Python course practical tasks

Задача #1

Задача #2

Задача #3 (Треба оновити ІР для задачі)

Задача #4

Задача #5

Задача #6

Задача #7

## **Задача #1**

Написати парсер для логів аpache2:

* Вивести топ айпі за кількістю запитів
* Вивести найпопулярнiйшi сторiнки
* Вивід має бути красивий, без скобочок

Файл логів, який треба розпарсити:

<http://telegra.ph/Sample-log-01-27>

To learn:

* File read
* Work with strings(String.split() and etc.)
* Data structures: Dictionaries

## **Задача #2**

Написати парсер сайту<https://www.cvedetails.com/>

* Аргументом з командного рядка брати CVE ( CVE-2007-0994 )
* Витягувати наступну інформацію:
  + CVE
  + CVSS SCORE
  + Confidentiality Impact
  + Integrity Impact
  + Availability Impact
  + Access Complexity
  + Access Complexity
  + Authentication
  + Gained Access
  + Vulnerability type(s)
  + CWE ID
  + Products affected
  + Vendor
* Ігнорувати інформацію в дужках

Advanced:

* Не повторюватись в структурі даних, в якій зберігаєте результати
* Зберегти їх в окремий файл/базу даних
* Парсити для декількох CVE з командного рядка

To learn:

* Requests library
* HTML parsing (Beautiful Soup etc.)
* Data structures
* DB/File work

## **Задача #3 (Треба оновити ІР для задачі)**

Написати баннер грабер:

* Список айпішок має братись з файлу.
* Порт, який має грабатись, має братись з **аргументу команд-лайну**.
* Вивести результати файл.
* Якщо вказаний 80 порт, то замість банер грабінгу має надсилатись гет запит

Апійшки для сканування:

<http://telegra.ph/IPs-to-scan-02-23>

Стаття про банер грабінг в вікі:

<https://www.wikiwand.com/en/Banner_grabbing>

Violent python:

<https://www.csee.umbc.edu/wp-content/uploads/2014/05/ViolentPython-ICEW-2014.pdf>

Робота з аргументами командної строки:

<http://www.tutorialspoint.com/python/python_command_line_arguments.htm>

Робота протоколу HTTP:

<https://ru.m.wikipedia.org/wiki/HTTP>

To learn:

* File write
* Sockets recieve
* args
* TCP/IP basics
* HTTP basics

## **Задача #4**

Написати веб сервер, використовуючи бібліотеку socket і протокол TCP/IP:

* Программа має надавати доступ до файлів в директорії, з якої вона була запущена.
* Має бути можливість ходити по директоріях

Advanced:

* При переході на файл відтворювати зміст

To learn:

* Sockets bind
* TCP/IP
* Directories walk
* HTTP basics

Приклад роботи:

[http://repo.yandex.ru](http://repo.yandex.ru/)

## **Задача #5**

Брутфорсер вордпрессу:

1. Встановити віртуальну машину з WordPress
2. Написати брутфорсер логінів WordPress ( SERVER\_IP/wp-login форма )
3. Логіни та паролі брати з різних файлів

Advanced:

* Отримувати список логінів автоматично <https://hackertarget.com/wordpress-user-enumeration/>
* Брати як аргумент з командного рядка список серверів, які треба брутфорсити
* Зберігати знайдені Логіни і Паролі до них в файлі

To learn:

* VM configuration
* Requests
* Work with files
* WordPress exploit
* HTML parsing

## **Задача #6**

Криптолокер:

1. Написати програму, яка буде знаходити всі файли окрім system32 і файлів скрипта і шифрувати їх.
2. Встановити на віртуальну машину Windows.
3. Для шифрування має використовуватись будь-який симетричний шифр, оригінальний файл має ПЕРЕЗАПИСУВАТИСЬ.
4. Написати дешифратор.

Advanced:

* Написати сервер, який буде зберігати та відтворювати ключі для дешифрування. (спробуйте Flask або щось інше)
* Змінити заставку екрана після дешифрування з якимось текстом
* Зробити програму багатопоточною

To learn:

* Cryptolocking
* Client-server relations
* Web framework
* Multiprocessing

## 

## **Задача #7**

MMT Monitoring and management tool. (комплект з клієнта та сервера)

1. Клієнт(агент) встановлюється на декілька машин, та отримує команди з сервера.
2. По команді від сервера:
   1. Зробити скріншот і відправити на сервер.
   2. Виконати якусь команду командної строки.
   3. Показати повний список всіх директорій клієнта.
   4. Запустити перехват натиснутих клавіш, та передавати їх на сервер до отримання команди СТОП.
3. Обмін даними має бути за протоколом http, кожен клієнт має шифрувати данні в транзіті своїм ключем

Advanced level:

1. Додати наступні команди:
   1. Передати з клієнта на сервер файл.
   2. Показати всі процесси, які виконуються на клієнті.
   3. Зупинити процесс.
   4. Скачати та зберегти файл.
   5. Скачати файл, зберегти в %TEMP% та виконати.
   6. Запуск VNC сервера.
   7. Встановити новий кореневий сертефікат.
2. Реалізувати комунікацію через HTTPS

To learn:

* Client-server advanced
* System funtions
* OOP basics
* Objects serialization (pickle, json etc.)
* Malware theory