Филиал федерального государственного бюджетного образовательного учреждения высшего образования
«Национальный исследовательский университет «МЭИ»
в г. Смоленске

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБЕСПЕЧЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Направление подготовки: 10.04.01 «Информационная безопасность»

Магистерская программа «Безопасность автоматизированных систем»

Уровень высшего образования: магистратура

Нормативный срок обучения: 2 года

Форма обучения: очная

Год набора: 2022

Смоленск

Методические материалы составил:
канд. техн. наук, доцент кафедры
«Информационные технологии в экономике и управлении» _____ В.П. Фомченков

«28» _09_ 2021 г.

Заведующий кафедрой «Информационные технологии в экономике и управлении»:

_____ __д-р техн. наук, профессор_М.И. Дли__
подпись ФИО

«08» _10_ 2021 г.

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЛАБОРАТОРНЫХ РАБОТ ПО ДИСЦИПЛИНЕ

Лабораторные работы 8 шт. по 4 часа и 1 шт. – 2 часа:

Лабораторная работа 1. Мониторинг сетевых пакетов в IP-сетях.

Задания

1. Получить статистику по распределению сетевого трафика по протоколам.
2. Провести анализ сетевых блоков данных (сообщений и дейтаграмм) протоколов ICMP и UDP.
3. Выполнить мониторинг сессий протокола TCP.
4. Оформить отчет по проделанной работе.

Контрольные вопросы

1. Для каких целей проводится мониторинг трафика сети?
2. Основные возможности анализатора сетевого трафика Wireshark.
3. Как выполнить захват сетевого трафика рабочей станции?
4. Как можно определить принадлежность пакета узлу сети и протоколу?
5. Как получить общую статистику по захвату?
6. Как получить информацию о распределении трафика по протоколам?
7. Какой трафик потенциально опасен?
8. Назначение и структура сообщения протокола ICMP.
9. Сбор и анализ данных протокола ICMP по локальным узлам в программе Wireshark.
10. На сколько разделов разделено окно, в котором программа Wireshark отображает данные о сетевом трафике? Какая информация отображается в каждом разделе?
11. Назначение и структура дейтаграммы протокола UDP.
12. Сбор и анализ данных протокола UDP в программе Wireshark при обращении к серверу DNS.
13. Как используется протокол UDP при определении IP-адреса хоста по его доменному имени?
14. Каким образом в списке пакетов UDP можно найти запись стандартного запроса, к какому либо хосту? Какие сведения содержаться в этой строке.
15. Каким образом по сведениям о стандартном запросе можно определить IP и MAC-адреса компьютера-источника запроса, основного шлюза?
16. Какие сведения о стандартном DNS-запросе содержатся в окне User Datagram Protocol? В окне Doman Name System (query)?
17. Как изменяются роли источника и назначения в DNS-запросе и DNS-ответе?
18. Назначение и принцип работы протокола TCP.
19. Сбор и анализ данных протокола TCP в программе Wireshark.
20. Как называется процесс установления сеанса TCP между клиентом и сервером? Из каких этапов он состоит?
21. Каким образом в списке пакетов найти сегмент первого этапа трехэтапного квитирования? Как перейти на следующий сегмент трехэтапного квитирования?
22. Какие сведения о сегменте TCP содержатся в окне Transmission Control Protocol?

23. Каково назначение номера ISN (Initial Sequence Number - начальный номер последовательности) и как можно узнать его значение в просматриваемом сегменте TCP?

24. На основании какой информации из заголовка сегмента TCP можно сделать вывод о том, что соединение TCP настроено?

25. Каким образом в Wireshark можно отфильтровать пакеты соединения между двумя сокетами?

26. Как найти заключительный пакет TCP-сеанса?

Лабораторная работа 2. Исследование методов защиты сетевого трафика.

Задания

1. Определить конфигурацию сетевых узлов, провести анализ возможных сетевых угроз.

2. Провести мониторинг трафика сети.

