ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Федеральное государственное образовательное бюджетное учреждение
высшего профессионального образования
Московский технический университет связи и информатики
Кафедра «Информационная безопасность и автоматизация»

А.Г. Симонян, Т.Б.К. Бен Режеб

Практикум

по дисциплине

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Москва 2015

План УМД на 2015/16 уч. г.

Практикум

по дисциплине

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Составители: Симонян А.Г., к.т.н., доцент (МТУСИ)
Бен Режеб Т.Б.К., ассистент (МТУСИ)

Рецензент: Андрюков А.А., к.т.н., доцент (МТУСИ)

Рекомендовано к изданию кафедрой «ИБиА»
Протокол № 2 от 28.10.2014 г.

Лабораторная работа №1

Изучение пакетов антивирусной защиты. Антивирус Касперского

Цель работы: Ознакомиться с распространенной программой антивирусной защиты Антивирус Касперского. Освоить методы работы с антивирусом, выполнить сравнительный анализ с антивирусным ПО Dr.Web.

1. Краткие теоретические сведения

1.1. Основные каналы распространения вирусов и других вредоносных программ

Для того чтобы создать эффективную систему антивирусной защиты компьютеров и корпоративных сетей, необходимо четко представлять себе, откуда грозит опасность. Вирусы находят самые разные каналы распространения, причем к старым способам постоянно добавляются новые.

- **Классические способы распространения.***Файловые вирусы* распространяются вместе с файлами программ в результате обмена носителями и программами, загрузки программ из локальной или глобальной сетей. *Загрузочные вирусы*может попасть в компьютер, когда пользователь забывает зараженную носитель подключенный к компьютеру, а затем перезагружают ОС (при этом разрешена загрузка с этого носителя). Загрузочный вирус также может быть занесен на компьютер вирусами других типов. *Макрокомандные вирусы* распространяются в результате обмена зараженными файлами офисных документов, такими как файлы MicrosoftWord, Excel, Access.

Если зараженный компьютер подключен к локальной сети, вирус легко может оказаться на дисках файл-серверов, а оттуда через каталоги, доступные для записи, попасть на все остальные компьютерные сети. Так начинается вирусная эпидемия. Системному администратору следует помнить, что вирус имеет в сети такие же права, что и пользователь, на компьютер которого этот вирус пробрался. Поэтому он может попасть во все сетевые каталоги, доступные пользователю. Если же вирус завелся на рабочей станции администратора сети, последствия могут быть очень тяжелые.

- **Электронная почта.**В настоящее время глобальная сеть Интернет является основным источником вирусов. Большое число заражения вирусами происходит при обмене письмами по электронной почте. Электронная почта служит одним из каналов распространения вирусов, так как вместе с сообщениями часто отправляются, например офисные документы.

Заражения вирусами могут осуществляться как непреднамеренно, так и по злому умыслу. Например, пользователь зараженного макровирусом редактора, сам того не подозревая, может рассылать зараженные письма адресатам, которые, в свою очередь, отправляют новые зараженные письма и т.д. С другой стороны, злоумышленник может преднамеренно послать по электронной почте вместе с вложенным файлом исполняемый модель вирусной или «троянской» программы, вредоносный программный сценарий Visual-Basic, зараженную или «троянскую» программу в виде заставки экрана монитора, словом — любой опасный программный код.

Распространители вирусов часто пользуются для маскировки тем фактом, что диалоговая оболочка MicrosoftWindows по умолчанию не отображает расширение зарегистрированных файлов. Например, FreeCreditCart.txt.exe, будет показан пользователю как FreeCreditCart.txt. если пользователь попытается открыть такой файл, будет запущена вредоносная программа.

Сообщения электронной почты часто приходят в виде документов HTML, которые могут включать ссылки на элементы управления ActiveX, апплеты Java и другие активные компоненты. Из-за ошибок в почтовых клиентах злоумышленники могут воспользоваться такими активными компонентами для внедрения вирусов и «троянских» программ на компьютер пользователя. При получении сообщения в формате HTML почтовый клиент показывает его содержимое в своем окне. Если сообщение содержит вредоносные активные компоненты, они сразу же запускаются и выполняют заложенные в них функции. Чаще всего таким способом распространяются «троянские» программы и черви.

- **«Троянские» Web-сайты.**Пользователи могут получить вирус или «троянскую» программу во время простой навигации по сайтам Интернета, посетив «троянский» Web-сайт. Ошибки в браузерах пользователей зачастую приводят к тому, что активные компоненты «троянских» Web-сайтов (элементы управления ActiveX и апплеты Java) внедряют на компьютеры пользователей вредоносные программы. Здесь используется тот же самый механизм, что и при получении сообщений электронной почты в формате HTML. Но заражение происходит незаметно: активные компоненты Web-страниц могут внешне никак себя не проявлять. Приглашение посетить «троянский» сайт пользователь может получить в обычном электронном письме.
- **Локальные сети.** Локальные сети также представляют собой путь быстрого заражения. Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в локальную сеть заражает один или несколько файлов на сервере. Пользователи при входе в эту сеть запускают зараженные файлы с сервера, и в результате вирус получает доступ на компьютеры пользователей.
- **Другие каналы распространения вредоносных программ.**Одним из серьезных каналов распространения вирусов являются пиратские копии программного обеспечения. Часто нелегальные копии на различных носителях содержат файлы, зараженные разнообразными типами вирусов. К источникам распространения вирусов следует отнести электронные конференции и файл-серверы FTP часто авторы вирусов выкладывают зараженные файлы сразу на несколько файл-серверов FTP или рассылают одновременно по нескольким электронным конференциям, причем зараженные файлы обычно маскируют под новые версии программных продуктов и даже антивирусов. Компьютеры, установленные в учебные заведения и интернет-кафе и работающие в режиме общего пользования, также могут легко оказаться источниками распространения вирусов. Если такой компьютер оказался зараженным вирусом с внешнего носителято файлы всех остальных пользователей, работающих на этом компьютере, могут оказаться зараженными.

По мере развития компьютерных технологий совершенствуются и компьютерные вирусы, приспосабливаясь к новым для себя сферам обитания. В любой момент может появиться компьютерный вирус, «троянская» программа или червь нового, неизвестного типа, либо известного типа, но нацеленного на новое компьютерное оборудование. Новые вирусы могут, использовать неизвестные или не существующие ранее каналы распространения, а также новые технологии внедрения в компьютерные системы. Чтобы исключить угрозу вирусного заражения, системный администратор корпоративной сети

должен не только внедрять методики антивирусной защиты, но и постоянно отслеживать новости в мире компьютерных вирусов.

1.2. Пакет антивирусной защиты Антивирус Касперского

Антивирус Касперского (англ. *Kaspersky Antivirus, KAV*) — антивирусное программное обеспечение, разрабатываемое Лабораторией Касперского. Предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, руткитов, adware, а также неизвестных угроз.

Антивирус Касперского предлагает следующие функции базовой защиты компьютера:

- Защита от вирусов, троянских программ и червей
- Защита от шпионских и рекламных программ
- Проверка файлов в автоматическом режиме и по требованию
- Проверка почтовых сообщений (для любых почтовых клиентов)
- Проверка интернет-трафика (для любых интернет-браузеров)
- Защита интернет-пейджеров (ICQ, MSN)
- Проактивная защита от новых вредоносных программ
- Проверка Java- и Visual Basic-скриптов
- Защита от скрытых и поврежденных ссылок
- Постоянная проверка файлов в автономном режиме
- Постоянная защита от фишинговых сайтов

2. Порядок выполнения лабораторной работы

1. Установить программу Антивирус Касперского. Обновить сигнатурные базы.
2. Ознакомиться с модулями, входящими в состав пакета Антивирус Касперского и зафиксировать основные настройки каждого из них.
3. Провести проверку на наличие угроз на компьютере и описать возможности, предоставляемые программой. Обнаружить хотя бы один вирус, описать его.
4. Выполнить сравнение антивирусных программ Антивирус Касперского и Dr. Web.

2.1. Обязательные иллюстрации к работе

1. Дать скриншоты окон установки антивируса Антивирус Касперского.

2. Привести скриншоты основных модулей, входящих в состав антивируса Антивирус Касперского, и основных его настроек.
3. Привести скриншот процесса сканирования с обнаружением вируса (или нескольких вирусов).

2.2. Пример выполнения практической части работы

На рисунках 2.1-2.6 лабораторной работы 2 приведены примеры полученных результатов при выполнении работы из антивируса Dr. Web

3. Контрольные вопросы

1. В чём заключаются классические методы распространения файловых вирусов?
2. В чём заключаются классические методы распространения загрузочных вирусов?
3. В чём заключаются классические методы распространения макрокомандных вирусов?
4. Каков основной принцип заражения по электронной почте?
5. Что зачастую приводит к внедрению вредоносных программ на компьютер через активные компоненты? К какому методу распространения вредоносного ПО это относится?
6. Существует ли жертва-посредник при заражении через локальную сеть между жертвой-источником и незаражёнными компьютерами?
7. Назовите другие каналы распространения вредоносных программ, кроме классических способов, электронной почты, сайтов, локальных сетей.
8. Перечислите методы и средства защиты информации.
9. Что такое маска вируса?
10. Каков основной недостаток метода сравнения с эталоном?
11. Какова методика работы эвристического анализа?
12. Антивирусный мониторинг, суть метода.
13. Чем отличается проактивная защита от эвристического анализа?
14. На чём основан метод обнаружения изменений?
15. Что такое программы с автоматическим дозвоном?
16. Против какого типа вирусов направлены встраиваемые в BIOS антивирусы?
17. Какие методы защиты используют программы-фаги?
18. Категории фагов, описание?
19. Методика работы программ-фагов?

20. Какие программы-фаги обеспечивают более надёжную защиту, почему?
21. Что такое CRC-сканеры?
22. Назовите плюсы и минусы программ-ревизоров.
23. На чём основана работа программ-ревизоров?
24. Что такое вирусоопасные ситуации, какие антивирусные программы реагируют на них?
25. Лечение поражённых файлов программами-блокировщиками.
26. Какова основная функция программ-блокировщиков? Каковы их минусы?
27. Чем программы-иммунизаторы отличаются от CRC-сканеров?
28. Сколько типов иммунизаторов можно выделить, чем они отличаются?
29. Перечислите критерии качества антивирусной программы.
30. Назовите основные компоненты антивирусного комплекса, который обеспечит приемлемую защиту от вирусов, не перегружая и затормаживая систему. Обращаем внимание, что вариантов может быть несколько.
31. К каким вирусам относятся не имеющие сигнатур?
32. Какие вирусы способны перехватить запросы операционной системы на чтение/запись заражённых файлов? С какой целью они это делают?
33. Могут ли макровирусы являться стелс-вирусами?
34. Каким образом вирус может «обмануть» операционную систему так, что она будет считать место его расположения как свободный сектор?
35. Вирусы, построенные для работы на какой платформе, обладают неограниченными потенциальными возможностями?

