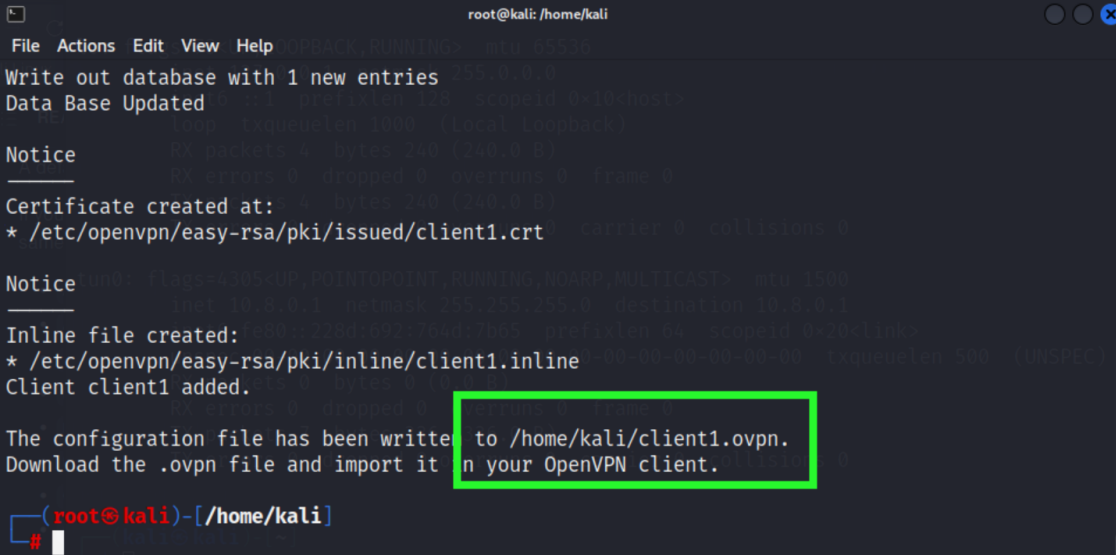


САМОСТОЯТЕЛЬНАЯ РАБОТА 4.3

ГАЙД

ШАГ 1. Заданием для этой самостоятельной работы является загрузить сформированный конфигурационный файл в ответ. То есть целью того задания является изучение его содержимого - того, что нужно, чтобы клиенты могли подключаться к VPN серверам. В конце установки OpenVPN было указано расположение файла, который нам нужен.



```
root@kali: /home/kali
File Actions Edit View Help
Write out database with 1 new entries
Data Base Updated
Notice
Certificate created at:
* /etc/openvpn/easy-rsa/pki/issued/client1.crt
Notice
Inline file created:
* /etc/openvpn/easy-rsa/pki/inline/client1.inline
Client client1 added.
The configuration file has been written to /home/kali/client1.ovpn.
Download the .ovpn file and import it in your OpenVPN client.
(root@kali)~[/home/kali]
```

ШАГ 2. Рассмотрим содержимое созданного конфигурационного файла:

```
client
proto udp
explicit-exit-notify
remote 1194
dev tun
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
verify-x509-name server_aaH5x5WlvhutFUda name
auth SHA256
auth-nocache
cipher AES-128-GCM
tls-client
tls-version-min 1.2
tls-cipher TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256
ignore-unknown-option block-outside-dns
setenv opt block-outside-dns # Prevent Windows 10 DNS leak
verb 3
<ca>
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIU FH4B8UugLqIFzt4q/QC1pAk9fxYwCgYIKoZIzj0EAwIw
-----END CERTIFICATE-----
</ca>
```

```

<cert>
-----BEGIN CERTIFICATE-----
MIIB2jCCAYCgAwIBAgIRANu3FcvjjNsChV+t3ckWyl8wCgYIKoZlZjOEAwIwHjEc

-----END CERTIFICATE-----
</cert>
<key>
-----BEGIN PRIVATE KEY-----
MIGHAgEAMBMGBYqGSM49AgEGCCqGSM49AwEHBG0wawIBAQQgROWqdP697CeL6l5l

-----END PRIVATE KEY-----
</key>
<tls-crypt>
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
75e3d72bd6a1013c957a3faa2d372864

-----END OpenVPN Static key V1-----
</tls-crypt>

```

По сути это текстовый файл, который считывает программа OpenVPN client для того, чтобы подключиться к серверу. В примере оставлены только первые строки последовательностей ключей и сертификатов.

В этом файле содержатся настройки для подключения:

DNS, протокол, по которому идет соединение, подключаемый порт (и IP адреса, но не в нашем случае, так как мы его не указывали), методы шифрования и аутентификации и может быть указано еще многое другое.

ШАГ 3. В этом файле также в указаны все ключи и сертификаты. И часто бывает нужно поделиться с кем-то файлом конфигурации, чтобы подключился другой человек, но по своим сертификатам и ключам. Поэтому в задании нужно будет из файла удалить содержимое всех ключей и сертификатов, кроме корневого <ca> </ca>.

То есть содержимое файла для ответа будет иметь вид примерно такой:

```

client
proto udp
explicit-exit-notify
remote 1194
dev tun
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
verify-x509-name server_aaH5x5WlvhutFUda name
auth SHA256
auth-nocache
cipher AES-128-GCM
tls-client

```

```
tls-version-min 1.2
tls-cipher TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256
ignore-unknown-option block-outside-dns
setenv opt block-outside-dns # Prevent Windows 10 DNS leak
verb 3
<ca>
-----BEGIN CERTIFICATE-----
MIIB1zCCAX2gAwIBAgIUFH4B8UugLqIFzt4q/QC1pAk9fxYwCgYIKoZIzj0EAwIw
HjEcMBoGA1UEAwwTY25fQXdQOFRldlFua2w1aHIQUzAeFw0yMzA2MjgxNjAzMTIa
Fw0zMzA2MjUxNjAzMTIaMB4xHDAaBgNVBAMME2NuX0F3UDhUdXZRbmNzNWWh5UFMw
WTATBgkcqhkJOPQIBBgqhkJOPQMBAwNCAATWAMOpXX0l4e7/S0vIZikyX7DFnWZs
VyJWjsfzEChI+AV49QWICq+VUZIGILir1lInVvxCOtgIEVwDqP9dRXNo4GYMIGV
MAwGA1UdEwQFMAMBAf8wHQYDVR0OBBYEFNGTpd4qje2pbO2RiJldLcr3iESwMFkG
A1UdlwRSMFCAFNGTpd4qje2pbO2RiJldLcr3iESwOSKkIDAeMRwwGgYDQDDBNj
bI9Bd1A4VHV2UW5rbDVoeVBTghQUfgHxS6AuogXO3ir9ALWkCTI/FjALBgNVHQ8E
BAMCAQYwCgYIKoZIzj0EAwIDSAAwRQIhAPO55hCgS8xnWBynp5hyYfN2rlyDKluM
dP2HqJro0Q82AiAaPHGEov+e0TiZR4WTwsfUoPz+XR8uUJMz0+oweHomFA==
-----END CERTIFICATE-----
</ca>
<cert>
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
</cert>
<key>
-----BEGIN PRIVATE KEY-----

-----END PRIVATE KEY-----
</key>
<tls-crypt>
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----

-----END OpenVPN Static key V1-----
</tls-crypt>
```