Локальная аутентификация с использованием Рутокен MFA

Введение

Рутокен MFA - это средство двухфакторной аутентификации, которое обеспечивает высокий уровень безопасности при доступе к системе. Использование Рутокен MFA позволяет защитить учетные записи пользователей от несанкционированного доступа, комбинируя два фактора: физический токен и пароль. В данной документации рассмотрены методы установки, настройки и использования Рутокен MFA для локальной аутентификации в НАЙС ОС, а также примеры использования и рекомендации по обеспечению безопасности.

Установка необходимых компонентов

Для использования Рутокен MFA в НАЙС ОС необходимо установить соответствующие драйверы и программное обеспечение. Используйте пакетный менеджер `tdnf` или `dnf` для установки необходимых пакетов:

```
$ sudo tdnf install pam_pkcs11
$ sudo tdnf install pcsc-lite
$ sudo tdnf install opensc
```

Настройка Рутокен MFA

После установки необходимых пакетов необходимо настроить систему для использования Рутокен MFA в процессе аутентификации.

Настройка PCSC-Lite

Для работы с Рутокен MFA необходимо настроить PCSC-Lite, который предоставляет интерфейс для работы с токенами. Запустите и настройте службу PCSC-Lite:

```
$ sudo systemctl start pcscd
$ sudo systemctl enable pcscd
```

Настройка OpenSC

OpenSC предоставляет поддержку для различных смарт-карт, включая Рутокен. Настройте OpenSC для работы с Рутокен:

```
$ sudo nano /etc/opensc/opensc.conf
```

Убедитесь, что в конфигурационном файле `opensc.conf` присутствует следующий раздел:

```
app default {
    framework pkcs15
    card_driver rutoken
}
```

Настройка PAM для использования Рутокен MFA

Для настройки PAM (Pluggable Authentication Modules) на использование Рутокен MFA необходимо отредактировать конфигурационные файлы PAM.

Настройка PAM для SSH

Откройте файл `/etc/pam.d/sshd` и добавьте следующие строки:

```
auth required pam_pkcs11.so
auth required pam_unix.so try_first_pass
```

Настройка PAM для локального входа

Откройте файл `/etc/pam.d/login` и добавьте следующие строки:

```
auth required pam_pkcs11.so
auth required pam_unix.so try_first_pass
```

Настройка конфигурации PAM_PKCS11

Откройте файл `/etc/pam_pkcs11/pam_pkcs11.conf` и добавьте или измените следующие строки:

```
use_pkcs11_module = opensc;

pkcs11_module opensc {
    module = /usr/lib64/opensc-pkcs11.so;
    description = "OpenSC PKCS#11 Module";
    slot_num = 0;
}
```

Привязка Рутокен MFA к учетной записи пользователя

Для привязки Рутокен MFA к учетной записи пользователя необходимо создать сертификат и импортировать его на токен.

Создание сертификата пользователя

Создайте сертификат для пользователя, используя OpenSSL:

```
$ openssl req -newkey rsa:2048 -nodes -keyout user.key -x509 -days 365 -out
user.crt
```

Эта команда создаст новый ключ и самоподписанный сертификат для пользователя.

Импорт сертификата на Рутокен

Для импорта сертификата на Рутокен используйте утилиту `pkcs11-tool` из пакета OpenSC:

```
$ pkcs11-tool --module /usr/lib64/opensc-pkcs11.so -l --write-object user.crt --
type cert --id 1 --label "User Certificate"
```

Команда запросит PIN-код токена и импортирует сертификат на устройство.

Проверка аутентификации с использованием Рутокен MFA

После настройки системы и привязки Рутокен к учетной записи пользователя можно проверить работу аутентификации.

Проверка локального входа

Попробуйте выполнить локальный вход в систему с использованием Рутокен MFA. При этом система должна запросить вставку токена и ввод пароля.

Проверка входа по SSH

Попробуйте выполнить вход по SSH в систему с использованием Рутокен MFA. При этом система также должна запросить вставку токена и ввод пароля.

Обеспечение безопасности при использовании Рутокен MFA

Для обеспечения безопасности при использовании Рутокен MFA следует учитывать следующие рекомендации:

Использование надежных PIN-кодов

Убедитесь, что пользователи используют надежные PIN-коды для своих токенов. Это поможет предотвратить их компрометацию.

Регулярное обновление программного обеспечения

Обеспечьте регулярное обновление драйверов и программного обеспечения для Рутокен MFA для защиты от известных уязвимостей:

```
$ sudo tdnf update pam_pkcs11 pcsc-lite opensc
```

Ограничение доступа к конфигурационным файлам

Ограничьте доступ к конфигурационным файлам системы аутентификации, установив соответствующие права доступа:

```
$ sudo chmod 600 /etc/pam.d/sshd
$ sudo chmod 600 /etc/pam.d/login
$ sudo chmod 600 /etc/pam_pkcs11/pam_pkcs11.conf
```

Регулярный мониторинг и аудит

Регулярно проверяйте логи системы и проводите аудит использования токенов для выявления подозрительной активности.

Использование резервных токенов

Рекомендуйте пользователям использовать резервные токены на случай утери или повреждения основного токена. Это поможет избежать сбоев в доступе к системе.

Обучение пользователей

Обучайте пользователей правильному использованию Рутокен MFA и мерам безопасности, таким как защита PIN-кода и физическая безопасность токена.

Практические примеры использования Рутокен MFA

Рассмотрим несколько практических примеров настройки и использования Рутокен MFA для локальной аутентификации в НАЙС ОС.

Пример 1: Настройка локальной аутентификации с использованием Рутокен MFA

Установка необходимых компонентов

```
$ sudo tdnf install pam_pkcs11
$ sudo tdnf install pcsc-lite
$ sudo tdnf install opensc
```

Настройка PCSC-Lite

```
$ sudo systemctl start pcscd
$ sudo systemctl enable pcscd
```

Настройка PAM для локального входа

Откройте файл `/etc/pam.d/login` и добавьте следующие строки:

```
auth required pam_pkcs11.so
auth required pam_unix.so try_first_pass
```

Привязка Рутокен к учетной записи

```
$ openssl req -newkey rsa:2048 -nodes -keyout user.key -x509 -days 365 -out
user.crt
$ pkcs11-tool --module /usr/lib64/opensc-pkcs11.so -l --write-object user.crt --
```

```
type cert --id 1 --label "User Certificate"
```

Пример 2: Настройка аутентификации по SSH с использованием Рутокен MFA

Установка необходимых компонентов

```
$ sudo tdnf install pam_pkcs11
$ sudo tdnf install pcsc-lite
$ sudo tdnf install opensc
```

Настройка PCSC-Lite

```
$ sudo systemctl start pcscd
$ sudo systemctl enable pcscd
```

Настройка PAM для SSH

Откройте файл `/etc/pam.d/sshd` и добавьте следующие строки:

```
auth required pam_pkcs11.so
auth required pam_unix.so try_first_pass
```

Привязка Рутокен к учетной записи

```
$ openssl req -newkey rsa:2048 -nodes -keyout user.key -x509 -days 365 -out
user.crt
$ pkcs11-tool --module /usr/lib64/opensc-pkcs11.so -l --write-object user.crt --
type cert --id 1 --label "User Certificate"
```

Пример 3: Регулярное обновление программного обеспечения

Обновление драйверов и программного обеспечения

```
$ sudo tdnf update pam_pkcs11 pcsc-lite opensc
```

Пример 4: Ограничение доступа к конфигурационным файлам

Установка прав доступа

```
$ sudo chmod 600 /etc/pam.d/sshd
$ sudo chmod 600 /etc/pam.d/login
$ sudo chmod 600 /etc/pam_pkcs11/pam_pkcs11.conf
```

Заключение

Рутокен MFA предоставляет мощные средства для обеспечения двухфакторной аутентификации, что значительно повышает уровень безопасности при доступе к системе. Использование Рутокен MFA в НАЙС ОС позволяет защитить учетные записи пользователей от несанкционированного доступа, комбинируя два фактора: физический токен и пароль.

Следуя приведенным рекомендациям и примерам, вы сможете эффективно настроить и использовать Рутокен MFA для локальной аутентификации в НАЙС ОС. Регулярный мониторинг, аудит и обновление программного обеспечения помогут поддерживать высокий уровень безопасности и надежности вашей системы.

Использование средств двухфакторной аутентификации требует осознания потребностей и рисков, связанных с защитой информации. Обеспечьте соблюдение разработанных политик и обучайте пользователей правильному использованию Рутокен MFA. Следуя этим принципам, вы сможете создать надежную и безопасную систему, способную эффективно защищать важные данные и предотвращать несанкционированный доступ.