

# How to scan malware and rootkits on Linux server

There are many tools to help scan Linux servers for malware and rootkits. This article will provide some of the best options to help deal with these cyber-enemies.

Worms, viruses, malware and rootkits are a concern for every server administrator. When the system is infected, it can collect sensitive information and cause financial damage.

1. Differentiate viruses, trojans, worms and rootkits

Fortunately, there are many tools that help scan Linux servers for malware and rootkits. This article will provide some of the best options to help deal with these cyber-enemies.

1. Top 7 best free antivirus software for Linux
2. Install AntiVirus on Ubuntu
3. 7 best antivirus programs for Ubuntu

## 1. Clam AV

This command-line antivirus software is designed to integrate closely with mail servers and is available on all systems including prominent Linux distributions like SuSE, Fedora and Ubuntu.

Installing this software on Ubuntu is easy with the following command:

```
sudo apt install clamav clamav-daemon
```

```
jeff@everliving: ~  
File Edit View Search Terminal Help  
jeff@everliving:~$ sudo apt-get install clamav clamav-daemon  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
libegl-mesa0:i386 libegl1:i386 libgbm1:i386 libllvm6.0 libllvm6.0:i386  
libllvm7 libllvm7:i386 libpkcs11-helper1 libsdl-ttf2.0-0  
libwayland-egl1-mesa:i386 libwayland-server0:i386 libxcb-xfixes0:i386  
linux-image-4.13.0-46-generic openvpn php7.1-common stunnel4  
x11proto-dri2-dev x11proto-gl-dev  
Use 'sudo apt autoremove' to remove them.  
The following additional packages will be installed:  
clamav-base clamav-freshclam clamdscan curl libclamav7 libcurl4 libllvm3.9  
libtftm1 php-curl php7.2-curl  
Suggested packages:  
clamav-docs daemon libclamunrar7  
The following packages will be REMOVED:  
libcurl3 php7.1-curl virtualbox-5.2  
The following NEW packages will be installed:  
clamav clamav-base clamav-daemon clamav-freshclam clamdscan libclamav7  
libcurl4 libllvm3.9 libtftm1 php7.2-curl  
The following packages will be upgraded:  
curl php-curl  
2 upgraded, 10 newly installed, 3 to remove and 37 not upgraded
```

After installation, Clam AV can be used from the terminal to the entire system and to clean all infected files. In addition, Clam AV also provides powerful real-time scanning and source tracking utilities.

To run a simple test for the server file system, use the following command from the root directory:

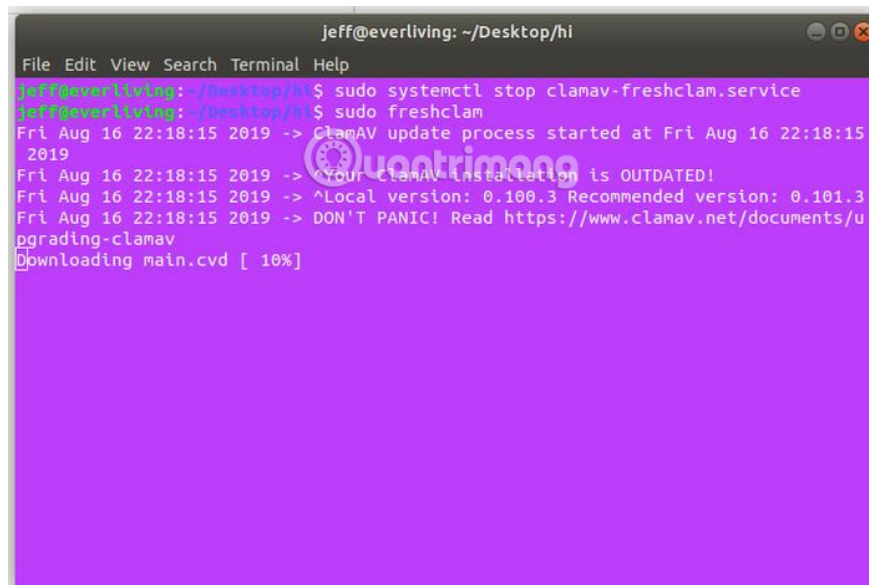
```
clamscan -r -i
```

The above command will ask Clam AV to perform a recursive scan (check the file in the file) and print the infected document to the terminal. However, before running this command, you need to allow Clam AV enough time to install its virus signature database on the machine. You can cancel the service and restart it manually with the following command:

```
sudo systemctl stop clamav-freshclam.service
```

