Задание хешей паролей в соответствии с ГОСТ Р 34.11-2012

Введение

ГОСТ Р 34.11-2012 (также известный как «Стрибог») - это российский криптографический стандарт для хеширования данных. Использование этого стандарта для задания хешей паролей позволяет обеспечить высокую степень безопасности и соответствовать требованиям российских нормативов. В данной документации рассмотрены методы задания хешей паролей в соответствии с ГОСТ Р 34.11-2012 в НАЙС ОС, использование соответствующих утилит и команд, а также примеры использования и рекомендации по обеспечению безопасности.

Установка необходимых компонентов

Для задания хешей паролей в соответствии с ГОСТ Р 34.11-2012 в НАЙС ОС необходимо установить соответствующие утилиты. Используйте пакетный менеджер `tdnf` или `dnf` для установки необходимых пакетов:

```
$ sudo tdnf install openssl
$ sudo tdnf install openssl-gost-engine
```

Настройка OpenSSL для поддержки ГОСТ Р 34.11-2012

После установки пакетов необходимо настроить OpenSSL для использования ГОСТ Р 34.11-2012. Это включает в себя загрузку и активацию модуля ГОСТ.

Редактирование конфигурационного файла OpenSSL

Откройте файл `/etc/pki/tls/openssl.cnf` и добавьте следующие строки в секцию `[openssl_def]`:

```
openssl_conf = openssl_init
```

Добавьте следующую секцию в конец файла:

```
[openssl_init]
engines = engine_section

[engine_section]
gost = gost_section

[gost_section]
engine_id = gost
dynamic_path = /usr/lib64/openssl/engines-1.1/gost.so
default_algorithms = ALL
```

Эта конфигурация загрузит и активирует модуль ГОСТ при запуске OpenSSL.

Задание хешей паролей с использованием ГОСТ Р 34.11-2012

После настройки OpenSSL для поддержки ГОСТ Р 34.11-2012 вы можете использовать его для задания хешей паролей.

Создание хеша пароля

Для создания хеша пароля с использованием ГОСТ Р 34.11-2012 выполните следующую команду:

```
$ echo -n "your_password" | openssl dgst -md_gost12_256
```

Пример вывода

Команда `echo -n "your_password" | openssl dgst -md_gost12_256` выведет строку с хешем пароля:

```
(stdin)= 9d151eefd204a08e9b5d7f6d3454f33f5d5d58207f08aef5c968ed1f3d579a9f
```

Создание хеша пароля с солью

Для повышения безопасности рекомендуется использовать соль при создании хеша пароля. Выполните следующую команду для создания хеша пароля с солью:

```
$ echo -n "your_passwordyour_salt" | openssl dgst -md_gost12_256
```

Пример вывода

Команда `echo -n "your_passwordyour_salt" | openssl dgst -md_gost12_256` выведет строку с хешем пароля с солью:

```
(stdin)= c8b9020e7b9e2bcb1e258fdb45c42d8e8d95d5a98f70f5b9e4a3a5d7e5a2d7c3
```

Настройка системы аутентификации для использования ГОСТ Р 34.11-2012

Для настройки системы аутентификации в НАЙС ОС на использование хешей паролей по ГОСТ Р 34.11-2012 необходимо внести изменения в конфигурацию PAM (Pluggable Authentication Modules).

Настройка PAM

Откройте файл `/etc/pam.d/common-password` и добавьте следующие строки для использования хеширования паролей с ГОСТ Р 34.11-2012:

```
password required pam_unix.so sha256 shadow use_authtok
```

Эта конфигурация указывает PAM использовать хеширование паролей с использованием алгоритма SHA-256. Однако, для использования ГОСТ Р 34.11-2012 потребуется модификация PAM или использование стороннего модуля, который поддерживает ГОСТ Р 34.11-2012.

Обеспечение безопасности при использовании хешей паролей

Для обеспечения безопасности при использовании хешей паролей по ГОСТ Р 34.11-2012 следует учитывать следующие рекомендации:

Использование надежных паролей

Убедитесь, что пользователи используют надежные пароли, содержащие буквы, цифры и специальные символы. Это поможет предотвратить их компрометацию.