Лабораторная работа №2

Изучение межсетевых экранов. Zone Alarm.

Цель работы: Ознакомиться с принципами работы межсетевых экранов. Освоить методы работы с распространенной программой межсетевого экранирования Zone Alarm.

1. Краткие теоретические сведения

1.1. Сетевые экраны

Любой персональный компьютер (ПК), подключенный к Internet - потенциальная цель. Как только обнаружен открытый порт, хакер может взло-

мать ПК с помощью Троянской программы, spyware или злонамеренного червя.

Существуют несколько типов атак на удаленные системы, простейшей из которой является атака троянской програмой. Чаще всего пользователь получает ее по электронной почте или через icq, skype (пользователю посылают файл, обещая что-нибудь). Попавшись на эту уловку, пользователь запускает его и вирус поселяется на ПК.

Есть несколько средств борьбы с вирусами. Простейшим способом является использование антивируса, но часто бывает, что антивирусная программа не может определить или противодействовать вредоносной программе, например отправляющей с компьютера пользователя различными способами информацию или личные данные. В этом случае на помощь может придти *файервол* - программа, позволяющая ограничить доступ приложений к локальным и глобальным сетям. Ярким примером работы файервола может служить такой пример: на ПК появилась - программа, собирающая пароли и всевозможную информацию, а затем отсылающая ее компьютер злоумышленника. Но поскольку на компьютере установлена программа-файервол, то при попытке отосылки, файервол сообщает пользователю, что программа X пытается получить доступ к интернету. Пользователю остается только запретить такой доступ, а также попытаться вычислить злоумышленника по ip-адресу, на который была сделана попытка отправления данных. В качестве файервола можно на пример использовать, программу Zone Alarm.

1.2. Zone Alarm

Zone Alarm является брандмауэром, разработанным для использования на домашнем компьютере или рабочем месте в организации. На основании выбранного уровня безопасности, ZoneAlarm блокирует или разрешает установление соединений с локальной сетью и Интернетом, предупреждает о попытках установить несанкционированные соединения и предотвращает их.

Zone Alarm содержит следующие модули: файервол, контроллер работы программ, «замок» для программ, имеющих выход в Интернет, инструменты для установления уровней безопасности и зон безопасности, функцию MailSafe для проверки вложений к почтовым сообщениям.

В Zone Alarm предусмотрен режим работы Stealth, позволяющий пользователю оставаться невидимым из Сети; контроллер работы программ не позволит отправить информацию с ПК в Интернетбез ведома пользователя , даже, если пользователь «прозевал» троянскую программу; «замок» закроет

доступ посторонним к программам по команде или синхронно с началом работы скринсейвера и т.д.

Программа проста в установке. Сразу после установки она уже настроена. По умолчанию стоит высший уровень защищенности для интернета и средний для локальной сети. Третий уровень защиты просто спрячет компьютер в сети от различных атак, т.е. пользователь становится практически невидимым для хакеров и остальных «охотников за информацией». Zone Alarm позволяет заблокировать использование сервисов Windows (открытие на доступ папок и принтеров) и запрещает использование "неправильных" портов. Поскольку все программы, обращающиеся к сети, выполняются на том же компьютере, что и брандмауэр, появляется дополнительная возможность контроля, недоступная при использовании брандмауэров, установленных на других узлах в локальной сети. Т.е. Zone Alarm позволяет осуществлять контроль использования сети различными приложениями

С помощью Zone Alarm каждому приложению на компьютере можно разрешить или запретить обращаться к локальной сети и сети Интернет. О попытках нового приложения обратиться к сети пользователь извещается мгновенно, при этом ему предлагается выбор - разрешить доступ к сети или нет. Таким образом, при совместном использовании антивируса и фаервола у вредоносных программ практически не остается никаких шансов. Более того, можно заблокировать, например, попытки электронной регистрации каких-либо приложений, сохранив таким образом конфиденциальность, при работе с личной информацией. Все всплывающие сигнализаторы неопознанной сетевой активности будут понятны самым неопытным пользователям и предлагают всего два варианта - допустить соединение или отказаться от него. Как уже говорилось, Zone Alarm спросит, хочет ли пользователь, чтобы программа запомнила этот его выбор на будущее. Все без исключения обращения к сети протоколируются, даже если пользователь отключит вывод информационных сообщений о детектировании разрешенных соединений.

Настройка программы Zone Alarm. Настройка программы рассчитана даже на неопытного пользователя. Обычный брандмауэр работает на основе списка заданных пользователем правил - какие виды соединений с сетью являются допустимыми и как реагировать на недопустимые соединения. Это наиболее универсальный подход, позволяющий нейтрализовать большую часть сетевых атак, не затрудняя работу пользователю.

Даже опытные сетевые администраторы нередко допускают ошибки в конфигурировании, от чего резко снижается эффективность защиты.

В Zone Alarm используется достаточно простой подход - пользователь выбирает нужный ему «уровень безопасности» для работы в Интернет и для локальной сети. На основе этого выбора Zone Alarm самостоятельно определяет правила работы.

Разработчики данного файерволла также позаботились и об удобстве пользователя, позволяя простым перемещением движка-регулятора задавать любой из трех предустановленных уровней защиты, причем отдельно настраиваются две зоны - локальная сеть и интернет. Характеристики этих установок легко изменить, если вас в них что-то не устраивает.

Zone Alarm использует STEALTH-режим, который «прячет» все неиспользуемые порты, предотвращая ответы о текущем статусе порта, запрашиваемые, например, при сканировании ПК в поисках бреши. Несмотря на кажущуюся простоту программы, она способна блокировать множество потенциальных угроздля системы из интернета. При активизации экранной заставки или во время простоя ПК программа может при необходимости полностью закрывать выход в интернет, что повышает уровень безопасности забывчивых пользователей, особенно при постоянном подключении к Сети.

Для локальной зоны лучше установить среднюю степень защиты, чтобы сохранить сетевой доступ к открытым на доступ ресурсам сети - немаловажно, что при этом пользователь сам определяет, что относится к локальной зоне. К счастью, в этом случае не нужно вводить IP-адрес каждого ПК в локальной сети - достаточно задать диапазон адресов или маску.

Интересной особенностью программы является возможность блокирования доступа в интернет с использованием всего одной кнопки.

Применение брандмауэра. Zone Alarm реализует один из наиболее сложных и эффективных методов защиты от сетевых атак - брандмауэр. При этом ошибиться в его установке и настройке довольно трудно. Поэтому использование программы будет весьма эффективным для защиты от троянских программ и несанкционированного доступа к ресурсам. Стоит отметить, что блокирование несанкционированных соединений из сети происходит путем "проглатывания" пакетов. Это создает у атакующего иллюзию, что по данному IP-адресу вообще не существует компьютера, подключенного к сети.

Кроме того, Zone Alarm может осуществлять контроль содержимого, передаваемого через сетевые соединения. Это защита от вирусов, баннеров, всплывающих окошек, различного "мусора" и нежелательных активных элементов веб-страниц.

Опция MailSafe, предотвращающая запуск потенциально опасных скриптов, полученных по электронной почте. В отличие от антивирусных программ, эта функция не даст пользователю запустить новые, неизвестные антивирусам деструктивные скрипты.

Главной особенностью Zone Alarm является криптографическая подпись для тех приложений, которым пользователь доверяет выход в сеть. Эта функция делает невозможным маскировку одной программы под другую (как часто делают троянские программы). Например, "троян", попавший на компьютер, пытается получить доступ в сеть, но на ПК стоит файервол. Тогда он пытается сделать себе «липовое» разрешение на доступ в сеть, т.е. программа может «замаскироваться» под Internet Explorer и без проблем пользоваться интернет. Но при использовании Zone Alarm такого произойти не может из-за того, что программа подписывает ВСЕ приложения, получающие доступ в сеть. Проще говоря, каждая программа получает свой идентификационный номер, который, к тому же, шифруется.

2. Порядок выполнения лабораторной работы

1. Установить программу Zone Alarm. Проверить и при необходимости обновить.
2. Ознакомиться и зафиксировать основные настройки различных пунктов меню.
3. Настроить должным образом программу Zone Alarm.
4. Обнаружить хотя бы одну попытку доступа на компьютер, зафиксировать реакцию фаервола Zone Alarm.
5. Провести попытку войти на доступный сетевой ресурс и на другие компьютеры локальной сети, зафиксировать реакцию фаервола Zone Alarm.

Обязательные иллюстрации к работе

1. Дать скриншоты окон установки программы ZoneAlarm.
2. Привести скриншоты основных настроек программы ZoneAlarm.
3. Привести скриншот процесса обнаружения атаки
4. Привести скриншот процесса обнаружения попытки программ получить исходящее соединение.
5. Привести скриншот окна правил для программ

3. Контрольные вопросы.

1. Какие виды межсетевых экранов вы знаете?
2. В каких узлах локальной сети следует устанавливать межсетевые экраны ?
3. Почему при создании правил фильтрации в случае, если пользователем отмечен протокол IP, блокируется доступ к указанию порта ?
4. Работу каких протоколов нужно разрешить в фаерволе, если необходимо предоставить возможность выхода в Интернет ?
5. Работу каких протоколов нужно разрешить в фаерволе, если необходимо предоставить возможность работы с электронной почтой ?
6. Какая политика по умолчанию более надежна с точки зрения безопасности ?
7. Для каких атак могут быть использованы широковещательные сообщения?
8. Зачем нужен пакетный фильтр?
9. На каком уровне модели OSI/ISO работает пакетный фильтр?
10. Что такое трансляция адресов (NAT)? Зачем она используется?

Лабораторная работа №3

«Изучение программного пакета анализа сетевого трафика Wireshark»

Цель работы: Получение навыков анализа протоколов с помощью программного обеспечения Wireshark

1. Основные теоретические сведения

Анализ сетевого трафика является одной из задачей управления и администрирования компьютерной сетью. Анализатор трафика, или сниффер (от англ. to sniff - нюхать) - сетевой анализатор трафика, программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа сетевого трафика для всех узлов сети. Во время работы сниффера сетевой интерфейс переключается в режим прослушивания, что и позволяет ему получать пакеты, адресованные другим интерфейсам в сети.
Перехват трафика может осуществляться:

- обычным "прослушиванием" сети, что эффективно при использовании в сегменте концентраторов (хабов), но малоэффективно при использо-

вании коммутаторов (свитчей), поскольку на сниффер попадают лишь отдельные фреймы;
- подключением сниффера в разрыв канала;
- ответвлением (программным или аппаратным) трафика и направлением его копии на сниффер;
- через анализ побочных электромагнитных излучений и восстановление, таким образом, прослушиваемого трафика;
- через атаку на канальном (MAC) или сетевом (IP) уровне, приводящую к перенаправлению трафика на сниффер с последующим возвращением трафика в надлежащий адрес.

В начале 1990-х снифферы широко применялись хакерами для захвата пользовательских логинов и паролей, которые в ряде протоколов передаются в незашифрованном или слабо зашифрованном виде, а использование хабов позволяло захватывать трафик в больших сегментах сети практически без риска быть обнаруженным.

В наше время снифферы находят применение в сетевом администрировании. Анализ прошедшего через сниффер трафика позволяет:

- Обнаружить паразитный, вирусный и закольцованный трафик, наличие которого увеличивает загрузку сетевого оборудования и каналов связи. Однако снифферы для этих целей являются не очень эффективными. Для этих целей используют сбор разнообразной статистики серверами и активным сетевым оборудованием.
- Выявить в сети вредоносное и несанкционированное ПО, например, сетевые сканеры, флудеры, трояны, клиенты пиринговых сетей и другие (для этого используют специализированные снифферы - мониторы сетевой активности).
- Локализовать неисправность сети или ошибку конфигурации сетевых агентов, что особенно важно при работе сетевых администраторов.

Одним из простых и свободно распространяемых программных продуктов этого класса является Wireshark. Программа распространяется под свободной лицензией GNU GPL. Существуют версии для большинства типов UNIX, в том числе GNU/Linux, FreeBSD, OpenBSD, Mac OS X, а также для Windows (http://www.wireshark.org).

Как и большинство программ такого класса, Wireshark содержит следующие основные компоненты: фильтр захвата, буфер кадров, декодер протоколов, фильтр отображения захваченных кадров и модуль статистики с элементами экспертной системы. К несомненным достоинствам Wireshark относятся:

- наличие реализаций для Unix и Windows;
- наличие исходного кода программы;
- возможность захвата трафика в сетевых сегментах различных базовых технологий;
- возможность анализа огромного числа протоколов (более 700);
- возможность экспорта/импорта файлов данных в формат распространенных анализаторов (несколько десятков форматов);
- мощная и удобная система поиска и фильтрации информации в буфере пакетов;
- наличие элементов экспертной системы;
- возможность сохранения на диск выделенного фрагмента пакета;
- наличие полезных утилит командной строки для осуществления захвата трафика и обработки сохраненных файлов.

2. Порядок выполнения лабораторной работы

1. Установите программное обеспечение Wireshark и библиотеку WinPCap. Инсталлятор требуемой версии библиотеки WinPCap содержится в дистрибутиве Wireshark.
2. Запустите установленное ПО Wireshark.
3. Выполните команду меню«Capture - Options», после чего выберите в открывшемся окне сетевое подключение компьютера для анализа трафика.
4. Уберите маркер напротив опции «Capture packets in promiscuous mode» для захвата только пакетов адресованных вашему компьютеру (кадры с широковещательным адресом также будут захватываться). В таком режиме работы число захваченных пакетов будет существенно меньше, что облегчит выполнение заданий.

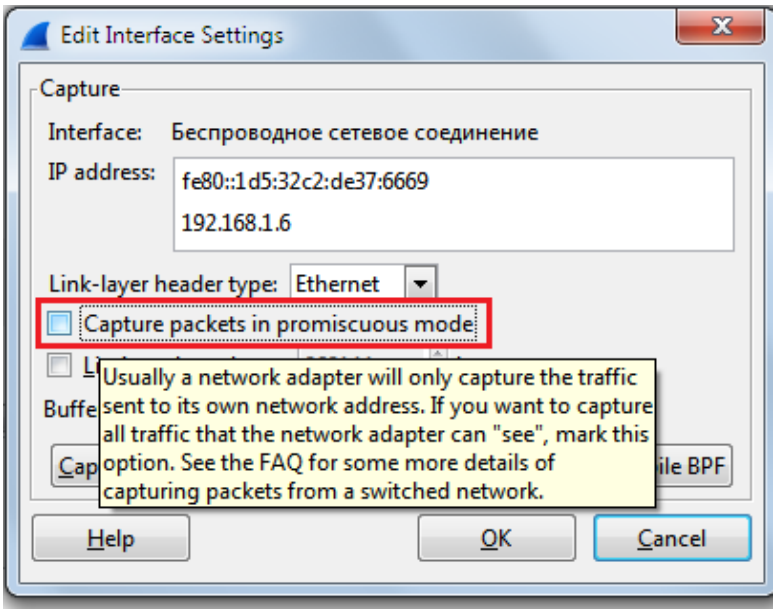


Рис. 5.1. Окно настроек интерфейсов для захвата трафика.

5. Выполните в командной строке Windows команду «arp –d» для очистки кэша протокола ARP.
6. Запустите процесс захвата сетевого трафика, нажав кнопку «Capture».
7. В командной строке выполните команду ping 8.8.8.8 (в качестве параметра команды можно использовать IP-адрес сервера). По завершении команды Ping остановите захват сетевого трафика, нажав кнопку «Stop» в рабочем окне Wireshark.
8. Для отображения только ICMP-пакетов в строке ввода «Filter» введите значение «icmp» и нажмите на кнопку «Apply».



Рис. 5.2. Строка ввода фильтра.

9. Используйте значение фильтра «frame.number> 20» и отобразите скриншотом полученный результат.
10. Выясните в чем разница между значениями фильтров «!(ip.addr == X.X.X.X)» и «ip.addr != X.X.X.X».
11. Отобразите только ICMP-запросы. Для этого выберите ICMP-пакет и, нажав на строку Type правой кнопкой, примените поле Type как фильтр.

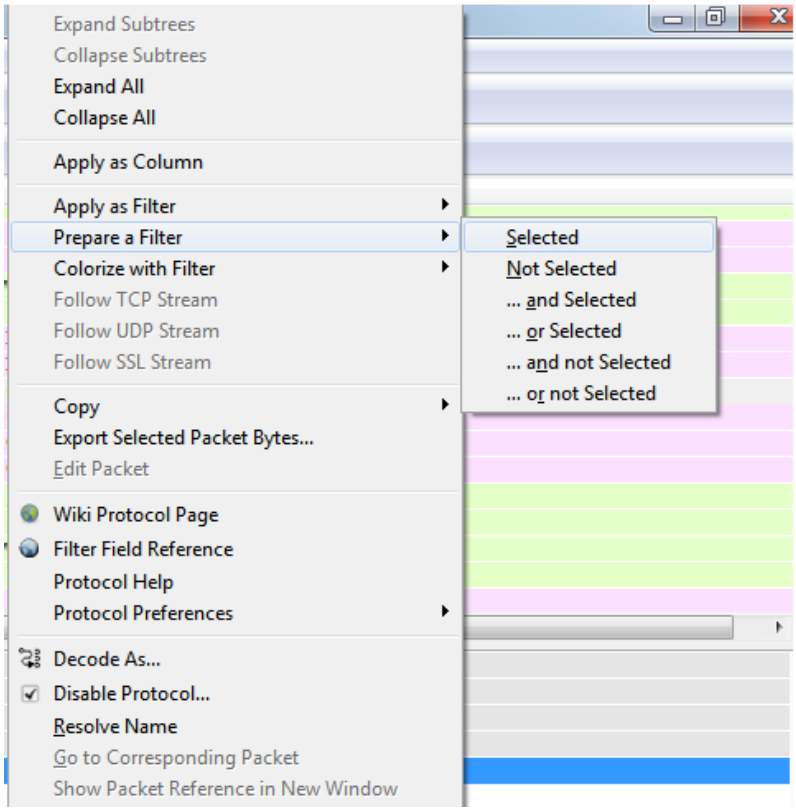


Рис. 5.3. Опция создания фильтра.

12. Отобразите все кадры переданные узлом, исключая ICMP-пакеты. Для этого в строке фильтра введите значение «!icmp» и примените фильтр.
13. Найдите все пакеты с помощью выражения фильтрации «icmp.type==0»

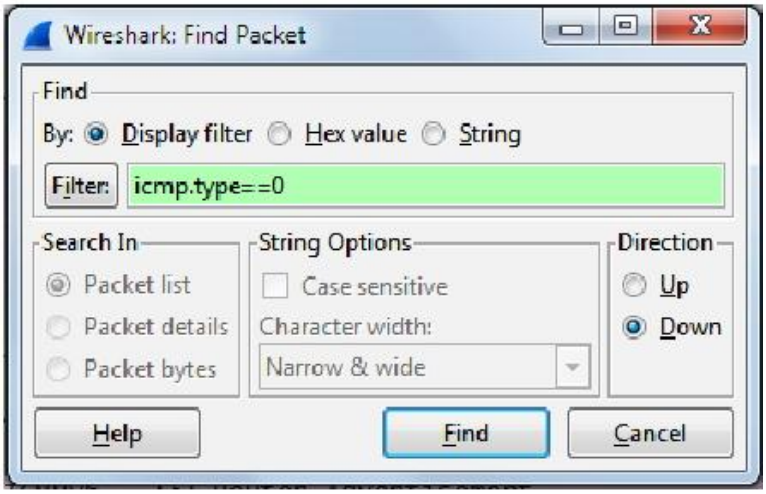


Рис. 5.4. Окно поиска пакета.

После данного действия в Wireshark выделится найденная строка

14. Найдите все пакеты по строке «reply» в строке общей информации о пакете.

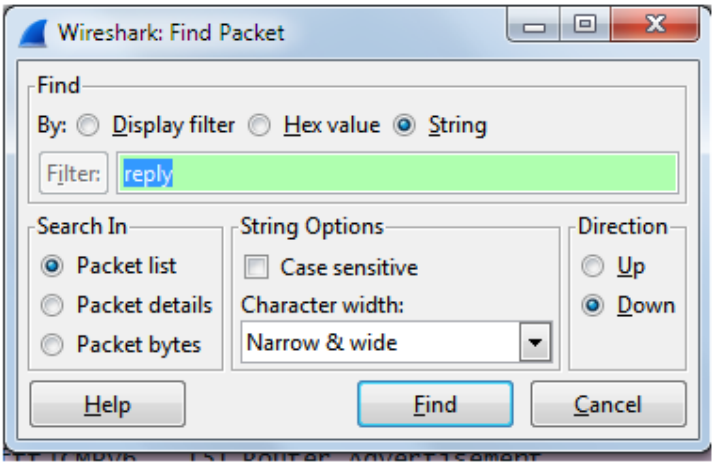


Рис. 5.5. Окно поиска по пакетам

15. Найдите все пакеты по строке «reply» в панели декодера протоколов.