3. Настроить сетевые экраны.

4. Оформить отчет по проделанной работе.

Контрольные вопросы

1. В чем состоят различия возможностей локального и сетевого входа в систему?
2. Настройка общего доступа к дискам и папкам компьютера.
3. Каким образом настроить удаленный доступ к рабочему столу?
4. С какими угрозами информационной безопасности связано предоставление удаленного доступа к рабочему столу.
5. Для каких целей проводится мониторинг трафика сети?
6. Основные возможности анализатора сетевого трафика.
7. Как выполнить захват сетевого трафика рабочей станции?
8. Как можно определить принадлежность пакета узлу сети и протоколу?
9. Как получить общую статистику по захвату?
10. Как получить информацию о распределении трафика по протоколам?
11. Какой трафик потенциально опасен?
12. Каким образом можно использовать протокол IPSec для блокирования ICMP-трафика?

Лабораторная работа 3. Проектирование защищенной виртуальной локальной сети.

Задания

1. В сети, построенной при выполнении лабораторной работы № 4, запустить используемую по умолчанию виртуальную сеть Vlan1.

2. Создать магистральную связь trunk между коммутаторами.

3. Сконфигурировать виртуальную сеть Vlan2 для компьютеров PC2 и PC4.

4. Сконфигурировать виртуальную сеть Vlan3 для компьютеров PC1 и PC3.

5. Оформить отчет по проделанной работе.

Контрольные вопросы

1. Дайте определение виртуальной локальной сети (VLAN).
2. Что нужно сделать, чтобы заработала используемая по умолчанию виртуальная локальная сеть vlan1?
3. Что из себя представляет магистральная связь (Trunk link), каково ее назначение?
4. Как создать магистральную связь trunk между коммутаторами?
5. Для каких целей используется режим связи доступа (Access link)?

6. Из каких этапов состоит процесс конфигурирования виртуальных локальных сетей?

7. Как сконфигурировать виртуальную сеть для компьютеров, входящих в эту виртуальную сеть?

Лабораторная работа 4. Защита канальной инфраструктуры сети.

Контрольные вопросы

1. Каковы цели и механизм атаки канального уровня типа MAC-flooding?
2. Каковы цели и механизм атаки канального уровня типа MAC-spoofing?
3. Какую защиту позволяет реализовать механизм port security?
4. Какие методы построения списков разрешенных MAC-адресов вы знаете?
5. В чем состоят настройки механизма port security на коммутаторе?
6. Описать назначение и принцип работы механизма port security sticky для статического метода формирования MAC-адресов.
7. Возможно ли применение механизма port security для защиты от атак типа ARP spoofing и DHCP spoofing?

Лабораторная работа 5. Проектирование защищенной корпоративной сети.

Задания

1. Собрать сеть, состоящую из двух коммутаторов, двух маршрутизаторов и четырех компьютеров, принадлежащих разным сетям 172.16.10.0 и 172.16.20.0.
2. Установить соединение между двумя маршрутизаторами по последовательному интерфейсу.
3. Настроить статические маршруты для передачи пакетов между сетями 172.16.10.0 и 172.16.20.0.
4. Настроить доступ из сети 172.16.10.0 к серверу сети 172.16.30.0.
5. Оформить отчет по проделанной работе.

Контрольные вопросы

1. Дайте определение маршрутизации, маршрута, таблицы маршрутов, маршрутизатора.
2. Как соединить маршрутизаторы по последовательному интерфейсу?
3. Как настраивается интерфейс маршрутизатора, подключенный к внешней сети?
4. Как настраивается интерфейс маршрутизатора, подключенный к внутренней сети?
5. Каким способы задания маршрутов вы знаете?
6. Как задать статический маршрут к определенной сети?
7. К каким интерфейсам маршрутизатора можно подключить конечное оборудование?

Лабораторная работа 6. Сетевая защита на базе межсетевых экранов.

