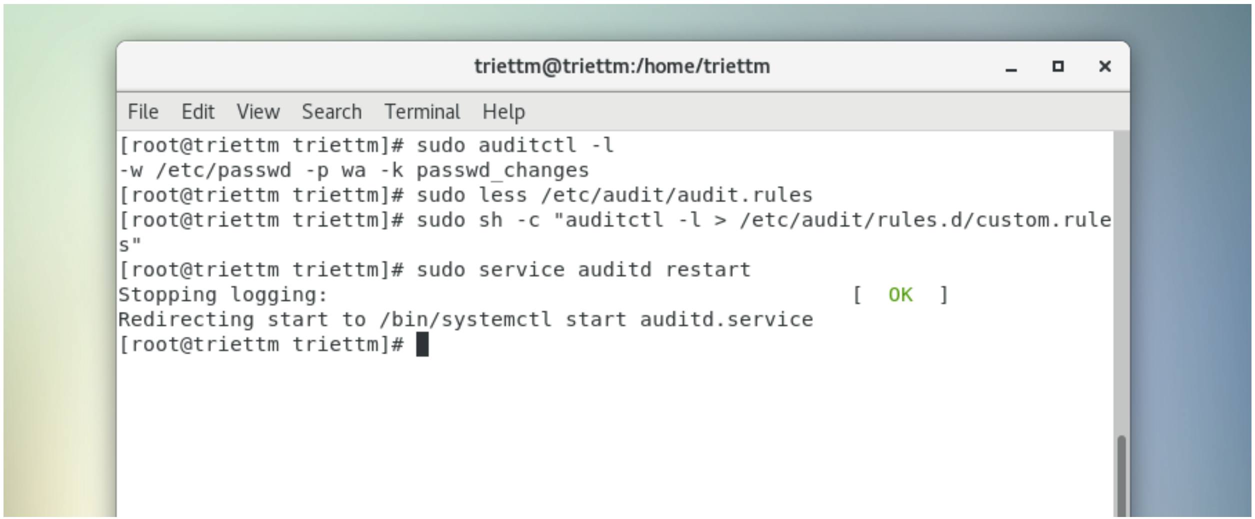
The auditctl -l command shows us that the rule is indeed there.



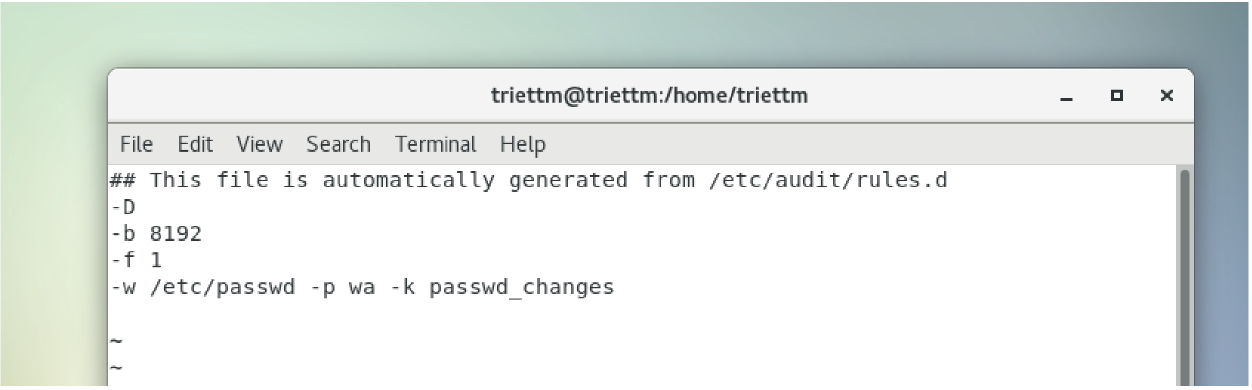
triettm@triettm:/home/triettm
File Edit View Search Terminal Help

```
## This file is automatically generated from /etc/audit/rules.d
-D
-b 8192
-f 1

~
~
~
~
~
```

Here's the breakdown for this file:
-D: This will cause all rules and watches that are currently in effect to be deleted, so that we can start from a clean slate. So, if I were to restart the auditd daemon right now, it would read this audit.rules file, which would delete the rule that I just now created.
-b 8192: This sets the number of outstanding audit buffers that we can have going at one time. If all of the buffers get full, the system can't generate any more audit messages.
-f 1: This sets the failure mode for critical errors, and the value can be either 0, 1, or 2. A -f 0 would set the mode to silent, meaning that auditd wouldn't do anything about critical errors. A -f 1, as we see here, tells auditd to only report the critical errors, and a -f 2 would cause the Linux kernel to go into panic mode. According to the auditctl man page, anyone in a high-security environment would likely want to change this to -f 2. For our purposes though, -f1 works.


