

LAB 2 – 3: Install and Use ClamAV

OS Install

```
(khanhNNHE191159@kali)-[~]
$ uname -a
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64
GNU/Linux

(khanhNNHE191159@kali)-[~]
$ cat /proc/version
Linux version 6.11.2-amd64 (devel@kali.org) (x86_64-linux-gnu-gcc-14 (Debian 14.2.0-6)
14.2.0, GNU ld (GNU Binutils for Debian) 2.43.1) #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1
kali1 (2024-10-15)
```

Scan a directory:

```
(khanhNNHE191159@kali)-[~/Downloads]
$ sudo clamscan --infected --remove --recursive Test/

[sudo] password for khanhNNHE191159:

----- SCAN SUMMARY -----
Known viruses: 8706605
Engine version: 1.4.2
Scanned directories: 1
Scanned files: 2
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 21.338 sec (0 m 21 s)
Start Date: 2025:05:20 02:45:00
End Date: 2025:05:20 02:45:22

(khanhNNHE191159@kali)-[~/Downloads]
$
```

Scan 2 files:

```
(khanhNNHE191159@kali)-[~/Downloads/Test]
$ cat test.txt
hello word

(khanhNNHE191159@kali)-[~/Downloads/Test]
$ cat Clam_HelloWorld.ndb
Clam_HelloWorld:0:*:68656c6c6f*776f726c64

(khanhNNHE191159@kali)-[~/Downloads/Test]
$ ls
Clam_HelloWorld.ndb  test.txt

(khanhNNHE191159@kali)-[~/Downloads/Test]
$ clamscan -d Clam_HelloWorld.ndb test.txt
Loading:      0s, ETA:  0s [=====] 1/1 sigs
Compiling:    0s, ETA:  0s [=====] 40/40 tasks

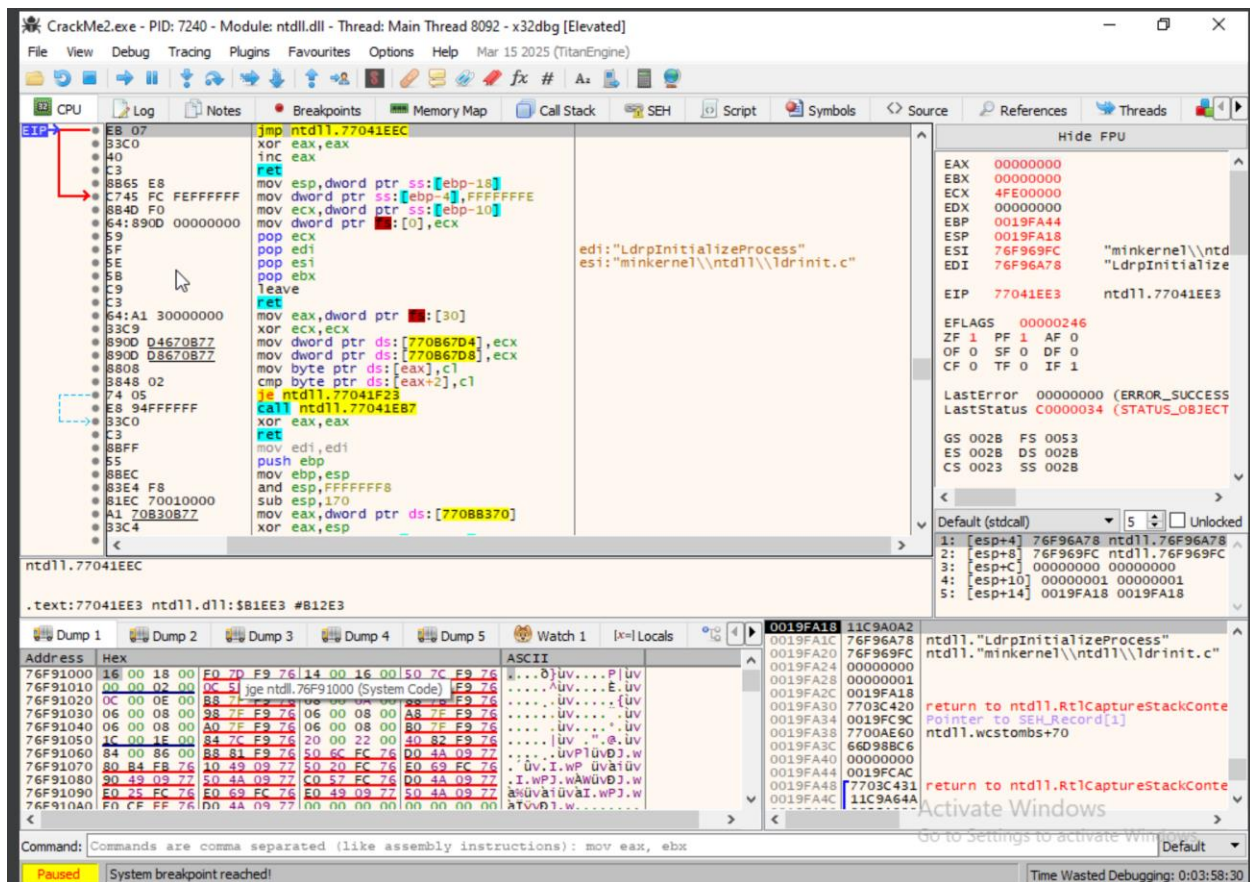
/home/kali/Downloads/Test/test.txt: OK

----- SCAN SUMMARY -----
Known viruses: 1
Engine version: 1.4.2
Scanned directories: 0
Scanned files: 1
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 0.004 sec (0 m 0 s)
Start Date: 2025:05:20 02:51:42
End Date: 2025:05:20 02:51:42

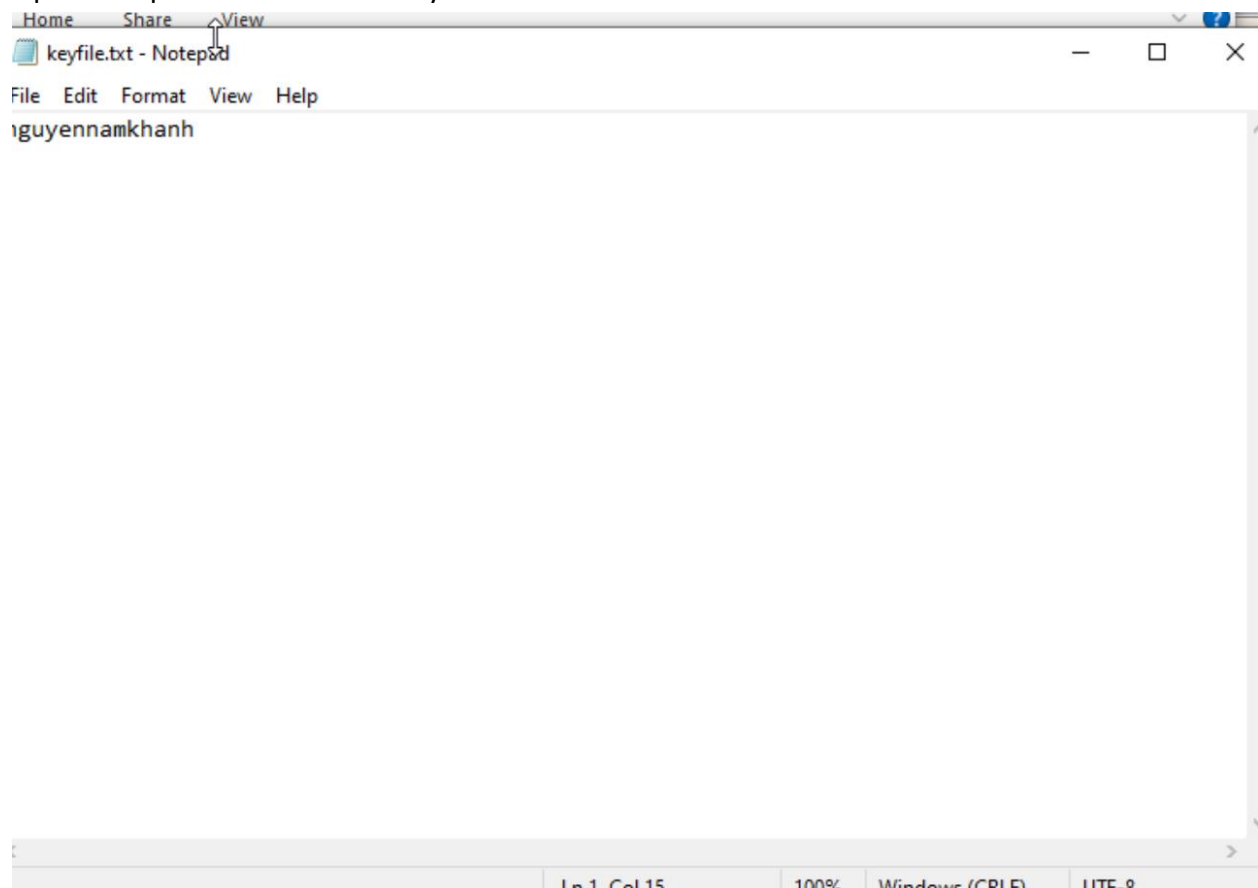
(khanhNNHE191159@kali)-[~/Downloads/Test]
$ █
```

CRACK ME 2:

Open crackme2.exe in x32dbg



Open notepad and create file keyfile.txt and save with ANSI form in folder Downloads



Run again and see a correct output

