Санкт-Петербургский Политехнический Университет Петра Великого

Кафедра компьютерных систем и программных технологий

Отчёт по лабораторной работе №2

Курс: «Администрирование компьютерных сетей»

Тема: «Тестирование компьютерной сети на основе TCP/IP»

Выполнил студент:

Бояркин Никита Сергеевич
Группа: 13541/3

Проверил:

Малышев Игорь Алексеевич

Санкт-Петербург
2018 г.

Содержание

Лабораторная работа №2

1.1 Цель работы

- Изучение утилит и систем администрирования TCP/IP-сетей
- Мониторинг и анализ характеристик TCP/IP-сетей

1.2 Программа работы

- Составить паспорт сети, объединяющий карту сети (физическая и логическая топология с указанием числовых и символических имён хостов, номенклатур аппаратных и программных платформ хостов и сетевых компонентов), характеристики направления и интенсивности (для совокупного по всем типам пакетов и раздельного по каждому типу пакетов) сетевого трафика.
- Представить и прокомментировать все конфигурационные файлы, определяющие состояние как отдельных хостов сети, так и подсетей/сетей.
- Оценить производительность/загрузку сети в целом и её отдельных компонентов.
- Оценить уязвимость системных (хосты) и сетевых (службы) ресурсов сети относительно внешних атак.
- Составить перечень задач, которые необходимо решить системному/сетевому администратору для улучшения характеристик производительности и безопасности сети.

1.3 Утилиты

Для иллюстрации работы утилит была использована ОС Ubuntu, которая является частью ККС из предыдущей работы.

1.3.1 Утилита ifconfig/ipconfig

Запуск утилиты ifconfig/ipconfig без аргументов отображает список активных сетевых интерфейсов и их параметры. Запуск утилиты ifconfig/ipconfig с названием интерфейса в качестве аргумента выводит информацию о нем.

```
nikita@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.40.32  netmask 255.255.255.0  broadcast 192.168.40.255
        inet6 fe80::8296:8dda:7b3a:d6ab  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:19:e9:96  txqueuelen 1000  (Ethernet)
        RX packets 16  bytes 1278 (1.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 98  bytes 9665 (9.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4229  bytes 255729 (255.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4229  bytes 255729 (255.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Рис. 1.1: Вывод информации об активных сетевых адаптерах

1.3.2 Утилита arp

Утилита командной строки arp используется для отображения и изменения таблиц преобразования IP-адресов в физические (MAC-адреса), используемые протоколом разрешения адресов (Address Resolution Protocol - ARP).

```
nikita@ubuntu:~$ arp -a
_gateway (192.168.40.2) at 00:0c:29:40:ea:47 [ether] on ens33
```

Рис. 1.2: Вывод arp таблицы

1.3.3 Утилита netstat

Утилита netstat предназначена для получения оперативной и статистической информации о состоянии сети. Она может выводить таблицу маршрутизации, активные подключения, открытые клиентские и серверные сокеты и др.

```
nikita@ubuntu:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.40.2    0.0.0.0         UG        0 0          0 ens33
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 ens33
192.168.40.0    0.0.0.0         255.255.255.0   U         0 0          0 ens33
```

Рис. 1.3: Вывод таблицы маршрутизации

1.3.4 Утилита hostname

Утилита hostname устанавливает или отображает символическое имя хоста.

```
nikita@ubuntu:~$ hostname
ubuntu
```

Рис. 1.4: Вывод текущего имени хоста

1.3.5 Утилита ping

Утилита ping позволяет определить доступность узла сети при помощи ICMP протокола.

```
nikita@ubuntu:~$ ping 8.8.8.8 -c 3
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=6.02 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=6.09 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=6.05 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 6.023/6.057/6.093/0.028 ms
```

Рис. 1.5: Определение доступности узла 8.8.8.8

1.3.6 Утилита traceroute

Утилита traceroute производит трассировку маршрута до конечного узла при помощи наращивания последовательного TTY на ICMP пакетах.

