

2

## Инструкция по эксплуатации

1. Обновите пакеты репозиториев ваших машин:

```
sudo apt update & sudo apt upgrade
```

- 2. Импортировать файл со скриптом на вашу виртуалку, можете просто скопировать содержимое, создать файл .py и вставить туда, не забудьте сохранить
- 3. Запустите скрипт от рута

```
sudo python3 file.py
```

- 4. Зайдите в настройки сети, пропишите на своем пк в DNS адрес вашей виртуалки
- 5. Откройте браузер и введите полное доменное имя ваших сайтов

```
http://site.test.dns
Второй сайт нужно открыть как https://site2.test.dns
```

6. Вот сам скрипт, который все сделает за вас:

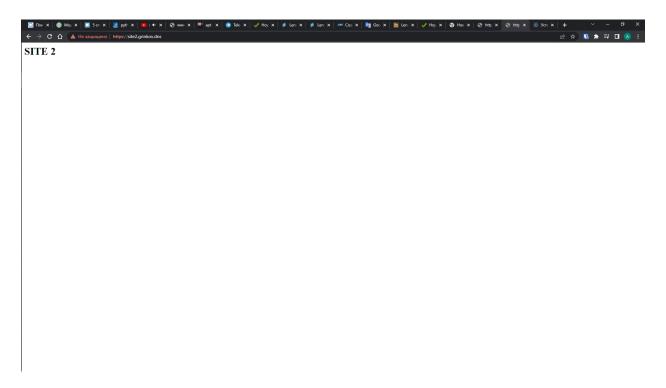
```
#!/bin/python3
import os
import subprocess
import time
import re
import io
#######НЕОБХОДИМЫЕ ЗНАЧЕНИЯ####################
user = subprocess.getoutput("whoami")
ip = subprocess.getoutput("hostname -I")
reversip = ('.'.join([ip.split('.')[2],ip.split('.')[1],ip.split('.')[0]]))
reversip2 = (' '.join([ip.split('.')[3]]))
file5 = '/etc/bind/named.conf.options'
with open(file5 , "w") as f:
f.write("options {\n"
        '\tdirectory "/var/cache/bind";\n'
       "\tforwarders {\n"
             "\t\t8.8.4.4;\n"
        "\t};\n"
        "\trecursion yes;\n"
        "\tdnssec-validation auto;\n"
        "\tlisten-on \{\n"
             "\t\t127.0.0.1;\n"
             "\t\t"+ip+";\n"
             "\t\t};\n"
        "\t};")
name_zone = input("Введите название зоны, например 'test.dns' или 'test'\n")
file6 = '/etc/bind/named.conf.local'
with open(file6 , "w") as f:
           f.write('zone \"'+name_zone+'\" {\n'
           'type master;\n'
          'file \"/etc/bind/'+name_zone+'.forward\";\n'
           '};\n'
           '\n'
```

```
'zone \"'+reversip+'.in-addr.arpa\" \{\n'
           'type master;\n'
          'file \"/etc/bind/'+name_zone+'.revers\";\n'
           '};')
os.system("sudo touch /etc/bind/"+name_zone+".forward /etc/bind/"+name_zone+".revers")
name_site = input("Введи доменное имя первого сайта: ")
name_site2 = input("Введи доменное имя второго сайта: ")
file7 = '/etc/bind/'+name_zone+'.forward'
with open(file7 , "w") as f:
          f.write(';\n'
'; BIND data file for local loopback interface\n'
';\n'
'$TTL
        604800\n'
                        localhost.'+name_zone+'. root.localhost.'+name_zone+'. (\n'
'@
                                    ; Serial\n'
                             2
                                       ; Refresh\n'
                         86400
                                      ; Retry\n'
                       2419200
                                      ; Expire\n'
                        604800 )
                                      ; Negative Cache TTL\n'
';\n'
'@
                               \tlocalhost.'+name_zone+'.\n'
               IN
                        NS
'localhost
                                      \t127.0.0.1\n'
                       IN
                               Α
''+name_site+'
                                              '+ip+'\n
                        IN
                               Α
''+name_site2+'
                                               '+ip+'\n')
                        IN
                                Α
file8 = '/etc/bind/'+name_zone+'.revers'
with open(file8 , "w") as f:
          f.write(';\n'
'; BIND reverse data file for local loopback interface\n'
':\n'
'$TTI
        604800\n'
                        localhost.'+name_zone+'. root.localhost.'+name_zone+'. (\n'
'@
        IN
               SOA
                             1
                                      ; Serial\n'
                         604800
                                       ; Refresh\n'
                        86400
                                       ; Retry\n'
                       2419200
                                       ; Expire\n'
                        604800 )
                                       ; Negative Cache TTL\n'
';\n'
'@
        IN
                NS
                        localhost.'+name_zone+'.\n'
''+reversip2+'
                 IN
                        PTR localhost.'+name_zone+'.\n'
''+reversip2+'
                 IN
                          PTR
                                 '+name_site+'.'+name_zone+'.\n'
''+reversip2+'
                  IN
                          PTR
                                 '+name_site2+'.'+name_zone+'.\n')
os.system("sudo rm -rf /var/www/html")
os.system("sudo rm -rf /etc/apache2/sites-available/000-default.conf")
name_dir = input("Введи название директории в которой будет храниться index.html твоего первого '"'МЕGA'"' сайта\n")
os.system("sudo mkdir /var/www/"+name_dir)
os.system("sudo touch /var/www/"+name_dir+"/index.html")
file1 = '/var/www/'+name_dir+'/index.html'
with open(file1 , "w") as f:
   f.write("<h1>SITE 1 </h1>")
while True:
    name dir2 = input("Введи название директории в которой будет храниться index.html твоего второго '"'MEGA'"' сайта\n")
    if name_dir != name_dir2:
       os.system("sudo mkdir /var/www/"+name_dir2)
       os.system("sudo touch /var/www/"+name_dir2+"/index.html")
       break
    else:
       print("Уже сущетвует")
file2 = '/var/www/'+name_dir2+'/index.html'
with open(file2 , "w") as f:
   f.write("<h1>SITE 2 </h1>")
file3 = '/etc/apache2/sites-enabled/'+name_site+'.conf'
with open(file3 , "w") as f:
    f.write("<VirtualHost *:80>\n"
   "\tServerAdmin admin@"+name_site+"\n"
   "\tServerName "+name_site+"."+name_zone+"\n"
   "\tDocumentRoot /var/www/"+name_dir+"\n"
   "\tErrorLog ${APACHE_LOG_DIR}/error.log\n"
   \verb| "\tCustomLog ${APACHE\_LOG\_DIR}/access.log combined \\ \verb| " | \\
"</VirtualHost>")
print ("НАСТРОЙКА СЕРТИФИКАТА, ВНИМАНИЕ!, в Common Name нужно указать полное доменное имя вашего 2-го сайта --->"+name_site2+"."+name_zone+
      "ВСЕ ОСТАЛЬНЫЕ НАСТРОЙКИ СЕРТИФИКАТА МОЖЕТЕ ПРОСТО ПРОЖАТЬ Enter\n")
os.system("sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apac
```