Контрольные вопросы

1. Дайте определение межсетевого экрана (МЭ). Какие функции он выполняет?
2. Какие типы МЭ можно выделить по признаку охвата контролируемых потоков данных?
3. Какие типы МЭ можно выделить в зависимости от уровня, на котором происходит управление доступом?

4. Какие типы МЭ можно выделить в зависимости от реализации возможности отслеживания активных соединений?
5. Назовите дополнительные механизмы защиты и управления информационными потоками, реализуемые в МЭ?
6. Что собой представляет первичная фильтрация пакетов, и каким образом её можно реализовать на маршрутизаторе?
7. В чем состоит основная идея технологии CBAC?

Лабораторная работа 7. Управление трафиком межсетевого взаимодействия.

Задания

1. Для заданных исходных данных сети рассчитать подсети IPv4.
2. Построить топологию сети.
3. Назначить IP-адреса хостам сети. Проверить изолированность хостов в пределах подсетей.
4. Соединить подсети 0 и 1.
5. Настроить доступ к серверам сети и сетевым принтерам для подсетей 0 и 1.
6. Оформить отчет о проделанной работе.

Контрольные вопросы

1. Дайте определение маршрутизатора. Что такое шлюз?
2. Какова топология соединения подсетей с помощью маршрутизатора?
3. Какие настройки необходимо выполнить, чтобы хосты двух подсетей, соединенных через маршрутизатор, стали видеть друг друга?
4. Дайте определение списка управления доступом (ACL). Для каких целей он используется?
5. Какие существуют типы и способы создания ACL-списков?
6. Из каких этапов состоит создание ACL-списка?
7. Каков синтаксис именованного расширенного списка?
8. Каким образом созданный список прикрепляется к интерфейсу маршрутизатора?
9. Как просмотреть списки доступа маршрутизатора? Как удалить список доступа?
10. Что собой представляет шаблон маски правила списка? Для каких целей он используется? В чем его отличие от маски сети?
11. Что такое обратная маска? Каким образом её можно использовать для формирования шаблона маски правила списка?
12. Каково действие шаблонов host и any в правиле списка доступа?

Лабораторная работа 8. Конфигурирование безопасной сетевой инфраструктуры IoT.

Контрольные вопросы

1. Дайте определение таким понятиям как «Индустрия 4.0», «Промышленный Интернет», «Интернет вещей», «Умное предприятие», «Умный дом».
2. Какие функциональные уровни имеет архитектура IoT?
3. Что вы отнесете к сетевой инфраструктуре IoT?
4. Из каких устройств состоит интеллектуальная домашняя сеть?
5. Что необходимо сделать, чтобы подключить новое сетевое устройство в интеллектуальную домашнюю сеть? Какие способы подключения вы знаете?
6. Каким образом добавляется проводное устройство ввода-вывода?

7. Как добавить беспроводное устройство ввода-вывода?
8. Каким образом настаивается интеллектуальное сетевое устройство?
9. Какие механизмы обеспечивают защиту сетевой инфраструктуры IoT от несанкционированного доступа?

Лабораторная работа 9. Конфигурирование и настройка беспроводного канала связи в соответствии с требованиями информационной безопасности.

Задания

1. Создать модель локальной сети с подключением компьютера, ноутбука и смартфона через Wi-Fi маршрутизатор.
2. Настроить сеть маршрутизатора.
3. Настроить беспроводные каналы связи в соответствии с требованиями информационной безопасности.
4. Оформить отчет по проделанной работе.

