

Настройка парольной политики в популярных ОС

17.08.2009

Продолжая тему, начатую в предыдущей статье [“Настройка парольной политики в СУБД Oracle”](#), опубликованной 21 июля этого года, стоит обратить внимание на выполнение стандарта PCIDSS в области парольной политики для пользователей операционных систем. В данной статье будут рассмотрены операционные системы, которые чаще всего встречаются в области применения стандарта PCIDSS при проведении аудита на соответствие.

Алексей Трошичев, аудитор информационной безопасности компании Digital Security

При выполнении мероприятий по приведению информационной инфраструктуры организации в соответствие требованиям стандарта PCI DSS следует обращать внимание не только на настройки парольных политик приложений, но и на настройки политик используемых операционных систем.

В первую очередь, имеет смысл перечислить требования стандарта, касающиеся парольной политики.

Согласно стандарту PCI DSS 1.2, парольная политика должна соответствовать следующим требованиям:

1. Срок действия пароля – не более 90 дней (требование 8.5.9).
2. Длина пароля – не менее 7 символов (требование 8.5.10).
3. Пароль должен содержать как цифровые, так и буквенные символы (требование 8.5.11).
4. Каждый обновлённый пароль должен отличаться от 4-х предыдущих (требование 8.5.12).
5. Учётная запись временно блокируется (30 минут) после 6 неудачных попыток логина (требование 8.5.13).
6. Рабочая сессия пользователя блокируется не более чем через 15 минут простоя (требование 8.5.14).

После того, как мы определились с требованиями, перейдём к конкретным рекомендациям для популярных ОС.

Установка Парольной Политики в ОС LINUX

В OS Linux требования к паролю задаются в файле `/etc/login.defs`.

- Для выполнения требования **1** в файле `/etc/login.defs` установите значение для переменной `PASS_MAX_DAYS`, равное 90. Затем установите 0 для `PASS_MIN_DAYS`.
- Для выполнения требований **2 и 3** в файле `/etc/pam.d/common-password` добавьте строчку `password required pam_cracklib.so dcredit=-1 lcredit=-1 minlen=7`

Таким образом, мы устанавливаем требования, по которым пароль должен содержать минимум 7 символов, в которых минимум 1 цифра, и минимум 1 буква.

Следует добавить, что не лишним будет включить требование содержания в пароле минимум одной заглавной буквы, а также увеличить количество символов до 8:

```
password required pam_cracklib.so dcredit=-1 lcredit=-1 lcredit ==-1  
minlen=8
```

- Для выполнения требования 4 в файле `/etc/pam.d/common-password` в строку `password required pam_unix.so md5` добавьте параметр

```
remember=4
```

Выполните следующие команды для обновления параметров (необходимо выполнять с правами администратора):

```
touch /etc/security/opasswd
```

```
chown root:root /etc/security/opasswd
```

```
chmod 600 /etc/security/opasswd
```

- Для выполнения требования 5 в файле `/etc/login.defs` установите значение для переменных `LOGIN_RETRIES` и `LOGIN_TIMEOUT` 6 и 1800 соответственно .
- Для выполнения требования 6 в файле `/etc/ssh/sshd_config` установите значение для переменной `ClientAliveInterval`, равное 900.

Установка Парольной Политики в ОС HP-UX

В HP-UX управление паролями сильно упрощено, так как происходит через один конфигурационный файл, находящийся по умолчанию в `/etc/default/security`. Все следующие параметры устанавливаются в этом файле.

- Для выполнения требования 1 установите

```
PASSWORD_MAXDAYS=90  
PASSWORD_MINDAYS=0
```

- Для выполнения требования 2 установите

```
MIN_PASSWORD_LENGTH=7 (рекомендуем 8)
```

- Для выполнения требования 3 установите

```
PASSWORD_MIN_LOWER_CASE_CHARS=1  
PASSWORD_MIN_DIGIT_CHARS=1
```

Дополнительно рекомендуется установить `PASSWORD_MIN_UPPER_CASE_CHARS=1`

- Для выполнения требования 4 установите

```
PASSWORD_HISTORY_DEPTH=4
```

- Для выполнения требования 5 установите

```
AUTH_MAXTRIES=6
```

Разблокировка логина происходит вручную администраторами (root) с помощью команды

```
userdbset -d -u [имя пользователя] auth_failures
```

- Для выполнения требования 6 в файле `/etc/ssh/sshd_config` установите значение для переменной `ClientAliveInterval`, равное 900.