```
nikita@ubuntu:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  _gateway (192.168.40.2)  0.416 ms  0.338 ms  0.310 ms
 2  192.168.40.57 (192.168.40.57)  0.545 ms  0.232 ms  0.290 ms
 3  192.168.32.2 (192.168.32.2)  1.042 ms  1.039 ms  1.028 ms
 4  * * *
 5  * * *
 6  * * *
```

Рис. 1.6: Трассировка маршрута до узла 8.8.8.8

1.4 Построение карты сети

Построим карту сети для ККС из предыдущей лабораторной работы. Для этого на Windows XP установим утилиту LanState. При запуске программы, были указаны следующие диапазоны (сегменты сети) для сканирования:

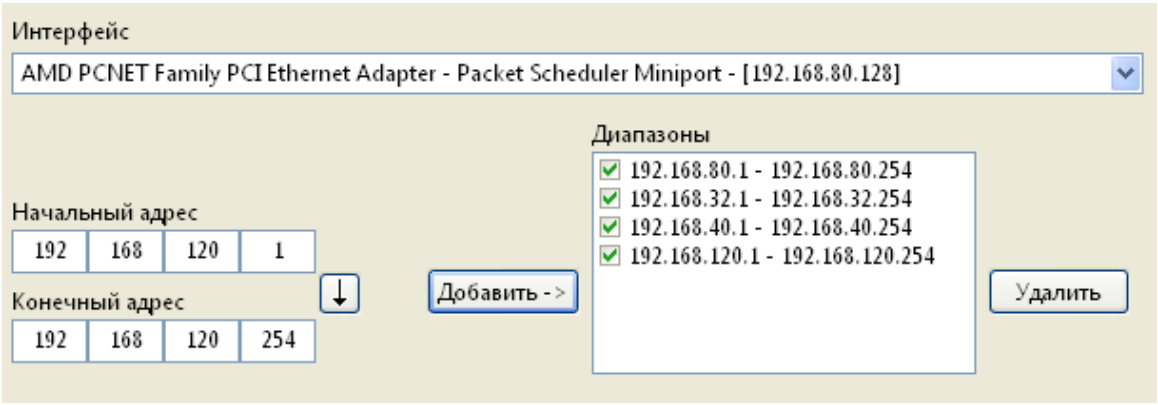

Рис. 1.7: Установка диапазонов сети для сканирования

В результате сканирования были найдены следующие узлы:

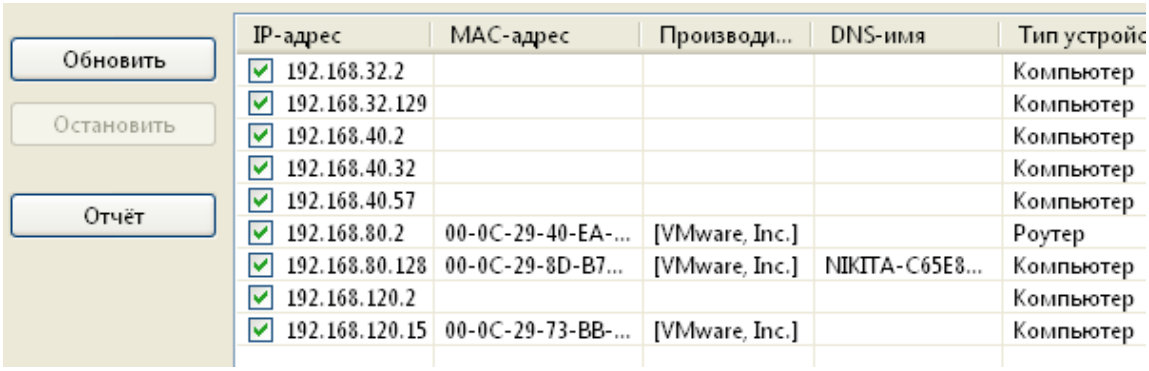

Рис. 1.8: Найденные узлы

В результате чего была построена следующая карта сети:

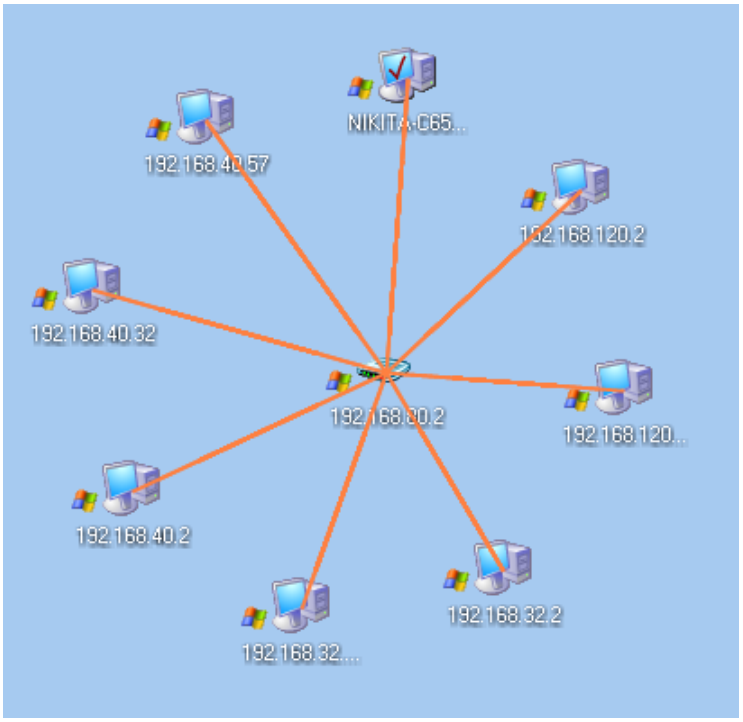

Рис. 1.9: Карта сети

Программа не смогла определить точную карту сети, типы операционных систем, она видит лишь ближайший маршрутизатор, в данном случае – это FreeBSD (хост 192.168.80.2).

1.5 Поиск уязвимых узлов

Для поиска уязвимых узлов на Windows XP установим программу XSpider. При запуске программы, были указаны следующие узлы для сканирования:

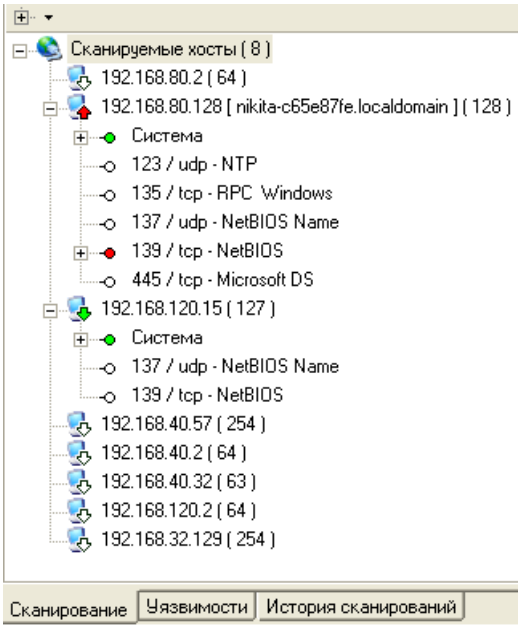

Рис. 1.10: Результат сканирования всех узлов сети

Уязвимыми указались узлы с Windows XP и Windows 98. В unix-подобных системах известных уязвимостей не обнаружено.

1.6 Оценка пропускной способности

Оценим пропускную способность через утилиту iperf:

```
# ./iperf -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 32.0 KByte (default)
------------------------------------------------------------
[  4] local 192.168.40.57 port 5001 connected with 192.168.40.2 port 40000
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-10.0 sec  20.0 MBytes  16.8 Mbits/sec
[  5] local 192.168.40.57 port 5001 connected with 192.168.40.32 port 53378
[  5]  0.0-10.0 sec  1.41 GBytes  1.21 Gbits/sec
```

Рис. 1.11: Сервер iperf на NetBSD

```
nikita@ubuntu:~$ iperf -c 192.168.40.57
------------------------------------------------------------
Client connecting to 192.168.40.57, TCP port 5001
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.40.32 port 53378 connected with 192.168.40.57 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec  1.41 GBytes  1.21 Gbits/sec
```

Рис. 1.12: Клиент iperf на Ubuntu

```
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\Administrator>cd C:\Program Files\iperf-2.0.9-win32

C:\Program Files\iperf-2.0.9-win32>iperf.exe -c 192.168.40.57
------------------------------------------------------------
Client connecting to 192.168.40.57, TCP port 5001
TCP window size: 63.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.80.128 port 1050 connected with 192.168.40.57 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.2 sec  20.1 MBytes  16.6 Mbits/sec
```

Рис. 1.13: Клиент iperf на Windows XP

Пропускная способность узла с Ubuntu оказалась примерно в 75 раз выше, чем у узла с ОС Windows XP.

1.7 Вывод

Построение корректной карты сети оказалось не простой задачей. Помимо шлюза достаточно сложно установить реальную топологию узлов сети.

Поиск уязвимостей наглядно показал, что устаревшие версии операционных систем содержат множество уязвимостей, особенно рассчитанные на пользователя по типу ОС семейства Windows.

Тестирование пропускной способности выявило, что узел с устаревшей Windows XP имеет пропускную способность в 75 раз меньшую, чем узел с обновленной Ubuntu. Такое различие можно попробовать объяснить версией ОС или версией утилиты.