ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Факультет безопасности информационных технологий

Кафедра проектирования и безопасности компьютерных систем

Дисциплина:

«Технологии и методы программирования»

Лабораторная работа №3

Выполнил:

Студент группы N33471

Гаврилова Вероника

Проверил:

Ищенко А. П.

Санкт-Петербург

2021г.

ЗАДАНИЕ:

А) Выполняется в локальной операционной системе.

1. Создать текстовый документ (sys.tat), в котором будет содержаться «Системная информация».
2. Написать программу-инсталлятор sys_doc.exe для этого документа, которая под видом установки обновления (с отображением строки прогресса обновления) к какой-нибудь программе (например, Блокнот или Paint):

· Запрашивает у пользователя папку (должен быть вариант использования существующей папки и вариант создания собственной) для копирования «Системной информации».

· Записывает в папку файл с исполняемым кодом программы secur.exe (аналог требований к template.tbl из лабораторной работы №1), защищающей sys.tat.

· Собирает (возможную) информацию о компьютере, на котором устанавливается программа.

· Кодирует эту информацию и записывает в файл sys.tat.

· Подписывает её личным ключом пользователя программы и записывает подпись, например, в реестр Windows в раздел HKEY_CURRENT_USER\Software\Фамилия_студента как значение параметра Signature.

· Запускает secur.exe для защиты sys.tat от несанкционированного доступа.

· Прописывает запуск программы secur.exe при выполнении функции Open для sys.tat, чтобы защита срабатывала и после перезагрузки ОС (есть несколько способов такой «привязки»).

3. В саму программу защиты secur.exe включить следующий функционал:

· Запрос у пользователя информации об имени раздела реестра с электронной цифровой подписью (фамилией студента).

· Считывание подписи из указанного выше раздела реестра, которая проверяется с помощью открытого ключа пользователя.

· Разрешение или запрет просмотра «Системной информации» в файле sys.tat в зависимости от правильности указания ключа.

4. При неудачной проверке работа защищаемой программы должна прекращаться с выдачей соответствующего сообщения.
5. Собираемая о компьютере информация включает в себя как минимум:

· Имя пользователя,

· Имя компьютера,

· Конфигурацию компьютера (память и процессор, как минимум) и версию ОС.

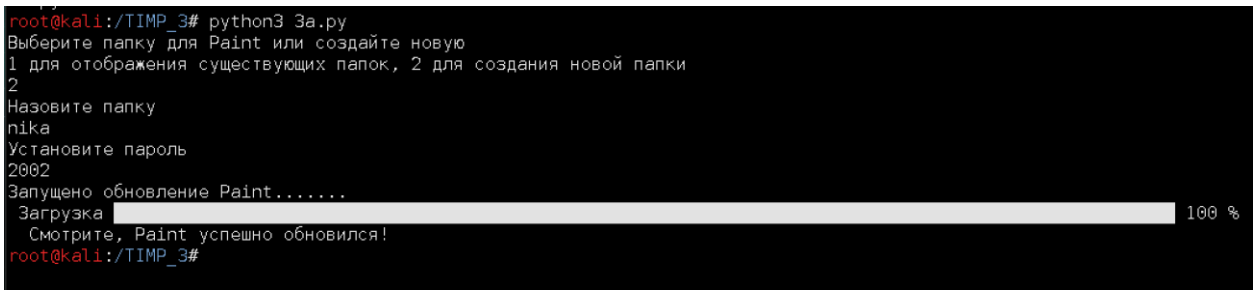
Б) Выполняется в локальной сети (или виртуальной).

6. Создать скрипт, который удалённо и незаметно для пользователя (пользователь открывает какую-нибудь веб-страничку от создателя скрипта) собирает информацию о нём, его компьютере и системе (п.5 предыдущего задания) и записывает её на какой-либо локальный сетевой диск (доступный создателю скрипта) в папку с именем IP или Mac-адреса пользовательской машины.
7. Продумать доступ к этой информации (можно писать на удалённый диск).
8. Протестировать на 3–5 клиентах и получить статистику о них.