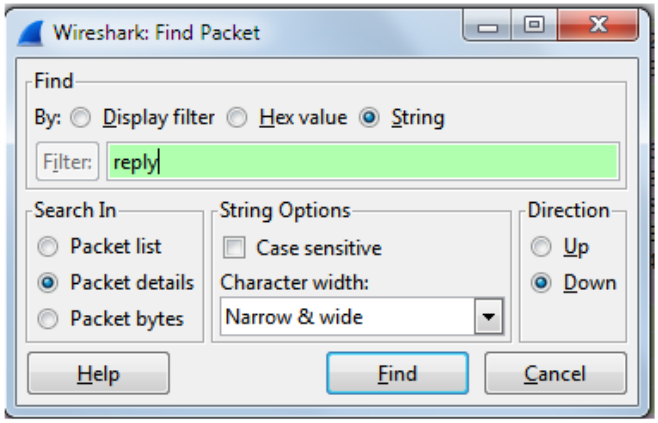


Рис. 5.6. Окно поиска по содержимому пакета

16. Проанализируйте результаты поиска в пунктах 14-15.
17. Пометьте первый и последний пакет, относящийся к команде Ping. Для этого примените фильтр «icmp», выбрав первый пакет правой кнопкой мыши и выбрав пункт «MarkPacket». Аналогичные действия необходимо произвести с последним пакетом.
18. Сохраните все захваченные кадры в файле с названием «arp-ping». Дляэтоговыберитепункт «File» — «Export Specified Packets…».
19. Сохраните в файле с именем «Ping» только трафик команды Ping. Для этого примените фильтр «icmp» и сохраните только отображаемые пакеты.
20. Сохраните первый пакет из типов пакетов ICMP-запрос. Для этого выберитеданный пакет и нажмите «File» — «Export Packet Dissection» — «as Plain_Text file».

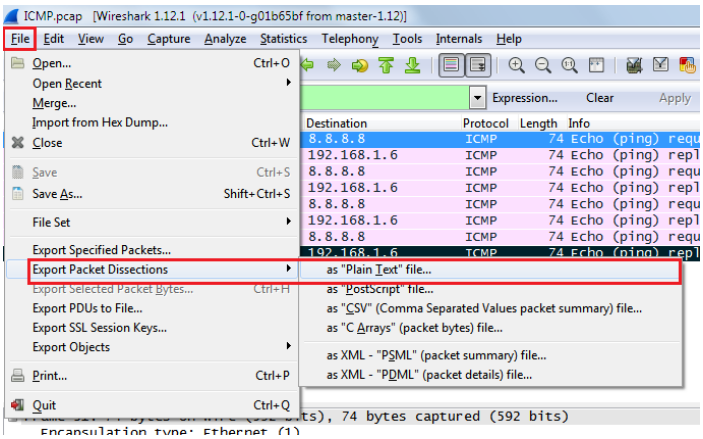


Рис. 5.7. Сохранение файла отчета

Далее введите название файла и выберите нужные параметры.

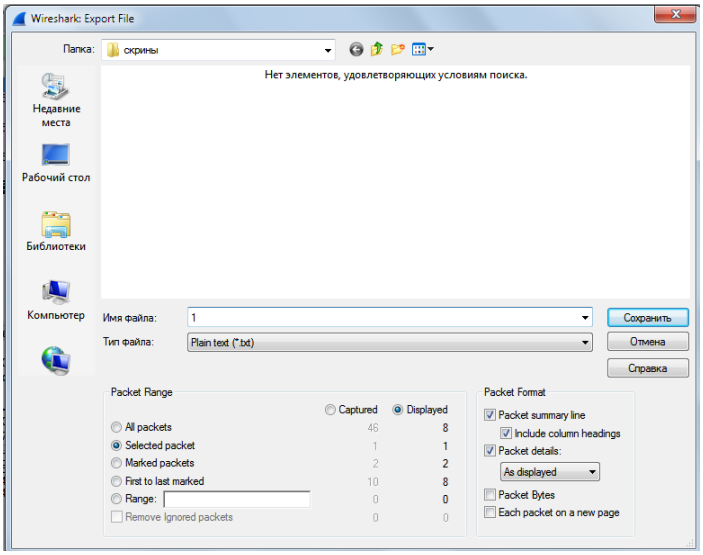


Рис. 5.8. Окно сохранения файла отчета

Выясните, как взаимосвязаны выбранные вами пакеты.

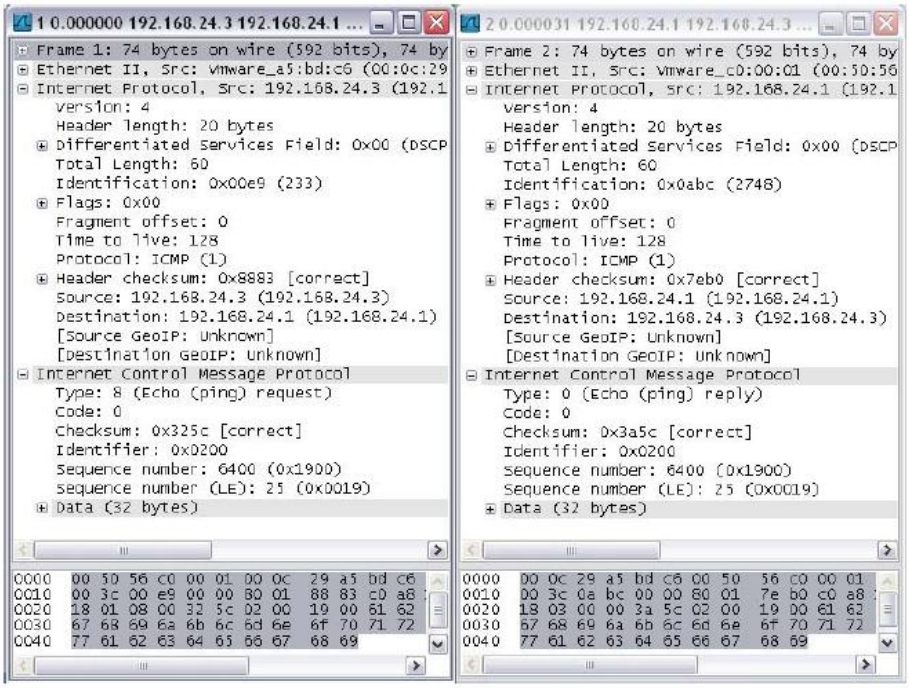


Рис. 5.9. Иллюстрация выбранных пакетов в отдельном окне

21. Отключите анализ заголовка IP. Для этого нажмите «Analyze» — «Enableprotocols…», снимите галочку напротив пункта IPv4 и нажмите на кнопку «Apply».

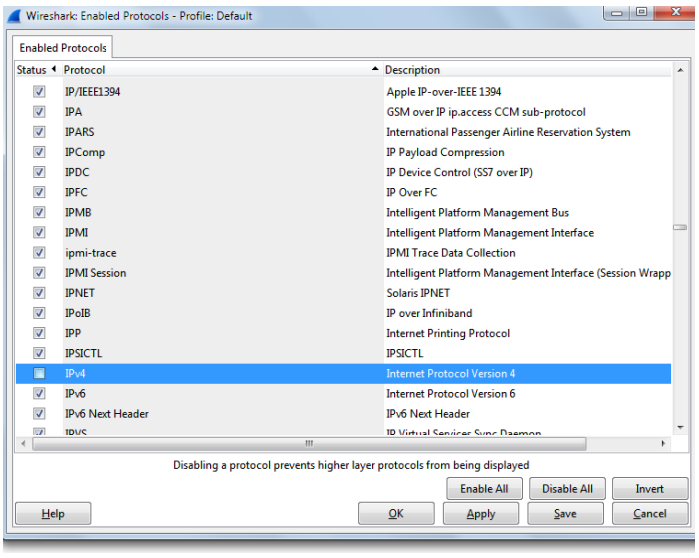


Рис. 5.10. Опции настройки протоколов

22. Отобразите два пакета ARP (reply и request) и ответьте на контрольные вопросы.

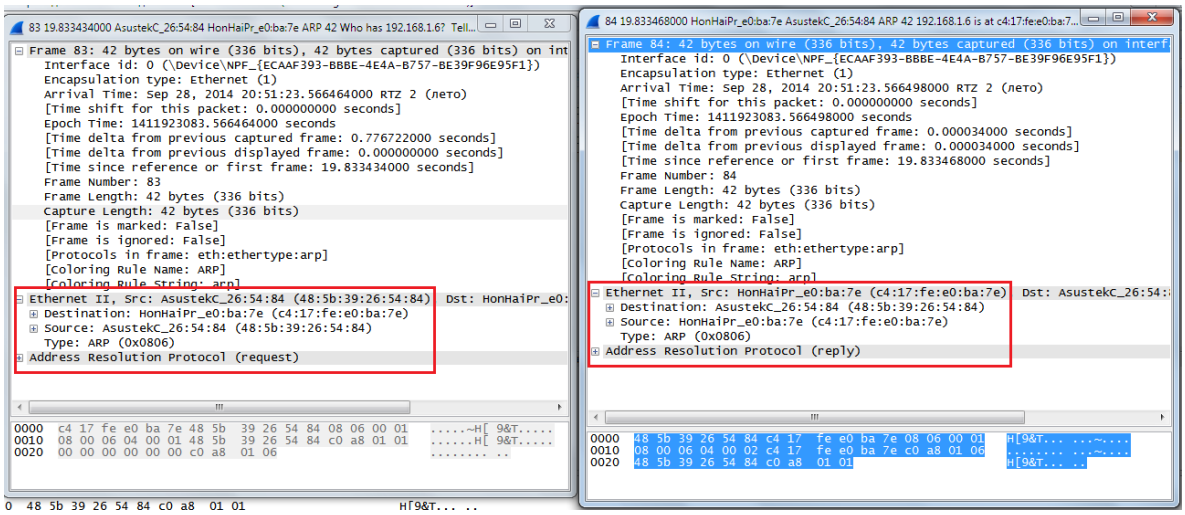


Рис. 5.11. Сравнение пакетов ответа и запроса.

3. Контрольные вопросы

1. Какое значение поля «тип протокола» в кадре Ethernet указывает на протокол ARP?
2. По какому MAC-адресу отправлен запрос ARP?
3. По какому MAC-адресу отправлен ответ ARP?
4. Каким полем идентифицируются запрос и ответ ARP?
5. В каких полях заголовка ARP передан запрос вашего узла?
6. В каких полях заголовка ARP передан ответ вашему узлу?

Лабораторная работа №6
«Изучение системы обнаружения атак Snort»

Цель работы: Получение навыков работы с программой Snort, изучение принципов создания правил обработки трафика

1. Основные сведения о системе обнаружения атак Snort

Snort — бесплатная система обнаружения атак с открытым кодом, разработанная Мартином Рошем. Программное обеспечение Snort является сетевой системой обнаружения атак, основанной на сигнатурном анализе. Сигнатуры атак описываются при помощи правил, позволяющих выявлять интересующую администратора информацию в полях заголовков и содержимом передаваемых по сети пакетов. Также в Snortреализовано несколько препроцессоров, выполняющих более сложные операции по анализу трафика.