Контрольные вопросы

1. Дайте определение беспроводной сети?
2. Какие основные стандарты WLAN определяет IEEE? Чем они отличаются?
3. Что означает аббревиатура Wi-Fi?
4. Какие стандарты WLAN обеспечивают скорости передачи больше 1 Гбит/с?
5. Какие рекомендации присутствуют в наборе протоколов 802.11x?
6. Какие устройства и каналы связи используются при построении беспроводных сетей?
7. Назовите основных разновидности использования Wi-Fi при построении локальных сетей.
8. Какие настройки беспроводного роутера для работы с сетью предусмотрены на вкладке «Network Setup»?
9. Какие настройки беспроводного роутера для работы с сетью предусмотрены на вкладке «Wireless»?
10. Какие настройки беспроводного роутера для работы с сетью предусмотрены на вкладке ««Wireless Security»»?
11. Как настроить компьютер на подключение в сеть через беспроводный роутер?
12. Как настроить ноутбук на подключение в сеть через беспроводный роутер?
13. Как настроить смартфон на подключение в сеть через беспроводный роутер?
14. Какие настройки необходимо выполнить в «сети провайдера»?
15. Что собой представляет технология NAT и для каких целей она используется?

Полный комплект методического обеспечения лабораторных работ по дисциплине «Информационная безопасность компьютерных сетей» в формате pdf-файлов расположен на кафедральных ресурсах в аудитории 210. Преподаватель, ведущий лабораторные работы, выдает раздаточный материал в начале семестра.

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ

Практические занятия 9 шт. по 2 часа.

Практическое занятие 1. Формирование политики информационной безопасности компании.

Вопросы для обсуждения

1. Дайте определение политики информационной безопасности.
2. Какие вы можете назвать принципы формирования политики информационной безопасности?
3. Назовите виды политики информационной безопасности?
4. Структура документа «Политика информационной безопасности».
5. Каково содержание раздела «Объекты защиты» документа «Политика информационной безопасности»?
6. Каково содержание раздела «Основные угрозы безопасности информации» документа «Политика информационной безопасности»?
7. Сформулируйте предложения по формированию политики информационной безопасности организации (по вариантам)?

Практическое занятие 2. Формирование политики безопасности компьютерных сетей.

Вопросы для обсуждения

1. Какие составляющие политики информационной безопасности компании следует отнести к безопасности компьютерных сетей?
2. Какова структура и содержание разделов документа «Политика межсетевого взаимодействия»?
3. Какова структура и содержание разделов документа «Политика использования VPN»?
4. Какова структура и содержание разделов документа «Правила работы в локальной вычислительной сети»?
5. Сформулируйте предложения по формированию политики безопасности компьютерной сети организации (по вариантам)?

Практическое занятие 3. Разработка требований по защите компьютерных сетей на основе стандартов информационной безопасности компьютерных сетей и сетей связи.

Вопросы для обсуждения

1. Что собой представляет система сертификации ГОСТ Р?
2. Что означают аббревиатуры ГОСТ Р ИСО и ГОСТ Р МЭК?
3. Является ли система сертификации ГОСТ Р обязательной?
4. В каких стандартах сформулированы требования, предъявляемые к информационной безопасности компьютерных сетей и сетей связи?
5. Что из себя представляет система сертификации ГОСТ Р?
6. В каких стандартах сформулированы требования, предъявляемые к информационной безопасности компьютерных сетей?
7. Каковы основные положения стандарта ГОСТ Р ИСО/МЭК 27033-1-2011?

8. Какие вопросы в области защиты компьютерных сетей регулирует стандарт ГОСТ Р ИСО/МЭК 27033-3-2014?

9. Нормативное регулирование обеспечения безопасности функционирования российского сегмента сети Интернет.

10. Сформулируйте требования по защите компьютерной сети организации (по вариантам)? Какими стандартами вы при этом руководствовались?

Практическое занятие 4. Разработка требований по защите промышленных компьютерных сетей на основе стандартов информационной безопасности промышленных систем и сетей.

