Министерство науки и высшего образования РФ
ФГБОУ ВО «Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ И САМОСТОЯТЕЛЬНОЙ РАБОТЫ

СТУДЕНТОВ ПО ДИСЦИПЛИНЕ

«Основы построения защищенных компьютерных сетей»

для студентов специалитета по специальности
10.05.01 Компьютерная безопасность,

Ульяновск, 2021

Методические указания для выполнения лабораторных работ и самостоятельной работы студентов по дисциплине «Основы построения защищенных компьютерных сетей» для студентов специальности 10.05.01 «Компьютерная безопасность» / составитель: Клочков А.Е. - Ульяновск: УлГУ, 2021.

Настоящие методические указания предназначены для студентов специалитета по специальности 10.05.01 «Компьютерная безопасность», изучающих дисциплину «Основы построения защищенных компьютерных сетей». В работе приведены рекомендуемая литература по дисциплине, основные темы курса и вопросы в рамках каждой темы, указания по выполнению лабораторных работ.

Студентам следует использовать данные методические указания при выполнении лабораторных работ и при подготовке к экзамену по данной дисциплине.

Рекомендованы к введению в образовательный процесс Ученым советом факультета математики, информационных и авиационных технологий УлГУ (протокол № 4/21 от 18 мая 2021 г.)

СПИСОК РЕКОМЕНДОВАННОЙ ЛИТЕРАТУРЫ

1. Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 368 с. — ISBN 978-5-4497-0931-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102069.html. — Режим доступа: для авторизир. пользователей
2. Костин, В. Н. Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей : учебное пособие / В. Н. Костин. — Москва : Издательский Дом МИСиС, 2018. — 31 с. — ISBN 978-5-906953-53-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/98200.html — Режим доступа: для авторизир. пользователей
3. Ковган, Н. М. Компьютерные сети : учебное пособие / Н. М. Ковган. — Минск : Республиканский институт профессионального образования (РИПО), 2019. — 179 с. — ISBN 978-985-503-947-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/93384.html — Режим доступа: для авторизир. пользователей
4. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/473348.
5. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/471159.
6. Практикум по выполнению лабораторных работ по дисциплине Системы обнаружения вторжений в компьютерные сети / составители Д. В. Костин. — Москва: Московский технический университет связи и информатики, 2016. — 42 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/61546.html — Режим доступа: для авторизир. пользователей
7. Учебно-методическое пособие по выполнению курсового проекта по дисциплине «Методы и средства защиты информации в компьютерных сетях» / составители О. И. Шелухин. — Москва : Московский технический университет связи и информатики, 2015. — 35 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/61741.html — Режим доступа: для авторизир. пользователей
8. http://www.securitylab.ru – российский портал по компьютерной безопасности.
9. http://www.pgpru.com – русскоязычный сайт, посвященный криптографическому стандарту PGP.
10. http://www.docload.spb.ru/Basesdoc/45/45674/index.htm – основные термины и определения в области технической защиты информации (согласно Приказу Федерального агентства по техническому регулированию и метрологии от 6 апреля 2005 г. № 77-ст)

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Типовые угрозы сетевой безопасности

Тема № 1. Сетевые атаки

Стадии проведения сетевой атаки. Классификация сетевых угроз, уязвимостей и атак. Атаки на реализации сетевых протоколов, отдельные узлы и службы. Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI. Проблемы обеспечения конфиденциальности, целостности и доступности информации на различных уровнях модели ISO/OSI.

Тема № 2. Механизмы реализации атак в сетях TCP/IP

Удалённое определение версии ОС с использованием особенностей реализации стека протоколов TCP/IP. Методы сканирования портов. Методы обнаружения пакетных сниферов. Методы обхода МЭ.

Тема № 3. Методы перехвата сетевых соединений в сетях TCP/IP

Имперсонация вслепую. Десинхронизация TCP-соединений. Атаки, направленные на сетевую инфраструктуру.

Тема № 4. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак

Принуждение к ускоренной передаче. Атаки, направленные на отказ в обслуживании. Изменение конфигурации и состояния хостов. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации. Технические меры защиты от сетевых атак.