Взаимодействие с ПО Snortпроисходит с помощью команд, составленных по определенным правилам. Правила составления команд состоят из двух частей: заголовка и набора атрибутов. Заголовок, в свою очередь, состоит из:

1. Указания действия, которое необходимо выполнить (alert, log, pass и др.).
   Действие alertпозволяет создать предупреждающее событие и сохранить содержимое пакета для дальнейшего анализа. Действие logпозволяет сохранить содержимое пакета для дальнейшего анализа. Действие passиспользуется для игнорирования определенных пакетов.
2. Протокола (tcp, udp, icmp, ip).
3. IP-адреса и маски подсети источника и приемника информации, а также информации о портах источника и приемника.

Запуск и дальнейшая работа с ПО Snortосуществляется с помощью командной строки. В таблице 1 приведен список основных флагов для запуска программы.

Таблица 1. Список параметров СОА Snort

Параметр	Описание
-c <rules>	Использовать файл правил<rules>

-E	Добавлять предупреждения в журнал регистрации событий Windows (не создавая log-файла)
-h <hn>	Задать домашнюю сеть (homenetwork)<hn>
-i <if>	Подключиться к сетевому интерфейсу номер <if>
-I	Добавлять к предупреждению наименование интерфейса
-K <mode>	Режим регистрации предупреждений: pcap (по умолчанию) — в двоичном формате, ascii— в текстовом формате, none— без регистрации
-l <ld>	Сохранять результаты регистрации в каталог <ld>
-L <file>	Сохранять результаты регистрации в указанный файл формата tcpdump
-n <cnt>	Завершить работу программы после получения <cnt> пакетов
-N	Не сохранять в файлах регистрации содержимого пакетов
-p	Анализировать только пакеты, отправленные на локальный адрес, и широковещательные пакеты
-r <tf>	Прочитать и обработать файл <tf>, записанный в формате tcpdump
-S <n=v>	Установить значение переменной nфайла правил, равной v
-U	Записывать временные метки в универсальном скоординированном времени (UTC)
-v	Отображать на экране заголовки всех перехваченных пакетов
-V	Показать версию Snort
-W	Показать доступные сетевые интерфейсы
-X	Сохранять в файле журнала регистрации событий содержимое перехваченных пакетов в «сыром» виде, начиная с канального уровня модели OSI
-y	Добавить месяц, день и год в отображаемые и сохраняемые временные отметки
-?	Показать помощь по параметрам командной строки

Для запуска Snort необходимо выполнить следующую команду:

```
snort –i<интерфейс> -c<файл конфигурации> -
l<расположение log-файла>
```

где

<интерфейс> — порядковый номер интерфейса, полученный с помощью команды «snort -W»;

<файл конфигурации> — путь к файлу, в котором хранятся правила;

<расположение log-файла> — путь к папке, где находится log-файл программы.

Пример команды:

```
snort -i 3 -c ../etc/my.conf -l ../log
```

Примечание: при записи команд используются именно черты «/» для указания пути файла.

Таблица 2. Примеры правил COA Snort

№	Описание	Правило
1	Обнаружение входящих эхо-запросов	alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg: "Incoming ECHO REQUEST"; itype: 8;)
2	Обнаружение исходящих эхо-запросов	alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg: "Outgoing ECHO REPLY"; itype: 0;)
3	Обнаружение больших ICMP-пакетов	alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg: "Incoming large ICMP packet"; dsize: >800;)
4	DoS-атака Winnuke	alert tcp $EXTERNAL_NET any -> $HOME_NET 135:139 (msg: "DoS Win-nuke attack"; flags: U+;)
5	Запрос на подключение к 139 порту (SMB)из внешней сети	alert tcp $EXTERNAL_NET any -> $HOME_NET 139 (msg: "NETBIOS SMB IPC$ share access"; flags: A+; content: "|00|"; offset: 0; depth: 1; content: "|FF|SMB|75|"; offset: 4; depth: 5; content: "\\IPC$|00|"; nocase;)

6	Обнаружение сканирования портов методом NULL	`alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"NULL port scanning"; flags:!FSRPAU;)`
7	Обнаружение сканирования портов методом XMAS	`alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"XMAS port scanning"; flags:FPU+;)`

2. Порядок выполнения лабораторной работы

1. Установите COA Snort
2. Откройте окно командной строки Windows и с помощью команды «cd» перейдите в директорию, где установлено ПО Snort.
3. Перейдите в папку bin.
4. Отобразите список доступных сетевых интерфейсов командой:
   `snort -W`

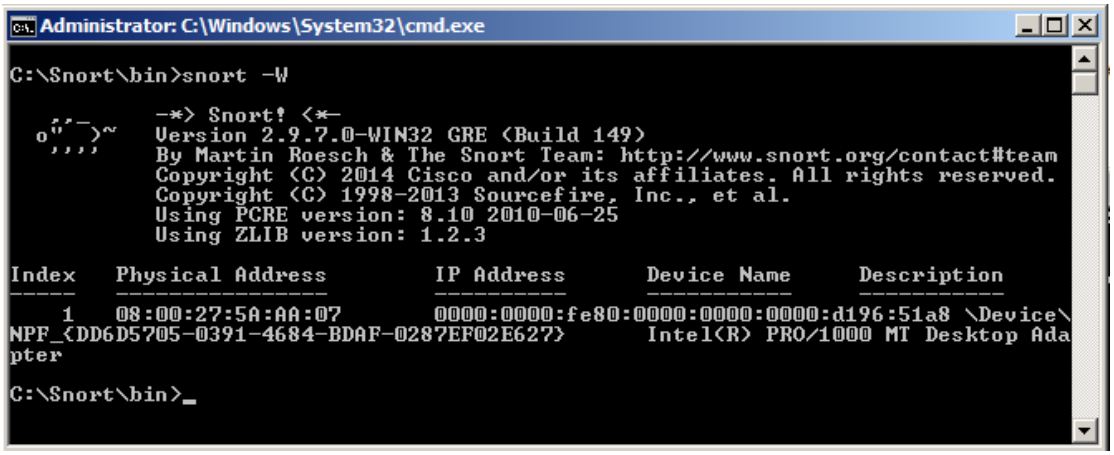


Рис. 6.1. Отображение сетевых интерфейсов.

5. Запустите Snort на выбранном интерфейсе в режиме анализатора пакетов, указав параметры завершения работы программы после приема третьего пакета.
   `snort -v -i 1 -n 3`
6. Произведите отправку или прием пакетов. Например, откройте браузер или выполнить в командной строке эхо-запрос на любой узел сети командой «ping».

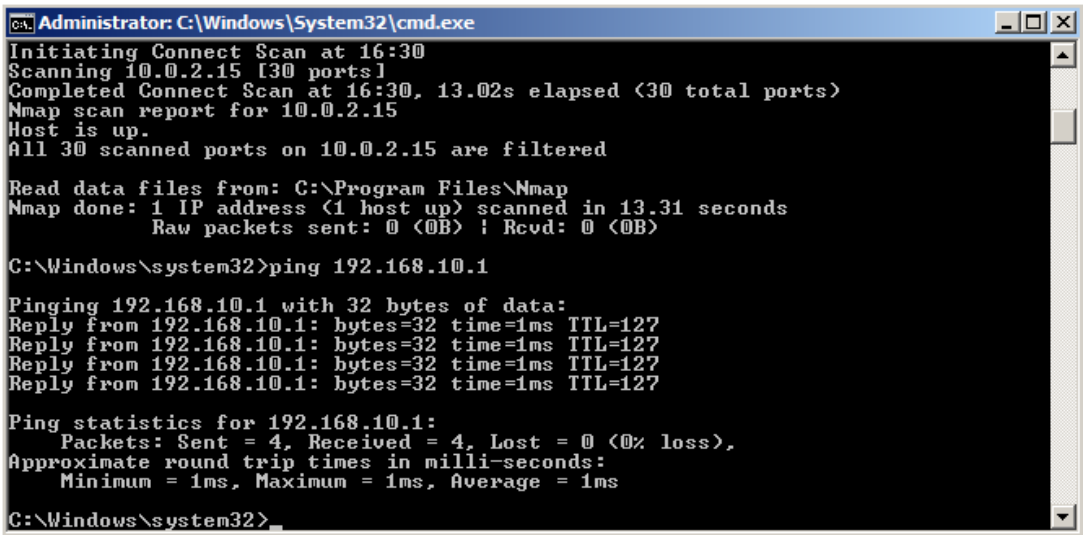


Рис. 6.2. Генерация эхо-запроса.

7. Убедитесь в том, что передаваемые (принимаемые) пакеты перехватываются и отображаются в окне программы Snort.
8. Создайте в каталоге Snort\etc\ файл с именем «my»и расширением .conf, содержащий следующие строки:
   ```
   varHOME_NET<IP-адрес вашего компьютера>
   var EXTERNAL_NET !$HOME_NET
   ```
9. Добавьте в созданный файл «my.conf» одно из перечисленных в таблице 2 правил, например, правило обнаружение входящих эхо-запросов.
   ```
   alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg: "Incoming ECHO request"; sid: 1; itype: 8;)
   ```
   В случае если в файле конфигурации указано несколько правил, необходимо указать параметр «sid», указывающий на порядок применения правила.
10. Запустите СОА Snort, указав необходимый сетевой интерфейс, файл конфигурации, а также расположение log-файла программы.
    ```
    snort –i <интерфейс> -c ../etc/my.conf –l ../log
    ```
11. Выполните несколько эхо-запросов с помощью другого компьютера сети.
    ```
    ping<IP-адрес вашего компьютера>
    ```
12. Зафиксируйте обнаружение icmp-пакетов программой Snort.
13. Дополните файл «my.conf» строками:
    ```
    preprocessor flow: stats_interval 0 hash 2
    preprocessor sfportscan: proto { all } scan_type { all } sense_level { medium } logfile { portscan.log }
    ```

для настройки препроцессора sfPortscan.

14. Используйте утилиту nmap для проверки обнаружения сканирования портов программой Snort. Используйте следующие команды для запуска сканирования:
    `nmap <IP-адрес вашего компьютера> -v –sT –p <диапазон портов>` — для сканирования методом с полным циклом подключения (метод Connect);

    `nmap <IP-адрес вашего компьютера> -v –sS –p <диапазон портов>` — для сканирования с неполным циклом подключения (метод SYN);

    `nmap <IP-адрес вашего компьютера> -v –sN –p <диапазон портов>` — для сканирования при помощи TCP-пакета со сброшенными флагами (метод NULL);
    `nmap <IP-адрес вашего компьютера> -v –sX –p <диапазон портов>` — для сканирования при помощи TCP-пакета со всеми установленными флагами (метод XMAS);
15. Выясните, какие методы сканирования позволяют практически выявлять наличие открытых портов.