Followed by the command:

```
sudo freshclam
```

A terminal window titled 'jeff@everliving: ~/Desktop/hi' showing the execution of 'sudo systemctl stop clamav-freshclam.service' and 'sudo freshclam'. The output indicates that the ClamAV update process started at Fri Aug 16 22:18:15 2019, and that the current installation is outdated. It shows the local version as 0.100.3 and the recommended version as 0.101.3. A warning message says 'DON'T PANIC! Read https://www.clamav.net/documents/upgrading-clamav'. The terminal also shows 'Downloading main.cvd [ 10%]'.

To automatically delete virus files from the system during the scan, use the following command:

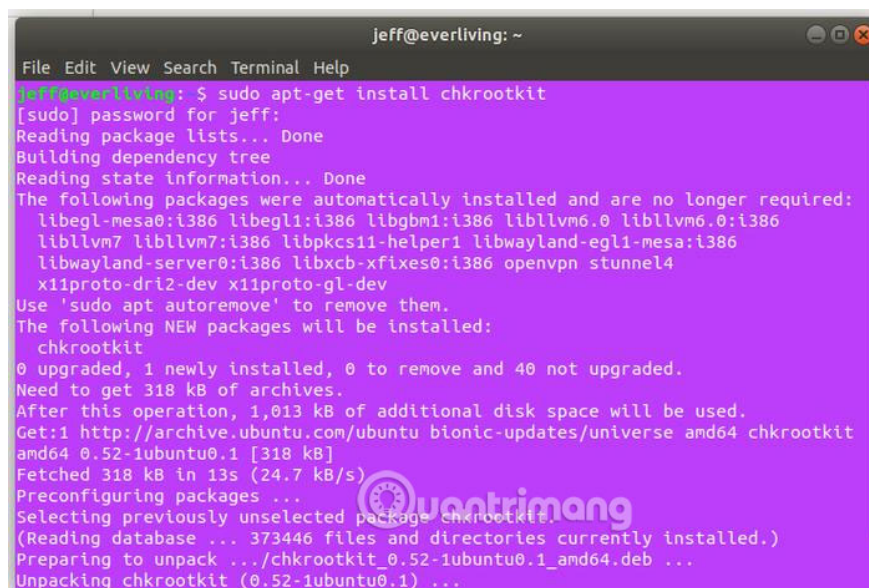
```
clamscan -r -i --remove
```

## 2. Chkrootkit

This tool runs several tests to detect kernel modules that have downloaded malware, worms and rootkits.

For Ubuntu, this tool is in the official software store, use the following command to install it:

```
sudo apt install chkrootkit
```

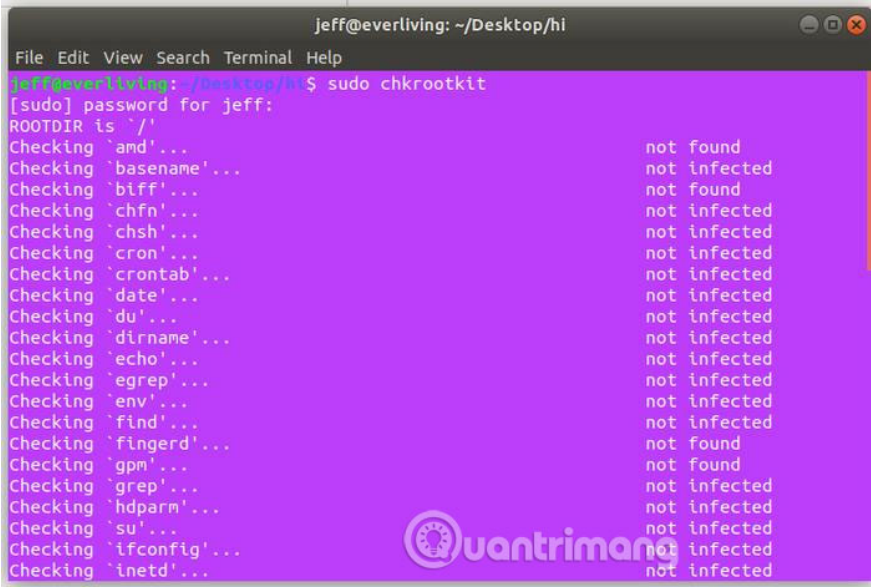
A terminal window titled 'jeff@everliving: ~' showing the execution of 'sudo apt-get install chkrootkit'. The terminal output shows the package lists being read, the dependency tree being built, and the state information being read. It lists several packages that were automatically installed and are no longer required, including libegl-mesa0:i386, libegl1:i386, libgbm1:i386, libllvm6.0, libllvm6.0:i386, libllvm7, libllvm7:i386, libpkcs11-helper1, libwayland-egl1-mesa:i386, libwayland-server0:i386, libxcb-xfixes0:i386, openvpn, stunnel4, x11proto-dri2-dev, and x11proto-glx-dev. It then shows that the following NEW packages will be installed: chkrootkit. The terminal also shows the disk space requirements and the download progress of the package.

