Развертывание центра сертификации для построения защищенных SSL – соединений

Практическая часть

Цель работы

Изучение технологии цифровых сертификатов инфраструктуры открытых ключей PKI и получение навыков построения зашифрованной сети на базе этой технологии.

Схема лабораторной работы

На данном рисунке показана схема, которую вы должны будете исследовать в процессе выполнения лабораторной работы.

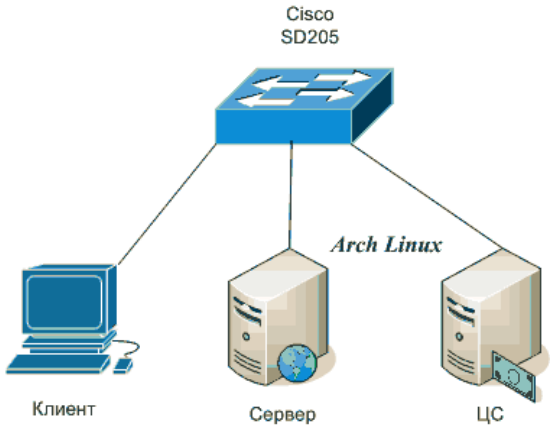

Рисунок. Топология фрагмента сети PKI

Задание и порядок выполнения работы

Задание А Самостоятельная работа.

1) Инсталируйте незашифрованное веб-соединение между Клиеном и Сервером.

Для этого на Сервере запустите веб-сервер *Apache*. С помощью утилиты *tcpdump* убедитесь, что данные передаются без шифрования.

2) Создайте защищенное соединения между Клиентом и Сервером.

Для этого создайте центр сертификатов ЦС средствами *openssl*. Сгенерируйте необходимые ключи и сертификаты. Настройте веб-сервер и веб-браузер. Убедитесь, что передаваемые данные шифруются.

Задание В Самостоятельная работа с указаниями пошагового выполнения.

1). Скоммутируйте сеть в соответствии с топологией сети, представленной на рисунке.

2). Запустите на Сервере веб-сервер *Apache*.

3). Инициируйте соединение клиента с веб-сервером и с помощью утилиты tcpdump убедитесь, что данные передаются без шифрования.

4). Создайте центр сертификатов ЦС средствами пакета *openssl*.

5). Создайте корневой сертификат.

6). Создайте запрос на сертификацию в ЦС.

7). Подпишите запрос на сертификацию.

8). Настройте защищенное соединения между Клиентом и Сервером.

8.1). Перенесите с ЦС на Сервер файл закрытого ключа, файл цифрового сертификата и файл корневого сертификата.

8.2). В конфигурационном файле веб-сервера укажите пути до созданных файлов сертификата и закрытого ключа.

9). На Клиенте в веб-браузере импортируйте файл корневого сертификата для внесения его в список доверенных ЦС и настройте браузер на работу с сертификатом.

10). Инициируйте соединение клиента с веб-сервером по протоколу *https*. Средствами браузера изучите сертификат.

11). С помощью tcpdump изучите передаваемые пакеты и убедитесь, что передаваемая информация шифруется.

Задание С Самостоятельная работа пошагового выполнения задания **В** ***с ключевыми указаниями преподавателя.***

Требования к оформлению лабораторной работы

Отчет студента по проделанной работе оформляется в электронном и печатном виде и должен содержать:

1) титульный лист по принятой форме с название работы, ФИО студента,

2) цель работы, топологию сети с обозначением всех сконфигурированных портов и интерфейсов,

3) последовательность пошагового выполнения всех действий в соответствии с заданием **В**, а именно:

- листинги команд с комментариями,
- скриншоты выполнения команд,

4) анализ и выводы по работе,

5) ответы на контрольные вопросы.

Контрольные вопросы

1. Назовите основные компоненты PKI.
2. Назначение сертификатов.
3. Назовите основные этапы генерации цифрового сертификата.
4. Для чего нужен корневой сертификат?
5. Поясните процесс выпуска сертификата.
6. Обновление сертификата, выработка решения.
7. Отзыв сертификата, выработка решения.
8. Способы запроса сертификата, их отличия.
9. Что произойдет при истечении срока действия корневого сертификата?; промежуточного сертификата?
10. Как получить возможность использовать цифровую подпись?
11. Опишите способы получения сертификата.
12. Какие алгоритмы аутентификации используются службами PKI?
13. Какие алгоритмы шифрования используются службами PKI?
14. Опишите возможные иерархические структуры центров сертификации.
15. Что собой представляет пакет *OpenSSL*?

Литература, источники

1. James Boney, Cisco IOS in a Nutshell, O`Reilly, 2010
2. Wendell Odom, Interconnecting Networking Devices Cisco, Part 2, Cisco Press, 2010
3. ru.wikipedia.org/wiki
4. www.opennet.ru/base/sec/openssl.txt.html
5. OpenSSL - http://ru.wikipedia.org/wiki/OpenSSL
6. www.archlinux.org/
7. www.linuxguide.it/command_line/linux_commands_ru.html