Выполнение:

Часть А

1) Установка программы



2) После установки программы проверяем директорию. В директории появилась указанная при установке папка nika. Содержимое папки – sys.tat невозможно открыть от имени простого пользователя (nika@). Открываем файл secure.exe – скрипт просит ввести пароль, казанный при установке. После ввода пароля получаем закодированную информацию о системе.

```
root@kali:~# su nika
nika@kali:/root$ cd ..
nika@kali:/$ cd TIMP_3
nika@kali:/TIMP_3$ ls
3a.py  nika
nika@kali:/TIMP_3$ cd nika
nika@kali:/TIMP_3/nika$ ls
secure.exe  sys.tat
nika@kali:/TIMP_3/nika$ cat sys.tat
cat: sys.tat: Permission denied
nika@kali:/TIMP_3/nika$ ./secure.exe
Enter secret key for reading system info from sys.tat : 2002
cm9vdFxuTGludXgga2FsaSA1LjguMC1rYWxpMi1hbWQ2NCAjMSBTTVAgRGViaWFuIDUuOC4xMC0xa2FsaTEgKDIwMjAtMDktMjIpIHg4Nl82NCBHTlUvTGlu
dXhcbkFyY2hpdGVjdHVyZTogICAgICAgICAgICAgICAgICAgICAgICAgIHg4Nl82NFxuQ1BVIG9wLW1vZGUocyk6ICAgICAgICAgICAgICAgICAgMzItYml0LCA2NC1i
aXRcbkJ5dGUgT3JkZXI6ICAgICAgICAgICAgICAgICAgICAgICAgICAgIExpdHRsZSBFbmRpYW5cbkFkZHJlc3Mgc2l6ZXM6ICAgICAgICAgICAgICAgICAgICAgICAgICAgIDQzIGJp
dHMgcGh5c2ljYWwsIDQ4IGJpdHMgdmlydHVhbFxuQ1BVKHMpOiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
ICAgICAgICAgMC0zXG5UaHJlYWQocykgcGVyIGNvcmU6ICAgICAgICAgICAgICAgICAgICAxXG5Db3JlKHMpIHBlciBzb2NrZXQ6ICAgICAgICAgICAgICAgICAgICAxXG5Tb2Nr
ZXQocyk6ICAgICAgICAgICAgICAgICAgICAgICAgICAgICA0XG5OVU1BIG5vZGUocyk6ICAgICAgICAgICAgICAgICAgICAgICAgICAxXG5WZW5kb3IgSUQ6ICAgICAgICAg
ICAgICAgICAgICBHZW51aW5lSW50ZWxcbkNQVSBmYW1pbHk6ICAgICAgICAgICAgICAgICAgICAgICAgICAgIDZcbk1vZGVsOiAgICAgICAgICAgICAgICAgICAgICAgICAg
ICAgIDE0MlxuTW9kZWwgbmFtZTogICAgICAgICAgICAgICAgICAgICAgICAgICAgSW50ZWwoUikgQ29yZShUTSkgaTUtODI1OVUgQ1BVIEAgMi4zMEdIelxuU3RlcHBp
bmc6ICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
ICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
ICAgICAgICAgICAgICA0NjA3Ljc4XG5IeXBlcnZpc29yIHZlbmRvcjogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
ICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
IDEyOCBLaUJcbkwyIGNhY2hlOiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
bk5VTUEgbm9kZTAgQ1BVKHMpOiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
TVggdW5zdXBwb3J0ZWRcblZ1bG5lcmFiaWxpdHkgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
TWRzOiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
bG5lcmFibGVcblZ1bG5lcmFiaWxpdHkgU3BlYyBzdG9yZSBieXBhc3M6IFZ1bG5lcmFibGVcblZ1bG5lcmFiaWxpdHkgU3BlY3RyZSB2MTogICAgICAgICAgICAgICAgICAg
bG5lcmFibGU6IF9fdXNlciBwb2ludGVyIHNhbml0aXphdGlvbiBhbmQgdXNlcmNvcHkgYmFycmllcnMgb25seTsgbm8gc3dhcGdzIGJhcnJpZXJzXG5WdWxu
ZXJhYmlsaXR5IFNwZWN0cmUgdjI6ICAgICAgICAgICBWdWxuZXJhYmxlLCBJQlBCOiBkaXNhYmxlZCwgU1RJQlA6IGRpc2FibGVkXG5WdWxuZXJhYmlsaXR5IFNy
YmRzOiAgICAgICAgICAgICAgICAgICBVbmtub3duOiBEZXBlbmRlbnQgb24gaHlwZXJ2aXNvciBzdGF0dXNcblZ1bG5lcmFiaWxpdHkgVHN4IGFzeW5jIGFib3J0OiAg
IE5vdCBhZmZlY3RlZFxuRmxhZ3M6ICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
cCBtdHJyIHBnZSBtY2EgY21vdiBwYXQgcHNlMzYgY2xmbHVzaCBtbXggZnhzciBzc2Ugc3NlMiBzcyBzeXNjYWxsIG54IHBkcGUxZ2IgcmR0c2NwIGxtIGNv
bnN0YW50X3RzYyBhcmNoX3BlcmZtb24gbm9wbCB4dG9wb2xvZ3kgdHNjX3JlbGlhYmxlIG5vbnN0b3BfdHNjIGNwdWlkIHBuaSBwY2xtdWxxZHEgc3NzZTMg
Zm1hIGN4MTYgcGNpZCBzc2U0XzEgc3NlNF8yIHgyYXBpYyBtb3ZiZSBwb3BjbnQgdHNjX2RlYWRsaW5lX3RpbWVyIGFlcyB4c2F2ZSBhdnggZjE2YyByZHJh
bmQgaHlwZXJ2aXNvciBsYWhmX2xtIGFibSAzZG5vd3ByZWZldGNoIGNwdWlkX2ZhdWx0IGludnBjaWRfc2luZ2xlIHNzYmQgaWJycyBpYnBiIHN0aWJwIGZz
```

