**DirectAdmin Forums** (*http://www.directadmin.com/forum/index.php*)
- **How-To Guides** (*http://www.directadmin.com/forum/forumdisplay.php?f=40*)
- - **HOWTO: ProFTPD Antivirus using CLAMAV** (*http://www.directadmin.com/forum/showthread.php?t=30855*)

sHuKKo 05-09-2009 06:25 AM

**HOWTO: ProFTPD Antivirus using CLAMAV**

This howto is about making ProFTPD work with CLAMAV to scan all files uploaded by users using a FTP client.
Recently our customers are having real difficulty with Iframe viruses, Php shells and other kind of windows viruses are also a headache always.
ClamAV is already working with exim mail server in our servers for years. Why not make it also scan incoming FTP uploads.This will add more CPU Time to our servers, but preventing users to upload any kind of virus data makes sense.

How will this work? :
-we will add ClamAV support to ProFTPD using mod_clamav module.
-when a user uploads a file using FTP, ClamAV will scan incoming file after upload finishes.
-if any kind of virus like signature found by ClamAV, uploaded file will be deleted from server, notifying the FTP client.

1- we will need a working ClamAV installation on server before this. I prefer not to tell how to install ClamAV to server this time, because there is already a very handy script called update.script which can install ClamAV and tons of other stuff. I take portions of this script to automate my process. Thanks to original update.script creator!

If ClamAV is already installed and updating itself regularly please skip this step.

-INSTALL CLAMAV-

Code:

```
mkdir /usr/local/updatescript
cd /usr/local/updatescript
wget http://tools.web4host.net/update.script
chmod 755 update.script
```

Run it once.

Code:

```
./update.script
```

Install Clamav

Code:

```
./update.script CLAMAV
```

Clamav Installation Done!

2- Update ProFTPD with current version. And patch it using mod_clamav for ClamAV usage.

Code:

```
cd ~
wget http://www.serverdirekt.com/DA/FTPAV/ftpantivirus
chmod +x ftpantivirus
./ftpantivirus
```

-this script will download ProFTPD, download mod_clamav latest version, patch ProFTPD with mod_clamav, compile and install new ProFTPD package with ClamAV support.

3- We need to edit our clamav.conf file to allow TCPSocket connections to port 3310

Code:

```
nano /etc/clamd.conf
```

find #TCPSocket 3310 line and comment it out.
find #TCPAddr 127.0.0.1 line and comment it out.
Final file will look like this:

Code:

```
....................
# Path to a local socket file the daemon will listen on.
# Default: disabled (must be specified by a user)
LocalSocket /tmp/clamd

# Remove stale socket after unclean shutdown.
# Default: no
FixStaleSocket yes

# TCP port address.
# Default: no
TCPSocket 3310

# TCP address.
# By default we bind to INADDR_ANY, probably not wise.
# Enable the following to provide some degree of protection
# from the outside world.
# Default: no
TCPAddr 127.0.0.1
....................
```

4- Finally we need to edit proftpd.conf to use our new mod_clamav module.

Code:

```
nano /etc/proftpd.conf
```

inside <Global></Global> tags at the end add:

Code:

```
<IfModule mod_clamav.c>
  ClamAV on
  ClamServer localhost
  ClamPort 3310
  ClamMaxSize 5 Mb
</IfModule>
```

we do not want to scan files bigger than 5 Mb to save some CPU time.

5- Restart ClamAv and ProFTPD to test this out!

Code:

```
service clamd restart
service proftpd restart
```

6- Finally go to http://www.eicar.org/anti_virus_test_file.htm to download eicar test virus and upload it to your ftp server with your favorite FTP client.

If you see something like that on your FTP client logs, well done!

Code:

```
Command:        STOR eicar_com.zip
Response:        150 Opening BINARY mode data connection for eicar_com.zip
Response:        550 Virus Detected and Removed: Eicar-Test-Signature
Status:        Retrieving directory listing...
```

7- IF something goes wrong and your ClamAV enabled ftp server is not scanning files as it should.

first check ProFTPD if mod_clamav is activated

Code:

```
proftpd -vv
```

If you see mod_clamav.c under Loaded modules:
you have mod_clamav ready.

