Кам’янець-Подільський національний університет імені Івана Огієнка

Кафедра комп’ютерних наук

Навчальна дисципліна

**«Технології захисту інформації»**

Лабораторна робота №2

Дослідження шкідливого ПЗ (статичний/поведінковий аналіз)

Виконав:

студент 4-го курсу

групи KN1-B22

**Демченко Дмитро**

Кам’янець-Подільський – 2025

**Мета:** виконати базовий статичний та поведінковий аналіз підозрілого файлу.

**Опис середовища:**

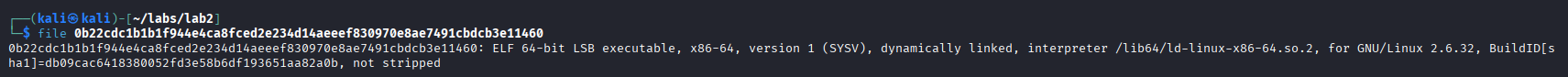
ПЗ для віртуальної машини: VMware® Workstation 17 Pro 17.6.4 build-24832109

, radare2 5.9.8 0 @ linux-x86-64, yara 4.5.4, strace -- version 6.16, ltrace 0.7.91, ClamAV 1.4.3/27787/Thu Oct 9 05:31:07 2025, Linux kali 6.12.38+kali-amd64, Local Kali ip: 192.168.135.128

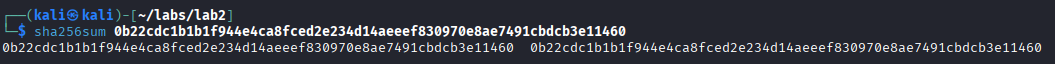
**Небезпечний файл**: <https://github.com/MalwareSamples/Linux-Malware-Samples/blob/main/0b22cdc1b1b1f944e4ca8fced2e234d14aeeef830970e8ae7491cbdcb3e11460>

**Команди:**

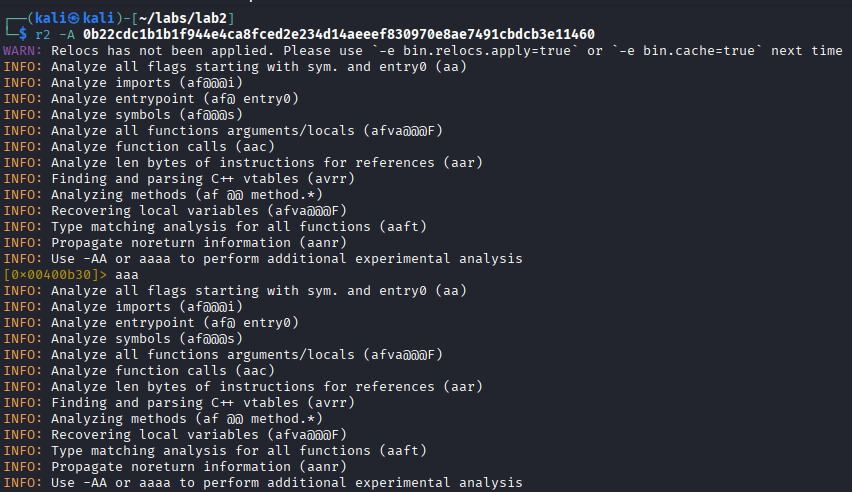
1) file 0b22cdc1b1b1f944e4ca8fced2e234d14aeeef830970e8ae7491cbdcb3e11460

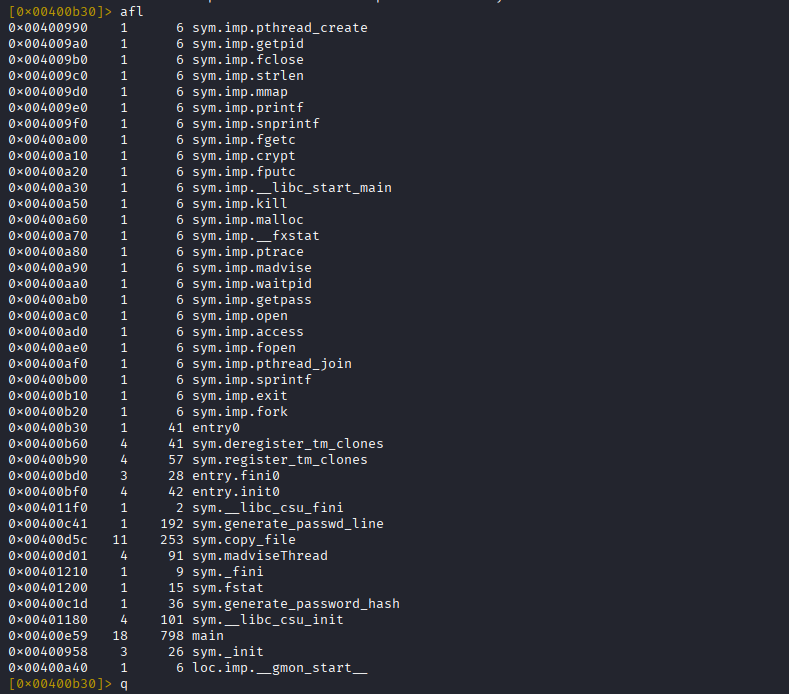


2) sha256sum 0b22cdc1b1b1f944e4ca8fced2e234d14aeeef830970e8ae7491cbdcb3e11460:



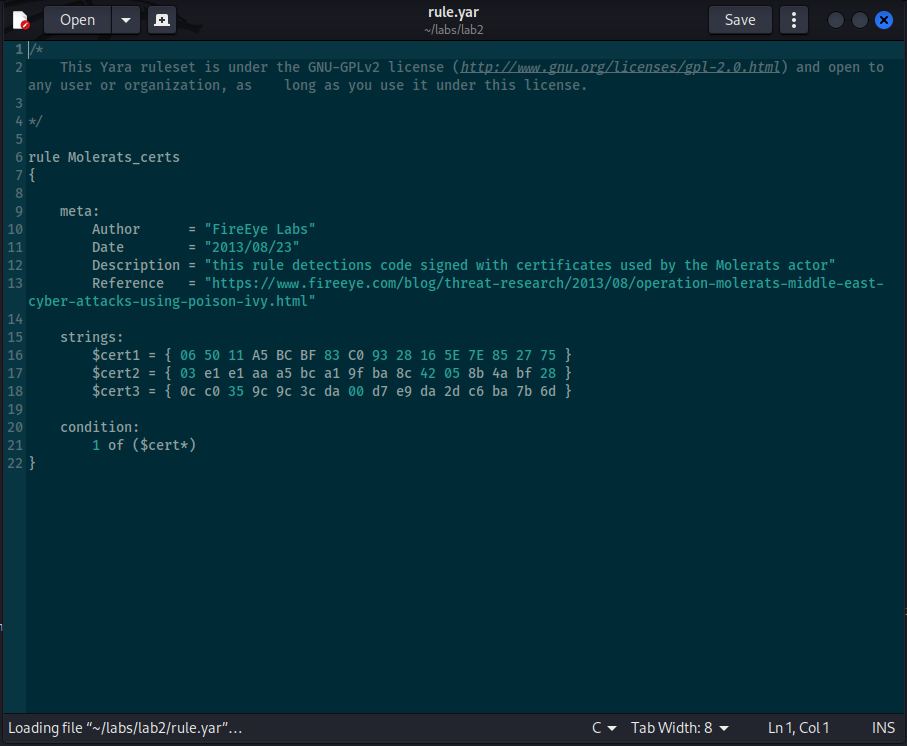
3) r2 -A 0b22cdc1b1b1f944e4ca8fced2e234d14aeeef830970e8ae7491cbdcb3e11460:

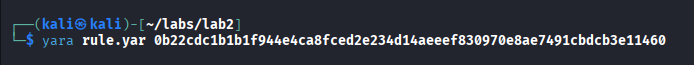




4) yara rule.yar 0b22cdc1b1b1f944e4ca8fced2e234d14aeeef830970e8ae7491cbdcb3e11460:

Rule.yar

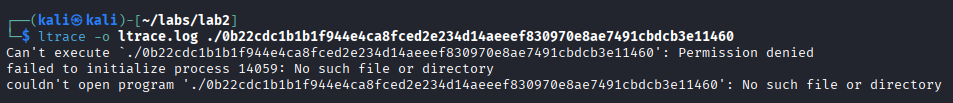




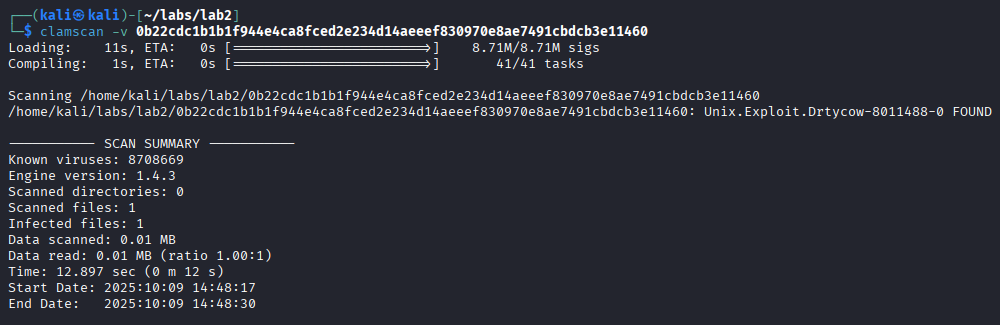
5) strace -o trace.log ./0b22cdc1b1b1f944e4ca8fced2e234d14aeeef830970e8ae7491cbdcb3e11460:



6) ltrace -o ltrace.log ./ 0b22cdc1b1b1f944e4ca8fced2e234d14aeeef830970e8ae7491cbdcb3e11460:



7) clamscan -v 0b22cdc1b1b1f944e4ca8fced2e234d14aeeef830970e8ae7491cbdcb3e11460



Файли:



**Висновок:** Під час виконання лабораторної роботи було здійснено аналіз вірусу з використанням інструментів ОС Kali Linux.