Unlike Clam AV, chkrootkit is a passive tool and lacks functionality to act on detected threats. You need to research and manually delete suspicious files found by this tool on the server's file system. Therefore you need to

copy the output for later reference.

To run this tool, use the following command:

```
sudo chkrootkit
```



```
jeff@everliving: ~/Desktop/hi
File Edit View Search Terminal Help
jeff@everliving:~/Desktop/hi$ sudo chkrootkit
[sudo] password for jeff:
ROOTDIR is '/'
Checking `amd'... not found
Checking `basename'... not infected
Checking `biff'... not found
Checking `chfn'... not infected
Checking `chsh'... not infected
Checking `cron'... not infected
Checking `crontab'... not infected
Checking `date'... not infected
Checking `du'... not infected
Checking `dirname'... not infected
Checking `echo'... not infected
Checking `egrep'... not infected
Checking `env'... not infected
Checking `find'... not infected
Checking `fingerd'... not found
Checking `gpm'... not found
Checking `grep'... not infected
Checking `hdparm'... not infected
Checking `su'... not infected
Checking `ifconfig'... not infected
Checking `inetd'... not infected
```

### 3. AIDE

The name of this tool stands for the phrase Advanced Intrusion Detection Environment, a completely free alternative to the Tripwire analog tool.

AIDE allows close monitoring of system files to monitor time and how they are modified or accessed in other ways. This tool is very easy to install from Ubuntu's official software store with the apt command.

```
sudo apt install aide
```

```
jeff@everliving: ~
File Edit View Search Terminal Help
jeff@everliving:~$ sudo apt install aide
[sudo] password for jeff:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libegl-mesa0:i386 libegl1:i386 libgbm1:i386 libllvm6.0 libllvm6.0:i386
  libllvm7 libllvm7:i386 libpkcs11-helper1 libsdl-ttf2.0-0
  libwayland-egl1-mesa:i386 libwayland-server0:i386 libxcb-xfixes0:i386
  openvpn php7.1-common stunnel4 x11proto-dri2-dev x11proto-gl-dev
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  aide-common bsd-mailx postfix
Suggested packages:
  procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre postfix-ldap
  postfix-sqlite sasl2-bin dovecot-common postfix-cdb postfix-doc
The following NEW packages will be installed:
  aide aide-common bsd-mailx postfix
0 upgraded, 4 newly installed, 0 to remove and 40 not upgraded.
Need to get 2,059 kB of archives.
After this operation, 6,864 kB of additional disk space will be used.
Do you want to continue? [Y/n] 
```

