СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

Р.Р. Фаткиева

Основы построения защищенных компьютерных сетей

Методические материалы по практическим работам

СПбГЭТУ «ЛЭТИ», 2021 г.

1 ПРАКТИЧЕСКИЕ РАБОТЫ

1.1 Общие положения и методика оценивания результатов

В процессе обучения по дисциплине «Основы построения защищенных компьютерных сетей» студент обязан выполнить 6 практических работ. Под выполнением практических работ подразумевается подготовка к работе, проведение экспериментальных исследований, подготовка отчета и его защита на коллоквиуме. После каждых практических работ предусматривается проведение коллоквиума на 2, 3, 4, 5, 6, 7 неделях, на которых осуществляется их защита работ. Выполнение практических работ студентами осуществляется в бригадах до 2 человек. Оформление отчета студентами осуществляется индивидуально в соответствии с принятыми в СПбГЭТУ правилами оформления студенческих работ. Отчет оформляется после выполнения экспериментальных исследований и представляется преподавателю на проверку. После проверки отчет либо возвращается (при наличии замечаний) на доработку, либо подписывается к защите. Практические работы защищаются студентами индивидуально. Каждый 21 студент получает вопрос по теоретической и практической части после чего ему предоставляется время для подготовки ответа. На защите практической работы студент должен показать: понимание и умение объяснять особенности применяемых методов, возможные области их применения и т.д., прогнозировать реакции исследуемого объекта на различные воздействия, навыки и умения, приобретенные при выполнении практических работы. При обсуждении ответа преподаватель может задать несколько уточняющих вопросов. В случае если студент демонстрирует достаточное знание вопроса, работа считается зачтенной. Текущий контроль включает в себя выполнение, сдачу в срок отчетов и их защиту по всем практическим работам, по результатам которой студент получает допуск к экзамену. Критерием оценки работы на коллоквиумах является оценка, выставляемая по 5ти балльной шкале в соответствии со следующими критериями: оценка в 5 баллов выставляется при отличном выполнении задания, то есть при наличии полных (с детальными пояснениями и выкладками), оригинальных и правильных решений задач, дополненных при необходимости документами, полученными

в результате реализации (проверки) решения, верных ответов и высококачественного оформления работы. оценка в 4 балла выставляется при правильном выполнении задания, то есть при наличии полных (с пояснениями и выкладками), оригинальных и правильных решений задач, дополненных при необходимости документами, полученными в результате реализации (проверки) решения, верных ответов. Оценка в 3 балла выставляется при наличии отдельных неточностей в ответах (включая грамматические ошибки) или неточностях в решении задач непринципиального характера (описки и случайные ошибки арифметического характера). 22 Оценка в 2 и ниже баллов выставляется в случаях, когда в ответах и в решениях задач имеются неточности и ошибки, свидетельствующие о недостаточном понимании вопросов и требующие дополнительного обращения к тематическим материалам.

самостоятельной работы студентов

Контроль самостоятельной работы студентов осуществляется на практических занятиях студентов по методикам, описанным выше.

1.2 Содержание отчетов

- Титульный лист
- Формулировка задания
- Краткое описание выполнения основных этапов работы.
- Результаты работы сетевого взаимодействия исследуемых устройств.
- Выводы по работе

1.3 Практические работы

1.3.1 Основные принципы построения защищенных сетей. Проектирование защищенной компьютерной сети

Цель работы: изучение теоретического материала необходимого для построения сетевой инфраструктуры, получение практических навыков настройки сетей, основанных на технологии виртуальных сетей с использованием коммутаторов Cisco.

Задание:

Подготовить структурную схему сети и назначить IP-адреса всем устройствам сети:

- дать понятные названия всем устройствам сети;
- составить таблицу статических и динамических VLAN;
- составить план IP адресации выделив диапазон адресов для каждого из VLAN;
- составить таблицу портов подключенного оборудования.