triettm@triettm:/home/triettm
File Edit View Search Terminal Help

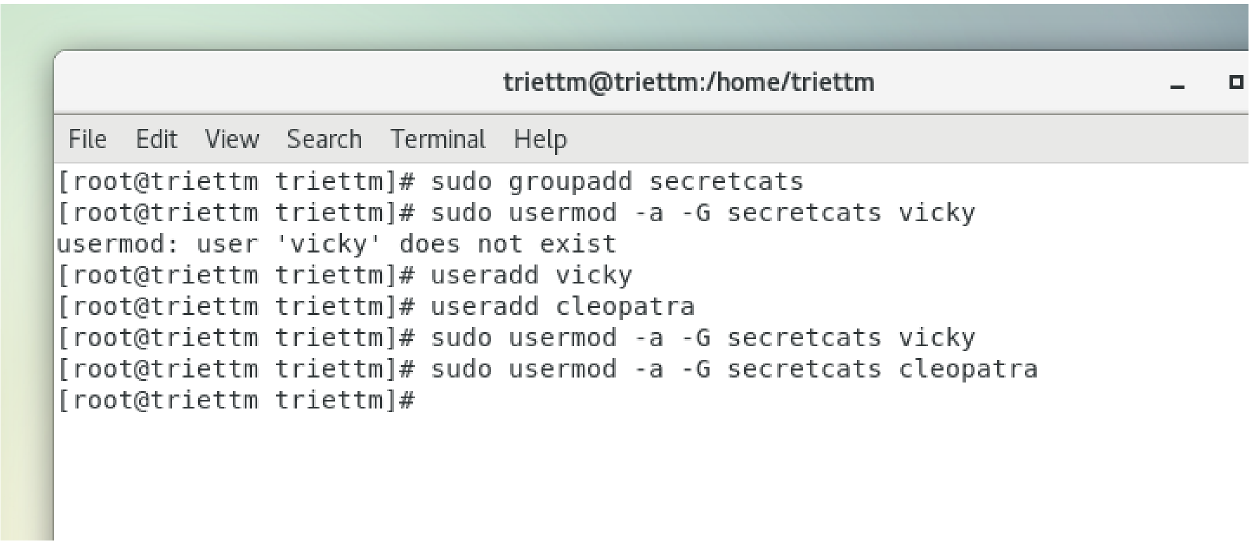
```
[root@triettm triettm]# sudo auditctl -l
-w /etc/passwd -p wa -k passwd_changes
[root@triettm triettm]# sudo less /etc/audit/audit.rules
[root@triettm triettm]# sudo sh -c "auditctl -l > /etc/audit/rules.d/custom.rule
s"
[root@triettm triettm]# sudo service auditd restart
Stopping logging:                                          [  OK  ]
Redirecting start to /bin/systemctl start auditd.service
[root@triettm triettm]# 
```


triettm@triettm:/home/triettm
File Edit View Search Terminal Help

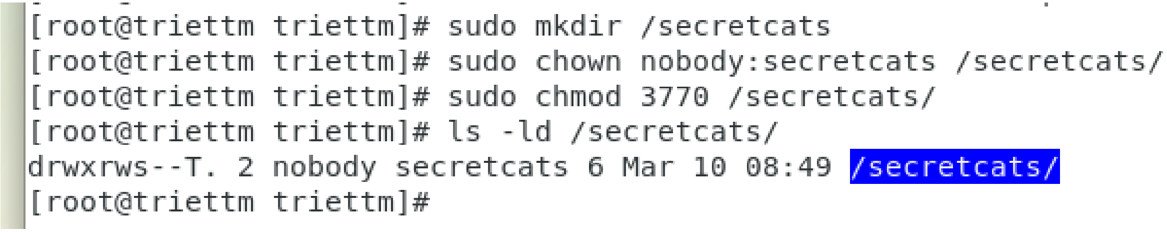
```
## This file is automatically generated from /etc/audit/rules.d
-D
-b 8192
-f 1
-w /etc/passwd -p wa -k passwd_changes

~
~
```

We add new rule to the file

Auditing a directory

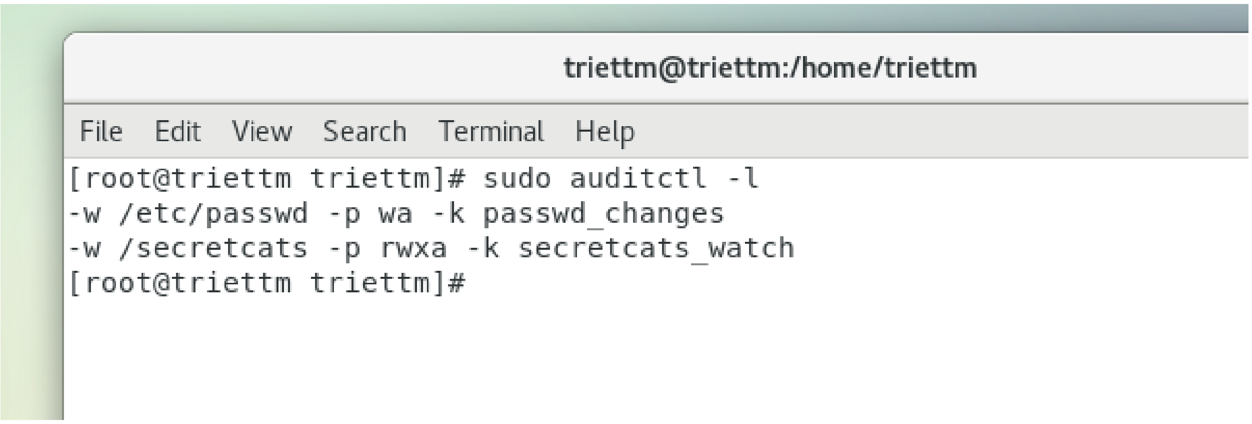


```
[root@triettm triettm]# sudo groupadd secretcats
[root@triettm triettm]# sudo usermod -a -G secretcats vicky
usermod: user 'vicky' does not exist
[root@triettm triettm]# useradd vicky
[root@triettm triettm]# useradd cleopatra
[root@triettm triettm]# sudo usermod -a -G secretcats vicky
[root@triettm triettm]# sudo usermod -a -G secretcats cleopatra
[root@triettm triettm]#
```



```
[root@triettm triettm]# sudo mkdir /secretcats
[root@triettm triettm]# sudo chown nobody:secretcats /secretcats/
[root@triettm triettm]# sudo chmod 3770 /secretcats/
[root@triettm triettm]# ls -ld /secretcats/
drwxrws--T. 2 nobody secretcats 6 Mar 10 08:49 /secretcats/
[root@triettm triettm]#
```