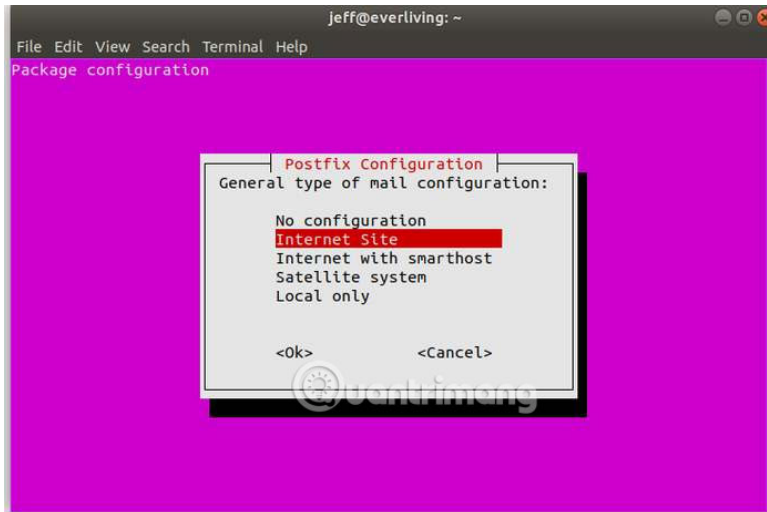
To complete the installation process, you need to configure Postfix through the options. To navigate these items, you can use the Tab key or the arrow keys, then press **Enter** to select. Postfix is used to send information to email addresses according to the time you set.

```
jeff@everliving: ~
File Edit View Search Terminal Help
Package configuration

Postfix Configuration

Please select the mail server configuration type that best meets your
needs.

No configuration:
  Should be chosen to leave the current configuration unchanged.
Internet site:
  Mail is sent and received directly using SMTP.
Internet with smarthost:
  Mail is received directly using SMTP or by running a utility such
  as fetchmail. Outgoing mail is sent using a smarthost.
Satellite system:
  All mail is sent to another machine, called a 'smarthost', for
  delivery.
Local only:
```

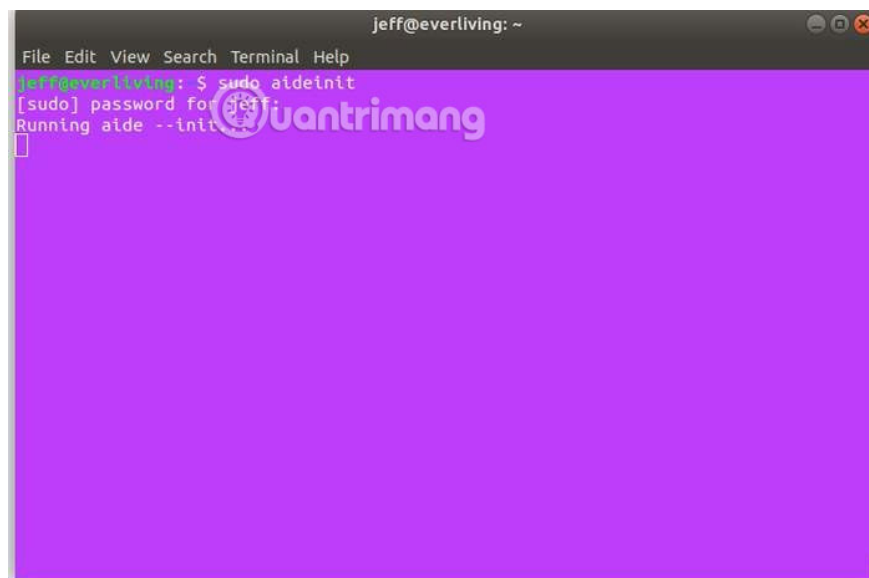


AIDE configuration requires file processing in the following addresses:

```
/var/lib/aide /etc/aide
```

First, create the database and configuration file by running the following command:

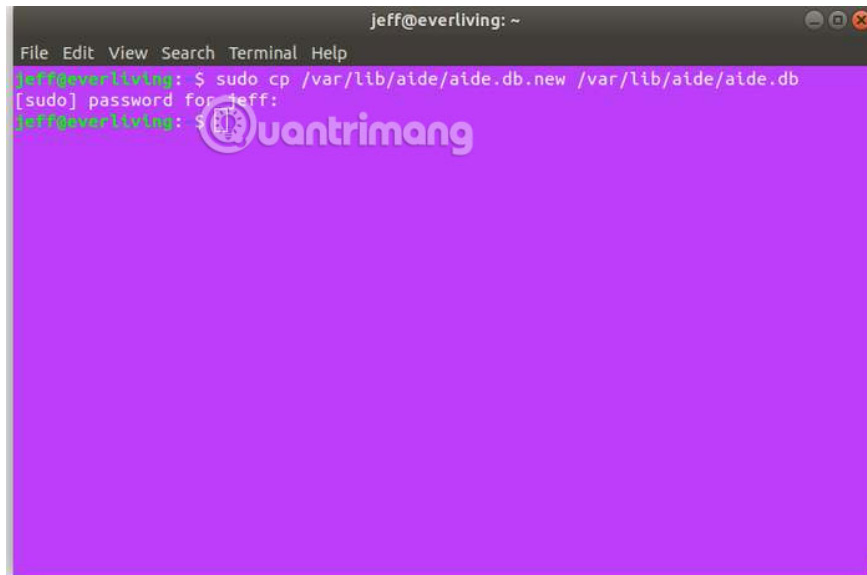
```
sudo aideinit
```



Once completed, this process to the database and configuration file created in / var / lib / aide / in the name aide.db.new and aide.conf.autogenerated. Both need to be copied into aide.db and aide.conf respectively to work properly.

Create a copy of the database file with the new name easily with the following command:

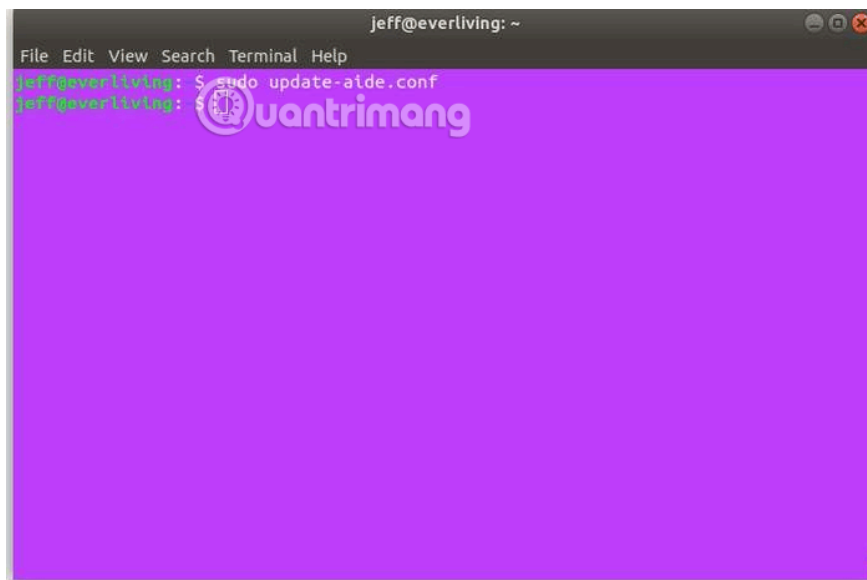
```
sudo cp /var/lib/aide/aide.db.new /var/lib/aide/aide.db
```



```
jeff@everliving: ~  
File Edit View Search Terminal Help  
jeff@everliving: $ sudo cp /var/lib/aide/aide.db.new /var/lib/aide/aide.db  
[sudo] password for jeff:  
jeff@everliving: $
```

Before renaming and copying the configuration file, update it with the following command:

```
sudo update-aide.conf
```



```
jeff@everliving: ~  
File Edit View Search Terminal Help  
jeff@everliving: $ sudo update-aide.conf  
jeff@everliving: $
```

Once you've updated the configuration file, copy it to the correct directory with the following command:

```
sudo cp /var/lib/aide/aide.conf.autogenerated /etc/aide/aide.conf
```

Now, AIDE will work on the server and actively monitor HASHED of the file system it created.

You can configure AIDE to not scan specific folders, run periodically and many other things by modifying the configuration file. However, with the following command you can see enough information on the system output:

```
aide -c /etc/aide/aide.conf -C
```

AIDE is most effective when its configuration is accessed from read-only addresses because rootkits can allow attackers to edit files.

The tools mentioned in this article will help you scan Linux servers for malware and rootkits with a variety of techniques. Rootkits are the hardest digital threat to solve, but they can be prevented with appropriate software.

You finished reading the article "**How to scan malware and rootkits on Linux server**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.