Лабораторная работа №7

«Создание защищенной компьютерной сети»

Цель работы: Получение навыков защиты компьютерной сети с помощью операционной системы Cisco IOS

1. Установка и начальная настройка эмулятора

Так как актуальная версия эмулятора (0.8.7) распространяется и является переносной (Portable) версией, то для немедленного использования программы достаточно скачать её с официального сайта: http://www.gns3.net/download/ и запустить от имени администратора.

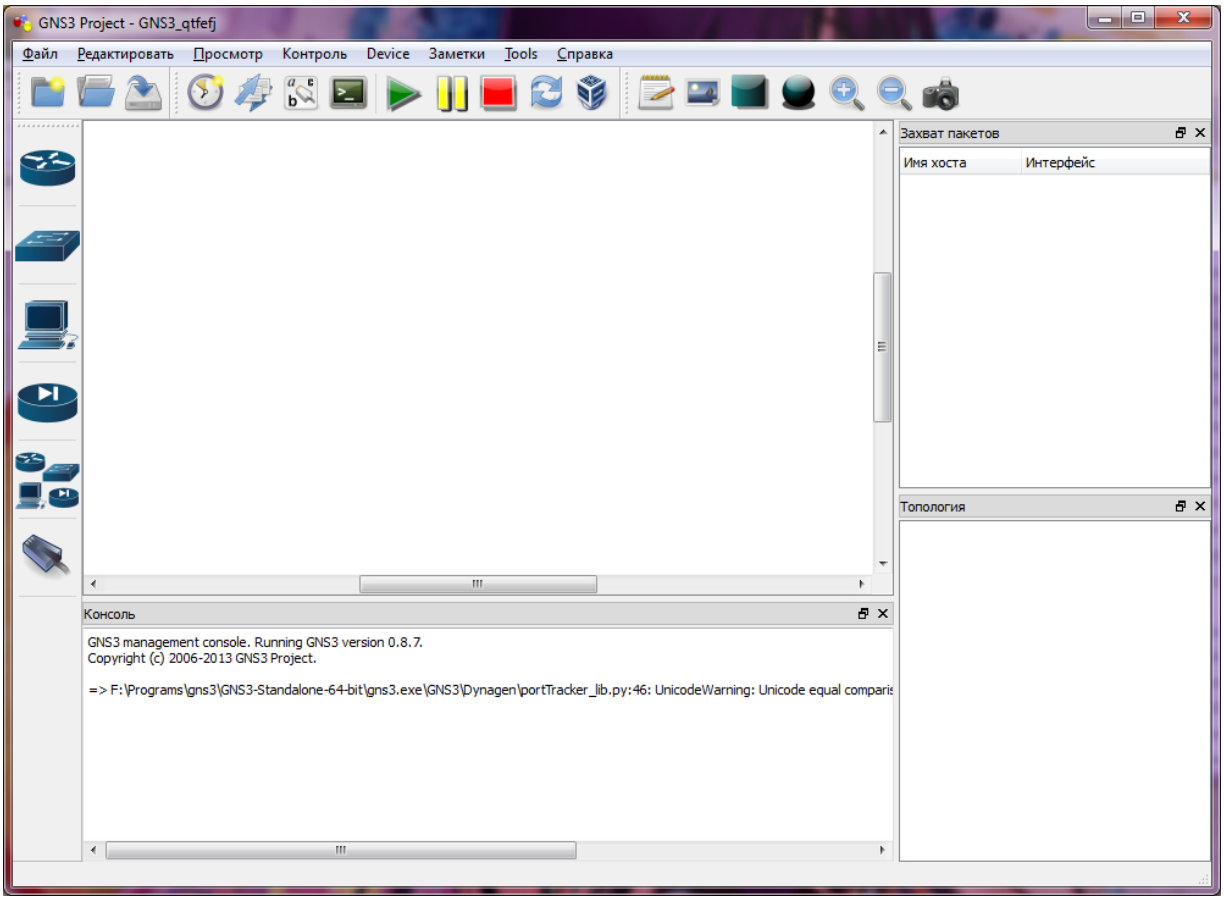


Рис. 7.1. Главное окно программы

Для начальной настройки эмулятора необходимо пройти по вкладке «Редактировать - Настройки» (Edit ->Preferences), где во вкладке «Основное(General)» и выбрать язык, а также указать папку проекта и папку для образов. Далее, во вкладке «Dynamips» указать путь для запуска и рабочую папку. Затем, перейдя по вкладке «Образы IOS и гипервизоры», указываем файл образа, платформу и модель для последующей работы с маршрутизатором (рис. 7.2). В данном примере будет рассматриваться модель маршрутизатора Cisco c7200.

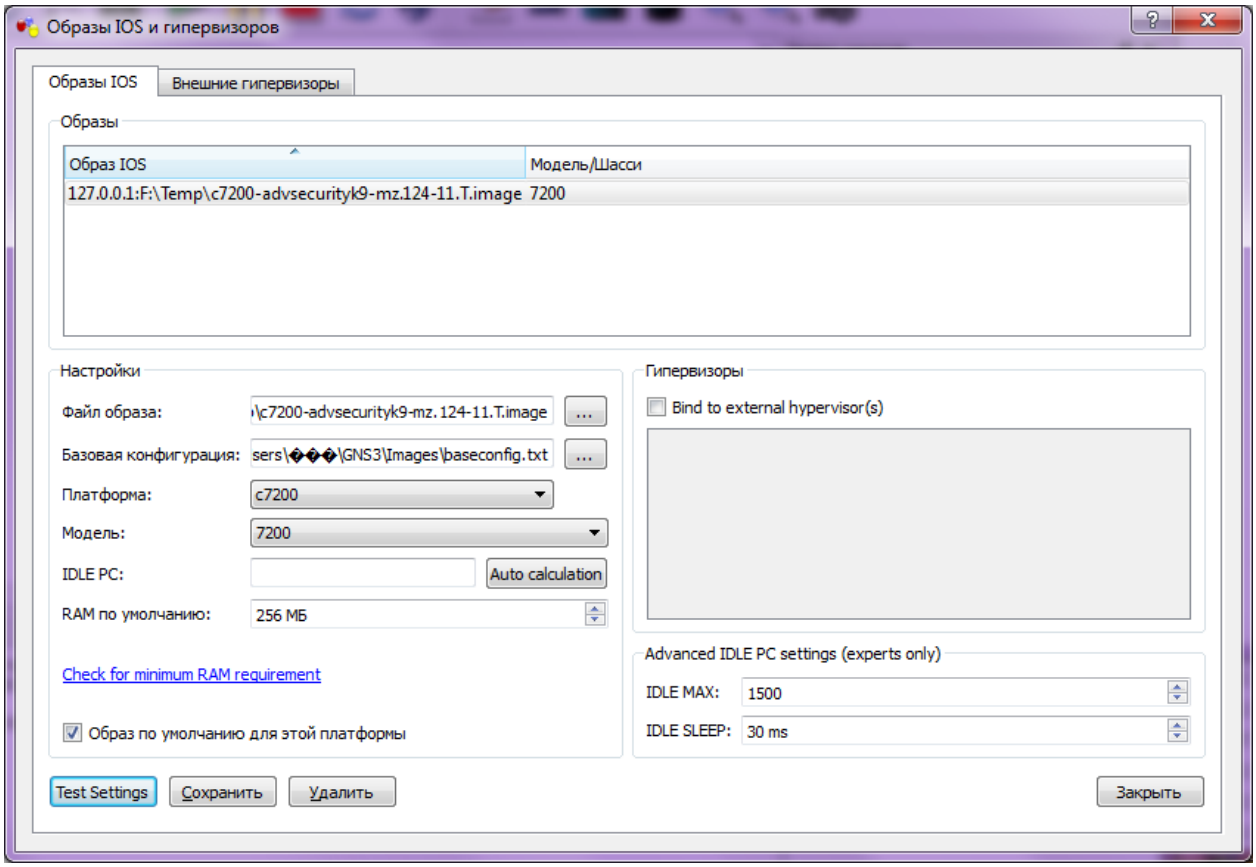


Рис. 7.2. Окно «Образы IOS и гипервизоров»

2. Работа с маршрутизатором

Существует множество контекстов конфигурирования при работе с консолью маршрутизатора. Ниже перечислены встречающиеся наиболее часто:

- router (config)# - глобальный
- router (config-if)# - интерфейса
- router (config-router)# - динамической маршрутизации
- router (config-line)# - терминальной линии

Команды для перехода в данные контексты будут показаны дальше непосредственно на примере. Выход из контекстов производится командой exit.

Имена сетевых интерфейсов также могут быть сокращены, например, вместо «ethernet 1/0» достаточно написать «e1/0».

2.1. Начальная конфигурация маршрутизатора

Для начала необходимо установить имя маршрутизатора. Для этого необходимо перейти из пользовательского режима в режим администратора, открываемый командой enable, а затем в глобальный режим:

router# config terminal (config ter всокращенномварианте)

router(config)#hostname <*имя_маршрутизатора*>

Далее необходимо установить пароль администратора (пароль будет требоваться для выполнения команды enable):

lab1(config)#enable secret <пароль>

Отключить обращения в DNS (в том случае, если DNS-сервер не используется в лабораторной сети):

lab1(config)#no ip domain-lookup

Сконфигурировать консоль и виртуальные терминалы: отключить таймер неактивности, отключить интерпретацию неизвестных команд как указаний открыть сеанс Telnet, включить режим синхронной регистрации:

lab1(config)#line con 0
lab1(config-line)#exec-timeout 0 0
lab1(config-line)#transport preferred none
lab1(config-line)#logging synchronous

Обратите внимание, что по умолчанию маршрутизатор выводит сообщения на консоль поверх ввода оператора, и чтобы продолжить ввод команды, оператор должен помнить, в каком месте его прервали. После указания logging synchronous после каждого выведенного сообщения маршрутизатор будет заново выводить часть команды, уже введенной оператором к моменту появления сообщения, и оператор может легко продолжить ввод.

Виртуальный терминал назначается оператору, подключившемуся к маршрутизатору по протоколу Telnet. На доступ через виртуальный терминал следует назначить пароль. Это делается командами:

lab1(config-line)#line vty 0 4
lab1(config-line)#login
lab1(config-line)#password *password*

Из соображений безопасности, если маршрутизатор напрямую подключен к публичным сетям, например, Интернет, виртуальные терминалы реко-

мендуется заблокировать, а доступ к маршрутизатору осуществлять только по консольной линии.

2.2. Настройка интерфейсов

Для перехода в режим настройки необходимого интерфейса следует, находясь в глобальном режиме, выполнить команду:
lab1(config)#interface Ethernet 1/0

По умолчанию все интерфейсы выключены. Интерфейс включается командой:
lab1(config-if)#no shutdown

Работоспособность настроек физического и канального уровней можно проверить командой в контексте администратора:
lab1#show interface <имя_интерфейса>

Сообщения об изменении состояния физического и канального уровней любого интерфейса выводятся маршрутизатором на консоль. Команда show interface также выводит сведения об используемом протоколе канального уровня, IP-адресе и статистику отправленных и полученных данных и ошибок.

