Описание курса «Основы сетевой безопасности. Часть 2: Технологии туннелирования»

Целевая аудитория

Курс «Основы сетевой безопасности. Часть 2: Технологии туннелирования» разработан совместно с факультетом вычислительной математики и кибернетики (ВМК) Московского государственного университета имени М. В. Ломоносова.

Курс предназначен для сетевых администраторов, желающих изучить теоретические основы сетевой безопасности и получить практические навыки по развертыванию и настройке **виртуальных частных сетей**, для студентов и аспирантов направлений ВПО 01.03.02 «Прикладная математика и информатика» и 02.03.02 «Фундаментальная информатика и информационные технологии», а также для всех, кто интересуется современными сетевыми технологиями и принципами обеспечения сетевой безопасности.

Предварительная подготовка

Данный курс требует прохождения курса «Основы сетевых технологий. Часть 1: Основы передачи и коммутации данных в компьютерных сетях», а также знания основ сетевого взаимодействия и стека протоколов TCP/IP.

Сертификаты

После прохождения курса, слушатель может получить сертификат ВМК МГУ им. Ломоносова, а после сдачи сертификационного экзамена – сертификат D-Link.

Сертификационный экзамен состоит из практической части, сдаваемой в учебном центре ВМК МГУ им. Ломоносова, и теста на портале дистанционного обучения D-Link.

Теоретическая часть курса может быть самостоятельно изучена слушателем на портале дистанционного обучения и сертификации D-Link. В этом случае для получения сертификата слушатель может сдать практический экзамен в учебном центре ВМК МГУ им. Ломоносова, и тест на портале дистанционного обучения D-Link. Также слушатель может изучить только практическую часть курса в учебном центре ВМК МГУ им. Ломоносова и сдать сертификационный экзамен.

Описание курса

Длительность курса – 72 академических часа. Курс включает лекционную (32 часа) и практическую (40 часов) части. Слушатели могут изучить теоретическую часть курса в учебном центре ВМК МГУ им. Ломоносова или самостоятельно на портале дистанционного обучения и сертификации D-Link.

Целью курса является изучение принципов и получение практических навыков создания безопасной сетевой инфраструктуры с использованием межсетевых экранов D-Link DFL-860E (имеют сертификат ФСТЭК).

По окончании курса слушатели будут

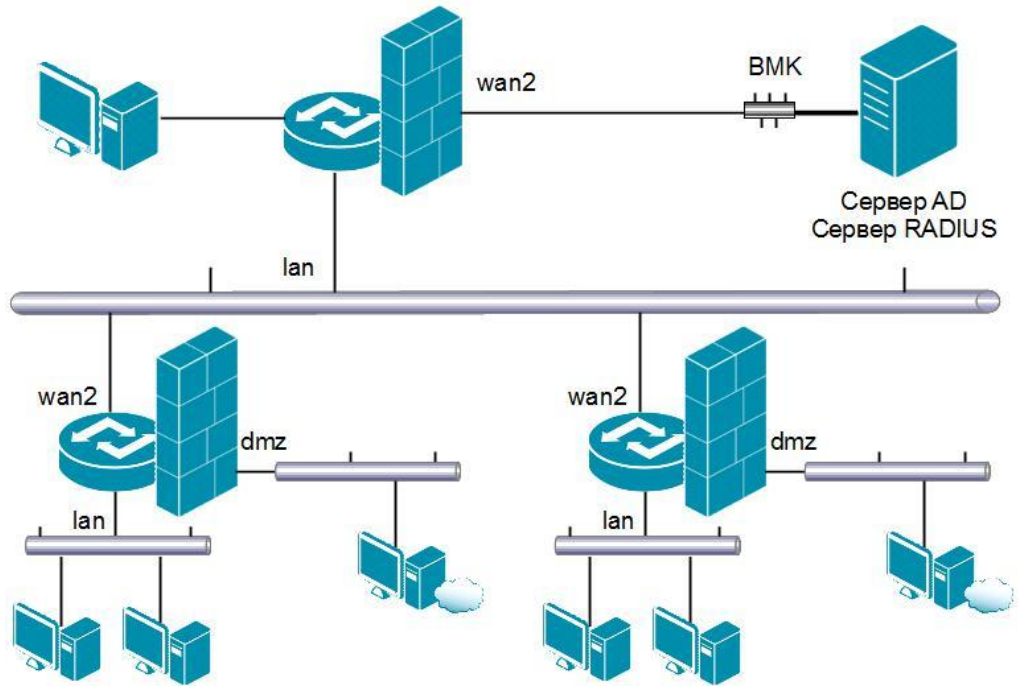
- знать:
  - основы криптографических механизмов безопасности;
  - технологии туннелирования;
  - способы хранения учетных записей;
- иметь практические навыки:
  - использования различных протоколов туннелирования.

Оборудование

Для проведения лабораторных работ на 1 рабочее место требуется следующее оборудование:
- 3 компьютера, один из которых выступает в роли Web-сервера;
- 1 межсетевой экран DFL-860E;
- кабели Ethernet.

Дополнительно:
- 1 компьютер, выступающий в роли сервера, на котором установлен контроллер домена (сервер AD) и RADIUS-сервер.

