Лабораторная работа № 3

Первые шаги к безопасной ОС

В этой работе требуется выполнить настройки в операционной системе, которые позволят повысить безопасность и производительность рабочей станции.

Задание 1. Управление службами

Используя графические инструменты или непосредственно редактируя файлы настроек, выполните следующие действия:

1. Просмотрите запущенные службы (если непонятно, что за служба, посмотрите информацию о ней).
2. Ненужные службы потребляют ресурсы и создают дополнительные уязвимости в системе безопасности. Отключите ненужные службы (по крайней мере очевидные), обратите внимание на `CUPS`.
3. Включите (если ещё не включен) «SSH-сервер».
4. Установите интерпретатор (для «Apache») «PHP», «phpMyAdmin», веб-сервер «Apache», СУБД «MariaDB». Запустите и проверьте установленные продукты.

   Службы в UNIX/Linux системах запускаются с правами `root`. Войдя под `root` для запуска службы (демона) `apache` нужно набрать в командной строке следующую команду:
   `service httpd start`

   Аналогично запускаются и другие службы (буква `d` в конце имени указывает на то, что это служба, «демон»).

   Проверить «Apache» можно в браузере, набрав адрес своей машины (на своей машине можно ввести `localhost` или `127.0.0.1`).
5. Установите «запуск служб при включении» для «Apache» (`httpd`) и «MariaDB» (`mysqld`) через GUI или `chkconfig` (текстовый интерфейс для `/etc/rc[0-6].d`).
6. Просмотрите запущенные службы с помощью утилиты `systemctl`, установленные службы с помощью `systemctl list-unit-files`. Запущена ли служба `ssh`? Если не запущена, то запустите.

   Запустить службу из консоли можно и через утилиту `systemctl` с командой `start` и названием службы, например: `systemctl start ssh`.

   Посмотрите открытые порты (`systemctl list-sockets`). Чтобы увидеть не только активные соединения, воспользуйтесь командой `systemctl list-sockets -all`.
7. Добавьте в отчёт список запущенных служб и список открытых портов (вместе с командами).

Задание 2. Изменение заданных по умолчанию настроек

Используя графические инструменты или непосредственно редактируя файлы настроек, выполните следующие действия:

1. Посмотрите в настройках список зарегистрированных пользователей. Посмотрите *информацию об учётной записи* пользователя (свой логин). Посмотрите *информацию о пароле* пользователя, включите срок действия пароля `365 дней`, предупреждать об изменении за `неделю`. Если есть пользователь «Гость» (guest), заблокируйте его учётную запись.

   Список активных пользователей можно вывести командой `who`.

   Посмотрите *свойства* своей *Домашней папки*. Измените *права* (`просмотр`, `изменение`, `доступ`) на эту папку, в соответствии с Вашими потребностями.
2. Все СУБД рекомендуется сначала проверять из консоли. Консоль для «MariaDB» называется `mysql` (так же, как и для СУБД «MySQL»). Запустите консоль «MariaDB» (из под root).

   Узнайте (в Интернете), какой логин и пароль администратора СУБД «MariaDB» и др. СУБД. Попробуйте зайти через графический интерфейс (`http://localhost/phpmyadmin`).

   Попробуйте зайти на чужой компьютер, как `user`, и запустить консоль `mysql`.

3. Посмотрите в Интернете пароли по умолчанию для «MySQL»/«MariaDB» и др. сервисов. Добавьте этот список в отчёт.

   Исправьте обнаруженный недостаток. Для «MariaDB» («MySQL») изменить пароль можно следующей командой:
   `mysqladmin -u пользователь password новый_пароль`

   После изменения пароля войти через консоль можно только с ключом `-p`:
   `mysql -p [-u пользователь]`

   Ещё раз проверьте работу веб-сервера и СУБД (через веб-интерфейс).

   Добавьте в отчёт содержимое окна консоли (терминала).

Задание 3. Защита ОС

1. Откройте «параметры входа в систему», посмотрите текущие настройки. Посмотрите, кому разрешено *выключать* и *перезагружать компьютер*.

   Запретите вход в систему и работу в обычном режиме для пользователя `root`.

   Не допускайте *автоматический вход* в систему и вход без пароля.

2. Включите *файервол*. Разрешите доступ только к тем службам, которые у Вас используются. Проверьте открытые порты (см. предыдущую работу). Проверьте доступность сервисов с хоста (из основной ОС) или с другой машины.

3. Выполните *настройку аутентификации* для системных утилит. Не допускайте к настройкам сети и системы никого, кроме `root`.

Задание 4. Резервное копирование

1. Создайте новый виртуальный диск размером 200 МБ с названием `backups` и подключите к своей виртуальной машине.

2. Используя утилиту для работы с дисками (например, `drakdisk`), задайте для `backups` файловую систему `ext4`, отформатируйте его и примонтируйте в `/mnt/.backups`.

3. Используя доступный инструмент, составьте «План резервного копирования»:

   - тип — версионное резервное копирование;
   - источники — папка `Документы`;
   - место хранения — диск `backups` (`/mnt/.backups`);
   - расписание — интервал 1 день;
   - дополнительно — проверка целостности.

4. Выполните резервное копирование. Посмотрите файл журнала, добавьте его содержимое в отчёт.