Локальная аутентификация по Рутокен MFA в РЕД ОС

Установка необходимых пакетов

Для работы нам понадобиться 3 пакета:

- pam-u2f модуль PAM с поддержкой технологий аутентификации U2F и FIDO2.
- pamu2fcfg пакет создает конфигурацию для модуля pam-u2f и осуществляет процедуру регистрации аутентификатора U2F/FIDO2.
- fido2-tools пакет для управления аутентификатором U2F/FIDO2 (например, сброс токена или назначения PIN-кода).

Для установки этих пакетов необходимо открыть терминал и выполнить команду:

```
$ sudo dnf install fido2-tools pam-u2f pamu2fcfg -y
```

В РЕД ОС Рутокен МFA можно использовать в двух сценариях аутентификации:

- Как второй фактор после ввода логина и пароля в виде прикосновения к токену.
- Как замена ввода пароля на ввод PIN-кода Рутокен MFA и прикосновение к токену.

Установка нового PIN-кода для Рутокен MFA

- 1. Запустить терминал.
- 2. Подключить Рутокен МFA.
- 3. Вывести список подключенных устройств. Для этого выполнить команду:

```
$ fido2-token -L
```

Вывод команды должен быть следующим:

```
/dev/hidrawl: vendor=0x0a89, product=0x0093 (Aktiv Co. FIDO)
```

Нам понадобится строка /dev/hidraw1

4. Выполним команду установки нового PIN-кода:

```
$ fido2-token -S /dev/hidrawl
```

5. Дважды введем новый PIN-код:

```
Enter new PIN for /dev/hidrawl:
Enter the same PIN again:
```

Рутокен MFA готов к работе.

Настройка второго фактора

- 1. Запустить терминал.
- 2. Выполнить команду:

```
$ mkdir -p /tmp/aktivco
```

- 3. Подключить Рутокен МFA
- 4. Выполнить команду:

```
$ pamu2fcfg > /tmp/aktivco/u2f_keys
```

В процессе выполнения команды необходимо будет прикоснуться к устройству Рутокен МFA.

5. Выполнить команду:

```
$ sudo mkdir -p /etc/aktivco
```

6. Выполнить команду:

```
$ sudo mv /tmp/aktivco/u2f_keys /etc/aktivco/u2f_keys
```

7. Выполнить команду:

```
$ sudo nano /etc/pam.d/system-auth
```

8. Добавить строку:

```
auth sufficient pam_u2f.so authfile=/etc/aktivco/u2f_keys
```

- 9. Сохранить файл /etc/pam.d/system-auth
- 10. Выполнить команду:

```
$ sudo nano /etc/pam.d/password-auth
```

11. Добавить строку:

```
auth sufficient pam_u2f.so authfile=/etc/aktivco/u2f_keys
```

- 12. Сохранить файл /etc/pam.d/password-auth
- 13. Проверить что запрашивается касание в момент входа пользователя, выполнив команду:

```
$ su user
```

Настройка связки PIN-код+касание:

- 1. Запустить терминал.
- 2. Выполнить команду:

```
$ pamu2fcfg -u <username> > /tmp/u2f_mappings
# <username>
```

В процессе выполнения команды необходимо будет прикоснуться к устройству Рутокен МFA.

3. В результате должен появиться файл со следующим содержимым:

```
$ cat /tmp/u2f_mappings
user:hOzdi1ekgoVWLEzQH20uWJmoA3Dwno53zd2WCvlApHwfMVp/zz3+awUbeCL0E3pe,jzL+t6w7vhBgR2wwO+61
/g8aliGNbDUpYZj6mxLXain4F1bQB0rvnwzP3n+n/GIXUp50iui0Du7/aKP/pE27PQ==,es256,+presence
```

4. Выполнить команду:

```
$ sudo mv /tmp/u2f_mappings /etc/u2f_mappings
```

5. Выполнить команду:

\$ sudo nano /etc/pam.d/system-auth

6. Добавить строку:

auth sufficient pam_u2f.so authfile=/etc/u2f_mappings cue pinverification=1

- 7. Сохранить файл /etc/pam.d/system-auth
- 8. Выполнить команду:

\$ sudo nano /etc/pam.d/password-auth

9. Добавить строку:

 $\verb| auth sufficient pam_u2f.so authfile=/etc/u2f_mappings cue pinverification=1| \\$

- 10. Сохранить файл /etc/pam.d/password-auth
- 11. Проверить что запрашивается РІN-код Рутокен МFA при входе пользователя, выполнив команду:

\$ su user
Please enter the PIN:
Please touch the device.

12. Проверить графический вход в систему. Вводим пин-код и прикасаемся к токену:

