ПРАКТИЧЕСКАЯ РАБОТА №3

Мониторинг сетевого трафика

Цель работы: Получить практические навыки по работе с анализаторами сетевого трафика. На практике ознакомиться с различиями в принципах работы активного сетевого оборудования. Уяснить особенности взаимодействия сетевого и канального уровней на примере стека TCP/IP. Выяснить отличия форматов кадров Ethernet. Познакомиться с консольными утилитами диагностики и анализа сетевых соединений.

Необходимо: Компьютер с установленной средой виртуализации Virtual Box. Виртуальные машины MS Windows и Linux. Административные учетные записи на виртуальных машинах. Сетевое подключение по протоколу IP. Доступ к глобальной сети Интернет. Программный пакет Wireshark.

Краткие теоретические сведения

На начальном уровне перехват и анализ сетевого трафика осуществляется на отдельном хосте. Для этого используются программы «Анализаторы трафика», или «снифферы». Эти программы позволяют осуществить перехват всего трафика по выбранному сетевому интерфейсу и его деинкапсуляцию до прикладного уровня. Как правило они обладают средствами фильтрации и поиска в перехваченном наборе кадров. Наиболее известным кроссплатформенным решением является Wireshark.

Кроме них существуют стандартные консольные утилиты arp, netstat (Windows, Linux), ss, lsof и tcpdump (Linux). Как правило, подобные утилиты работают на сетевом уровне и выше.

К назначению средств анализа начального уровня относятся анализ текущих соединений на хосте и поиск неисправностей при сетевом взаимодействии

Порядок выполнения работы:

Часть 1. Wireshark.

1. Установите на виртуальном хосте программу Wireshark.
2. Настройте виртуализацию сети в VirtualBox, так чтобы получать трафик приходящий нареальный сетевой адаптер (пропустите этот пункт если Wirwshark работает на реальном хосте).
3. Настройте перехват трафика, так чтобы он завершился после сбора 15 Мб (для увеличения интенсивности генерации кадров открыть любой сайт в браузере).
   Используя инструментарий статистики определите:
4. Узел с максимальной активностью (по объему переданных данных),
5. Узел осуществивший наибольшее количество широковещательных рассылок,

6. Самый активный TCP-порт на хосте (по количеству переданных пакетов)
7. Постройте на одной координатной сетке постройте графики интенсивности TCP и UDP трафика (пункт Io Graphs).
8. Постройте граф связей только для пакетов, содержащих сообщения протокола HTTP (пункт Flow Graph)

   Напишите фильтры которые выделяют из общего числа пакеты:
9. Относящиеся к работе протоколов HTTP и FTP при работе в качестве клиента операционной системы на которой запущена среда виртуализации (или самого хоста если среда виртуализации не используется).
10. Все кадры Ethernet, отправленные с сетевого интерфейса хоста, на котором запущена среда виртуализации (или самого хоста, если среда виртуализации не используется).
11. Напишите фильтр, отбирающий только широковещательные сообщения. Определите назначение как минимум 3-х широковещательных рассылок разных протоколов.
12. Определить адреса, на которые поступают данные кадры и пакеты для канального и сетевого уровня
13. Напишите фильтры для каждой из трех широковещательных рассылок, выбранных в пункте 11.
14. На основании собранной статистики определить, к какому типу коммутационного оборудования подключен используемый компьютер (концентратор, коммутатор или маршрутизатор).

Часть 2. Консольные утилиты.

15. Запустите одновременно виртуальную машины Linux и Windows. Убедитесь, что на Windows есть ssh клиент putty, а на Linux telnet клиент. Если их нет, то установите клиенты. Программа putty доступна на http://www.putty.org/. Telnet клиент на Linux доступен в репозитариях (для CentOS команда yum install telnet).
16. Настройте между ними внутреннюю сеть и установите на сетевых интерфейсах IP адреса из сети 192.168.0.0/24 (маска 255.255.255.0).
17. Запустите на Windows Telnet-сервер (консоль Службы / Services)
18. С Windows с помощью терминального клиента Putty подключитесь к SSH серверу на Linux.
19. С Linux с помощью telnet клиента подключитесь к Windows машине.
20. Используя утилиту netstat или lsof (для Linux) вывести все активнее (прослушиваемые) порты на обоих платформах. Используя утилиту netstat или ss (для Linux) все открытые соединения на обоих платформах.
21. С помощью команды tcpdump на Linux настроить вывод на экран содержимого пакетов от Windows-хоста по протоколу telnet.
22. Завершите ssh и telnet соединения. На одном из хостов запустите перехват трафика Wireshark и начните ssh и telnet сессии заново.
23. С помощью фильтров отберите трафик telnet и ssh. Сравните содержимое сообщений прикладного уровня в обоих случаях.

В отчет:

1. Предоставить снимки экрана по п. 4-8.
2. Предоставить тексты фильтров 9,10,11,13.
3. Также в отчёте предоставить ответы на вопросы:
4. Какие типы кадров Ethernet бывают, в чем их отличия?

5. Какой тип кадров Ethernet используется в анализируемой сети? Почему именно он?
6. Как можно определить тип используемого коммутационного оборудования, используя сетевую статистику? Какой тип коммутационного оборудования использовался в сети?
7. На какие адреса сетевого уровня осуществляются широковещательные рассылки?
8. На какой канальный адрес осуществляются широковещательные рассылки?
9. Для чего применяются перехваченные широковещательные рассылки в п. 11?
10. Как с помощью утилиты arp просмотреть arp-кэш и как его очистить. В каких случаях может понадобиться последняя операция?
11.
12. Приведите командные строки из п. 20 и 21.
13. Какой из двух протоколов telnet или ssh явялется более защищенным? Почему?