Раздел 2. Криптографические методы защиты информации в компьютерных сетях

Тема № 5. Криптографические протоколы обеспечения безопасности

Протоколы аутентификации на прикладном уровне. Протокол Kerberos. Протоколы аутентификации на транспортном уровне. Протокол SSL/TLS. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI.

Тема № 6. Защита виртуальных частных сетей (VPN)

Назначение, основные возможности, принципы функционирования и варианты реализации VPN. Организация туннелирования на различных уровнях модели ISO/OSI. Достоинства и недостатки применения VPN. Протокол IPSEC. Протоколы AH и ESP. Особенности работы протокола IP SEC в туннельном и транспортном режимах. Протокол управления ключами ISAKMP/Oakley. Использование протокола L2TP для организации виртуальных частных сетей.

Тема № 7. Разработка защищенных сетевых приложений

Аутентификация, шифрование, обеспечение целостности с использованием программного интерфейса SSPI. Программный интерфейс OpenSSL.

Раздел 3. Программно-аппаратные средства обеспечения безопасности в компьютерных сетях

Тема № 8. Средства защиты локальных сетей при подключении к Интернет

Межсетевые экраны (МЭ). Место и роль МЭ в обеспечении сетевой безопасности. Классификация МЭ. Требования к МЭ. Основные возможности и схемы развертывания МЭ. Достоинства и недостатки МЭ. Построение правил фильтрации. Методы сетевой трансляции адресов (NAT). Шлюзы уровня приложений. Реализация сетевой политики безопасности с использованием МЭ. Методы обхода межсетевых экранов.

Тема № 9. Защита серверов и рабочих станций.

Средства и методы предотвращения и обнаружения вторжений. Системы обнаружения вторжений (СОВ). Назначение и возможности средств обнаружения вторжений на хосты, протоколы и сетевые службы. Место и роль средств обнаружения вторжений в общей системе обеспечения сетевой безопасности. Классификация СОВ. Выявление атак на основе сигнатур атак и выявления аномалий. Аудит прикладных служб. Средства обнаружения уязвимостей сетевых служб. Способы
противодействия вторжениям. Системы виртуальных ловушек (Honey Pot и Padded Cell).

МЕТОДИЧЕСКИЕ УКАЗАНИЯ И ЗАДАНИЯ К ЛАБОРАТОРНЫМ РАБОТАМ

Цель. Лабораторный практикум по дисциплине направлен на изучение студентами всех современных подходов для обеспечения информационной безопасности современных операционных систем. Охватывает клиентские операционные системе (на базе Microsoft Windows 10 и Alt Linux), а также серверные операционное системы (на базе Microsoft Server 2026R2 и Alt Linux Server). В соответствии с руководящими документами обучение происходит на сертифицированные версиях операционных систем.
Методология основывается на самостоятельном обучении студентов решению стандартных задач на основе технической документации, теоретического материала. Все работы обладают дифференцированной линейно растущей сложностью выполнению и созданы на основе стандартных практических задач современного предприятия. Поиск технической информации, а также подбор необходимого решения производиться самостоятельно студентами в открытых источниках и контролируется в ходе лабораторных занятий и процессе демонстрации полученного решения.
Результат. Полученные решения демонстрируются студентом для каждого из типа операционных систем. При необходимости демонстрируется ход выполнения работы.
Требования к оборудованию. Для выполнения работ студенты используют несколько виртуальных машин с различными версиями операционных систем. Возможно самостоятельное выполнение лабораторных работ вне лаборатории. Компьютер с жестким диском – 100 Gb, ОЗУ: 8 Gb, Windows 10 Pro, BaseAlt (Альт Рабочая станция, Альт сервер), Kali Linux, Oracle Virtual Box, Putty, PGP, Apache, nginx, Statistica, Origin. По желанию студента все виртуальные машины могут быть развернуты на выделенном сервере виртуальных машин в лаборатории. Для моделирования работы сетей используется CISCO Packet Tracer. Сеть лаборатории представляет собой гетерогенную сеть, включающую в себя индивидуальный набор следующего оборудования:

1. Коммутатор L2, L3.
2. Маршрутизатор L3 с функциями VPN.
3. Маршрутизатор Континет КШ 25.
4. Маршрутизатор VipNet Координатор.