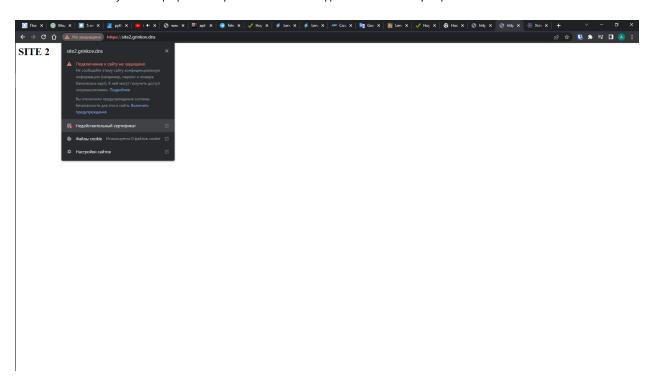
```
file9 = '/etc/apache2/conf-available/ssl-params.conf'
with open(file9 , "w") as f:
           f.write('SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH\n'
'SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1\n'
'SSLHonorCipherOrder On\n'
'Header always set X-Frame-Options DENY\n'
'Header always set X-Content-Type-Options nosniff\n'
'SSLCompression off\n'
'SSLUseStapling on\n'
'SSLStaplingCache "shmcb:logs/stapling-cache(150000)"\n'
'SSLSessionTickets Off')
file10 = '/etc/apache2/sites-enabled/default-ssl.conf'
with open(file10 , "w") as f:
    f.write("<IfModule mod_ssl.c>\n"
        "\t<VirtualHost _default_:443>\n"
               "\t\tServerAdmin admin@"+name_site2+"\n"
               "\t\tServerName "+name_site2+"."+name_zone+"\n"
               "\t\tDocumentRoot /var/www/"+name_site2+"\n"
               "\t\tErrorLog ${APACHE_LOG_DIR}/error.log\n"
               "\t\tCustomLog ${APACHE_LOG_DIR}/access.log combined\n"
               "\t\tSSLEngine on\n"
               "\t\tSSLCertificateFile
                                           /etc/ssl/certs/apache-selfsigned.crt\n"
               "\t\tSSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key\n"
                '\t\t<FilesMatch "\.(cgi|shtml|phtml|php)$">\n'
                               "\t\t\tSSLOptions +StdEnvVars\n"
               "\t\t</FilesMatch>\n"
               "\t\t</Directory>\n"
       "\t</VirtualHost>\n"
"</IfModule>")
file4 = '/etc/apache2/sites-enabled/'+name_site2+'.conf'
with open(file4 , "w") as f:
    f.write("<VirtualHost *:80>\n"
   "\tServerAdmin admin@"+name_site2+"\n"
   "\tServerName "+name_site2+"."+name_zone+"\n"
   "\tDocumentRoot /var/www/"+name_dir2+"\n"
   "\tErrorLog ${APACHE_LOG_DIR}/error.log\n"
   \verb| "\tCustomLog ${APACHE\_LOG\_DIR}/access.log combined \\ \verb| " | \\
"</VirtualHost>")
os.system("sudo ufw allow 'Apache Full'")
os.system("sudo ufw delete allow 'Apache'")
os.system("sudo a2enmod ssl")
os.system("sudo a2enmod headers")
os.system("sudo a2ensite default-ssl")
os.system("sudo a2enconf ssl-params")
print ("Перезапуск APACHE2 и BIND9")
os.system("sudo systemctl restart apache2 bind9")
time.sleep(3)
print("1. Директории с файлами сайтов index.html хранятся в /var/www/[название ваших сайтов]\n"
                       "2. Настройки вашей forward и revers зон хранятся в /etc/bind/[название вашей зоны].forward .revers\n"
                       "3. Настройки виртуальных хостов хранятся в /etc/apache2/sites-available/[название ваших сайтов] conf"
                       "4. Сертификат сайта храниться в файле /etc/ssl/certs/apache-selfsigned.crt\n"
                       "5. Закрытый ключ сайта храниться в файле /etc/ssl/certs/apache-selfsigned.key\n")
```

