

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
import sys
```

```
#######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]]))
os.system("sudo apt install -y nginx bind9 dnsutils")
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};")
os.system("clear")
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'
'@
        IN
                S0A
                        localhost.'+name_zone+'. root.localhost.'+name_zone+'. (\n'
                             2
                                     ; Serial\n'
                         604800
                                      ; Refresh\n'
                        86400
                                      ; Retry\n'
                       2419200
                                     ; Expire\n'
                        604800 )
                                     ; Negative Cache TTL\n'
';\n'
'@
                        NS
                               \tlocalhost.'+name_zone+'.\n'
                ΤN
                                       \t127.0.0.1\n'
'localhost
                        IN
```

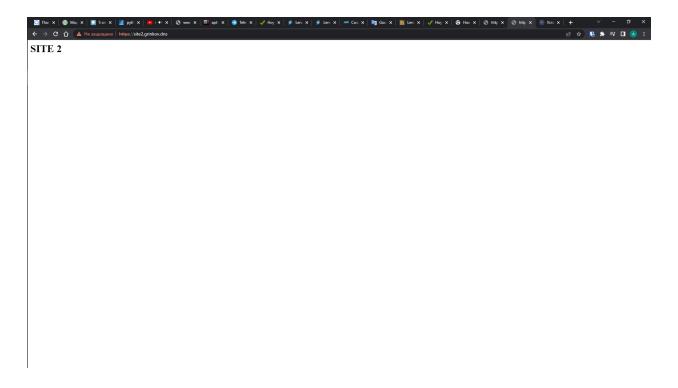
```
'+ip+'\n'
''+name_site+'
                                 Α
''+name_site2+'
                         IN
                                 Α
                                                 '+ip+'\n')
file8 = '/etc/bind/'+name_zone+'.revers'
with open(file8 , "w") as f:
           f.write(';\n'
'; BIND reverse data file for local loopback interface\n'
';\n'
'$TTL
        604800\n'
' @
        IN
                 SOA
                         localhost.'+name_zone+'. root.localhost.'+name_zone+'. (\n'
                               1
                                     ; Serial\n'
                          604800
                                        ; Refresh\n'
                          86400
                                        ; Retry\n'
                                       ; Expire\n'
                        2419200
                         604800 )
                                       ; Negative Cache TTL\n'
';\n'
        IN
                 NS
                        localhost.'+name_zone+'.\n'
''+reversip2+'
                           PTR
                                 localhost.'+name_zone+'.\n'
                 IN
''+reversip2+'
                           PTR
                                   '+name_site+'.'+name_zone+'.\n'
                  ΙN
''+reversip2+'
                                   '+name_site2+'.'+name_zone+'.\n')
                  ΙN
                           PTR
##HACTРОЙКА NGINX##################
os.system("sudo touch /etc/nginx/sites-enabled/default2")
os.system("sudo rm -rf /var/www/html")
os.system("clear")
name_dir = input("Введи название директории в которой будет храниться index.html твоего пе
рвого '"'MEGA'"' 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 твое
го 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/nginx/sites-enabled/default'