Для поддержания работы сетей используется выделенный Коммутатор L3, L3 сконфигурированный для работы независимых сегментов сети.
Требования к оформлению лабораторной работы. Все файлы, используемые в лабораторной работе, должны быть представлены в одном каталоге и иметь наименования, описывающие хранимую в файле информацию. Например: ssh_client_key.txt – содержит информацию о клиентском ключе для SSH. Должен быть файл read.me с текстовым описанием всех настроек, которые были использованы для выполнения лабораторной работы разбитых на секции. Например:

```
[BaseAlt (Альт Рабочая станция, Альт сервер)Server]
IPv4=10.2.0.1/24
DNS=10.2.0.2
gateway: 10.2.0.3
; Обозначение комментария
```

Имена полей должны быть написаны латинскими буквами. Секции могут включать в себя подсекции.

Лабораторная работа №1. Строение сетей

Цель. Изучение базовых механизмов получения информации о конфигурации сети. Получение навыков работы с различными программами, позволяющими определить конфигурацию сети или конфигурацию отдельного устройства в сети. Требуется для выполнения всех последующих лабораторных работ.
Задача. Все задачи необходимо выполнить на ОС MS Windows 10 и BaseAlt (Альт Рабочая станция, Альт сервер).

- Для каждой из операционных систем установить следующее программное обеспечение:
  - Сканер безопасности Nmap (ZenMap - с графическим режимом)
  - Wireshark
  - Putty
  - whois
  - tranceroute
  - nslookup
- Произвести анализ сайта 80.250.180.133. Обнаружить все открытые порты и протоколы. Составить схему расположения данного ресурса. Установить DNS имена расположенных на указанном IP адресе серверов. Получить информацию о владельце данного сайта.
- Произвести подключение к серверу 62.76.32.162 по протоколу ssh (стандартный порт).
- Произвести перехват пакетов ssh протокола направляемых к данному серверу при помощи Wireshark. Внимание! Необходимо показать перехват пакетов при получение первого ключа шифрования SSH.
- Для обоих серверов указать номер автономной системы и её владельца.
- Подключиться к WiFi сети университета.
- Вычислит IP адрес шлюза выхода в интернет.
- Определить протокол шифрования трафика.

Лабораторная работа №2. Удалённый доступ по протоколу SSH

Цель. Изучение возможностей протокола SSH для получения удалённого доступа к серверу. Применение функцию шифрования каналов связи при использовании протокола SSH.
Задача №1. Все задачи необходимо выполнить на BaseAlt (Альт Рабочая станция, Альт

сервер), с использованием ОС MS Windows в качестве клиентской операционной системы.

- Установить систему openSSH сервер на ОС BaseAlt (Альт Рабочая станция, Альт сервер) и putty на ОС MS Windows.
- Создать ключ серверного шифрования информации.
- Установить соединение с данным сервером с другого клиента, на котором запущен WireShark. Перехватить ключ серверного шифрования.
- Запретить передачу ключа по отрытому каналу.
- Создать ключ клиента.
- Записать ключ клиента на отчуждаемый носитель информации.
- Установить соединение с другой ОС используя ключ клиента. Перехватить трафик и проанализировать полученные пакеты. Объяснить увиденный результат.
- Создать ключи шифрования на клиенте используя puttyGen. Переписать их на отчуждаемый носитель.
- Установить клиентские ключи шифрования для openSSH.
- Произвести соединение с сервером.

Задача №2. Все задачи необходимо выполнить на BaseAlt (Альт Рабочая станция, Альт сервер), с использованием ОС MS Windows в качестве клиентской операционной системы.

- Отключить клиентский компьютер на ОС MS Windows от сети Интернет.
- Настроить работы протокола SSH в режиме PORT FORWARDING.
- Создать «проброс» порта из внутренней защищенной сети через сервер до сайта www.ulsu.ru и протоколов HTTP и HTTPS.
- Перехватить отправленные пакеты с информацией и продемонстрировать использование шифрования информации.

Лабораторная работа №3. Использование VPN

Цель. Изучение возможностей программного обеспечения VPN для создания защищенных компьютерных сетей. Получение навыков работы со стандартным программным обеспечением для создания защищенных каналов связи.