For further investigation we can run our ProFTPD server in debug mode to see what's going on:

Code:

```
service proftpd stop
proftpd -n -d 10
```

Try to login and upload eicar test virus to your FTP now, you will see what's going on under the hood in good detail...

FINAL NOTE: I tested this only on Centos 5.x i386 and X86_64 servers. So there is no guarantee that it will work on any other O/S.

### tillo

05-09-2009 07:05 AM

Nice tutorial, thanks! I believe you wrote "mod_proftpd" instead of "mod_clamav" a few times though.

### sHuKKo

05-09-2009 07:10 AM

Quote:

> Originally Posted by **tillo** (Post 156457)
> *Nice tutorial, thanks! I believe you wrote "mod_proftpd" instead of "mod_clamav" a few times though.*

Yes you're absolutely right!
I changed all mod_proftpd's to mod_clamav's.
Thank you very much for pointing this :)

### magic1000

05-10-2009 04:32 AM

Oh very good!
I test upload a c99 shell, it was removed! :):)

### Brightlayer

05-10-2009 12:58 PM

I am getting nothing, it's all installed, patched and what not.

It just gives me a message saying no virus has been detected in any file that I upload.

```
Going to virus scan absolute filename = '/home/admin/eicar_com.zip' with relative filename = '/eicar_com.zip'.
mod_clamav/0.10: Connecting to remote Clamd host '127.0.0.1' on port 3310
ROOT PRIVS at mod_clamav.c:252
ROOT PRIVS: ID switching disabled
PRIVS_RELINQUISH: ID switching disabled
Successfully reconnected to Clamd.
No virus detected in filename = '/home/admin/eicar_com.zip'.
dispatching POST_CMD command 'STOR eicar_com.zip' to mod_ratio
dispatching POST_CMD command 'STOR eicar_com.zip' to mod_xfer
dispatching LOG_CMD command 'STOR eicar_com.zip' to mod_log
dispatching LOG_CMD command 'STOR eicar_com.zip' to mod_xfer
Transfer completed: 184 bytes in 0.05 seconds
```

### sHuKKo

05-10-2009 04:20 PM

Chris
download a eicar test virus directly to server and scan it using clamav on the server.

Code:

```
wget http://www.eicar.org/download/eicar_com.zip
clamscan eicar_com.zip
```

If clamav installed correctly it *must* find the virus

your proftpd log looks very good. everything is working as it should be.
maybe the av software on your client pc removes the test virus before you try to upload it :)

### Brightlayer

05-10-2009 06:02 PM

```
[root@fuchsia ~]# clamscan eicar_com.zip
eicar_com.zip: Eicar-Test-Signature FOUND

----------- SCAN SUMMARY -----------
Known viruses: 549222
Engine version: 0.95.1
```

```
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 4.480 sec (0 m 4 s)
```

That worked fine, and I have tried this on a development machine with no antivirus, so it's not the client pc deleting the virus before it uploads.

## sHuKKo

05-11-2009 01:16 AM

Chris
In that case I really don't have a clue about this.
I tried to replicate the same situation in 5 of my servers.
Each time it works!

## daveyw

05-11-2009 01:54 AM

Can you check if mod_clam is installed?

Code:

```
proftpd -vv
```

Ive just installed this on my box without any problems;

Quote:

```
[11-5-2009 9:56:16] 150 Opening BINARY mode data connection for eicar_com.zip
[11-5-2009 9:56:16] 550 Virus Detected and Removed: Eicar-Test-Signature
```

## Brightlayer

05-11-2009 06:09 AM

This is the output from the version parameter on the proftpd build.