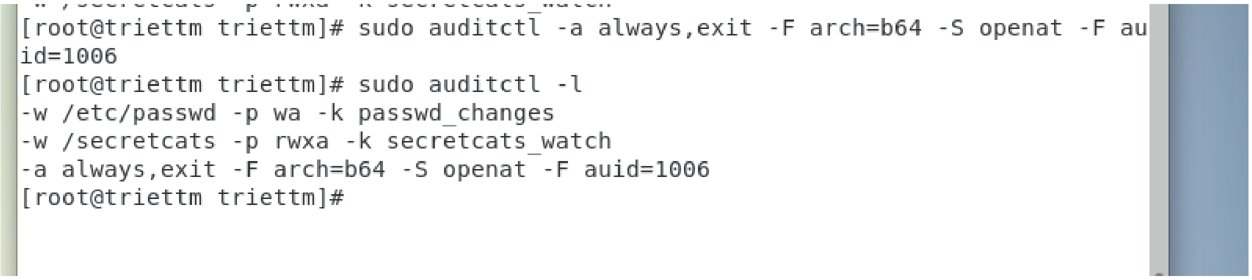
Vicky and Cleopatra want to be absolutely sure that nobody gets into their stuff, so they requested that I set up an auditing rule for their directory:



```
[root@triettm triettm]# sudo auditctl -l
-w /etc/passwd -p wa -k passwd_changes
-w /secretcats -p rwxa -k secretcats_watch
[root@triettm triettm]#
```

As before, the -w denotes what we want to monitor, and the -k denotes the name of the audit rule. This time, I left out the -p option because I want to monitor for every type of access. In other words, I want to monitor for any read, write, attribute change, or execute actions. (Because this is a directory, the execute action happens when somebody tries to cd into the directory.)

Auditing system calls

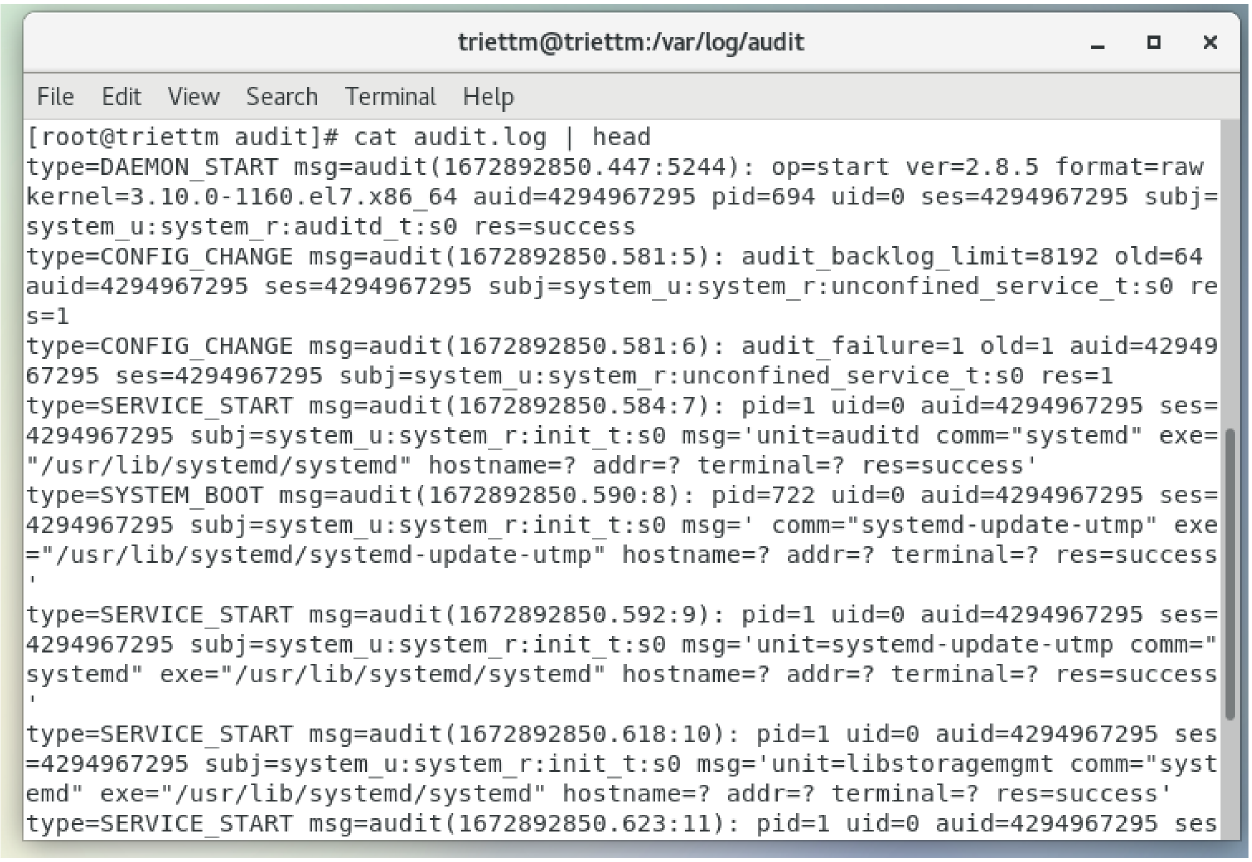


```
-w /secretcats -p rwxa -k secretcats_watch
[root@triettm triettm]# sudo auditctl -a always,exit -F arch=b64 -S openat -F au
id=1006
[root@triettm triettm]# sudo auditctl -l
-w /etc/passwd -p wa -k passwd_changes
-w /secretcats -p rwxa -k secretcats_watch
-a always,exit -F arch=b64 -S openat -F auid=1006
[root@triettm triettm]#
```