Контрольные вопросы:

1. Какое нормативноправовое обеспечение необходимо учитывать при построении защищённой сети?
2. Какие виды документов разрабатываются при построении сети?
3. 3. Как формируется модель угроз и модель нарушителя информационной безопасности при построении компьютерной сети?
4. Какие основные типы оборудования входят в сетевую инфраструктуру?
5. Как осуществляется IP адресация в сети?
6. Перечислите основные элементы многоуровневой системы обеспечения защиты при передаче информации по каналам связи.

Вопросы коллоквиума. Тема: Введение. Основные принципы построения защищенных сетей.

1. Теоретические основы построения защищенных сетей. Планирование сети.
2. Нормативноправовое обеспечение при построении защищённой сети. Обзор и анализ существующих стандартов в области обеспечения сетевого взаимодействия.
3. Модель угроз и модель нарушителя информационной безопасности компьютерной сети.
4. Сетевые атаки. Классификация сетевых атак.
5. Механизмы реализации атак в сетях.
6. Формирование требования к средствам защиты при построении защищённых компьютерных сетей.
7. Основные этапы разработки проектных решений по системам обеспечения информационной безопасности на базе компьютерных сетей.
8. Программноаппаратные средства хранения данных.

9. Типы оборудования при передаче данных. Обеспечение безопасности.

10. Основные элементы многоуровневой системы обеспечения защиты при передаче информации по каналам связи.

1.3.2 Основные принципы построения защищенных сетей. Настройка операционной системы CISCO IOS. Пользовательский и административный режимы. Режимы конфигурирования

Цель работы: изучение теоретического материала об основных функциях маршрутизатора, формирование практических навыков первоначальной настройки специализированной ОС Cisco IOS.

Выполнить первоначальную настройку сетевых параметров ОС Cisco IOS маршрутизатора Cisco 2811 с рабочей станции администратора сети, используя данные в таблице 1.

Таблица 2.1

Параметр	*Значение*
IP-адрес интерфейса Fa0/0	192.168.1.2/24
IP-адрес интерфейса Fa0/1	192.168.2.3/ 30
Стандартный шлюз	192.168.1.1.25
Имя маршрутизатора	R1-7
Домен	net. institute
Пароль доступа enable	
Локальный пользователь/пароль	

Выбор пула адресов осуществлять в соответствие с номером, выданным преподавателем, длина пароля должна быть стойкой к перебору. В окне консоли клиента необходимо вводить числовые значения, которые требуются для получения результата. Настройку маршрутизатора Cisco 2811 осуществлять через рабочую станцию и консольный шнур с интерфейсом RS-232.

Контрольные вопросы:

1. Перечисляйте механизмы реализации атак на маршрутизатор.
2. . Сформулируйте основные требования к средствам защиты маршрутизаторов.
3. Вычислить номер сети и номер узла для адреса 67.38.173.245 и маски 255.255.240.0

4. Вычислить номер сети и номер узла для адреса 192.168.74.66 и маски 255.255.255.192
5. Маска 255.255.254.0 и номер сети 192.168.74.0. Определить соответствующий блок адресов и их количество.
6. Маска 255.255.240.0 и номер сети 67.38.160.0. Определить соответствующий блок адресов и их количество.

1.3.3 Сетевые протоколы передачи информации. Развертывание сети с использованием VLAN

Цель работы: изучение теоретического материала о сегментации сети, формирование практических навыков настройки коммутаторов и защиты сетевой инфраструктуры коммутации.

Задание:

Разработать VLAN с номерами для рабочих станций, коммутаторов и маршрутизаторов в соответствии со схемой, представленной в практической работе 1, настроить маршрутизацию между этими VLAN при их подключении по магистральному каналу, а также выполнить настройки в соответствии с приведенными рекомендациями.