Настройка IP-адреса интерфейса (рис. 7.3) производится командой:
lab1(config-if)#ip address <адрес><маска>

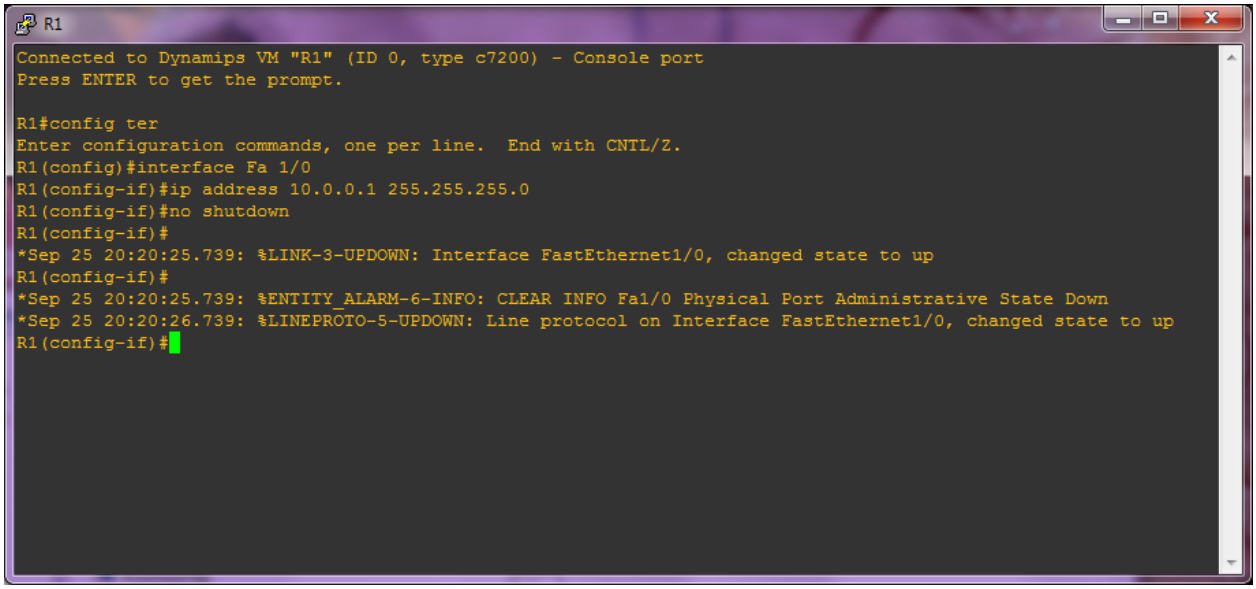


Рис. 7.3. Настройка IP-адреса маршрутизатора

Подробная информация о параметрах протокола IP доступна в контексте администратора по команде:
lab1#show ip interface <имя_интерфейса>

Краткая сводная таблица состояний IP-интерфейсов:
lab1#show ip interface brief

2.3. Назначение статических маршрутов

Маршруты, ведущие в сети, к которым маршрутизатор подключен непосредственно, автоматически добавляются в маршрутную таблицу после конфигурирования интерфейса при условии, что интерфейс работоспособен («line protocol up»). Для назначения дополнительных статических маршрутов в контексте глобальной конфигурации вводится команда (одна строка):
router(config)#ip route <IP-адрес><маска><интерфейс><IP-адрес следующего_маршрутизатора>

Маршрут активен только тогда, когда следующий маршрутизатор достижим — то есть существует маршрут в сеть, где находится следующий маршрутизатор. Напротив, статический маршрут будет неактивен, если следующий маршрутизатор не достижим по разным причинам, если, например, его интерфейс находится в нерабочем состоянии.

Управление таблицей маршрутизации на маршрутизаторах в большой распределенной сети является сложной задачей. Поэтому часто используют специальные протоколы маршрутизации. Маршрут по умолчанию назначается командой:
router(config)#ip route 0.0.0.0 0.0.0.0 fastethernet 1/1 <IP-адрес следующего маршрутизатора>

Просмотреть таблицу маршрутов можно в контексте администратора по команде:
router#show ip route

2.4. Регистрация событий

Диагностические сообщения выводятся маршрутизатором на консольную линию. Для того чтобы эти сообщения дублировались в виртуальные терминалы (то есть в telnet-соединения), в контексте администратора в соответствующем терминале подается команда
lab1#teminal monitor 14
Закрепить это положение в конфигурации можно следующим образом:
lab1(config)#linevty 0 4
lab1(config-line)#monitor

Вывод сообщений можно направить также во внутренний буфер или на syslog-сервер Unix. Направление в буфер:
lab1(config)#logging buffered [размер]

Буфер организован в виде очереди указанного размера в байтах, самые старые сообщения выбывают по прибытии новых. Размер буфера по умолчанию — 4096 байт. Просмотр буфера (и параметров регистрации):

lab1#show logging

Очистка буфера:

lab1#clear logging

Отправка сообщений на syslog-сервер:

lab1(config)#logging IP-адрес
lab1(config)#logging facility local7
lab1(config)#logging trap debugging

Последние две команды устанавливают источник сообщений (facility в терминах syslog) и минимальный уровень серьезности (level=debugging).

По умолчанию диагностические сообщения снабжаются метками времени, которые отсчитываются с момента загрузки маршрутизатора (system uptime). Для того чтобы время выводилось в обычном формате (дата, время суток), в конфигурации необходимо указать (рис. 7.4):

lab1(config)#service timestamps log datetime localtime
lab1(config)#service timestamps debug datetime localtime

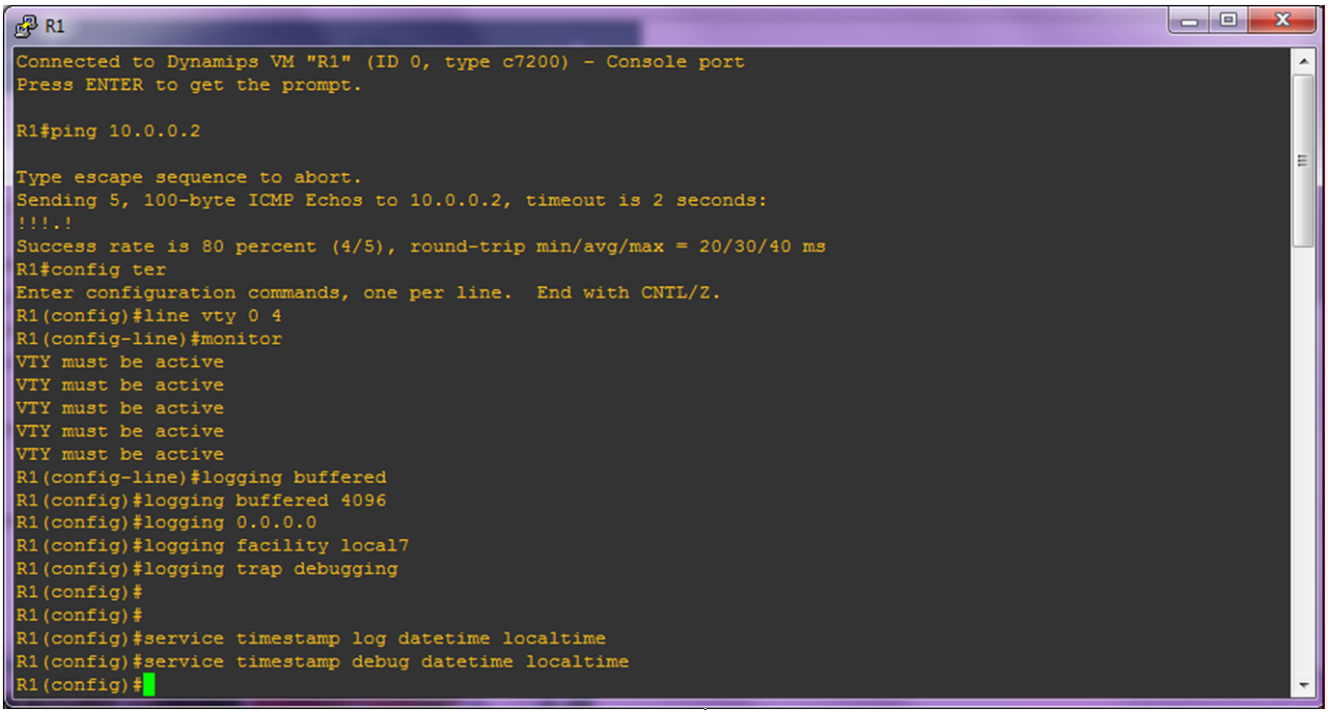


Рис.7.4. Регистрация событий

2.5. Списки доступа

Списки доступа (access lists) представляют собой общие критерии отбора, которые можно впоследствии применять при фильтрации дейтаграмм, для отбора маршрутов, определения приоритетного трафика и в других задачах.

2.5.1. Стандартные списки доступа

Списки доступа, производящие отбор по IP-адресам, создаются командами access-list в режиме глобальной конфигурации, каждый список определяется номером — числом в диапазоне 0-99. Каждая такая команда добавляет новый критерий отбора в список:

router(config)# access-list <номер_списка><{deny | permit}><IP-адрес> [маска_шаблона]

IP-адрес и маска шаблона записываются в десятично-точечной нотации, при этом в маске шаблона устанавливаются биты, значение которых в адресе следует игнорировать, остальные биты сбрасываются. При этом сетевая маска (netmask) и маска шаблона (wildcard) — это разные вещи. Например, чтобы строка списка сработала для всех узлов с адресами 1.16.124.xxx, адрес должен быть 1.16.124.0, а маска — 0.0.0.255, поскольку значения первых 24 бит жестко заданы, а значения последних 8 бит могут быть любыми. Как видно в этом случае маска шаблона является инверсией соответствующей сетевой маски. Однако маска шаблона в общем случае не связана с сетевой маской и даже может быть разрывной (содержать чере-дования нулей и единиц). Например, строка списка должна сработать для всех нечетных адресов в сети 1.2.3.0/24. Соответствующая комбинация адреса и маски шаблона: 1.2.3.1 0.0.0.254.

Комбинация «адрес — маска шаблона» вида 0.0.0.0 255.255.255.255 (то есть соответствующая всем возможным адресам) может быть записана в виде одного ключевого слова any. Если маска отсутствует, то речь идет об IP-адресе одного узла.

Операторы permit и deny определяют положительное (принять, пропустить, отправить, отобрать) и отрицательное (отбросить, отказать, игнорировать) будет принято решение при срабатывании данного критерия отбора. Например, если список используется при фильтрации дейтаграмм по адресу источника, то эти операторы определяют, пропустить или отбросить дейтаграмму, адрес источника которой удовлетворяет комбинации «адрес — маска шаблона». Если же список применяется для идентификации какой-либо кате-

гории трафика, то оператор allow отбирает трафик в эту категорию, а deny — нет.