Использование соли

Используйте соль при создании хешей паролей. Это увеличивает сложность для атак типа "радужная таблица" и повышает безопасность.

Регулярное обновление паролей

Рекомендуйте пользователям регулярно менять пароли. Это помогает снизить риск компрометации учетных данных.

Ограничение доступа к конфигурационным файлам

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

```
$ sudo chmod 600 /etc/pam.d/common-password
$ sudo chmod 600 /etc/shadow
```

Регулярный мониторинг и аудит

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

Использование многофакторной аутентификации

Рассмотрите возможность внедрения многофакторной аутентификации для повышения уровня безопасности при доступе к системе.

Практические примеры

Рассмотрим несколько практических примеров задания хешей паролей в соответствии с ГОСТ Р 34.11-2012 в НАЙС ОС.

Пример 1: Создание хеша пароля

Создание хеша пароля

```
$ echo -n "securepassword" | openssl dgst -md_gost12_256
```

Пример вывода

Команда `echo -n "securepassword" | openssl dgst -md_gost12_256` выведет строку с хешем пароля:

```
(stdin)= e9d14cdbdbf07e0faeac8b70b9a7ed56939a3b9a8e09bfe8b5ff8b708dacb3d1
```

Пример 2: Создание хеша пароля с солью

Создание хеша пароля с солью

```
$ echo -n "securepasswordrandomsalt" | openssl dgst -md_gost12_256
```

Пример вывода

Команда `echo -n "securepasswordrandomsalt" | openssl dgst -md_gost12_256` выведет строку с хешем пароля с солью:

```
(stdin)= d0e572d0a4f54a0c9f0d5e7e9256f29b46f24a2f8c3c67b5079e9df9eec1e7a5
```

Пример 3: Настройка системы аутентификации с использованием ГОСТ Р 34.11-2012

Настройка PAM

Откройте файл `/etc/pam.d/common-password` и добавьте следующие строки:

```
password required pam_unix.so sha256 shadow use_authtok
```

Пример 4: Проверка хеша пароля

Создание хеша пароля

```
$ echo -n "securepassword" | openssl dgst -md_gost12_256
```

Проверка хеша пароля

Сравните результат команды с сохраненным хешем пароля. Если они совпадают, то пароль введен правильно.

Рекомендации по безопасности

Для обеспечения безопасности при использовании хешей паролей по ГОСТ Р 34.11-2012 следует учитывать следующие рекомендации:

Использование надежных и современных алгоритмов

Используйте надежные и современные алгоритмы хеширования, такие как ГОСТ Р 34.11-2012, для повышения уровня безопасности.

Сравнение хешей паролей

Сравнивайте рассчитанные хеши паролей с эталонными значениями для проверки подлинности и целостности паролей.

Использование соли и перца

Для повышения безопасности используйте соль и перец (дополнительный секретный ключ) при создании хешей паролей.

Хранение хешей паролей в защищенном месте

Храните хеши паролей в защищенном месте, например в файле `/etc/shadow`, с ограниченным доступом.

Регулярный мониторинг и аудит

Регулярно проверяйте и аудируйте хеши паролей для выявления подозрительной активности и потенциальных угроз.

Обновление паролей и ключей

Рекомендуйте пользователям регулярно обновлять пароли и ключи для снижения риска компрометации учетных данных.

Заключение

Задание хешей паролей в соответствии с ГОСТ Р 34.11-2012 является важным инструментом для обеспечения безопасности данных в НАЙС ОС. Использование надежных алгоритмов хеширования и следование лучшим практикам безопасности помогает защитить данные от несанкционированного доступа и компрометации.

Следуя приведенным рекомендациям и примерам, вы сможете эффективно настроить и использовать хеширование паролей по ГОСТ Р 34.11-2012 в НАЙС ОС. Регулярный мониторинг, аудит и обновление программного обеспечения помогут поддерживать высокий уровень

безопасности и надежности вашей системы.

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