Задача №1. Создание защищенного межсетевого взаимодействия сетей.

Изменить конфигурацию сети.

1. Скачать на локальный жесткий диск три образа операционных систем: MS Windows 10, MS Windows Server, BaseAlt (Альт Рабочая станция, Альт сервер).
2. Отключиться от общей сети лаборатории и включиться в один из маршрутизаторов MicroTik.
3. Назначить порты марштуризатора следующим образом: Порты №1,2 – VLAN1; Порты 3,4 – VLAN2;
4. Подключить виртуальные машины клиентских ОС к VLAN1.
5. Подключить виртуальную машину с сервером к VLAN2.
6. Создать ключи доступа и файлы конфигураций для клиентских компьютеров.
7. Установить VPN клиент и применить файлы конфигурации.
8. Передать файл по протоколу SMB в защищенной сети.

Задача №2. Использование АПКШ «Континент» для создания защищенной сети.

Изменить конфигурацию сети.

1. Подключить порт 3 к VLAN9.
2. Получить ключи шифрования для АПКШ «Континент» Сервер Доступа.
3. Подключить АПКШ «Континент» к VLAN1.
4. Настроить АПКШ «Континент» Сервер доступа в соответствии с руководством администратора.

5. Передать файл по протоколу SMB в защищенной сети.

Лабораторная работа №4. Работа с сертификатами SSL

Цель. Изучение возможностей центров сертификации (Certificate Authorities). Получение навыков работы с криптографическими ключами. Применение встроенных систем шифрования информации в стандартных приложениях операционных систем.
Задача. Для выполнения лабораторной работы используются ОС MS Windows и BaseAlt (Альт Рабочая станция, Альт сервер).

- Необходимо установить и настроить следующее программное обеспечение: OpenSSL
- Выдать сертификат SSL на свое имя: SN - должно содержать вашу ФИО. Также сертификат должен содержать ваш действующий EMAIL адрес.
- Скачать сертификат открытого ключа для Корейко Александра Ивановича.
- Установить сертификат в ОС и настроить электронную почту таким образом, чтобы отправляемые письма содержали вашу электронную подпись и были зашифрованы для получателя Корейко Александр Иванович.
- Установить локальный web сервер (apache, nginx).
- Выдать сертификат для локального веб сервера.
- Продемонстрировать работу по безопасному https соединению.
- Отчет по лабораторной работе должен содержать файл электронного письма в формате SMIME, а также файл сертификата.

Лабораторная работа №5. Моделирование виртуальной сети

Цель. Ознакомление с методами моделирования сетей. Знакомство с телекоммуникационным оборудованием компании CISCO. Решение практических задач.
Задание. Выполняется в программном обеспечении Cisco Packet Tracer

Ваша фирма переезжает в новый бизнес-центр, где она арендовала 3 помещения, на 1-м, 2-м и 3-м этаже. У вас есть ограниченный набор оборудования:

- 3 коммутатора Cisco 2960
- Маршрутизатор Cisco 1941
- роутер Cisco WRT300N

Вас попросили разработать схему сети со следующими требованиями:

- Любой компьютер компании может связываться с любым другим компьютером, но при этом, каждое помещение должно быть изолировано.
- На третьем этаже должна быть установлена WiFi точка доступа. Точка должна иметь пароль ulsu30years, должны выдаваться первые 20 адресов. SSID должен быть скрыт.
- На втором этаже установлен WEB сервер. Доступ к нему должны иметь все компьютеры по локальному имени "sharepoint".
- На первом этаже 3 рабочих места, на втором 2 рабочих места и сервер, третий 10 рабочих мест, в том числе 5 беспроводных.

  К сетевому оборудованию должен быть предоставлен безопасный доступ по SSH. Для доступа к оборудованию вас попросили создать административную виртуальную сеть "mi6".

Лабораторная работа №6. Обнаружение вторжений

Цель. Изучение возможностей современного программного обеспечения для обнаружения вторжений. Управление правилами безопасности, анализ журналов событий.

Задача. Установка и настройка систем обнаружения вторжений в сети. Проведение атаки на защищенный сегмент сети. Для проведения атаки рекомендуется использовать

специализированный дистрибутив ОС – Kali Linux.