Контрольные вопросы:

1. Для чего необходимо сегментация сети?
2. Какие протоколы используются при сегментации сети?
3. Где и когда используются access и trank port?
4. Почему необходимо настаивать магистральное соединение, какие недостатки и нарушения безопасности могут быть при его использовании?
5. Как осуществляется фильтрация трафика при использовании технологии VLAN?
6. . Назовите протоколы управления сетью.

Вопросы коллоквиума. Тема: Сетевые протоколы передачи информации.

1. Эталонная модель взаимодействия открытых систем (ISO OSI). Уровни и протоколы.

2. Стек протоколов TCP/IP. Обеспечение безопасности стека протокола TCP/IP. Протокол HTTP. Обеспечение защиты клиентсерверного соединения.

3. Теоретические и практические основы обеспечения сегментирования сети и использования технологии VLAN (сегментирование и зонирование сети, управления доменами и учетными записями домена).

4. Виды маршрутизации трафика. Протоколы маршрутизации.

5. Протоколы управления сетью.

6. Технологии резервирования каналов связи. Механизмы обеспечения пропускной способности.

7. Атаки на протокол ICMP. Методы обеспечения безопасности.

8. Определить класс, номер сети и номер узла. IPадрес 192.168.169.36

9. Вычислить номер сети и номер узла для адреса 192.168.74.66 и маски 255.255.255.192

10. Маска 255.255.240.0 и номер сети 67.38.160.0. Определить соответствующий блок адресов и их количество.

11. Определить полную маску, если ее краткая запись выглядит как /15.

1.3.4 Протоколы идентификации, аутентификации и авторизации. Построение маршрутизируемой лвс. Защита сетевой инфраструктуры. Настройка аутентификации маршрутизаторов

Цель работы: изучение теоретического материала о маршрутизации сетевого трафика, формирование практических навыков использование методов аутентификации по технологии AAA на основе протокола TACACS.

Задание:

На основании спроектированной в лабораторной работе 1 сетевой инфраструктуре настроить статическую и динамическую маршрутизацию и обеспечить защиту маршрутизаторов с применением механизмов аутентификации.

Контрольные вопросы:

1. Какое утверждение описывает результат ввода команды iproute 0.0.0.0 0.0.0.0 192.168.1.1 в маршрутизаторе?
2. Почему маршрутизаторы могут передавать данные только на сетевом уровне модели OSI?
3. Какой информацией должны обмениваться маршрутизаторы, чтобы достичь горизонта сходимости?

4. В чем отличие статической маршрутизации от динамической? Когда и в каких условиях ее целесообразно применять?
5. Каким образом маршрутизатор «узнает» о недоступности маршрута?
6. В каких случаях достаточно использовать аутентификацию маршрутизатора на самом устройстве, а в каких с использованием протоколов AAA?

Вопросы коллоквиума. Тема: Протоколы идентификации, аутентификации и авторизации.

1. Средства передачи аутентификационной информации.
2. Обеспечение защиты с использованием протоколов PAP, CHAP.
3. Обеспечение защиты с использованием протокола PAP.
4. Обеспечение защиты с использованием протокола CHAP.
5. Обеспечение защиты с использованием протокола IPsec.
6. Обеспечение механизмов авторизации.
7. Механизмы аутентификации при настройке маршрутизации трафика (аутентификация маршрутизаторов).
8. Аутентификация коммутаторов.
9. Основы настройки доступа к маршрутизатору по технологии AAA.
10. Настройка механизмов аутентификации при клиентсерверном соединении.

1.3.5 Межсетевое экранирование. Настройка ACLсписков на маршрутизаторе cisco

Цель работы: изучение теоретического материала о фильтрации сетевого трафика, формирование практических навыков построения список доступа и настройка NAT на межсетевом экране Cisco.

Задание:

Разработать правила фильтрации с номерами для рабочих станций, коммутаторов и маршрутизаторов в соответствии со схемой, представленной в практической работе 1, настроить правила управления доступом к серверам и рабочим станциям из ЛВС в сеть Интернет и из нее к серверам, расположенным в ЛВС. Доступ в сеть Интернет из сети осуществляет по технологии NAT.