Here's the breakdown:
-a always,exit: Here, we have the action and the list. The exit part means that this rule will be added to the system call exit list. Whenever the operating system exits from a system call, the exit list will be used to determine if an audit event needs to be generated. The always part is the action, which means that an audit record for this rule will always be created on exit from the specified system call. Note that the action and list parameters have to be separated by a comma.

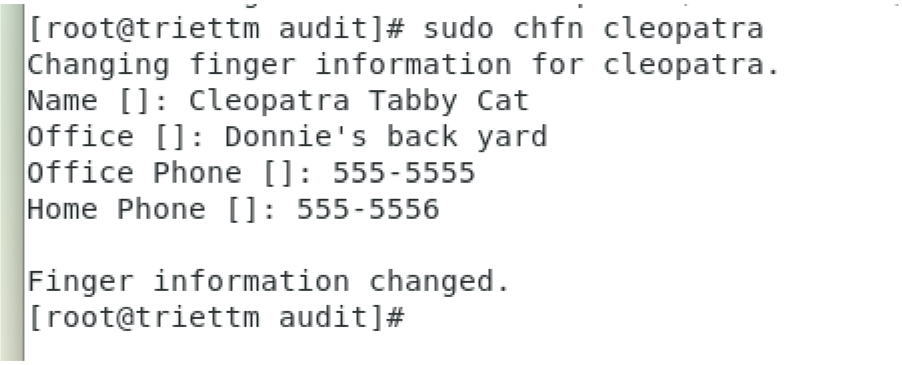
-F arch=b64: The -F option is used to build a rule field, and we see two rule fields in this command. This first rule field specifies the machine's CPU architecture. The b64 means that the computer is running with an x86_64 CPU. (Whether it's Intel or AMD doesn't matter.) Considering that 32-bit machines are dying off and that Sun SPARC and PowerPC machines aren't all that common, b64 is what you'll now mostly see.
-S openat: The -S option specifies the system call that we want to monitor. openat is the system call that either opens or creates a file.
-F auid=1006: This second audit field specifies the user ID number of the user that we want to monitor. (Charlie's user ID number is 1006.)