with open(file3 , "w") as f:
            f.write("server {\n"
        "\tlisten 80;\n"
        "\tserver_name "+name_site+"."+name_zone+";\n"
        "\troot /var/www/"+name_dir+";\n"
```

```
"\tindex index.html;\n"
        "\tlocation / {\n"
               "\t\ttry_files $uri $uri/ =404;\n"
        "\t}\n"
"}")
os.system("clear")
print ("НАСТРОЙКА СЕРТИФИКАТА, BHUMAHUE!, в Common Name нужно указать полное доменное имя
вашего 2-го сайта --->"+name_site2+"."+name_zone+"<---\n"
      "ВСЕ ОСТАЛЬНЫЕ НАСТРОЙКИ СЕРТИФИКАТА МОЖЕТЕ ПРОСТО ПРОЖАТЬ Enter\n")
os.system("sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/priva
te/nginx-selfsigned.key -out /etc/ssl/certs/nginx-selfsigned.crt")
os.system("sudo openssl dhparam -out /etc/ssl/certs/dhparam.pem 2048")
file8 = '/etc/nginx/snippets/self-signed.conf'
with open(file8 , "w") as f:
           f.write("ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;\n"
                   "ssl_certificate_key /etc/ssl/private/nginx-selfsigned.key;\n")
file9 = '/etc/nginx/snippets/ssl-params.conf'
with open(file9 , "w") as f:
           f.write("ssl_protocols TLSv1 TLSv1.1 TLSv1.2;\n"
"ssl_prefer_server_ciphers on;\n"
'ssl_ciphers "EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH";\n'
"ssl_ecdh_curve secp384r1;\n"
"ssl_session_cache shared:SSL:10m;\n"
"ssl_session_tickets off;\n"
"ssl_stapling on; \n"
"ssl_stapling_verify on;\n"
"resolver 8.8.8.8 8.8.4.4 valid=300s;\n"
"resolver_timeout 5s;\n"
'add_header Strict-Transport-Security "max-age=63072000; includeSubdomains; preload";\n'
"add_header X-Frame-Options DENY;\n"
"add_header X-Content-Type-Options nosniff;\n"
"ssl_dhparam /etc/ssl/certs/dhparam.pem;\n")
file10 = '/etc/nginx/sites-enabled/default2'
with open(file10 , "w") as f:
           f.write("server {\n"
        "\tlisten 80;\n"
        "\tserver_name "+name_site2+"."+name_zone+";\n"
        "\troot /var/www/"+name_dir2+";\n"
        "\tindex index.html;\n"
        "\treturn 301 https://$server_name$request_uri;\n"
        "\tlocation / {\n"
                "\t\ttry_files $uri $uri/ =404;\n"
        "\t}\n"
        "}\n"
        "\n"
        "server {\n"
       "# SSL configuration\n"
       "\tlisten 443 ssl http2;\n"
        "\tinclude snippets/self-signed.conf;\n"
        "\tinclude snippets/ssl-params.conf;\n"
```

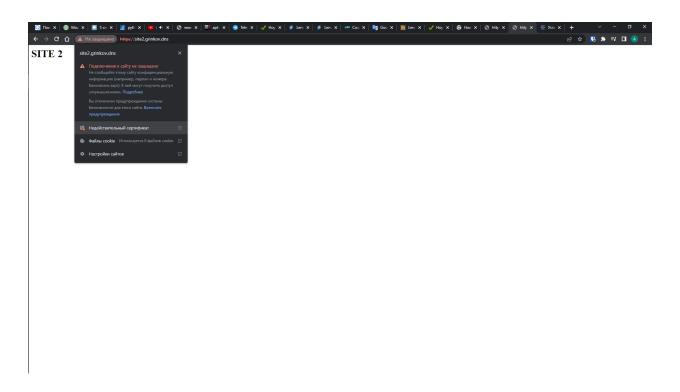
```
"\tserver_name "+name_site2+"."+name_zone+";\n"
        "\troot /var/www/"+name_dir2+";\n"
        "\tindex index.html;\n"
"}")
os.system("sudo ufw allow 'Nginx Full'")
os.system("sudo ufw delete allow 'Nginx HTTP'")
os.system("sudo systemctl restart bind9 nginx")
os.system("clear")
print ("Перезапуск NGINX и BIND9")
time.sleep(3)
print("1. Директории с файлами сайтов index.html хранятся в /var/www/[название ваших сайто
      "2. Настройки вашей forward и revers зон хранятся в /etc/bind/[название вашей зоны].