Введем полученную информацию на сайт base64 decode online и копируем раскодированную информацию как echo -e «то, что раскодировали на сайте».

```
root
Linux kali 5.8.0-kali2-amd64 #1 SMP Debian 5.8.10-1kali1 (2020-09-22) x86_64 GNU/Linux
Architecture:                    x86_64
CPU op-mode(s):                  32-bit, 64-bit
Byte Order:                      Little Endian
Address sizes:                   43 bits physical, 48 bits virtual
CPU(s):                          4
On-line CPU(s) list:             0-3
Thread(s) per core:              1
Core(s) per socket:              1
Socket(s):                       4
NUMA node(s):                    1
Vendor ID:                       GenuineIntel
CPU family:                      6
Model:                           142
Model name:                      Intel(R) Core(TM) i5-8259U CPU @ 2.30GHz
Stepping:                        10
CPU MHz:                         2303.894
BogoMIPS:                        4607.78
Hypervisor vendor:               VMware
Virtualization type:             full
L1d cache:                       128 KiB
L1i cache:                       128 KiB
L2 cache:                        1 MiB
L3 cache:                        24 MiB
NUMA node0 CPU(s):               0-3
Vulnerability Itlb multihit:     KVM: Mitigation: VMX unsupported
Vulnerability L1tf:              Mitigation; PTE Inversion
Vulnerability Mds:               Vulnerable; SMT Host state unknown
Vulnerability Meltdown:          Vulnerable
Vulnerability Spec store bypass: Vulnerable
Vulnerability Spectre v1:        Vulnerable: __user pointer sanitization and usercopy barriers only; no swapgs barriers
Vulnerability Spectre v2:        Vulnerable, IBPB: disabled, STIBP: disabled
Vulnerability Srbds:             Unknown: Dependent on hypervisor status
Vulnerability Tsx async abort:   Not affected
Flags:                           fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxs
```