Quote:

```
[root@fuchsia /]# proftpd -vv
ProFTPD Version: 1.3.2 (stable)
Scoreboard Version: 01040002
Built: Sun May 10 19:47:59 BST 2009

Loaded modules:
mod_cap/1.0
mod_clamav.c
mod_tls/2.2.1
mod_readme.c
mod_ratio/3.3
mod_ident/1.0
mod_facts/0.1
mod_delay/0.6
mod_site.c
mod_log.c
mod_ls.c
mod_auth.c
mod_auth_file/0.8.3
mod_auth_unix.c
mod_xfer.c
mod_core.c
```

## Brightlayer

05-11-2009 07:18 AM

I just want to find out if everyone who had this working, installed ClamAV using the 'update.script' or did you have an existing installation of it?

I have an existing install that I've modified the config to support the TCP socket connections, it is linked into Exim prior to this however, for scanning inbound email.

## sHuKKo

05-11-2009 07:44 AM

Quote:

> Originally Posted by **Brightlayer** (Post 156555)
> *I just want to find out if everyone who had this working, installed ClamAV using the 'update.script' or did you have an existing installation of it?*
>
> *I have an existing install that I've modified the config to support the TCP socket connections, it is linked into Exim prior to this however, for scanning inbound email.*

In my own tests and installations I always used update.script
Maybe your clamav installation paths are different.
backup your clamd.conf and reinstall clamav using update.script if possible.

Brightlayer

05-11-2009 08:59 AM

I'll give it a go, will drop a reply with my findings.

Brightlayer

05-11-2009 12:43 PM

Just installed ClamAV as per the 'update.script' and still the same result.

Brightlayer

05-11-2009 01:12 PM

At very last we have some joy, I have no idea what's different, just did a make uninstall and went back to basics. I used the scripts as a reference but did not actually execute any of them.

Quote:

```
Going to virus scan absolute filename = '/home/admin/eicar_com.zip' with relative filename = '/eicar_com.zip'.
mod_clamav/0.11rc: Connecting to remote Clamd host '127.0.0.1' on port 3310
ROOT PRIVS at mod_clamav.c:227
ROOT PRIVS: ID switching disabled
PRIVS_RELINQUISH: ID switching disabled
Successfully reconnected to Clamd.
mod_clamav/0.11rc: Virus 'Eicar-Test-Signature' found in '/home/admin/eicar_com.zip'
dispatching LOG_CMD_ERR command 'STOR eicar_com.zip' to mod_log
dispatching LOG_CMD_ERR command 'STOR eicar_com.zip' to mod_xfer
```

daveyw

05-11-2009 03:49 PM

I guess you have forgot to edit the clamd.conf. If needed you can send me a PM with your SSH login and a 'test' FTP to fix your problem.

Brightlayer

05-11-2009 03:57 PM

**daveyw**

I did not forget to do anything, it's just the first two builds with mod_clamav v0.10 did not show as working.

I proceeded to use mod_clamav v0.11rc1 and I saw some action with the scanning while in an ftp transaction, so it seems to be an issue with the version of mod_clamav, as that's the only thing I changed in the latest build.

daveyw

05-11-2009 04:04 PM

Mmmm i'm runnning the mod_clamav on CentOS 5.3 x86_64 without any problems (and for me he downloaded 0.11rc)

I guess he (sHuKKo) updated before I've installed it :P

sHuKKo

05-12-2009 12:26 AM

Quote:

> Originally Posted by **daveyw** (Post 156603)
> *Mmmm i'm runnning the mod_clamav on CentOS 5.3 x86_64 without any problems (and for me he downloaded 0.11rc)*
>
> *I guess he (sHuKKo) updated before I've installed it :P*

current versions I used in this howto are:

clamav: 0.95.1
proftpd: 1.3.2
mod_clamav: 0.11rc

I will update my script used in this howto whenever a new version appears.

Duboux

05-12-2009 02:01 AM

Will / how can this also work with file uploads via the web ?

All times are GMT -7. The time now is 02:38 PM.

Page 1 of 3 **1** 2 3 >

Show 20 post(s) from this thread on one page