Контрольные вопросы:

1. Какой диапазон номеров выделен для расширенных списков доступа IP?

2. Списки доступа какого типа позволяют блокировать отдельные порты?
3. Как конфигурируется NAT: глобально или для отдельного интерфейса?
4. Сконфигурируйте расширенный список доступа, блокирующий входящий трафик HTTP.
5. Сконфигурируйте на маршрутизаторе NAT для внутренней сети 192.168.3.23 и внешнего интернет соединения с адресом 115.68.43.1. Внутренний интерфейс – ethernet 0, внешний – serial 0; адрес внутреннего интерфейса – 192.168.3.1.

Вопросы коллоквиума. Тема: Межсетевое экранирование

1. Основные компоненты межсетевых экранов и особенности их функционирования.
2. Технология NAT.
3. Правила фильтрации сетевого контента и способы ограничения доступа к сетевой инфраструктуре.
4. Создание защищенных сегментов сетей с использованием межсетевых экранов. Политика сетевой безопасности.
5. Определение виртуальной частной сети (VPN). Преимущества VPN.
6. Типы VPNсетей. Технология туннелирования.
7. Виртуальные частные сети канального уровня.
8. Протоколы PPTP, L2TP принцип работы, настройка.
9. Технологии туннелирования. Протоколы IPSec. Сервисы безопасности IPsec.
10. Опишите результат ввода команды iproute 0.0.0.0 0.0.0.0 192.168.1.1 в маршрутизаторе.
11. Опишите результат ввода команды: router(config)#accesslist 100 permit tcp 192.168.1.0 0.0.0.255 eq 80 10.1.1.0 0.0.0.255 eq 443
12. Опишите результат ввода команды: router(config)#accesslist 100 deny tcp any host 172.16.1.5 gt 5000
13. Опишите результат ввода команды: accesslist 2 deny 194.12.34.0 0.0.0.255 accesslist 2 deny 132.7.0.0 0.0.255.255 accesslist 2 permit any
14. Применение стандартных списков доступа.
15. Применение расширенных списков доступа.

1.3.6 Построение защищенного сегмента беспроводной сети с использованием механизмов WPA2

Цель работы: изучение теоретического материала о технологии беспроводной передачи данных, формирование практических навыков применения методов и средств защиты беспроводной ЛВС, являющейся частью корпоративной ЛВС.

Задание:

Построить защищенный беспроводной сегмент ЛВС в соответствии со схемой, представленной в практической работе 1, расширяющий инфраструктуру ЛВС и позволяющий организовать подключение пользователей с использованием механизмов WPA2.

Контрольные вопросы:

1. Для чего требуется идентификатор SSID?
2. Как настроить ACL списки доступа на маршрутизаторе Wi-Fi?
3. Для чего необходимы диаграммы направленности антенн? Какие проблемы они выявляют?
4. Почему используется WPA2, если WPA3 обладает более широким спектром методов защиты?
5. Какие атаки возможно реализовать за счет использования атака глушения базовой станции?
6. К какой базовой станции произойдет подключение клиента при нахождении нескольких точек доступа в зоне видимости?

Вопросы коллоквиума. Тема: Беспроводные технологии.

1.Теоретические основы построения и архитектура беспроводных сетей.
2. Безопасность передачи данных в беспроводных технологиях.
3.Виды каналов. Уплотнение с частотным и временным разделением.
4.Беспроводные технологии. WiFi. Метод доступа CSMA/CA и проблема скрытого узла.
5.Построение сети Wifi в защищенном исполнении.
6.Обеспечение защиты стека протоколов Bluetooth.
7.Алгоритм WEP.
8.Алгоритмы WPA и WPA 2.

9. Методы анализа сетевого трафика. Идентификация уязвимостей сетевых приложений по косвенным признакам.
10. Методы прогнозирования сетевого трафика.