Using ausearch and aureport


triettm@triettm:/var/log/audit
File Edit View Search Terminal Help

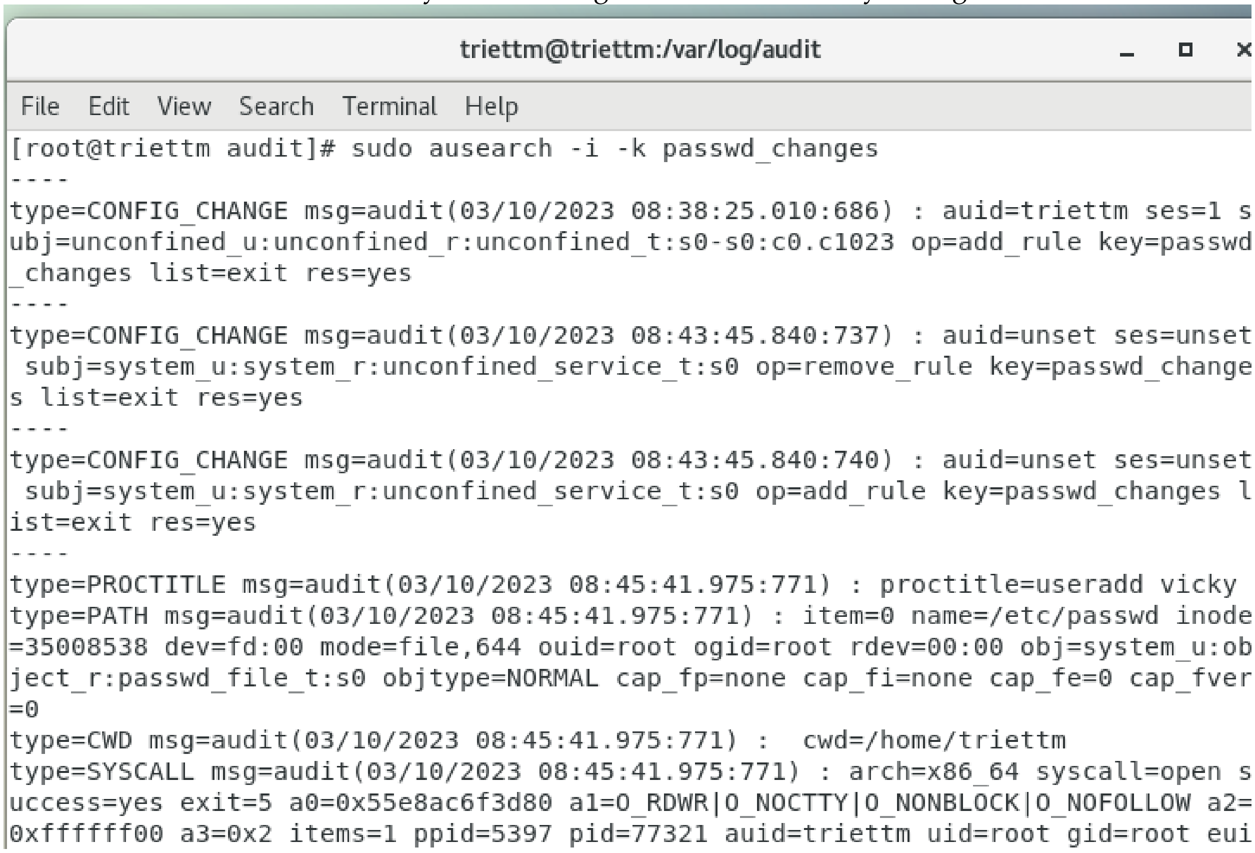
```
[root@triettm audit]# cat audit.log | head
type=DAEMON_START msg=audit(1672892850.447:5244): op=start ver=2.8.5 format=raw
kernel=3.10.0-1160.el7.x86_64 auid=4294967295 pid=694 uid=0 ses=4294967295 subj=
system_u:system_r:auditd_t:s0 res=success
type=CONFIG_CHANGE msg=audit(1672892850.581:5): audit_backlog_limit=8192 old=64
auid=4294967295 ses=4294967295 subj=system_u:system_r:unconfined_service_t:s0 re
s=1
type=CONFIG_CHANGE msg=audit(1672892850.581:6): audit_failure=1 old=1 auid=42949
67295 ses=4294967295 subj=system_u:system_r:unconfined_service_t:s0 res=1
type=SERVICE_START msg=audit(1672892850.584:7): pid=1 uid=0 auid=4294967295 ses=
4294967295 subj=system_u:system_r:init_t:s0 msg='unit=auditd comm="systemd" exe=
"/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
type=SYSTEM_BOOT msg=audit(1672892850.590:8): pid=722 uid=0 auid=4294967295 ses=
4294967295 subj=system_u:system_r:init_t:s0 msg=' comm="systemd-update-utmp" exe
="/usr/lib/systemd/systemd-update-utmp" hostname=? addr=? terminal=? res=success
'
type=SERVICE_START msg=audit(1672892850.592:9): pid=1 uid=0 auid=4294967295 ses=
4294967295 subj=system_u:system_r:init_t:s0 msg='unit=systemd-update-utmp comm="
systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success
'
type=SERVICE_START msg=audit(1672892850.618:10): pid=1 uid=0 auid=4294967295 ses
=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=libstoragemgmt comm="syst
emd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
type=SERVICE_START msg=audit(1672892850.623:11): pid=1 uid=0 auid=4294967295 ses
```

Searching for file change alerts



```
[root@triettm audit]# sudo chfn cleopatra
Changing finger information for cleopatra.
Name []: Cleopatra Tabby Cat
Office []: Donnie's back yard
Office Phone []: 555-5555
Home Phone []: 555-5556

Finger information changed.
[root@triettm audit]#
```

I'll now use ausearch to look for any audit messages that this event may have generated

