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.

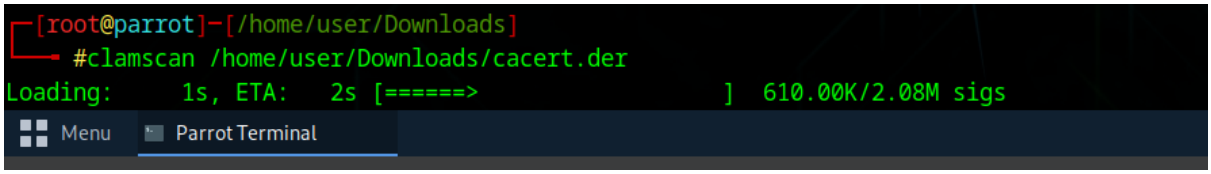
Where can we find this?

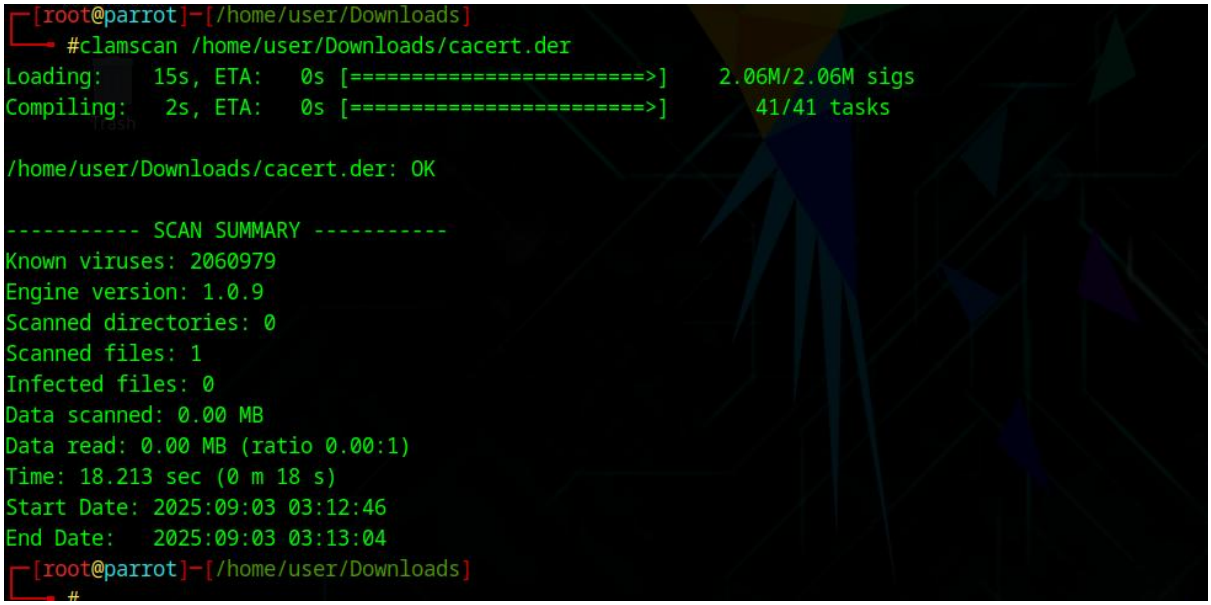
Command: aptitude search clamav

Exploring Virus Scanning - Clamav:

Steps:

Command : clamscan /path/to/file





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--