## 7. Импорт сертификата в браузер:

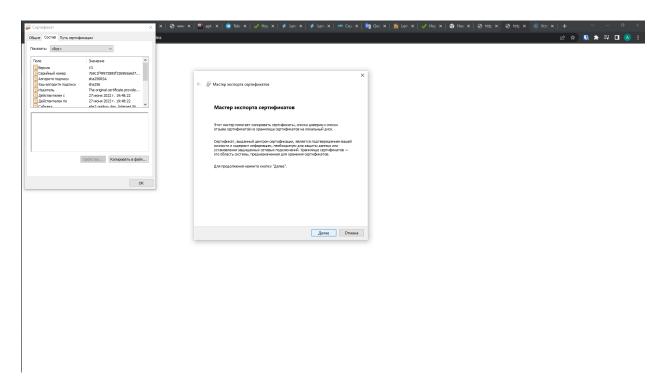
• Перейти на сайт https://site.test.dns:



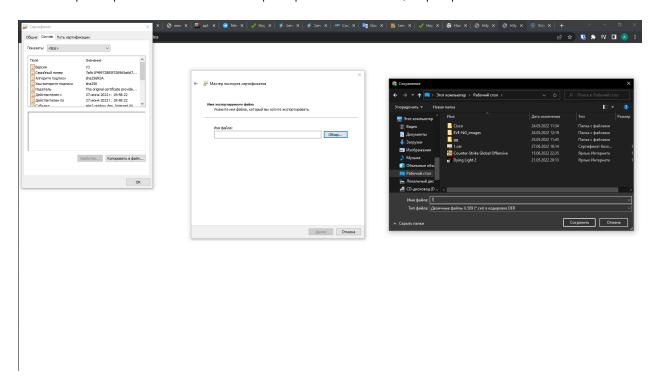
• Нажать на иконку "Не защищено" и перейти по ссылке "Недействительный сертификат"