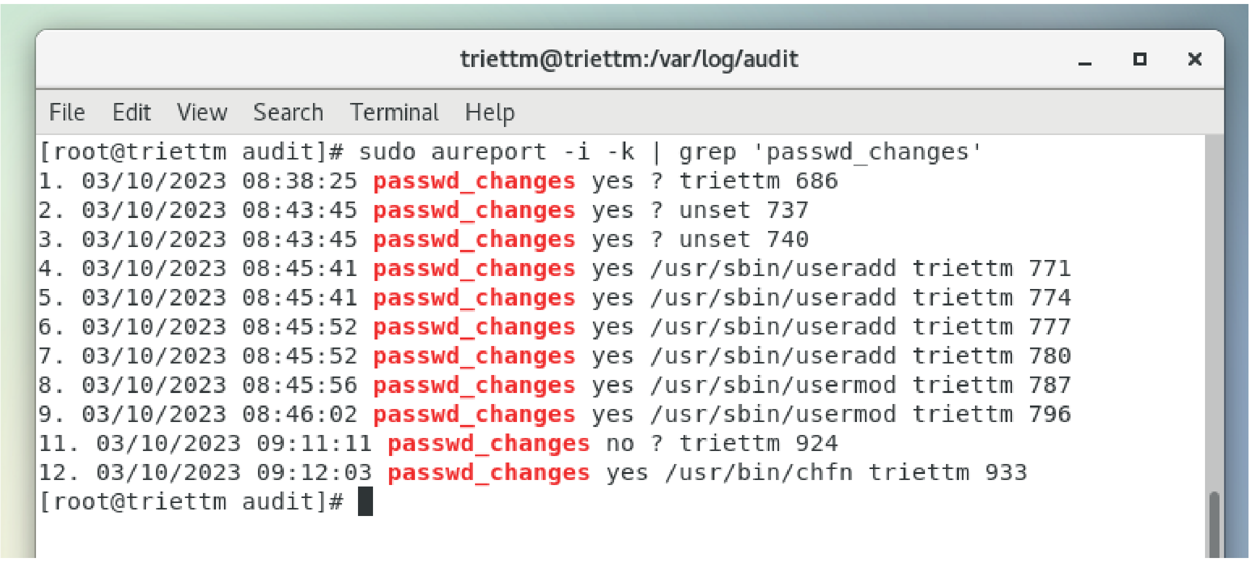

triettm@triettm:/var/log/audit
File Edit View Search Terminal Help

```
[root@triettm audit]# sudo ausearch -i -k passwd_changes
----
type=CONFIG_CHANGE msg=audit(03/10/2023 08:38:25.010:686) : auid=triettm ses=1 s
ubj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 op=add_rule key=passwd
_changes list=exit res=yes
----
type=CONFIG_CHANGE msg=audit(03/10/2023 08:43:45.840:737) : auid=unset ses=unset
 subj=system_u:system_r:unconfined_service_t:s0 op=remove_rule key=passwd_change
s list=exit res=yes
----
type=CONFIG_CHANGE msg=audit(03/10/2023 08:43:45.840:740) : auid=unset ses=unset
 subj=system_u:system_r:unconfined_service_t:s0 op=add_rule key=passwd_changes l
ist=exit res=yes
----
type=PROCTITLE msg=audit(03/10/2023 08:45:41.975:771) : proctitle=useradd vicky
type=PATH msg=audit(03/10/2023 08:45:41.975:771) : item=0 name=/etc/passwd inode
=35008538 dev=fd:00 mode=file,644 ouid=root ogid=root rdev=00:00 obj=system_u:ob
ject_r:passwd_file_t:s0 objtype=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_fver
=0
type=CWD msg=audit(03/10/2023 08:45:41.975:771) :  cwd=/home/triettm
type=SYSCALL msg=audit(03/10/2023 08:45:41.975:771) : arch=x86_64 syscall=open s
uccess=yes exit=5 a0=0x55e8ac6f3d80 a1=O_RDWR|O_NOCTTY|O_NONBLOCK|O_NOFOLLOW a2=
0xffffff00 a3=0x2 items=1 ppid=5397 pid=77321 auid=triettm uid=root gid=root eui
```

Here's the breakdown:

-i: This takes any numeric data and, whenever possible, converts it into text. In this case, it takes user ID numbers and converts them to the actual username, which shows up here as auid=donnie. If I were to leave the -i out, the user information would instead show up as auid=1000, which is my user ID number.

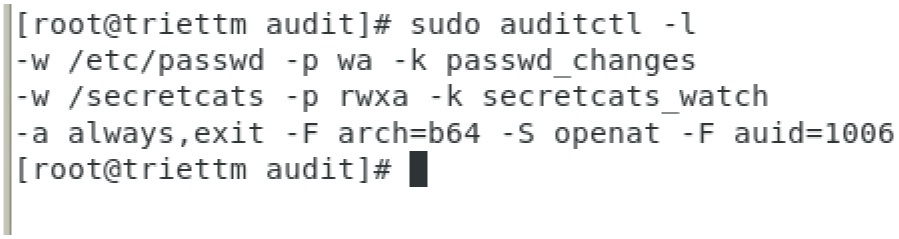
-k passwd_changes: This specifies the key, or the name, of the audit rule for which we want to see audit messages.


