Настройка OpenSSH доступа по Рутокен U2F

Параметры стенда

IP сервера 10.0.2.15

Имя удаленного пользователя user

Первичная настройка U2F

Удостовериться, в работоспособности U2F через демо-портал.

Если токен подключен к компьютеру, но светодиод не начинает мерцать и отсутствует реакция на нажатие кнопки, то надо согласно инструкции, записать в файл **/lib/udev/rules.d/70-u2f.rules** следующее:

/lib/udev/rules.d/70-u2f.rules

```
# Rutoken
KERNEL=="hidraw*", SUBSYSTEM=="hidraw", ATTRS{idVendor}=="0a89", ATTRS{idProduct}=="0090", TAG+="uaccess"
```

Перзапустите браузер, извлеките и вставьте токен заново. И еще раз проверьте работоспособность через демо-портал. Если аутентификация опять не прошла, то попробуйте перезапустить систему

Установка OpenSSH

Нам необходим OpenSSH версии 8.2 и выше, причем как на сервере так и на клиенте. Для начала попробуйте установить нужную версию OpenSSH из репозиториев. Это можно сделать с помощью команд:

```
# Debian
sudo apt-get update
sudo apt-get install openssh-client openssh-server

# Red Hat
sudo yum update
sudo yum install openssh-clients openssh-server
```

Далее узнаем, какая версия установлена с помощью команды:

```
sshd -V
```

Если версия ниже 8.2, то тогда приступим к ssh из исходников

Сборка из исходников

Для начала установим зависимые пакеты

```
# Debian
sudo apt-add-repository ppa:yubico/stable
sudo apt update
sudo apt install zlib1g-dev libfido2-dev libpam0g-dev libselinux1-dev libcbor-dev openssl libssl-dev autoconf
gcc make pkg-config libsystemd-dev

# Red Hat
sudo yum install autoconf gcc make pkg-config openssl-devel zlib-devel libselinux-devel libcbor-devel pam-devel
systemd-devel
```

Для пользователей Red Hat также необходимо поставить установить пакет libfido2, который можно взять тут.

Скачаем последнюю версию OpenSSH из репозитория

```
git clone https://github.com/openssh/openssh-portable
cd openssh-portable
git checkout V_8_2_P1
```

Для необходимо применить патч, который решает проблему с запуском ssh через systemctl

```
git apply systemd-readiness.patch
```

Теперь приступим непосредственно к сборке. Выполним команды

```
autoreconf -i
./configure --prefix=/usr --with-md5-passwords --with-pam --with-selinux --with-systemd --with-privsep-path=/var
/lib/sshd/ --sysconfdir=/etc/ssh --with-security-key-builtin
make -j4
sudo rm -rf /etc/ssh/* #
sudo make install
```

Сборка прошла успешно. Проверим, что ssh теперь имеет нужную версию:

```
sshd -V
```

На сервере

После того как сборка прошла успешно, в первую очередь выставим аутентификацию с использованием публичных ключей. Для этого в файле **/etc/ssh/sshd_config** раскомментируем строку

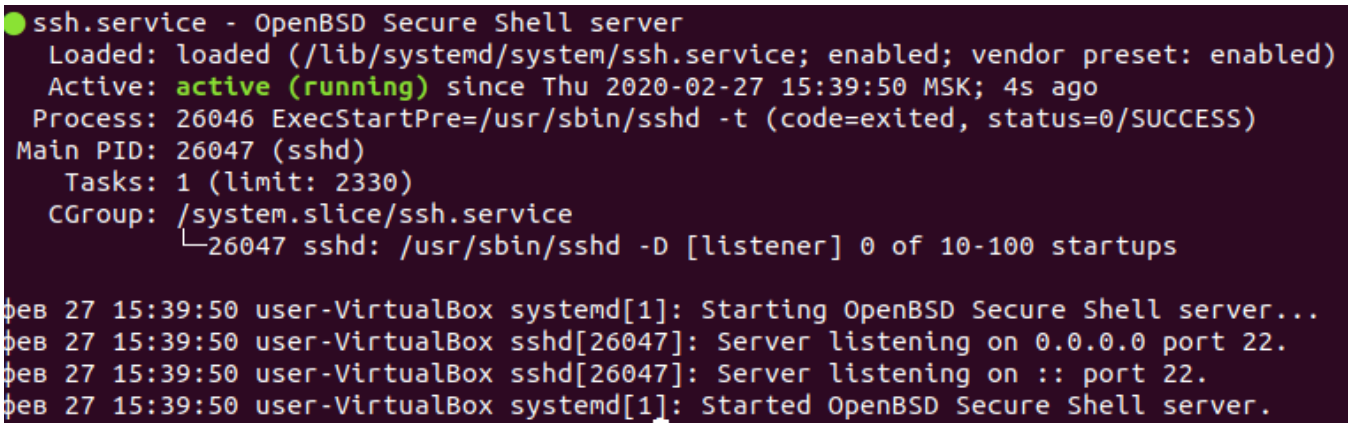
/etc/ssh/sshd_config

```
PubkeyAuthentication yes
```

Перезапускаем демона ssh и убедимся, что он запустился без ошибок

```
sudo systemctl restart sshd
sudo systemctl status sshd
```

Вывод должен быть примерно следующим:



В Red Hat возможна проблема связанная с неизвестной опцией *GSSAPIKexAlgorithms* передаваемой в качетсве аргумента sshd. Для того чтобы это исправить, нужно в файле **/etc/crypto-policies/back-ends/opensshserver.config** удалить данный аргумент и его параметры. Также в этом же файле нужно в опции PubkeyAcceptedKeyTypes нужно дописать sk-ecdsa-sha2-nistp256@openssh.com,sk-ssh-ed25519@openssh.com для прддержки аутентификации через U2F.

На клиенте

Создадим ключ на клиенте, требующий аутентификацию через U2F:

```
ssh-keygen -t ecdsa-sk
```

В процессе выполнения данной команды, токен был потребовать нажатие пользователя. Данный ключ запишется в файл внутри ФС, указанный вами, по умолчанию это $HOME/.ssh/id_rsa.pub Сгенерированный ключ копируем в файл ~/.ssh/authorized_keys лежащий на сервере

Попробуем осуществить аутентификацию (во время выполнения данной команды, должно быть взаимодействие с U2F):

```
~/.ssh$ ssh user@10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ECDSA key fingerprint is SHA256:pQ4vwrTm8OwwI7uhzfbbmrvHTM5d1bvMI0j49Xr6McQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.15' (ECDSA) to the list of known hosts.
Last login: Thu Feb 27 00:08:43 2020 from 127.0.0.1
```

Как видно аутентификация прошла успешно