How to check about infected files in clamav log files

Author : admin

I've just run clamav with low priority to check the whole drive of a server for infected files Phpshells and other unwanted script kiddie tools. This was part of my check up if the server is compromised, after yesterday's unexpected cracker break in one of our company servers

nice -n 19 clamav -r /* -l /var/log/clamav-scan.log

This exact server has about *100 Gigabytes of data* all contained on one hard disk partition;, thus check up of all files took a few hours. clamav is relatively slow, compared to DrWeb or nod32. But since I'm not in a hurry plus, we can't afford to spend some extra money to buy AV just for one scan I left it scanning in a separate screen sesion.

clamscan execution put some extra load on the server (which btw is used mainly for processing a multitude of SQL queries and provides some *HTTP access to few websites via Apache server*. After the scan was completed I ended up with enormous very clamav log file, listing all scanned files:

I checked the file content in vim, but as reviewing 119MB of log line by one! - is unthinkable task, e.g.:

debian:~# du -hsc /var/log/clamav_scan.log
119M /var/log/clamav_scan.log
119M total

I did quick review of *clamav_scan.log* and tailing it displays me::

tail -n 10 /var/log/clamav_scan.log
---------- SCAN SUMMARY ----------
Known viruses: 1270572
Engine version: 0.97.3
Scanned directories: 18927
Scanned files: 221445

Infected files: 44
Total errors: 287
Data scanned: 12457.43 MB
Data read: 97007.10 MB (ratio 0.13:1)
Time: 1842.362 sec (30 m 42 s)

Thus I needed a way to not read screen by screen all by screen to see what was detected as **Infected Files**, but just **show only infected files found by clamav**.

I didn't know how this done, so did a quick search in Google and found the question how to only grep infected files from clamav.log answered in Clamav-Users Mailing List read whole thread here

The thread suggests using:

[root@mail clamav]# cat clamd.log | grep -i "found"

Since cat-ing the log is worthless however it is much better to only do grep "found" clamd.log or as in my case file is *clamav_scan.log* do:

grep -i 'found' /var/log/clamav_scan.log

/usr/share/clamav-testfiles/clam.bz2.zip: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.d64.zip: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.ppt: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.tnef: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam-aspack.exe: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.exe.rtf: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.7z: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam_IScab_ext.exe: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.odc.cpio: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.newc.cpio: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.pdf: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam-wwpack.exe: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.ole.doc: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.cab: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam-mew.exe: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam-petite.exe: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.sis: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam-fsg.exe: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.exe: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam_cache_emax.tgz: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.exe.bz2: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam_ISmsi_int.exe: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.exe.szdd: ClamAV-Test-File FOUND

/usr/share/clamav-testfiles/clam.chm: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.arj: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam_IScab_int.exe: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.ea05.exe: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.tar.gz: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.exe.html: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.exe.binhex: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.impl.zip: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam-upack.exe: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.bin-be.cpio: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.mail: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.exe.mbox.uu: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.zip: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam-nsis.exe: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam_ISmsi_ext.exe: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam-yc.exe: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.bin-le.cpio: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam-upx.exe: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam-pespin.exe: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.exe.mbox.base64: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.ea06.exe: ClamAV-Test-File FOUND

Surprisingly all the "Infected" files turned to be a regular clamav scan (virus, spyware badware testfiles - i.e. clamav just use this file to check its database definitions works okay). Thus the supposingly ***Infected files: 44*** *turned to be just another false positive.*

Actually this grepping and logging of all scanned files, nevertheless they're not infected is completely useless. Thus it would have been much better if instead have run **clamscan** with cmd options:

debian:~# clamscan -r /* --infected

I hope ppl reading this article wouldn't repeat my "mistake".
In mean time after this thing here, maybe it will be a good idea to schedule *2 weeks* or *1 months* period clamscan of whole file system to make sure someone doesn't uploaded some malicious PHPShell script, exploit or other unwanted stuff.