triettm@triettm:/var/log/audit
File Edit View Search Terminal Help

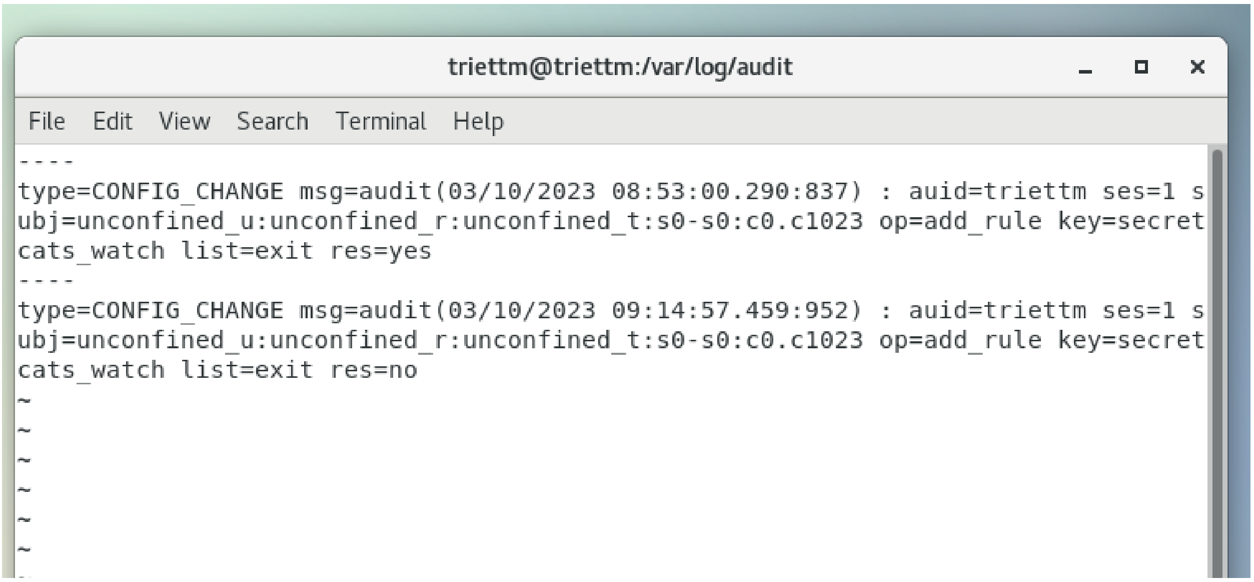
```
[root@triettm audit]# sudo aureport -i -k | grep 'passwd_changes'
1. 03/10/2023 08:38:25 passwd_changes yes ? triettm 686
2. 03/10/2023 08:43:45 passwd_changes yes ? unset 737
3. 03/10/2023 08:43:45 passwd_changes yes ? unset 740
4. 03/10/2023 08:45:41 passwd_changes yes /usr/sbin/useradd triettm 771
5. 03/10/2023 08:45:41 passwd_changes yes /usr/sbin/useradd triettm 774
6. 03/10/2023 08:45:52 passwd_changes yes /usr/sbin/useradd triettm 777
7. 03/10/2023 08:45:52 passwd_changes yes /usr/sbin/useradd triettm 780
8. 03/10/2023 08:45:56 passwd_changes yes /usr/sbin/usermod triettm 787
9. 03/10/2023 08:46:02 passwd_changes yes /usr/sbin/usermod triettm 796
11. 03/10/2023 09:11:11 passwd_changes no ? triettm 924
12. 03/10/2023 09:12:03 passwd_changes yes /usr/bin/chfn triettm 933
[root@triettm audit]# 
```

Searching for directory access rule violations

In our next scenario, we created a shared directory for Vicky and Cleopatra and created an audit rule for it that looks like this



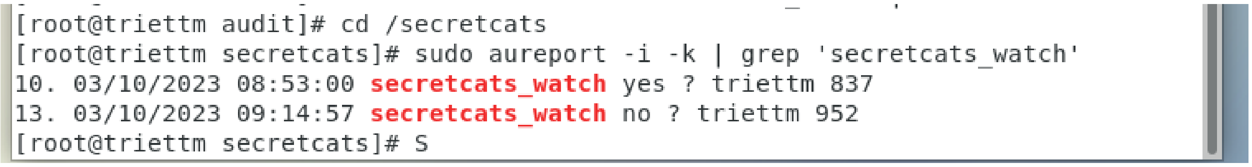
```
[root@triettm audit]# sudo auditctl -l
-w /etc/passwd -p wa -k passwd_changes
-w /secretcats -p rwxa -k secretcats_watch
-a always,exit -F arch=b64 -S openat -F auid=1006
[root@triettm audit]# █
```



triettm@triettm:/var/log/audit
File Edit View Search Terminal Help

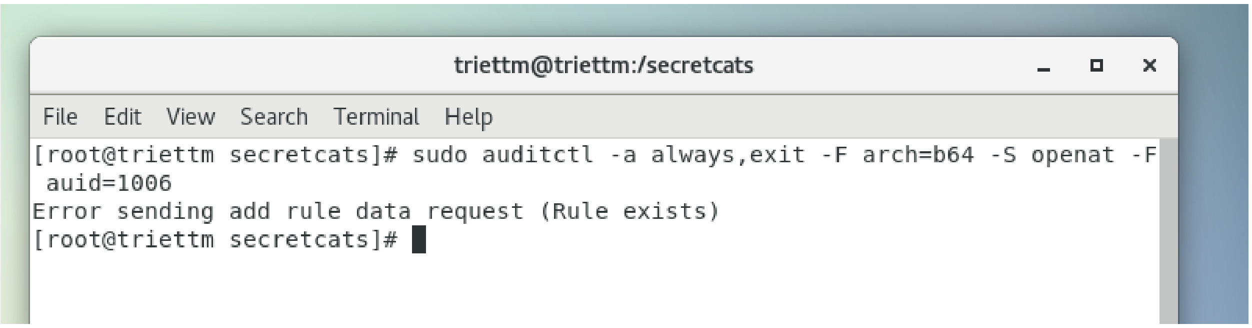
```
----
type=CONFIG_CHANGE msg=audit(03/10/2023 08:53:00.290:837) : auid=triettm ses=1 s
ubj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 op=add_rule key=secret
cats_watch list=exit res=yes
----
type=CONFIG_CHANGE msg=audit(03/10/2023 09:14:57.459:952) : auid=triettm ses=1 s
ubj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 op=add_rule key=secret
cats_watch list=exit res=no
~
~
~
~
~
~
```