Вопросы для обсуждения

1. Какими правовыми актами и нормативными документами регулируются вопросы обеспечения безопасности объектов критической инфраструктуры?
2. В каких стандартах сформулированы требования, предъявляемые к информационной безопасности промышленных систем автоматизации и промышленных сетей?
3. Какой российский стандарт описывает безопасность оборудования с ограниченными возможностями с точки зрения применения информационных технологий в домашних сетях?
4. Какие методы защиты каналов связи применяются на промышленных предприятиях?
5. Назовите основные положения стандарта ISA-99.
6. Назовите основные положения семейства стандартов IEC 62443.
7. В каких национальных стандартах РФ рассматриваются вопросы защиты промышленных систем и сетей?
8. Какие требования к составлению программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики предъявляет стандарт ГОСТ Р МЭК 62443-2-1-2015?
9. Каковы основные требования к системной безопасности ГОСТ Р МЭК 62443-3-3-2016?
10. Сформулируйте требования по защите промышленной сети организации (по вариантам)? Какими стандартами вы при этом руководствовались?

Практические занятия 5-6. Расчет адресного пространства IP-сети. Проектирование конфигурации IP-сети.

Вопросы для обсуждения

1. Какова структура IP-адреса версии IPv4.
2. Какие существуют классы IP-адресов?
3. Каким образом по IP-адресу сети можно определить класс сети?
4. Что такое широковещательный IP-адрес?
5. Что собой представляет маска сети, каково ее назначение?
6. Каковы стандартные маски подсетей для IP- адресов классов A, B, C как в десятичной нотации, так и в виде двоичных чисел?
7. Каким образом по IP-адресу и маске можно определить адрес сети? Первый и последний доступный IP-адреса сети? Широковещательный адрес сети?
8. Какие условия должны быть выполнены, чтобы компьютеры сети «видели» друг друга?

9. Какие существуют способы подключения к сетевому оборудованию для его конфигурирования? Какой способ предпочтительнее и почему? Что означает аббревиатура CLI?
10. Каким образом можно просмотреть текущую конфигурацию коммутатора?
11. Какие существуют виды конфигураций коммутатора? Где они хранятся?
12. Каким образом можно обезопасить себя от потери конфигурационной информации?
13. Какие способы изменения конфигурации коммутатора вы можете назвать?
14. Каким образом можно изменить имя коммутатора как хоста сети?
15. Как задаются IP-адреса и маски сети коммутаторам?
16. В какой секции конфигурационного файла хранится информация о IP-адресе и маске сети коммутатора?

Практические занятия: 7-8. Анализ безопасности трафика на примере протоколов TCP, UDP и ICMP.

Вопросы для обсуждения

1. Дайте определение DoS-атаки, что является её целью?
2. Назовите причины возникновения DoS-условия.
3. В чем состоит отличие DDoS-атаки?
4. Какие типы DoS-атак вы знаете?
5. Каковы особенности DoS-атаки типа TCP SYN Flood?
6. Каким образом можно смоделировать атаку TCP SYN Flood? Как её идентифицировать?
7. Каковы особенности DoS-атаки типа UDP Flood?
8. Каким образом можно смоделировать атаку UDP Flood? Как её идентифицировать?
9. Каковы особенности DoS-атаки типа ICMP Flood?
10. Каким образом можно смоделировать атаку ICMP Flood? Как её идентифицировать?
11. Какие выводы вы сделали по итогам практического занятия?

Практическое занятие 9. Безопасность сети на основе технологии сегментации трафика.

Вопросы для обсуждения

1. Что такое сегмент сети, подсеть?
2. По каким причинам целесообразно производить разбиение сети на подсети?
3. Какие методы сегментации сети вы знаете?
4. Каким образом осуществляется разбиение сети на подсети с помощью маски?
5. Как определить необходимое число разрядов на адрес подсети? На адрес хоста?
6. Какие меры необходимо предпринять, чтобы предотвратить несанкционированный доступ к ресурсам одной подсети из другой?
7. Как в сегментированной сети обеспечить прохождение трафика между подсетями?

Полный комплект методического обеспечения практических занятий по дисциплине «Информационная безопасность компьютерных сетей» в формате pdf-файлов

расположен на кафедральных ресурсах в аудитории 210. Преподаватель, ведущий практические занятия, выдает раздаточный материал перед занятиями.