Список доступа представляет собой последовательность из одного и более критериев отбора, имеющих одинаковый номер списка. Последовательность критериев имеет значение: маршрутизатор просматривает их по порядку; срабатывает первый критерий, в котором обнаружено соответствие образцу; оставшаяся часть списка игнорируется. Любые новые критерии добавляются только в конец списка. Удалить критерий нельзя, можно удалить только весь список. В конце списка неявно подразумевается критерий «отказать в любом случае» (deny any) — он срабатывает, если ни одного соответствия обнаружено не было.

Для аннулирования списка доступа следует ввести команду:
router(config)# no access-list <номер_списка>

Чтобы применить список доступа для фильтрации пакетов, проходящих через определенный интерфейс, нужно в режиме конфигурации этого интерфейса ввести команду
router(config-if)# ip access-group <номер_списка><{in | out}>

Ключевое слово in или out определяет, будет ли список применяться к входящим или исходящим пакетам соответственно. Входящими считаются пакеты, поступающие к интерфейсу из сети. Исходящие пакеты движутся в обратном направлении.

Только один список доступа может быть применен на конкретном интерфейсе для фильтрации входящих пакетов, и один — для исходящих. Соответственно, все необходимые критерии фильтрации должны быть сформулированы администратором внутри одного списка. В стандартных списках доступа отбор пакетов производится по IP-адресу источника пакета (рис. 7.5).

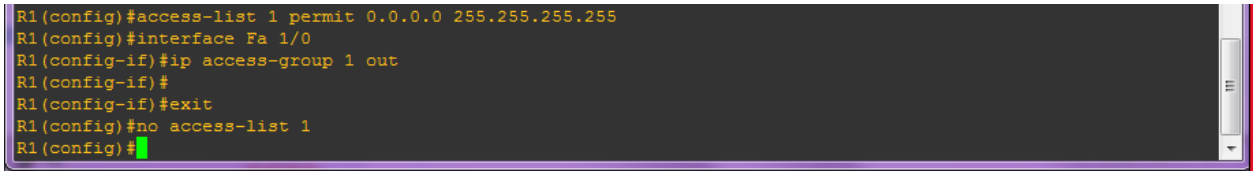


Рис. 7.5. Стандартные списки доступа

2.5.2. Расширенные списки доступа

Расширенные списки доступа создаются также с помощью команды access-list в режиме глобальной конфигурации, но номера этих списков лежат в диапазоне 100-199. Пример синтаксиса команды создания строки расширенного списка для контроля TCP-соединений:

router(config)# access-list <номер_списка><{deny | permit}> tcp <IP-адрес_источника><маска_шаблона> [оператор порт [порт]] <IP-адрес_получателя><маска_шаблона> [оператор порт [порт]] [established]

Маски шаблона для адреса источника и узла назначения определяются так же, как и в стандартных списках.

Оператор при значении порта должен иметь одно из следующих значений: lt (строго меньше), gt (строго больше), eq (равно), neq (не равно), range (диапазон включительно). После оператора следует номер порта (или два номера порта в случае оператора range), к которому этот оператор применяется. Комбинация опера-тор-порт, следующая сразу же за адресом источника, относится к портам источника. Соответственно, комбинация оператор-порт, которая следует сразу же за адресом получателя, относится к портам узла-получателя.

Применение этих комбинаций позволяет отбирать пакеты не только по адресам мест отправки и назначения, но и по номерам TCP- или UDP-портов. Кроме того, ключевое слово established определяет сегменты TCP, передаваемые в состоянии установленного соединения. Это значит, что строке, в которую включен пара-метр established, будут соответствовать только сегменты с установленным флагом ACK (или RST).

Пример: «запретить установление соединений с помощью протокола Telnet со всеми узлами сети 22.22.22.0 netmask 255.255.255.0 со стороны всех узлов Интернета, причем в обратном направлении все соединения должны устанавливаться; остальные TCP-соединения разрешены». Фильтр устанавливается для входящих сегментов со стороны Интернета (предположим, к Интернету маршрутизатор подключен через интерфейс FastEthernet 1/0).

```
router(config)# access-list 101 permit tcp any 22.22.22.0 0.0.0.255 eq 23 established
router(config)# access-list 101 deny tcp any 22.22.22.0 0.0.0.255 eq 23
router(config)# access-list 101 permit ip any any
router(config)# interface FastEthernet 1/0
router(config-if)# ip access-group 101 in
```

Указание ip вместо tcp в команде access-list означает «все протоколы». Отметим, что в конце каждого списка доступа подразумевается deny ip any any, поэтому в предыдущем примере мы указали permit ip any any для разрешения произвольных пакетов, не попавших под предшествующие критерии.

Вообще, в расширенных списках можно работать с пакетами любого IP-протокола. Для этого после оператора deny/permit надо указать название

протокола (ahp, esp, eigrp, gre, icmp, igmp, igrp, ipinip, ospf, tcp, udp) или его номер, которым он кодируется в поле Protocol заголовка пакета. Далее указываются адреса источника и узла назначения с масками и, возможно, дополнительные параметры, специфичные для данного протокола.

В конце команды access-list (расширенный) можно указать параметр log, тогда все случаи срабатывания данного критерия (то есть обнаружения пакета, соответствующего критерию), будут протоколироваться на консоль или как указано командой logging. После того, как протоколируется первый случай срабатывания, дальше сообщения посылаются каждые 5 минут с указанием числа срабатываний за отчетный период.

Просмотр имеющихся списков доступа (с указыванием числа срабатываний каждого критерия):

router# show access-lists

Более подробную статистику работы списков доступа можно получить, включив режим ip accounting. Режим включается в контексте конфигурирования интерфейса. Следующая команда включает режим учета случаев нарушения (то есть, пакетов, которые не были пропущены списком доступа на данном интерфейсе):

router(config-if)# ip accounting access-violations

Просмотр накопленной статистики (с указанием адресов отправителей и получателей пакетов):

router# show ip accounting access-violations

При конфигурировании запрещающих фильтров (в конце которых подразумевается deny all) администратор должен не забыть оставить «дверь» для сообщений протоколов маршрутизации, если они используются на конфигурируемом интерфейсе (рис. 7.6).

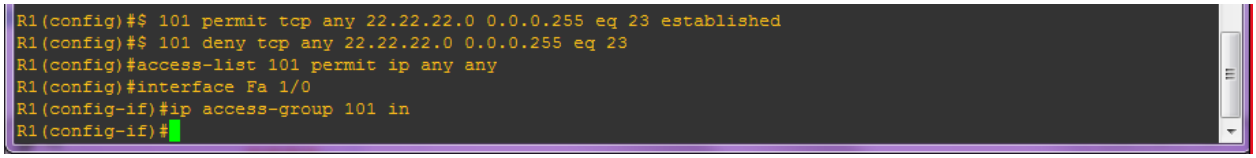


Рис. 7.6. Расширенные списки доступа

2.5.3. Динамические обратные списки доступа

Недостатком списков доступа, применяемых для фильтрации трафика, является то, что они формируются администратором статически до начала работы. В итоге администратор вынужден закладывать в них разрешения «на все случаи жизни».

Динамические обратные списки (reflexive access lists) предлагают способ решения проблемы. Они служат для автоматической фильтрации пакетов, следующих в обратном направлении относительно пакетов, пропущенных некоторым статическим списком. Динамические обратные списки открывают только те «двери», которые необходимо открыть для обслуживания данного конкретного сеанса обмена пакетами. В этом случае заранее формируется только один список — например, список 120 «пропускать UDP-пакеты с любого порта внутри на порт 53 снаружи», а для пропуска пакетов в обратном направлении список 121 формируется динамически:

```
router(config)# access-list 120 permit udp any any eq 53 reflect DNS_REPLIES
router(config)# access-list 121 evaluate DNS_REPLIES
router(config)# interface FastEthernet 1/0
router(config-if)# ip access-group 120 out
router(config-if)# ip access-group 121 in
```

Приведенный выше пример работает следующим образом. Когда внутренний узел A посылает сообщение с клиентского порта 3456 на порт 53 некоторого внешнего узла B, то соответствующий сегмент пропускается в узел B согласно списку 120. Кроме того, узел A ожидает, что и ответное сообщение от B с порта 53 на A порт 3456 будет пропущено маршрутизатором. Для этого маршрутизатор динамически создает (дополняет) список доступа 121 обратный к списку 120. Точнее, критерий отбора, содержащий указание evaluate DNS_REPLIES, будет обратным критерию отбора, содержащему указание reflect DNS_REPLIES с учетом параметров данного конкретного сеанса — адресов A и B и номера порта 3456. Иными словами, список 121 будет выглядеть: "пропускать UDP-пакеты с порта 53 узла B на порт 3456 узла A".

Динамически сформированный критерий отбора в списке 121 будет действовать до завершения сеанса между A и B. Завершение сеанса определяется таймером неактивности; кроме того, в TCP-сеансах отслеживаются сегменты с флагами FIN и RST. Таймер неактивности для всех динамических обратных списков устанавливается командой

```
router(config)# ip reflexive-list timeout <число_секунд>
```

Кроме того, таймер для конкретного критерия может быть установлен с помощью параметра timeout:

```
router(config)# access-list 120 permit udp any any eq 53 reflect DNS_REPLIES
    timeout 120
```

Список литературы

1. Е. Баранова, А. Бабаш, Информационная безопасность и защита информации, Издательство: РИОР, Инфра-М, 2014.
2. Н. Милославская, М. Сенаторов, А. Толстой, Управление рисками информационной безопасности, Издательство: Горячая Линия - Телеком, 2014.
3. В. Ищейнов, М. Мецатунян, Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации. Учебное пособие, Издательство: Форум, Инфра-М, 2014.
4. П. Девянин, Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Издательство: Горячая Линия - Телеком, 2013.
5. Мельников, В. П. Информационная безопасность и защита информации / В. П. Мельников. – М.: Академия, 2011.
6. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах / М.: ИД "ФОРУМ" - ИНФРА-М, 2010.
7. А. Н. Андрончик, М. Л. Борисенко, А. С. Коллеров, Н. И. Синадский, Д. А. Хорьков. Защита информации в компьютерных сетях. Практический курс: учебное пособие, под ред. Н. И. Синадского. – 3-е изд., перераб. и доп. – Екатеринбург: 2012. – 333 с.

План УМД на 2015/16 уч. г.

Айрапет Генрикович Симонян

Тауфик Бен Камель Бен Режеб

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Практикум

Подписано в печать . . г. Формат 60х90 1/16
Объем усл. п.л. Тираж 100 экз. Изд. № . Заказ № .

ООО «». Москва, ул. , д..