Лабораторная работа 6

Укрепление безопасности с помощью шифрования

В этой работе Вы должны познакомиться с наиболее распространёнными и доступными средствами криптографической защиты.

Задание 1. Знакомство с хешированием

1. Скачайте файл `AppScan_Setup.exe` с ftp://10.0.12.224/. Посмотрите информацию об утилитах `md5sum`, `sha1sum` и `shasum`.
2. Чему равна хеш-сумма файла `AppScan_Setup.exe`, посчитанная по алгоритму MD5?
3. Чему равна хеш-сумма файла `AppScan_Setup.exe`, посчитанная по алгоритму SHA-1?
4. Чему равна хеш-сумма файла `AppScan_Setup.exe`, посчитанная по алгоритму SHA-256?
5. Чему равна хеш-сумма фразы (панграммы) «`Широкая электрификация южных губерний даст мощный толчок подъёму сельского хозяйства.`» (в кодировке UTF-8), посчитанная по алгоритму SHA-512?

   Насколько сильно изменится хеш-сумма, если вместо буквы ‘`ё`’ написать ‘`е`’?

Задание 2. Настройка авторизации средствами веб-сервера Apache

После установки «Apache» создаётся каталог `/var/www`. Корень сайта (по умолчанию) — каталог `html`, расположенный в нём.

1. В корне своего сайта создайте каталог `private`, а в нём создайте `index.html`. В файле `index.html` напишите, что этот ресурс принадлежит «синим»/«красным» (в зависимости от Вашей принадлежности к команде). Можете, для выразительности, использовать графическое оформление страницы.
2. В этом каталоге создайте файл `.htaccess`. Укажите в нём кодировку исходного текста индексного файла. Поэкспериментируйте с различными кодировками (при этом в браузере кодировка страниц должна быть выставлена в автоматическое определение).

   Если изменения не наблюдаются, проверьте главный файл настроек — `httpd.conf` в каталоге `/etc/httpd/conf` (все локальные изменения параметров «Apache» должны быть разрешены).
3. Защитите каталог `private`.
   - Создайте пароли для всех пользователей Вашей команды. Файл с паролями разместите в каталоге выше корневого на один уровень.
   - Для аутентификации используйте хеширование MD5.
   - Создайте две группы — *red* и *blue*. Организуйте доступ для себя, проверьте. Организуйте доступ для своей группы, проверьте.
4. Поместите в отчёт URL своего веб-ресурса, логин и пароль (любой допустимый) для входа на него.

Задание 3. Обмен информацией с GnuPG

Используя «GnuPG», создайте необходимые ключи и проверьте их в работе.

1. Проверьте, установлен ли у Вас «GnuPG». Для этого наберите в командной строке

   ```
   gpg2 -h
   ```

   Если «GnuPG» отсутствует в системе, то установите его. Можно установить графический интерфейс управления ключами — «Kgpg».

2. Попробуйте *симметричное шифрование* (на каком-нибудь файле с данными):

```
gpg2 -c файл
```

Должен появиться файл с таким же именем и с суффиксом `.gpg`. Теперь его смело можно переносить в другое место (хоть на край света). Расшифровать файл можно командой

```
gpg2 --decrypt-files файл.gpg
```

3. Сгенерируйте (с помощью мастера) пару ключей (секретный и публичный) для *асимметричного шифрования*:

```
gpg2 --gen-key
```

После заполнения данных с помощью мастера, следует задать фразу-пароль. В качестве фразы-пароля, можно указывать достаточно длинные значения, многословные.

На генерацию ключей требуется ощутимое время, в течение которого надо проявлять активность (см. инструкцию на экране). При успешной генерации Вы увидите имя ключа (в строке gpg: ключ . . . помечен как абсолютно доверенный).

4. Добавьте в отчёт протокол выполнения команд.

5. Экспортируйте созданный ключ в текстовый *файл* (желательно в имени указывать тип ключа).

```
gpg2 --output файл --armor --export ключ
```

Вместо идентификатора ключа можно использовать имя или email (которые указывали при генерации ключей) как полностью так и частично.

Просмотрите получившийся файл. Положите его на свой веб-сайт, а в индексном файле сделайте на него ссылку. Разошлите открытый ключ товарищам по команде.

6. Чтобы получить секретный ключ, следует набрать команду

```
gpg2 --output файл --armor --export-secret-key ключ
```

7. Импортируйте к себе ключи товарищей по команде, полученные по почте или с их сайтов.

```
gpg2 --import файл
gpg2 --allow-secret-key-import --import файл
```

Далее найдите ключ, который Вы импортировали:

```
gpg2 --list-keys
```

и наберите

```
gpg2 --edit-key ключ
```

Откроется клиент для редактирования ключа, куда можно вбивать разные команды. Напишите `trust` Enter, из списка выберите `5 = I trust ultimately`. Потом `quit` Enter. Теперь импортированным ключом можно пользоваться.

8. Напишите секретный текстовый файл и зашифруйте его для конкретного получателя.

```
gpg2 --recipient Получатель --encrypt файл
```

В результате файл будет зашифрован. Теперь никто, кроме получателя, не сможет его расшифровать, даже Вы сами. Попробуйте расшифровать. Чтобы расшифровать файл, необходимо использовать следующую команду:

```
gpg2 --decrypt-files файл
```

«GnuPG» спросит ещё Ваш секретный пароль, который Вы указали, когда создавали ключ.

9. Добавьте в отчёт содержимое своего ключа и импортированных открытых ключей (в формате ASCII).

Задание 4. Шифрование дисков

1. Создайте новый виртуальный диск размером 50 МБ с названием `cryptoDisk` и подключите к своей виртуальной машине.
2. Используя утилиту для работы с дисками (например, `drakdisk`), задайте для `cryptoDisk` файловую систему `ext4` с шифрованием, отформатируйте его и примонтируйте в `/mnt/cryptoDisk`.
3. Скопируйте на этот диск информацию повышенной секретности (любые файлы с указанием на цвет вашей команды).
4. Размонтируйте этот диск, выключите виртуальную машину, отсоедините диск. Обменяйтесь дисками с одногруппниками, присоедините диск, включите машину и примонтируйте диск `cryptoDisk`. Попробуйте прочитать с него данные.
5. Добавьте в отчёт скриншоты подключения и использования диска `cryptoDisk`.