Настройка OpenSSH доступа по Рутокен MFA с доступом по PIN-коду

Описание стенда

- **Сервер:** ОС Ubuntu 22.04, OpenSSH 8.9p1, IP-адрес – 192.168.88.129.
- **Клиент 1:** ОС Ubuntu 23.10, OpenSSH 9.3p1, IP-адрес – 192.168.88.147.
- **Клиент 2:** Windows 10, OpenSSH Beta 9.5, IP-адрес – 192.168.88.1.

Настройка стенда

Настройка Клиента 1 (Ubuntu)

1. Для включение защиты по PIN-коду, установите пакет ssh-askpass:

```
$ sudo apt-get install ssh-askpass
```

2. Для того, чтобы запрашивался PIN-код, укажите ssh-agent:

```
$ eval "$(ssh-agent -s; SSH_ASKPASS=/usr/bin/ssh-askpass)"
```

3. Для генерации ключей:

```
$ ssh-keygen -t ecdsa-sk -O resident -O application=ssh:YourTextHere -O verify-required
Generating public/private ecdsa-sk key pair.
You may need to touch your authenticator to authorize key generation.
Enter file in which to save the key (/home/tester/.ssh/id_ecdsa_sk):
/home/tester/.ssh/id_ecdsa_sk already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/tester/.ssh/id_ecdsa_sk
Your public key has been saved in /home/tester/.ssh/id_ecdsa_sk.pub
The key fingerprint is:
SHA256:/vIIfHBajgeOHYoMjbzaE2eUoXU40jwSALfpuHjr9YA tester@tester2310
The key's randomart image is:
+-[ECDSA-SK 256]--+
|+.o+ .           |
| .ooO .          |
|  o= *           |
|.=. o            |
|+.o.  + S        |
|.+ooo* @         |
|o.E+= B =        |
|.o.o o +.o       |
|..+.  . .oo      |
+----[SHA256]-----+
```

4. Скопируйте открытый ключ на сервер:

```
$ ssh-copy-id -i /home/tester/.ssh/id_ecdsa_sk.pub tester@192.168.88.129
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/tester/.ssh/id_ecdsa_sk.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already
installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install
the new keys
tester@192.168.88.129's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'tester@192.168.88.129'"
and check to make sure that only the key(s) you wanted were added.
```

Настройка Клиента 2 (Windows)

1. Чтобы использовать Рутокен MFA для подключения в подсистеме WSL2, установите пакет OpenSSH Beta:

```
winget install "openssh beta"
```

2. Запустите оболочку WSL2 и добавьте переменную окружения для использования устройств FIDO2:

```
wsl
$ export SSH_SK_HELPER="/mnt/c/Program Files/OpenSSH/ssh-sk-helper.exe"
```

3. Скопируйте файлы ключей для подключения по ssh в папку ~/.ssh/:

```
$ cp /mnt/c/id_ecdsa_sk ~/.ssh
$ cp /mnt/c/id_ecdsa_sk.pub ~/.ssh
```

Настройка Сервера (Ubuntu)

Добавьте ключ "verify-required" в строку с ключом подключения в файле ~/.ssh/authorized_keys:

```
//   :
$ cat /home/tester/.ssh/authorized_keys
sk-ecdsa-sha2-nistp256@openssh.com
AAAAInNrLWVjZHNhLXNoYTItbmlzdHAyNTZAb3BlbnNzaC5jb20AAAAIbmlzdHAyNTYAAABBBGDUAOIwllamFgyF63KadbKHRhIwqdp3xVXzASQG
c9nbI8HiRT4EtsYYh9Fq6so+rm0R6eAUSWeR644SF4u0QSAAAAAQc3NoOllvdXJUZXh0SGVyZQ== tester@tester2310 verify-required
```

Подключение Клиента к Серверу

Подключение для Клиента 1 (Ubuntu)