Топология класса



Программа курса

Теория:

1. **Криптографические механизмы безопасности**

- **Алгоритмы симметричного шифрования**
  - Основные понятия
  - Области применения
  - Платформы

- Дополнительные требования
- Сеть Фейштеля
- Криптоанализ
- Используемые критерии при разработке алгоритмов
- Алгоритм DES
- Алгоритм тройной DES
- Алгоритм ГОСТ 28147
- Алгоритм AES
- Режимы выполнения алгоритмов симметричного шифрования
- Создание случайных чисел

- **Хэш-функции**
  - Требования к криптографическим хэш-функциям
  - «Парадокс дня рождения»
  - Хэш-функция MD5
  - Хэш-функция SHA-1
  - Сравнение SHA-1 и MD5
  - Хэш-функции SHA-2
  - Хэш-функция ГОСТ 3411
  - Код аутентификации сообщения
  - Стандарт HMAC
- **Алгоритмы асимметричного шифрования**
  - Основные требования к алгоритмам асимметричного шифрования
  - Криптоанализ алгоритмов с открытым ключом
  - Основные способы использования алгоритмов с открытым ключом
  - Алгоритм RSA
  - Алгоритм Диффи-Хеллмана
  - Стандарт цифровой подписи DSS
  - Криптография с использованием эллиптических кривых
- **Инфраструктура открытого ключа**

2. Технологии туннелирования

- **Протокол GRE**
- **Виртуальные частные сети**
  - Протоколы канального уровня
    - Терминология
    - Point-to-Point Protocol (PPP)
    - Способы передачи PPP по Ethernet
      - Протокол L2TP
      - Протокол PPTP
      - Протокол PPPoE
  - Семейство протоколов IPSec
    - Назначение семейства протоколов IPSec
      - Возможные способы реализации IPSec
      - Протоколы защиты трафика и понятие безопасной ассоциации
      - Понятие домена IPSec
      - Возможные топологии IPSec
    - Степень детализации управления трафиком
    - Протокол ESP
      - Обзор
      - Формат пакета ESP
      - Обработка трафика, выполняемая ESP
    - Политика безопасности
      - База данных политик безопасности (SPD)

        - База данных безопасной ассоциации (SAD)

    - Способы аутентификации участников и распределение ключей
        - Распределение ключей вручную
        - Автоматическое создание SA и распределение ключей
            - Форматы сообщений в протоколе IKE
            - Протокол IKE
            - Информационный обмен
            - Использование NAT в протоколе IPSec
            - Метод определения сбоя противоположной стороны IKE, основанный на наличии трафика
            - Протокол DPD
    - Проблемы выполнения
- Совместное использование протоколов L2TP и IPSec
    - Обзор
    - Примеры атак на протокол L2TP
    - Основные принципы совместного использования L2TP и IPSec
    - Детали IPSec-фильтрования для L2TP-защиты
    - Обсуждение безопасности
- **Протокол SSL/TLS**
    - Обзор
    - Протокол Записи
    - Протокол Рукопожатия
    - Добавление дополнительных возможностей в протокол

3. Аутентификация и хранение учетных записей

- **Топология сети**
- **Протокол RADIUS**
    - Основные понятия
        - Типы данных
        - Принципы функционирования RADIUS
    - Аутентификация RADIUS
        - Последовательность пакетов
        - Вызов / Ответ
        - Интероперабельность с PAP и CHAP
        - Использование прокси-сервера
        - Причина использования UDP
        - Использование повторных передач
        - Проверка жизнеспособности сервера
        - Формат пакета аутентификации
        - Атрибуты аутентификации
        - Обсуждение безопасности
    - Аккаунтинг RADIUS
        - Последовательность пакетов
        - Использование прокси-сервера
        - Формат пакета аккаунтинга
        - Типы пакетов
        - Атрибуты аккаунтинга
- **Протокол LDAP**
    - Введение
        - Преимущества LDAP
        - Принципы развертывания серверов LDAP
    - Основные характеристики LDAP
        - Способ хранения и доступа к информации
        - Распределенное множество серверов LDAP

- Описание протокола

Практика:

Технологии туннелирования

Лабораторная работа №1.	Соединение двух локальных сетей GRE-туннелем
Лабораторная работа №2.	Соединение двух локальных сетей IPSec в туннельном режиме, аутентификация с использованием общего секрета
Лабораторная работа №3.	Использование аутентификации по стандарту XAuth в протоколе IPSec
Лабораторная работа №4.	Соединение двух межсетевых экранов IPSec в транспортном режиме, аутентификация с использованием общего секрета
Лабораторная работа №5.	Использование преобразования NAT в протоколе IPSec
Лабораторная работа №6.	Использование протокола DPD в протоколе IPSec
Лабораторная работа №7.	Соединение двух локальных сетей протоколом L2TP, аутентификация с использованием общего секрета
Лабораторная работа №8.	Соединение двух локальных сетей протоколом GRE/IPSec в транспортном режиме
Лабораторная работа №9.	Соединение двух локальных сетей протоколом L2TP/IPSec в транспортном режиме
Лабораторная работа №10.	Соединение двух локальных сетей протоколом L2TP/IPSec в транспортном режиме, для одной из локальных сетей используется NAT

Аутентификация и хранение учетных записей

Лабораторная работа №11.	Использование локальной БД для хранения учетных записей
Лабораторная работа №12.	Использование сервера RADIUS для хранения учетных записей
Лабораторная работа №13.	Использование сервера LDAP/MS AD для хранения учетных записей
Лабораторная работа №14.	Аутентификация доступа к ресурсам с использованием браузера