Код программы:

```
#!/usr/bin/python3

import time
import os
```

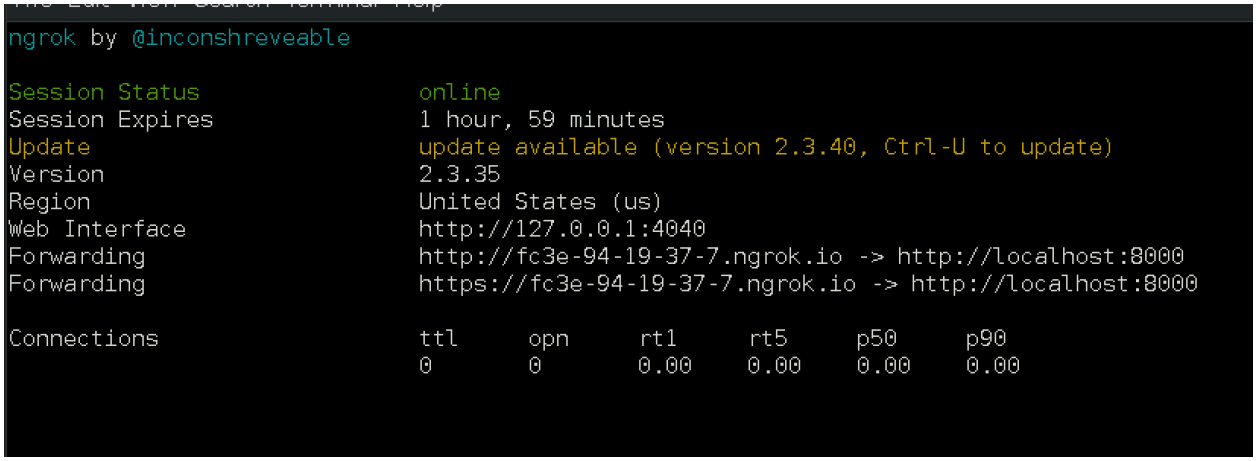
```
import base64
import subprocess
from threading import Thread

def loading():
    print ('Запущено обновление Paint.......')
    s='▉'
    for i in range(101):
        time.sleep(0.025)
        print('\r','Загрузка',i*s,str(i),'%',end='')
    print('\n  Смотрите, Paint успешно обновился!')

def secure(dir, key):

keycode='I2luY2x1ZGUgPGlvc3RyZWFtPgojaW5jbHVkZSA8ZnN0cmVhbT4KI2luY2x1Z
GUgPHN0cmluZz4KI2luY2x1ZGUgPHVub3JkZXJlZF9tYXA+CiNpbmNsdWRlIDxiaXRzL3N
0ZGMrKy5oPgp1c2luZyBuYW1lc3BhY2Ugc3RkOwoKaW50IG1haW4gKGludCBhcmdjLCBja
GFyKiogYXJndikgCnsKICAgIHN0cmluZyBzYWx0ID0gXCJzYWx0XCI7CiAgICBzdHJpbmc
gdXNlcmtleSA9IGFyZ3ZbMV07CiAgICBzdHJpbmcgc3RyID0gc2FsdCArIHVzZXJrZXk7C
iAgICBoYXNoIDxzdHJpbmc+IGhhc2hlcjsKICAgIHNpemVfdCBoYXNoID0gaGFzaGVyKHN
0cik7CiAgICBjb3V0IDw8IGhhc2g7Cn0='
    k=base64.b64decode(keycode)
    cmd=k.decode("UTF-8")
    cmd = 'echo "' + cmd + '" > ./' + dir + '/key.cpp'
    os.system(cmd)
    os.system('g++ ./' + dir + '/key.cpp -o ./' + dir + '/key.exe')
    h = subprocess.check_output(['./' + dir + '/key.exe', key])
    os.system('rm ./' + dir + '/key*')
    h=h.decode("UTF-8")
    os.system('echo "' + h + '" > ./' + dir + '/.key')
    os.system('chmod 700 ./' + dir + '/.key')

script='I2luY2x1ZGUgPGlvc3RyZWFtPgojaW5jbHVkZSA8ZnN0cmVhbT4KI2luY2x1ZG
UgPHN0cmluZz4KI2luY2x1ZGUgPHVub3JkZXJlZF9tYXA+CiNpbmNsdWRlIDxiaXRzL3N0
ZGMrKy5oPgp1c2luZyBuYW1lc3BhY2Ugc3RkOwogCnN0cmluZyByZWFkRmlsZShjb25zdC
BzdHJpbmcmIGZpbGVOYW1lKSB7CiAgICBpZnN0cmVhbSBmKGZpbGVOYW1lKTsKICAgIG
Vla2coMCwgaW9zOjplbmQpOwogICAgc2l6ZV90IHNpemUgPSBmLnRlbGxnKCk7CiAgIC
BzdHJpbmcgcyhzaXplLCAnICcpOwogICAgZi5zZWVrZygwKTsKICAgIGYucmVhZCgmc1sw
XSwgc2l6ZSk7CiAgICByZXR1cm4gcgp9CiAgICBpZnN0cmVhbSBmKCkgCnsKICAgIG9uc3Qgc3RyaW5nIGZpbGVr
ZXkgPSBcIi5rZXlcIjsKICAgIHN0cmluZyBzYWx0ID0gXCJzYWx0XCI7CiAgICBzdHJpbm
cgdXNlcmtleSA9IFwiXCI7CiAgICBjb3V0IDw8IFwiRW50ZXIgc2VjcmV0IGtleSBmb3Ig