- На ОС семейства BaseAlt (Альт Рабочая станция, Альт сервер) следует установить и настроить систему обнаружения вторжений Snort
- При помощи утилит предустановленных в дистрибутив Kali Linux произвести атаку на любой свой компьютер, подключенный к системе обнаружения вторжений Snort.
- Показать, как Snort обнаружил атаку на ваш ресурс.
- Создать правило, обнаруживающие ICMP атаки на ваш ресурс.
- Анализировать журнал событий и продемонстрировать обнаружение атаки.

Лабораторная работа №7. АПКШ «Континент» Обнаружение вторжений

Цель. Изучение возможностей комплекса АПКШ «Континент» для регистрации вторжений в локальную сеть.

Задача. Ознакомление с сертифицированными системами обнаружения вторжений в сети. Работа с правилами фильтрации и обнаружения атак.
Изменить конфигурацию сети.

1. Отключить рабочую станцию от локальной сети лаборатории и подключиться к маршрутизатору MicroTik.
2. Настроить порты маршрутизатора №1,2,3 в VLAN1.
3. Настроить порт маршрутизатора №4 в режим MIRRORING («зеркалирование»).
4. Подключить АПКШ «Континент» к порту №4.
5. Настроить АПКШ «Континент» Система обнаружения вторжений в режиме PROMISCUOUS_MODE.
6. Произвести ICMP атаку в сети.
7. Продемонстрировать результаты работы правил на АПКШ «Континент».

ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Стадии проведения сетевой атаки.
2. Классификация сетевых угроз, уязвимостей и атак.
3. Атаки на реализации сетевых протоколов, отдельные узлы и службы.
4. Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI.
5. Проблемы обеспечения конфиденциальности, целостности и доступности информации на различных уровнях модели ISO/OSI.
6. Удалённое определение версии ОС с использованием особенностей реализации стека протоколов TCP/IP.
7. Методы сканирования портов.
8. Методы обнаружения пакетных сниферов. Методы обхода МЭ.
9. Имперсонация вслепую. Десинхронизация TCP-соединений.
10. Атаки, направленные на сетевую инфраструктуру.
11. Принуждение к ускоренной передаче. Атаки, направленные на отказ в обслуживании.
12. Изменение конфигурации и состояния хостов. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации.
13. Технические меры защиты от сетевых атак.
14. Протоколы аутентификации на прикладном уровне.
15. Протокол Kerberos. Протоколы аутентификации на транспортном уровне. Протокол SSL/TLS.
16. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI.

17. Назначение, основные возможности, принципы функционирования и варианты реализации VPN.
18. Организация туннелирования на различных уровнях модели ISO/OSI. Достоинства и недостатки применения VPN.
19. Протокол IPSEC. Протоколы AH и ESP. Особенности работы протокола IP SEC в туннельном и транспортном режимах.
20. Протокол управления ключами ISAKMP/Oakley. Использование протокола L2TP для организации виртуальных частных сетей.
21. Аутентификация, шифрование, обеспечение целостности с использованием программного интерфейса SSPI. Программный интерфейс OpenSSL.
22. Межсетевые экраны (МЭ). Место и роль МЭ в обеспечении сетевой безопасности.
23. Классификация МЭ. Требования к МЭ. Основные возможности и схемы развертывания МЭ.
24. Достоинства и недостатки МЭ. Построение правил фильтрации.
25. Методы сетевой трансляции адресов (NAT). Шлюзы уровня приложений.
26. Реализация сетевой политики безопасности с использованием МЭ. Методы обхода межсетевых экранов.
27. Системы обнаружения вторжений (СОВ).
28. Назначение и возможности средств обнаружения вторжений на хосты, протоколы и сетевые службы.
29. Место и роль средств обнаружения вторжений в общей системе обеспечения сетевой безопасности.
30. Классификация СОВ. Выявление атак на основе сигнатур атак и выявления аномалий.
31. Аудит прикладных служб. Средства обнаружения уязвимостей сетевых служб.
32. Способы противодействия вторжениям.
33. Системы виртуальных ловушек (Honey Pot и Padded Cell).