Next, let's say that that sneaky Charlie guy logs in and tries to get into the /secretcats directory:



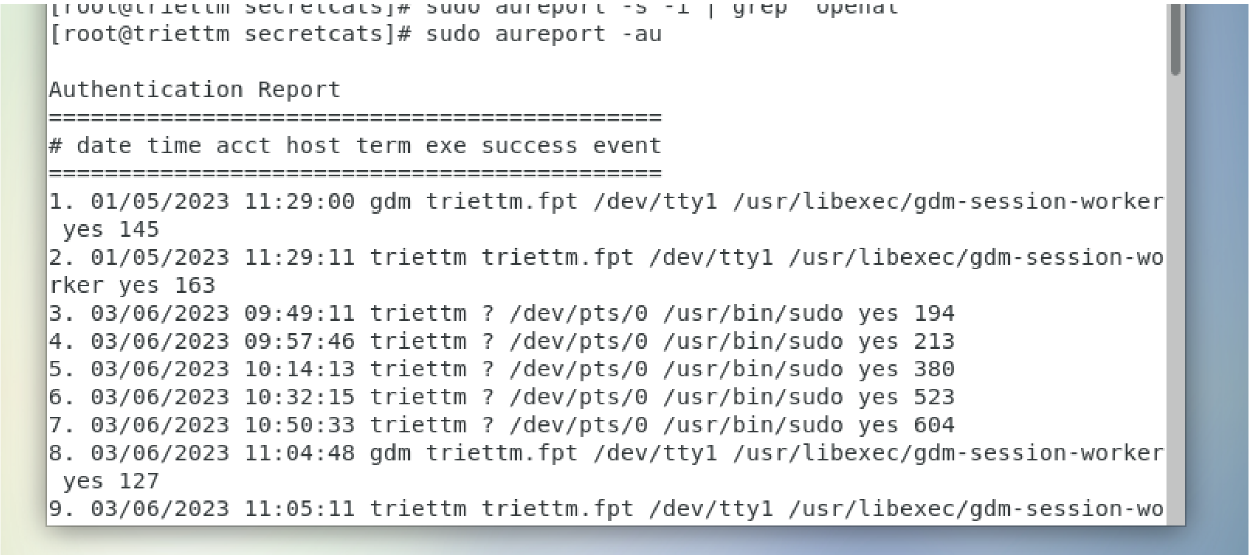
```
[root@triettm audit]# cd /secretcats
[root@triettm secretcats]# sudo aureport -i -k | grep 'secretcats_watch'
10. 03/10/2023 08:53:00 secretcats_watch yes ? triettm 837
13. 03/10/2023 09:14:57 secretcats_watch no ? triettm 952
[root@triettm secretcats]# S
```

Searching for system call rule violations



triettm@triettm:/secretcats
File Edit View Search Terminal Help

```
[root@triettm secretcats]# sudo auditctl -a always,exit -F arch=b64 -S openat -F
 auid=1006
Error sending add rule data request (Rule exists)
[root@triettm secretcats]# █
```



```
[root@triettm secretcats]# sudo aureport -s -i | grep "openat"
[root@triettm secretcats]# sudo aureport -au

Authentication Report
============================================
# date time acct host term exe success event
============================================
1. 01/05/2023 11:29:00 gdm triettm.fpt /dev/tty1 /usr/libexec/gdm-session-worker
 yes 145
2. 01/05/2023 11:29:11 triettm triettm.fpt /dev/tty1 /usr/libexec/gdm-session-wo
rker yes 163
3. 03/06/2023 09:49:11 triettm ? /dev/pts/0 /usr/bin/sudo yes 194
4. 03/06/2023 09:57:46 triettm ? /dev/pts/0 /usr/bin/sudo yes 213
5. 03/06/2023 10:14:13 triettm ? /dev/pts/0 /usr/bin/sudo yes 380
6. 03/06/2023 10:32:15 triettm ? /dev/pts/0 /usr/bin/sudo yes 523
7. 03/06/2023 10:50:33 triettm ? /dev/pts/0 /usr/bin/sudo yes 604
8. 03/06/2023 11:04:48 gdm triettm.fpt /dev/tty1 /usr/libexec/gdm-session-worker
 yes 127
9. 03/06/2023 11:05:11 triettm triettm.fpt /dev/tty1 /usr/libexec/gdm-session-wo
```