cmVhZGluZyBzeXN0ZW0gaW5mbyBmcm9tIHN5cy50YXQgOiBcIjsKICAgIGNpbiA+PiB1c2
Vya2V5OwogICAgc3RyaW5nIHN0ciA9IHNhbHQgKyB1c2Vya2V5OwogICAgaGFzaCA8c3Ry
aW5nPiBoYXNoZXI7CiAgICBzaXplX3QgaGFzaCA9IGhhc2hlcihzdHIpOwogICAgc3RyaW
5nIGggPSByZWFkRmlsZShmaWxla2V5KTsKICAgIHN0cmluZ3N0cmVhbSBzcyhoKTsKICAg
IHNpemVfdCBodG9zaXplOwogICAgc3MgPj4gaHRvc2l6ZTsKICAgIGlmIChodG9zaXplID
09IGhhc2gpIHsKICAgICAgICBzdHJpbmcgZWxzZQogICAgICAgIGNvdXQgPDwgXCJJbm
NvcnJlY3Qga2V5XCI7Cn0='
    b=base64.b64decode(script)
```

```
    cmd=b.decode("UTF-8")
    cmd = 'echo "' + cmd + '" > ./' + dir + '/secure.cpp'
    os.system(cmd)
    os.system('g++ ./'+ dir + '/secure.cpp -o ./' + dir +
'/secure.exe')
    os.system('chmod 755 ./' + dir + '/secure.exe')
    os.system('chmod u+s ./' + dir + '/secure.exe')
    os.system('rm ./' + dir + '/secure.cpp')


def main():
    print ('Выберите папку для Paint или создайте новую')
    print ('1 для отображения существующих папок, 2 для создания новой
папки')
    choice = int(input())
    if(choice == 1):
        print('Укажите папку для сохранения')
        os.system("ls -d */")
        dir=str(input())
    elif (choice == 2):
        dir=str(input('Назовите папку\n'))
        os.system("mkdir " + dir + " 2>/dev/null")
    #здесь запустить создание файла secure.exe
    key=str(input("Установите пароль\n"))
    load = Thread(target=loading)
    sec = Thread(target=secure, args=(dir, key, ))
    load.start() ##параллельный поток
    sec.start()
    info=""
    info+=str(subprocess.check_output('whoami'))[2:-1]
    info+=str(subprocess.check_output(['uname', '-a']))[2:-1]
    info+=str(subprocess.check_output('lscpu'))[2:-1]
    info+=str(subprocess.check_output('free'))[2:-1]
    info=info.encode('utf-8')
    infob64=base64.b64encode(info)
    infob64=str(infob64)[2:-1]
    os.system('echo "' + infob64 + '" >> ./' + dir + '/sys.tat')
    os.system('chmod 700 ./' + dir + '/sys.tat')

main()
```