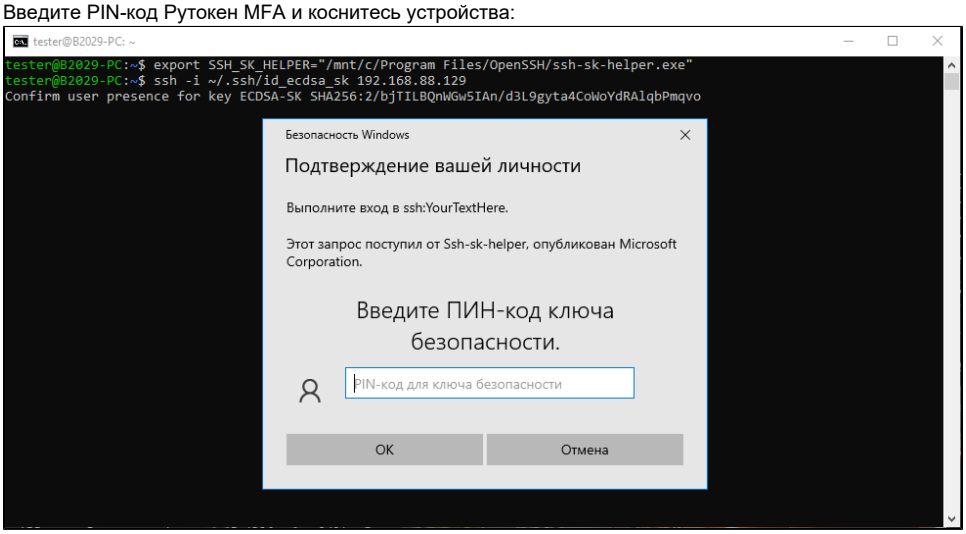
```
// PIN-  MFA     .
$ ssh -i ~/.ssh/id_ecdsa_sk 192.168.88.129
Confirm user presence for key ECDSA-SK SHA256:/vIIfHBajgeOHYoMjbzaE2eUoXU40jwSALfpuHjr9YA
Enter PIN for ECDSA-SK key /home/tester/.ssh/id_ecdsa_sk:
Confirm user presence for key ECDSA-SK SHA256:/vIIfHBajgeOHYoMjbzaE2eUoXU40jwSALfpuHjr9YA
User presence confirmed
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-94-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

   (ESM)  Applications .

0     .

15         ESM Apps.
    ESM Apps at https://ubuntu.com/esm

Last login: Wed Feb 14 14:16:10 2024 from 192.168.88.147
```

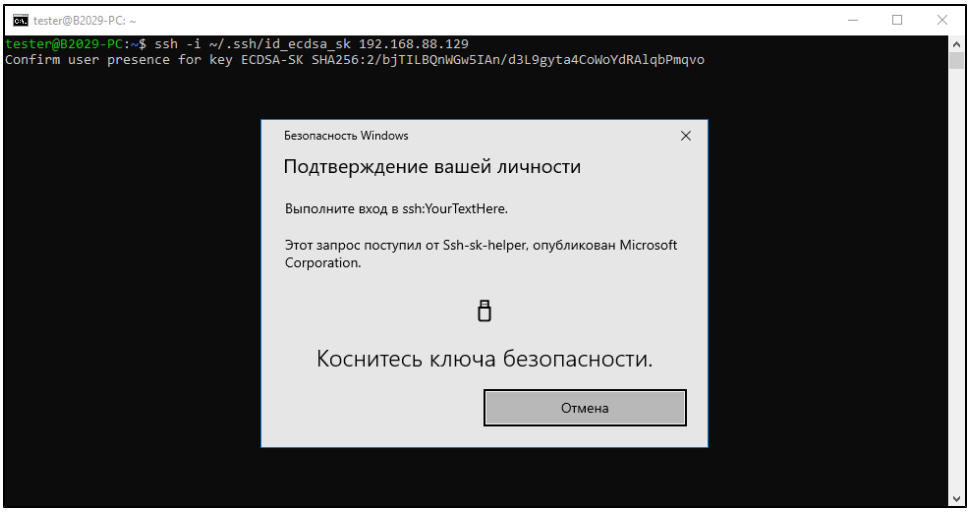
Подключение для Клиента 2 (Windows) с использованием WSL2

1. Запустите оболочку WSL2 и введите команду для подключения:

   ```
   wsl
   $ export SSH_SK_HELPER="/mnt/c/Program Files/OpenSSH/ssh-sk-helper.exe"
   $ ssh -i ~/.ssh/id_ecdsa_sk 192.168.88.129
   ```

2. Введите PIN-код Рутокен MFA и коснитесь устройства:





Подключение успешно установлено:

```
$ ssh -i ~/.ssh/id_ecdsa_sk 192.168.88.129
Confirm user presence for key ECDSA-SK SHA256:2/bjTILBQnWGw5IAn/d3L9gyta4CoWoYdRAlqbPmqvo
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-94-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

   (ESM)  Applications .

0     .

15         ESM Apps.
    ESM Apps at https://ubuntu.com/esm

Last login: Thu Feb 15 13:30:01 2024 from 192.168.88.1
```