МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра Інформаційної Безпеки

Аналіз та моніторинг кібербезпеки

Практичне завдання №5

Моніторинг стану кібербезпеки за допомогою індикаторів компрометації

Перевірив:
Козленко О. В.

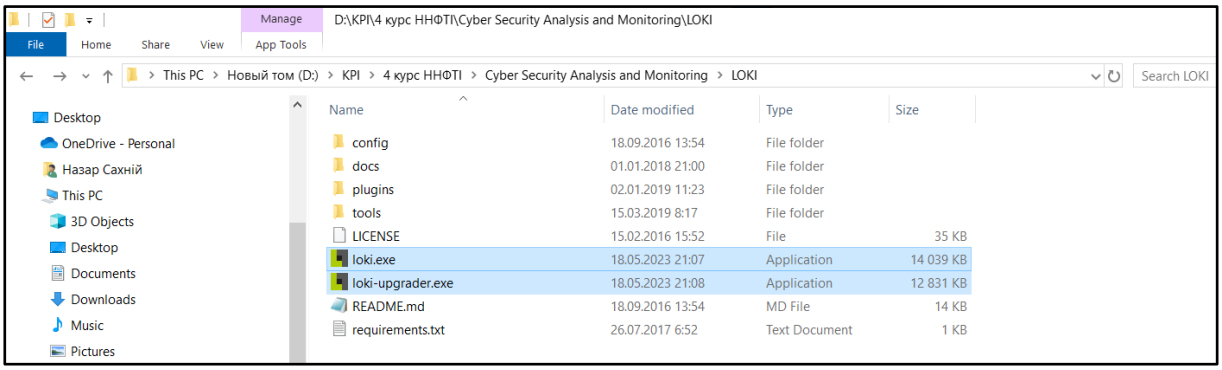
Виконав:
студент IV курсу
групи ФБ-01
Сахній Н. Р.

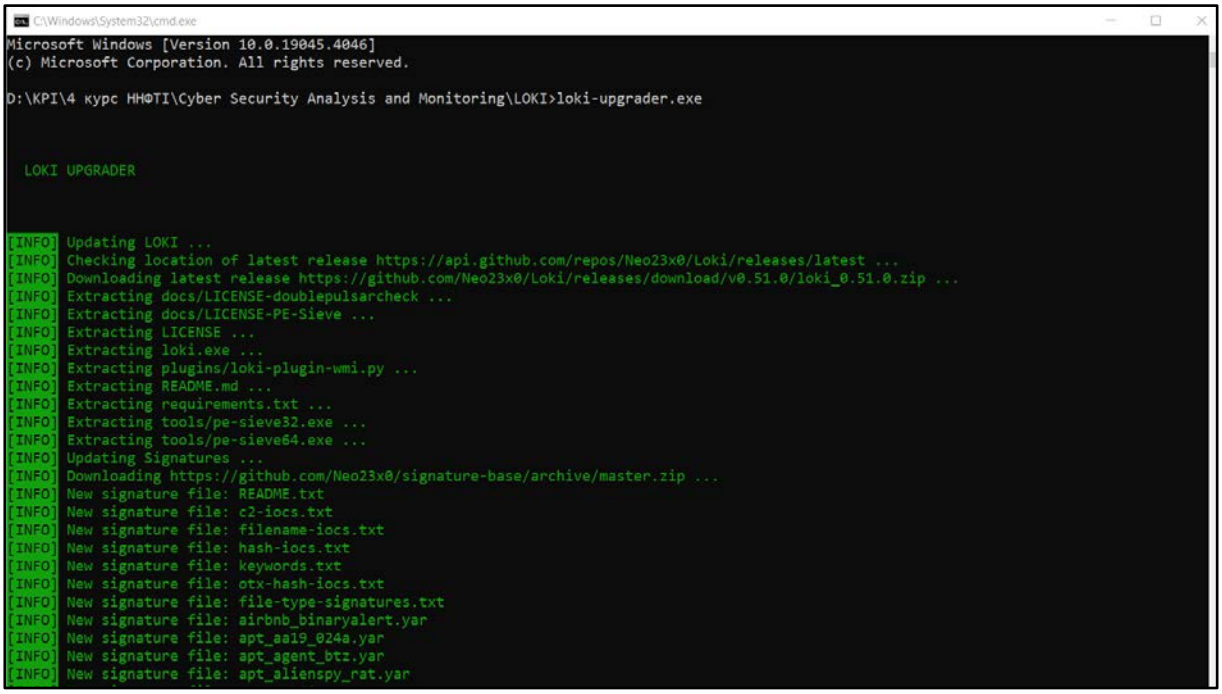
Київ 2024

Мета: Знайомство з індикаторами компрометації (IOC), способами їхнього документування та протоколювання. Отримання навичок з сканування ресурсів ІТС з метою виявлення можливих IOC.

Завдання: Проаналізувати можливі індикатори компрометації системи за допомогою утиліти LOKI (https://github.com/Neo23x0/Loki) з використанням створеного правила YARA.

1. Завантажимо утиліту LOKI та актуальну базу даних із IOC та YARA:





2. Напишемо примітивне YARA-правило для детектування NetworkMiner:

lab_NetworkMiner.yar - Notepad

File Edit Format View Help

```
rule NetworkMiner {
    meta:
        author = "FB-01 Sakhnii Nazar"
        filetype = "Win32 EXE"
        date = "02/03/2024"
        reference = "https://www.netresec.com/?page=NetworkMiner"
        description = "Detects NetworkMiner Tool"

    strings:
        $hex1 = {E1 ?1 3D ?? 78 F1 52}
        $hex2 = {78 3C FC 9D A7 7F 96 39 (55 | 43)}

        $string1 = "NetworkMiner"
        $string2 = "Eric Svensen"
        $string3 = "Netresec"

    condition:
        uint16(0) == 0x5a4d
        and filesize < 1000KB
        and (all of ($hex*) or any of ($string*))
        and not pe.imphash() == "c78c79e15150038b369fd30134d4484b"
}
```

Ln 24, Col 2 | 100% | Windows (CRLF) | UTF-8

3. Запустимо аналіз (сканування) деякої папки та виявимо той самий файл: