

**МІНІСТЕРСТВО ОСВІТИ, НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**

**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

**ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**

**Лабораторна робота 6**

**Аналiз конфiгурацiї**

***Варіант №5***

**Підготував:**

студент 4 курсу

групи ФІ-84

Коломієць Андрій Юрійович

**Email**:*andkol-ipt22@lll.kpi.ua*

**Викладач:**

**Київ – 2021**

**Аналiз конфiгурацiї**

***Мета роботи***

Отримати навички аналiзу налаштувань та середовища виконання ШПЗ для задач реагування на iнциденти.

***Постановка задачi***

Дослiдити методи роботи з структурованими даними за допомогою Kaitai Struct, динамiчного аналiзу процесiв Windows/Linux та аналiзу середовища емуляторiв антивiрусiв.

***Варiанти завдань***

• Створiть парсер конфiгурацiї з пам’ятi Вашої системи з лабораторної роботи 4. Впевнiться, що парсер працює пiсля застосування UPX та MPRESS на виконуваному файлi зразку.

• Проаналiзуйте 1-2 антивiруси з лабораторiї роботи 3 за допомогою методiв. Знайдiть iм’я системи, iм’я користувача,список процесiв, список файлiв на робочому столi, першi 32 байти notepad.exe. Для пришвидшення роботи рекомендується використати 256 зразкiв з theZoo, VirusShare або iнших джерел для отримання 1 байту за запит.

• Порiвняйте Вашi результати з попереднього пункту з колегою, що використовує той же антивiрус. Якi iндикатори спiвпадають?

***Виконання роботи***

Створiть парсер конфiгурацiї з пам’ятi Вашої системи з лабораторної роботи 4. Впевнiться, що парсер працює пiсля застосування UPX та MPRESS на виконуваному файлi зразку.

***Для Linux OS[[1]](#footnote-2)***

$ pidof python3

$ grep heap /proc /**<any\_pid>**/maps

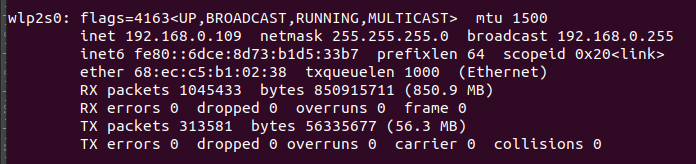
**<start\_memory\_address>** - **<end\_memory\_address>**  rw - p 00000000 00:00 0 [ heap ]

$ dd if =/proc /**<any\_pid>**/ mem bs =1 skip = $ ((**0 x<start\_memory\_address>** ) ) count = $ ((**0 x<end\_memory\_address>-<start\_memory\_address>** ) ) | egrep - ao **"(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)"**

***Результати роботи на включеному сервері***



***Дійсно IP адреса співпадає.***



***Для Windows OS[[2]](#footnote-3)***

#!/bin/env python

import winappdbg

from winappdbg import win32

import re

s=winappdbg.System ()

s.request\_debug\_privileges()

s.scan\_processes()

for p, path in s.find\_processes\_by\_filename("python.exe"):

pid = p.get\_pid()

bits = p.get\_bits()

print "pid %d (%d bits)" % (pid, bits)

mmap = p.get\_memory\_map()

mapf = p.get\_mapped\_filenames(mmap)

for m in mmap:

a = m.BaseAddress

fn = mapf.get(a,None)

if m.has\_content():

print "address 0x%x size 0x%x state 0x%x protect 0x%x type 0x%x[%s]" %(a,

m.RegionSize,m.State,m.Protect,m.Type,fn)

d = p.read(a,m.RegionSize)

cc = re.findall("\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}",d[::2])

if len(cc) > 0:

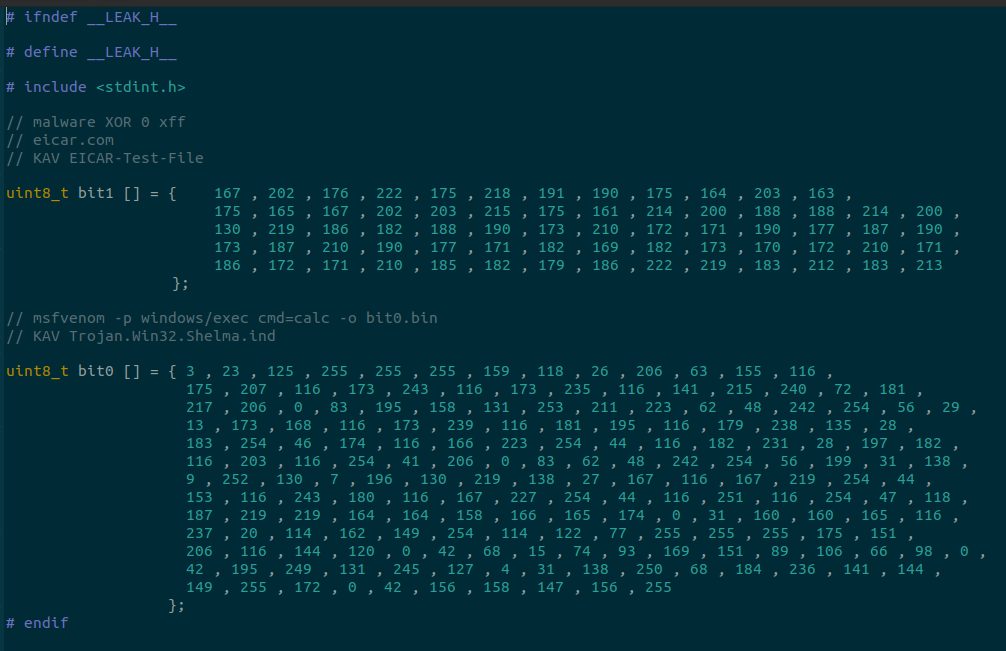
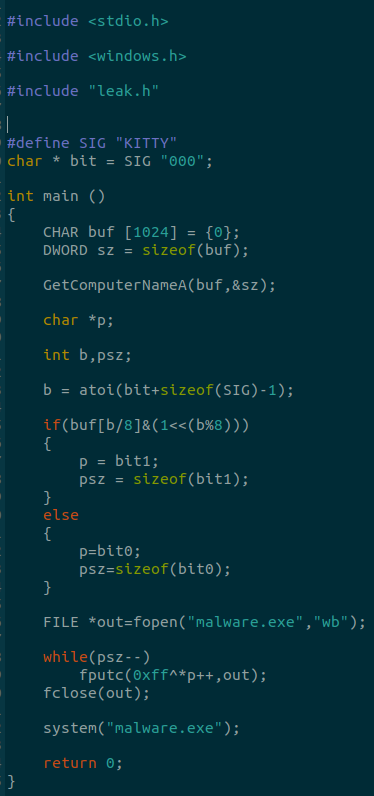
print cc

raw\_input()

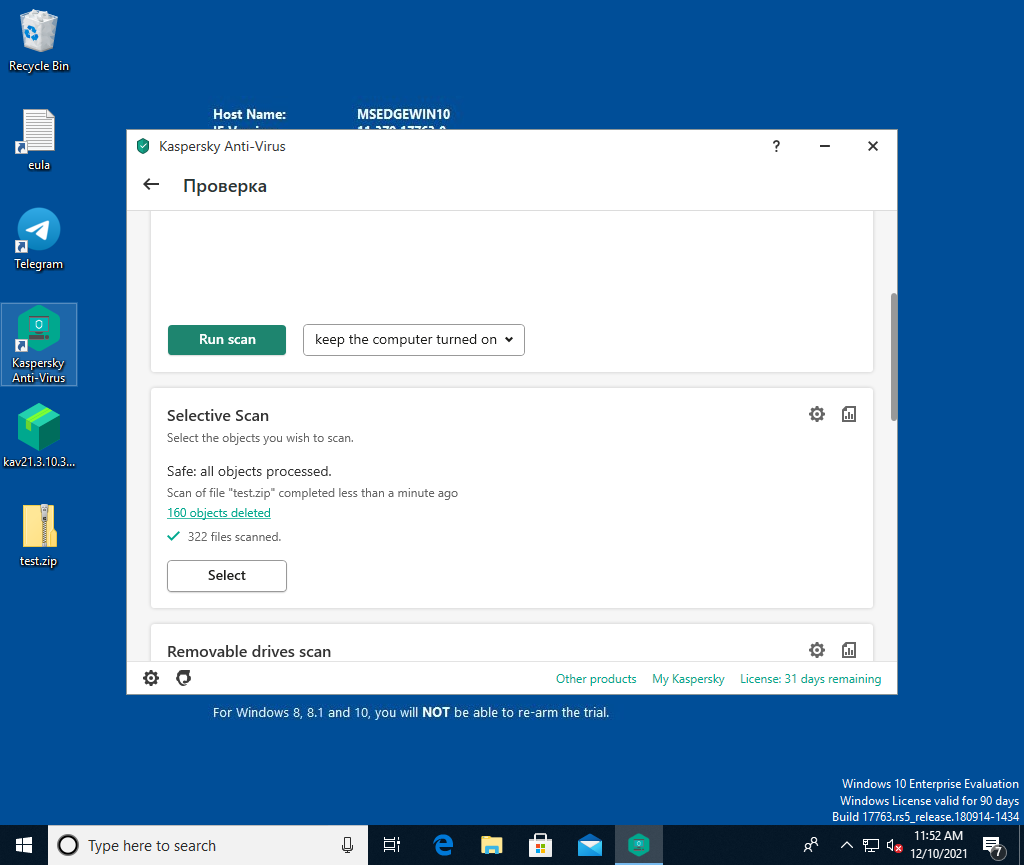
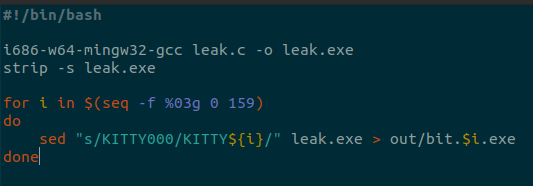
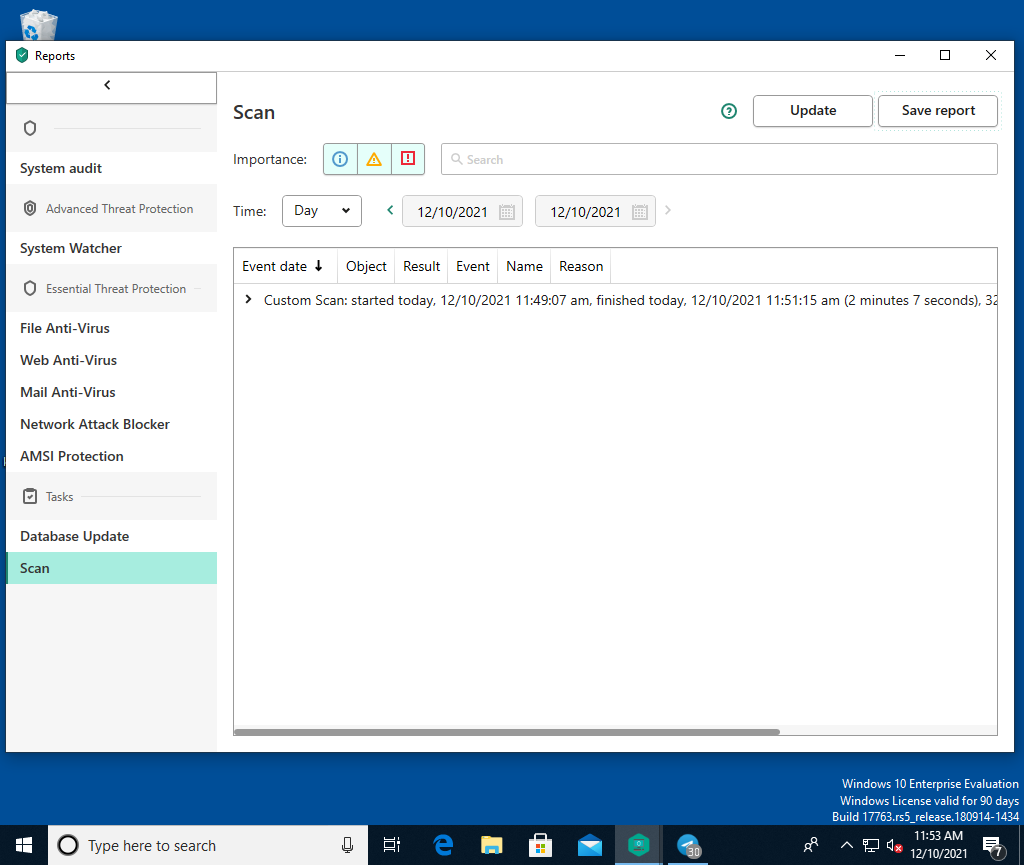
print("Hello")

***Результати роботи на клієнтській стороні***  
  
На диво **IP** в **Windows** на відміну від **Linux** маємо, як відправника так і отримувача.