forward .revers\n"
      "3. Настройки виртуальных хостов хранятся в /etc/nginx/sites-available/[название ваш
их сайтов].conf\n"
      "4. Сертификат сайта храниться в файле /etc/ssl/certs/nginx-selfsigned.crt\n"
      "5. Закрытый ключ сайта храниться в файле /etc/ssl/certs/nginx-selfsigned.key\n")
```

7. Импорт сертификата в браузер:

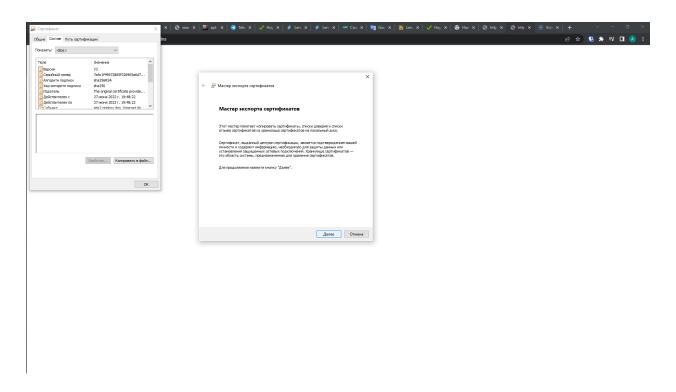
• Перейти на сайт https://site.test.dns:



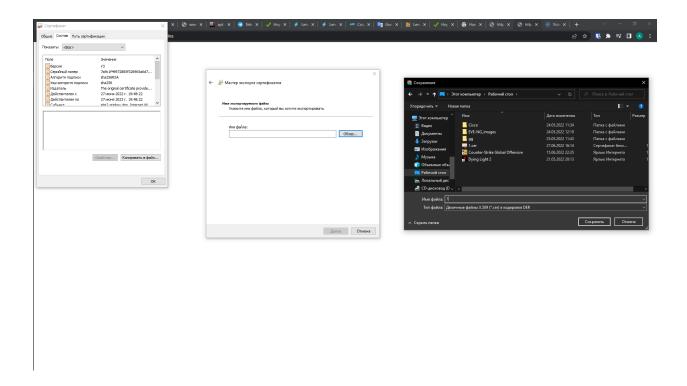
 Нажать на иконку "Не защищено" и перейти по ссылке "Недействительный сертификат"



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



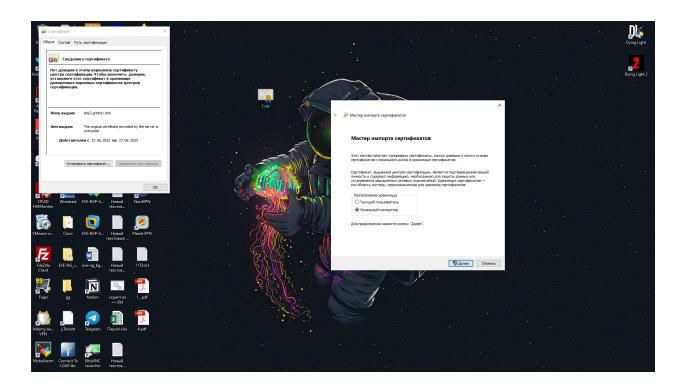
• В "Обзор" выберете Рабочий стол и назвите файл произвольным именем, например "1":



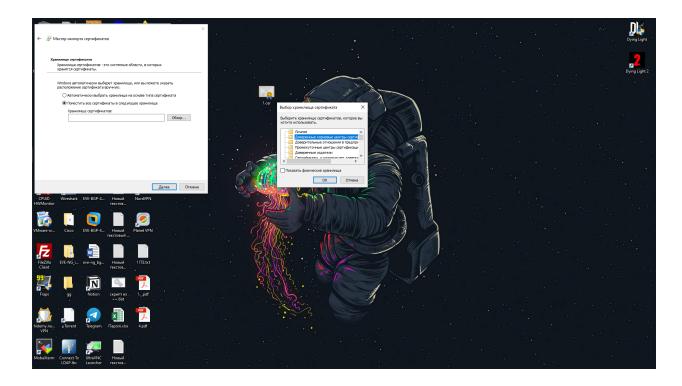
• Появится иконка с вашим названием, нажмите на нее, это ваш сертификат:



• 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