

# Day 47

## Exploitation Analyst

### Auditing and Virus Scan:

### Virus Scanning - Clamav:

#### What is Clamav?

ClamAV is an open-source antivirus engine used to detect malware, viruses, trojans, and other malicious threats on Linux and Unix-like systems.

- It provides on-demand scanning of files and directories.
- It can also be used for email gateway scanning (checking attachments).
- Signature databases are updated regularly with freshclam.
- It's widely used because it's lightweight and integrates easily with mail servers and security tools.

#### Where can we find this?

Command: aptitude search clamav

```
[root@parrot]~[/home/user]
#aptitude search clamav
p clamav - anti-virus utility for Unix - command-line interface
p clamav-base - anti-virus utility for Unix - base package
p clamav-cvupdate - ClamAV Private Database Mirror Updater Tool
p clamav-daemon - anti-virus utility for Unix - scanner daemon
v clamav-data -
p clamav-docs - anti-virus utility for Unix - documentation
p clamav-freshclam - anti-virus utility for Unix - virus database update utility
p clamav-milter - anti-virus utility for Unix - sendmail integration
p clamav-testfiles - anti-virus utility for Unix - test files
p clamav-testfiles-rar - anti-virus utility for Unix - test files
p clamav-unofficial-sigs - update script for 3rd-party clamav signatures
p libclamav-client-perl - Perl client for the ClamAV virus scanner daemon
p libclamav-dev - anti-virus utility for Unix - development files
p libclamav11 - anti-virus utility for Unix - library
p proftpd-mod-clamav - ProFTPD module mod_clamav
[root@parrot]~[/home/user]
```

### Exploring Virus Scanning - Clamav:

Steps:

Command : clamscan /path/to/file

```
[root@parrot]~[/home/user/Downloads]
#clamscan /home/user/Downloads/cacert.der
Loading: 1s, ETA: 2s [=====>] 610.00K/2.08M sigs
Menu Parrot Terminal
```

```
[root@parrot]~[/home/user/Downloads]
#clamscan /home/user/Downloads/cacert.der
Loading: 15s, ETA: 0s [=====>] 2.06M/2.06M sigs
Compiling: 2s, ETA: 0s [=====>] 41/41 tasks

/home/user/Downloads/cacert.der: OK

----- SCAN SUMMARY -----
Known viruses: 2060979
Engine version: 1.0.9
Scanned directories: 0
Scanned files: 1
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 18.213 sec (0 m 18 s)
Start Date: 2025:09:03 03:12:46
End Date: 2025:09:03 03:13:04
[root@parrot]~[/home/user/Downloads]
#
```

That output means your file cacert.der is clean

- ClamAV loaded ~2 million virus signatures.
- It scanned your .der file and found no infection.
- "OK" means nothing suspicious was detected.

--The End--