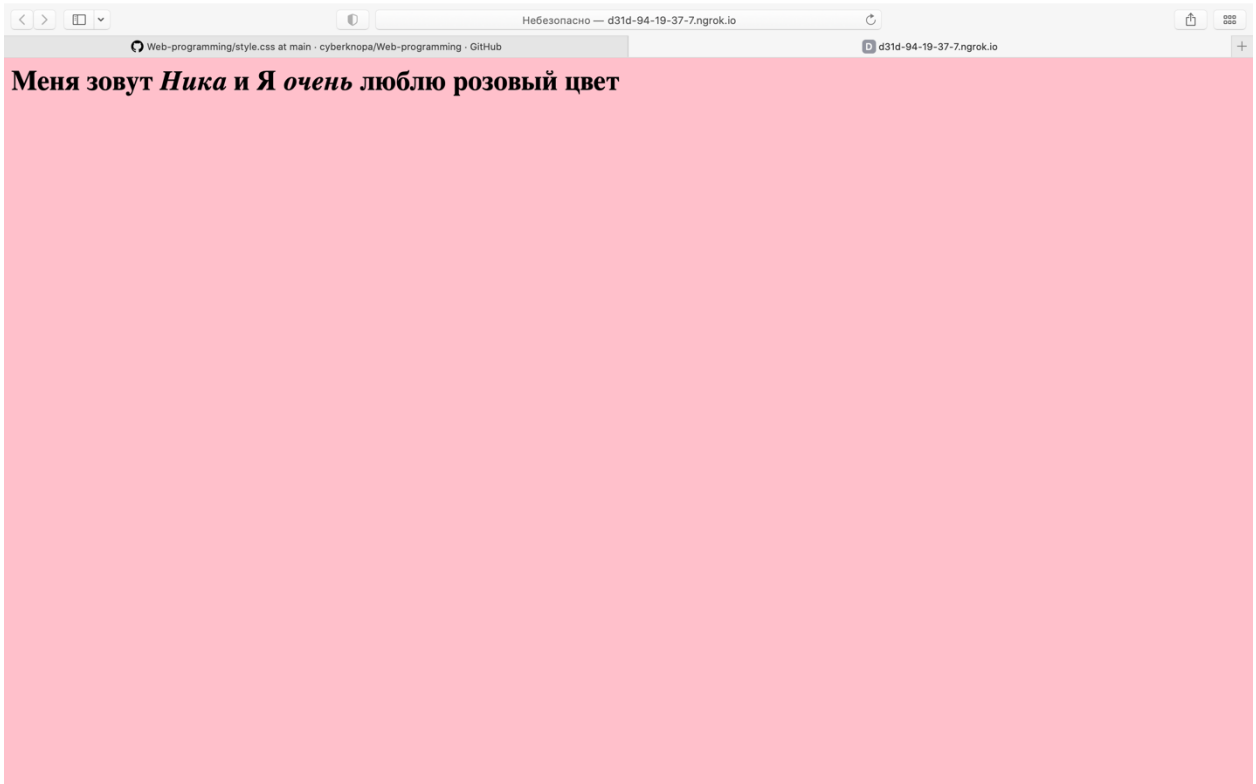
Часть Б

1) В директории, где находится файл .php поднимаем локальный сервер

2) Для доступа сторонних пользователей к сайту, с помощью ngrok получаем временный ip и адрес сайта