Проаналiзуйте 1-2 антивiруси з лабораторiї роботи 3 за допомогою методiв. Знайдiть iм’я системи, iм’я користувача,список процесiв, список файлiв на робочому столi, першi 32 байти notepad.exe. Для пришвидшення роботи рекомендується використати 256 зразкiв з theZoo, VirusShare або iнших джерел для отримання 1 байту за запит.  
 ***Код з методички***



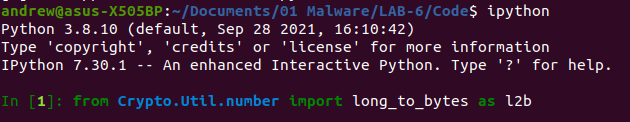
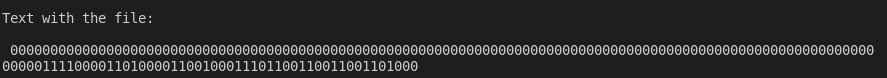
***Формуємо папаку з файлами та відправляємо на комп’ютер з антивірусом KAV***



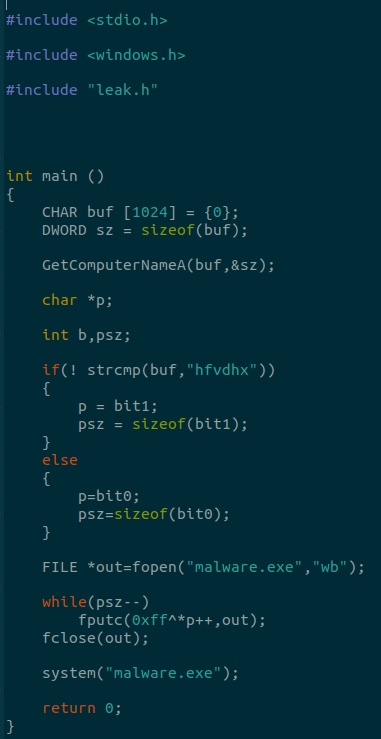
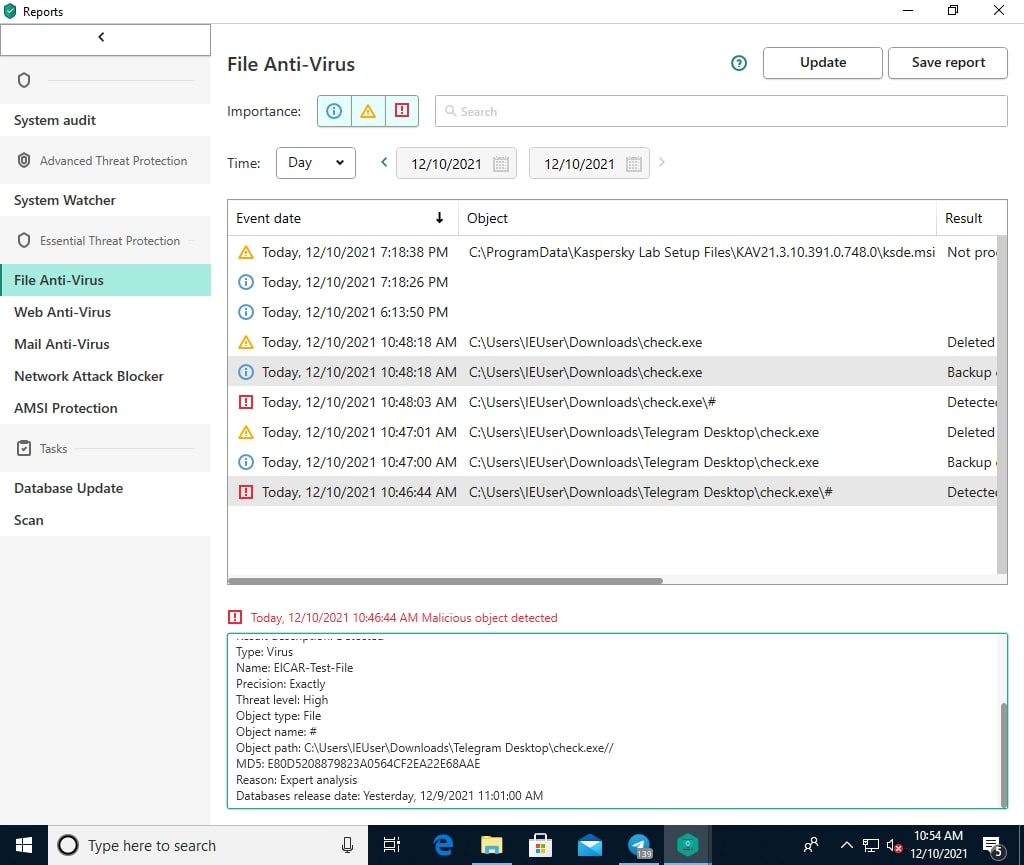
***Виділяємо біти в файлі за допомогою програми***



***Декодуємо отримані значення***



***Перевірка імені комп’ютера***



1. https://www.shellhacks.com/regex-find-ip-addresses-file-grep/ [↑](#footnote-ref-2)
2. https://stackoverflow.com/questions/10086572/ip-address-validation-in-python-using-regex [↑](#footnote-ref-3)