Установка Парольной Политики в Solaris

В Solaris управление паролями производится схожим с LINUX способом, хотя имеет некоторые особенности. Конфигурационный файл находится по умолчанию в `/etc/default/passwd`.

- Для выполнения требования 1 в файле `/etc/default/passwd` установите значение

```
MAXWEEKS=12
```

(Особенность Solaris заключается в том, что за единицу времени используется неделя)

- Для выполнения требования 2 в файле `/etc/default/passwd` установите значение

```
PASSLENGTH=7 (рекомендуем 8)
```

- Для выполнения требования 3 необходимо установить модуль `pam_cracklib`, который не входит в стандартную поставку Solaris. Далее необходимо в файле `etc/pam.d/common-password` добавить строку

```
password required pam_cracklib.so dcredit=-1 lcredit=-1 minlen=7
```

Таким образом мы устанавливаем требования, по которым пароль должен содержать минимум 7 символов, в которых минимум 1 цифра, и минимум 1 буква.

- Не лишним будет добавить требование содержания в пароле минимум одной заглавной буквы, а также увеличить количество символов до 8.

```
password required pam_cracklib.so dcredit=-1 lcredit=-1 lcredit =-1 minlen=8
```

- Для выполнения требования 4 необходимо добавить строку в файл `/etc/pam.conf`

```
other password requisite pam_history.so.1 history=4
```

Таким образом мы устанавливаем требование запрета использования 4х предыдущих паролей.

- Для выполнения требования 5 необходимо добавить следующие строки в файл `/etc/pam.conf` :

```
login    auth required    pam_dial_auth.so.1
login    auth sufficient    pam_unix_auth.so.1
login    auth required    pam_login_limit.so.1 count_limit=6
timeout_account=1800
```

- Для выполнения требования 6 в файле `/etc/ssh/sshd_config` установите значение для переменной `ClientAliveInterval` равное 900.

Установка Парольной Политики в Windows

В Windows 2003 Server все необходимые настройки осуществляются средствами пакета Administrative Tools (Start>Programs>Administrative Tools>Domain Security Policy>Password Policy). Ниже описана парольная политика для пользователей домена (настройки производятся на доменном контроллере).

- Для выполнения требования 1 параметр **Maximum password age** установите в значение 90.
- Для выполнения требования 2 параметр **Minimum password length** установите в значение 7.
- Для выполнения требования 3 параметр **Password meet complexity** установите в значение `enabled`.
- Для выполнения требования 4 параметр **Enforce password history** установите в значение 4.
- Для выполнения требования 5:
 1. Блокировка учетной записи после шести неудачных попыток ввода пароля производится в разделе Account Lockout Policy путем установки параметра Account lockout threshold в значение 6.
 2. Блокирование учетной записи пользователя не менее чем на 30 минут либо пока администратор не снимет блокировку осуществляется в разделе Account Lockout Policy при установке параметра Account lockout duration в значение 30.
- Для выполнения требования 6 блокирование рабочей сессии пользователя не более чем через 15 минут простоя настраивается в групповых политиках (User configuration > Administrative Templates > Control Panel > Display), параметры:

```
Screen Saver
Screen Saver executable name
Password protect the screen saver
Screen Saver timeout
```

Об авторе

Алексей Трошичев - аудитор информационной безопасности компании Digital Security. Специализируется на проведении аудитов защищенности, тестов на проникновение, анализе защищённости бизнес приложений и исследовательской деятельности в области информационной безопасности. Является сотрудником исследовательского центра Digital Security Research Group [DSecRG], занимающегося поиском и анализом уязвимостей приложений и операционных систем.

О стандарте PCI DSS

Стандарт PCI DSS (Payment Card Industry Data Security Standard) предназначен для обеспечения безопасности обработки, хранения и передачи данных о держателях платежных карт в информационных системах компаний, работающих с международными платежными системами Visa, MasterCard и другими. Стандарт разработан сообществом PCI Security Standards Council, в которое входят мировые лидеры на рынке платежных карт, такие как American Express, Discover Financial Services, JCB, MasterCard Worldwide и Visa International.

Под действие требований стандарта попадают банки, процессинговые центры, поставщики ИТ-услуг, торгово-сервисные предприятия, и иные организации, обрабатывающие транзакции по международным платежным картам. К части этих компаний международные платежные системы предъявляют требование о прохождении обязательного ежегодного аудита компанией, обладающей статусом QSA.

Текущая версия стандарта 1.2 выпущена 1 октября 2008 года.