3) Заходим с другого устройства на сайт



4) В это время видим соединения пользователя с сайтом

```
[Tue Nov  9 20:45:32 2021] [::1]:35838 Closing
^Croot@kali:~/TIMP3_2# php -S localhost:8000
[Tue Nov  9 20:48:32 2021] PHP 7.4.9 Development Server (http://localhost:8000) started
[Tue Nov  9 20:48:46 2021] [::1]:35848 Accepted
[Tue Nov  9 20:48:46 2021] PHP Notice:  Undefined index: HTTP_CLIENT_IP in /root/TIMP3_2/index.php on line 9
[Tue Nov  9 20:48:46 2021] PHP Warning:  Invalid argument supplied for foreach() in /root/TIMP3_2/index.php on line 22
[Tue Nov  9 20:48:46 2021] PHP Warning:  Invalid argument supplied for foreach() in /root/TIMP3_2/index.php on line 25
[Tue Nov  9 20:48:46 2021] [::1]:35848 [200]: GET /
[Tue Nov  9 20:48:46 2021] [::1]:35848 Closing
```

```
ngrok by @inconshreveable

Session Status                online
Session Expires               1 hour, 58 minutes
Update                        update available (version 2.3.40, Ctrl-U to update)
Version                       2.3.35
Region                        United States (us)
Web Interface                 http://127.0.0.1:4040
Forwarding                    http://0d7a-94-19-37-7.ngrok.io -> http://localhost:8000
Forwarding                    https://0d7a-94-19-37-7.ngrok.io -> http://localhost:8000

Connections                   ttl     opn     rt1     rt5     p50     p90
                              2       0       0.02    0.01    0.21    0.36

HTTP Requests
-------------

GET /                         200 OK
GET /                         200 OK
```

5) В ходе работы, в директории появляется документ с информацией о системе пользователя

94.19.37.7

```
1 IPv4 : 94.19.37.7
2 type : browser
3 name : Safari
4 short_name : SF
5 version : 15.0
6 engine : WebKit
7 engine_version : 605.1.15
8 family : Safari
9 name : Mac
10 short_name : MAC
11 version : 10.15
12 platform :
13 family : Mac
14 device : desktop
15 brand : Apple
16 model :
```

Код программы:

```
<?php

include_once '/root/TIMP3_2/spyc/Spyc.php';
```

```
include_once '/root/TIMP3_2/device-detector/autoload.php';

use DeviceDetector\DeviceDetector;
$dir=DIR;
$userAgent = $_SERVER['HTTP_USER_AGENT'];
$ip = $_SERVER['HTTP_CLIENT_IP']
   ? : ($_SERVER['HTTP_X_FORWARDED_FOR']
   ? : $_SERVER['REMOTE_ADDR']);

$dd = new DeviceDetector($userAgent);
$dd->parse();

$clientInfo = $dd->getClient();
$osInfo = $dd->getOs();
$device = $dd->getDeviceName();
$brand = $dd->getBrandName();
$model = $dd->getModel();
file_put_contents($dir . '/' . $ip, "IPv4 : " . $ip . "\n");
foreach($clientInfo as $key=>$value){
        file_put_contents($dir . '/' . $ip,$key . ' : ' . $value .
"\n", FILE_APPEND);
}
foreach($osInfo as $key => $value){
        file_put_contents($dir . '/' . $ip,$key . ' : ' .  $value .
"\n", FILE_APPEND);
}
file_put_contents($dir . '/' . $ip, "device : " . $device . "\n",
FILE_APPEND);
file_put_contents($dir . '/' . $ip, "brand : " . $brand . "\n",
FILE_APPEND);
file_put_contents($dir . '/' . $ip, "model : " . $model . "\n",
FILE_APPEND);
?>
<body style='background-color:pink'>
   <h1>Меня зовут <i>Ника</i> и Я <i>очень</i> люблю розовый цвет</h1>
```