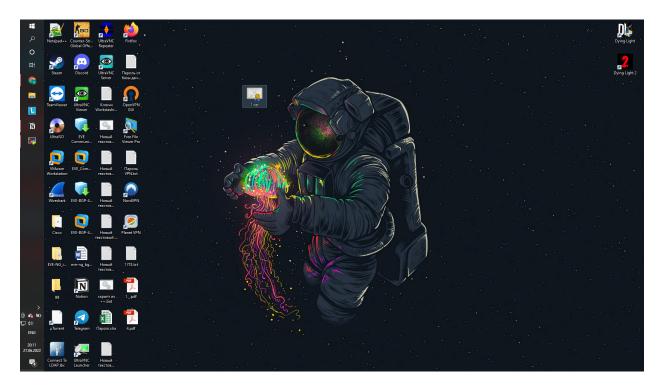
• В открывшемся окне перейдите на "Состав" → "Копировать файл"



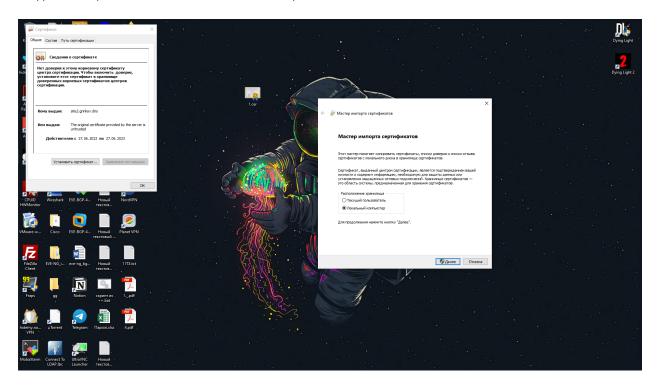
• В "Обзор" выберете Рабочий стол и назвите файл произвольным именем, например "1":



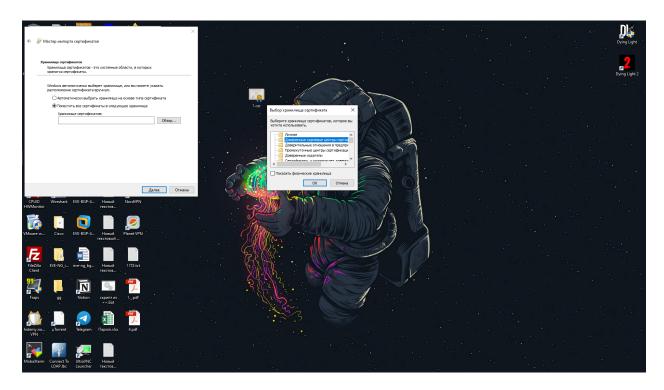
• Появится иконка с вашим названием, нажмите на нее, это ваш сертификат:



• Далее выберете Установить, Локальный компьютер



• Далее выберете Поместить все сертификаты в следующее хранилище, Доверенные корневые центры сертификации:



- На этом импорт завершен, теперь закройте все вкладки и браузер, очистите историю вашего браузера, в командной строке Windows сделайте команду ipconfig/flushdns
- Открывайте сайты в браузере

ВНИМАНИЕ - замок не закроется но соединение с шифрованием работать будет, Меркотан сказал замочек НЕ ОБЯЗАТЕЛЕН!!!

Хотите закрыть замок, разворачивайте двухуровневый центр сертификации чтобы браузер считал его доверенным

8. Создать задание для перезапуска сервера:

```
crontab -e
выбрать nano
написать в конце файла:
0 * * * * systemctl restart nginx.service
```

## 9. Запустить cron:

sudo /sbin/service cron start

## 10. По поводу curl:

- Проверка ваших сайтов curl, для этого вам нужно дописать в файл /etc/resolvconf адрес вашей виртуалки (nameserver 172.16.177...) и в search указать вашу доменную зону
- после этого в командной оболочке просто пишите curl и доменное имя вашего сайта