**110.2 Настройка безопасности системы**

Студент должен уметь настраивать систему на соответствие основным правилам безопасности.

**Изучаем**:

* устройство теневых паролей;
* отключение сетевых служб;
* суперсерверы;
* обработчики TCP.

Данный урок посвящен настройке сетевой безопасности в рамках LPI-1. При этом в нем не рассматриваются настройки межсетевого экрана, входа по сети и т.д., но разбираются вопросы запущенных сетевых служб и доступа к ним.

В первом видео повторно рассматриваются вопросы теневых паролей. Рассказывается о файле **/etc/nolgin** (его наличие не разрешает вход в систему никому кроме ***root***, после перезагрузки он удаляется автоматически).

Также рассматриваются вопросы управления сетевыми демонами. Современные RedHat и Debian используют систему инициализации ***systemd***, поэтому управление демонами осуществляется в них одинаковым способом.

Для управления демонами в директории **/etc/init.d/** находятся соответствующие файлы-скрипты. Возможно обращение к этим службам по скриптам, например:

***/etc/init.d/ssh stop*** *(остановить демон ssh);*

или при помощи стандартной команды **service**, например:

***service ssh status*** *(проверить статус демона ssh);*

или при помощи команды **systemctl**, например:

***systemctl start ssh*** *(запустить демон ssh).*

Вне зависимости от используемых команд, скрипты управления демонами обычно содержат следующие стандартные действия: *stop, start, restart, status, reload, disable, enable, is-enabled*.

Второе видео посвящено суперсерверам – процессам, управляющим всеми остальными процессами. В современных дистрибутивах инициализацией демонов занимается ***upstart*** или ***systemd***, однако суперсерверы все еще рассматриваются в качестве темы LPI. Суперсервер занимается прослушиванием сетевых портов, и в случае необходимости – запускает демоны, обслуживающие этот порт.

Классический суперсервер **inetd** настраивается при помощи файла конфигурации **/etc/inetd.conf**. В нем находятся правила, содержащие следующие элементы:

* ***service-name*** – имя демона (по нему определяется порт из /etc/services);
* ***socket-type*** – тип сокета ­(чаще всего stream или dgram – TCP и UDP соответственно);
* ***protocol*** – протоколы (TCP и UDP версий 4, 6, 4to6 b и т.д.);
* ***{wait|nowait}[/max-child[/max-connections-per-ip-per-minute]]*** – wait для UDP, создает много сокетов для демона, nowait для TCP – каждому сокету отдельный экземпляр деонма, максимальное число демонов и максимальное число соединений;
* ***user***[:group][/login-class] – от чьего имени запускать демон;
* ***server***-***program*** – путь к демону;
* ***server-program-arguments*** – аргументы запуска демона.

Кроме того, отдельные правила для отдельных демонов могут располагаться в директории **/etc/inetd.d**

Современной безопасной реализацией суперсервера является **xinetd**. Файл его конфигурации **/etc/xinetd.conf** также содержит набор правил, синтаксис которых сложнее классического inetd.

Также как и в inetd для xinetd существует отдельная директория для дополнительных правил **/etc/xinetd.d**

Дополнительно безопасность сетевых портов можно контролировать при помощи **TCP Wrappers** (обработчиков TCP): это простая текстовая БД, записи в которой позволяют ограничивать или разрешать доступ к сетевым демонам.

В них присутствуют дополнительные возможности – возврат комментариев, ведение логов, отправка сообщений и т.д. Они не являются сетевым экраном, через них работает даже локальный хост.

TCP Wrapper это файлы **/etc/hosts.allow** и **/etc/hosts.deny*.*** У файла с разрешениями (allow) приоритет над файлом запретов (deny). Если создан файл с разрешениями, то разрешено только то что указано в файле; если создан файл с запретами, то запрещено только то, что указано.

Синтаксис правил в файлах контроля доступа выглядит так: **имя\_демона список\_доступа**, например:

***ALL: mti.edu.ru EXCEPT @buhs*** *(разрешить доступ ко всем демонам из домена mti.edu.ru, кроме группы пользователей buhs);*

***tftpd: 192.168.0*** *(разрешить доступ к демону tftpd из сети 192.168.0)*