

FBD-202 Сетевое администрирование и безопасность FreeBSD

Дистрибутив: FreeBSD 8.1.

Категория слушателей: Практикующие администраторы FreeBSD систем с опытом работы от трех лет.

Предварительная подготовка

Требуются знания в объеме учебных курсов “Администрирование FreeBSD” FBD-101, “Сетевое администрирование FreeBSD” FBD-102 и “Углубленное администрирование FreeBSD” FBD-201.

Получаемые знания

На данном курсе слушатели:

- Изучат концепции защиты сетей с помощью фаерволлов,
- Научатся настраивать инфраструктурные серверы DNS, DHCP, NTP,
- Научатся настраивать систему строгой криптографической аутентификации Kereberos,
- Изучат «продвинутые» возможности OpenSSH и OpenSSL,
- Получат знания по работе с Apache, OpenLDAP, SAMBA, NFS
- Научатся строить VPN на базе IPsec.

Продолжительность курса: 5 дней / 50 ак. часов

Содержание курса:

Фаерволлы и управление трафиком.

- Концепции и возможности фаерволлов.
- Имеющиеся в FreeBSD фаерволлы.
- Применение IPFW.
- Применение IPFILTER.
- Применение OpenBSD PF.
- Управление трафиком (traffic shaping).
- Применение Dummynet.
- Применение ALTQ.

Сервер DNS BIND.

- Запуск в chroot.
- Использование rndc.
- Настройка мастер сервера для зоны и подчиненного сервера для зоны.
- Создание поддомена и делегирование.
- Форвардинг.
- Тестирование DNS с помощью nslookup, host, dig.
- Ограничение доступа.
- Журналирование.
- Динамические обновления зон.
- DNSSEC.

Сервер DHCP.

- Конфигурирование DHCP сервера.
- Файл dhcp.leases.
- Клиент DHCP.
- DHCP relay agent.

- Синхронизация времени с помощью NTP.
- Архитектура и терминология NTP.
- Использование ntpdate.
- Демон ntpd.
- Настройка ntpd.

Использование Kerberos.

- Установка KDC.
- Керберизация служб.
- Настройка аутентификации в Kerberos.

Возможности OpenSSH.

- Конфигурационные файлы и настройка OpenSSH.
- Генерация и передача ключей.
- Шифрование X трафика.
- Туннелирование.

Использование OpenSSL.

- Основы криптографической защиты.
- Конфигурационные файлы.
- Криптографические сертификаты.
- Утилиты.

Построение VPN с помощью IPsec.

- Принципы работы IPsec.
- Варианты организации VPN.
- Настройка VPN.
- Проверка и отладка.

Сервер HTTP Apache.

- Программа apachectl.
- Настройка ограничений количества подключений и т.п..
- Ограничение доступа.
- Аутентификация пользователей.
- Виртуальные узлы.
- CGI.
- Использование и настройка PHP.
- Использование mod_perl.
- Использование HTTPS.
- Настройка журналирования.
- Модуль mod_redirect.

Прокси сервер Squid.

- Запуск Squid и опции командной строки.
- Настройка ACL.
- Запрет обращения к заданным URL.
- Ограничения для пользователей.
- Аутентификация пользователей.
- Журналы Squid.
- Анализаторы журналов Squid.

Использование OpenLDAP.

- Идеология и организация LDAP.

- Настройка сервера slapd.
- Утилиты управления службой каталогов.
- Поиск информации в LDAP.
- Миграция в LDAP.
- Аутентификация в LDAP.

Сетевая файловая система NFS.

- Конфигурационные файлы NFS.
- Команды NFS.
- Ограничение доступа.

Использование SAMBA.

- Конфигурационные файлы Samba 3.
- Samba 3, как PDC.
- Samba 3, как BDC.
- Настройка WINS.
- Настройка профилей пользователей.
- Аутентификация.

Электронная почта.

- Настройка Sendmail.
- Ограничение доступа.
- Почтовые псевдонимы.
- Виртуальные узлы.
- Таблица mailertable.
- Таблица genericstable.
- Почтовые квоты.
- Аутентификация в Sendmail.
- Управление очередью.
- Система procmail.
- MTA Postfix.
- Архитектура postfix.
- Конфигурационные файлы postfix.
- Утилиты postfix для эмуляции sendmail.
- Форматы mbox и Maildir.
- Антиспам.
- Протоколы POP3 и IMAP.
- Сервер Dovecot.
- Сервер Courier IMAP.