

САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ПЕТРА ВЕЛИКОГО

Институт компьютерных наук и технологий
Высшая школа интеллектуальных систем и суперкомпьютерных технологий

Дисциплина «Администрирование компьютерных сетей»

ОТЧЁТ
по лабораторной работе № 2
на тему
«Тестирование компьютерной сети на основе TCP/IP»

Выполнил:
Дроздов Никита Дмитриевич
Группа: 3540901/02001
Проверил:
Малышев Игорь Алексеевич

Санкт-Петербург
2021

Оглавление

Цели работы	3
Ход работы	4
Тестирование утилит	4
Вывод	12

Цели работы

1. Изучение утилит и систем администрирования TCP/IP;
2. Мониторинг и анализ характеристик TCP/IP сетей.

Ход работы

Компьютерная сеть использовалась созданная ранее в рамках лабораторной работы №1. ПО для виртуализации VMware Workstation PRO 16.

Схема созданной ранее сети:

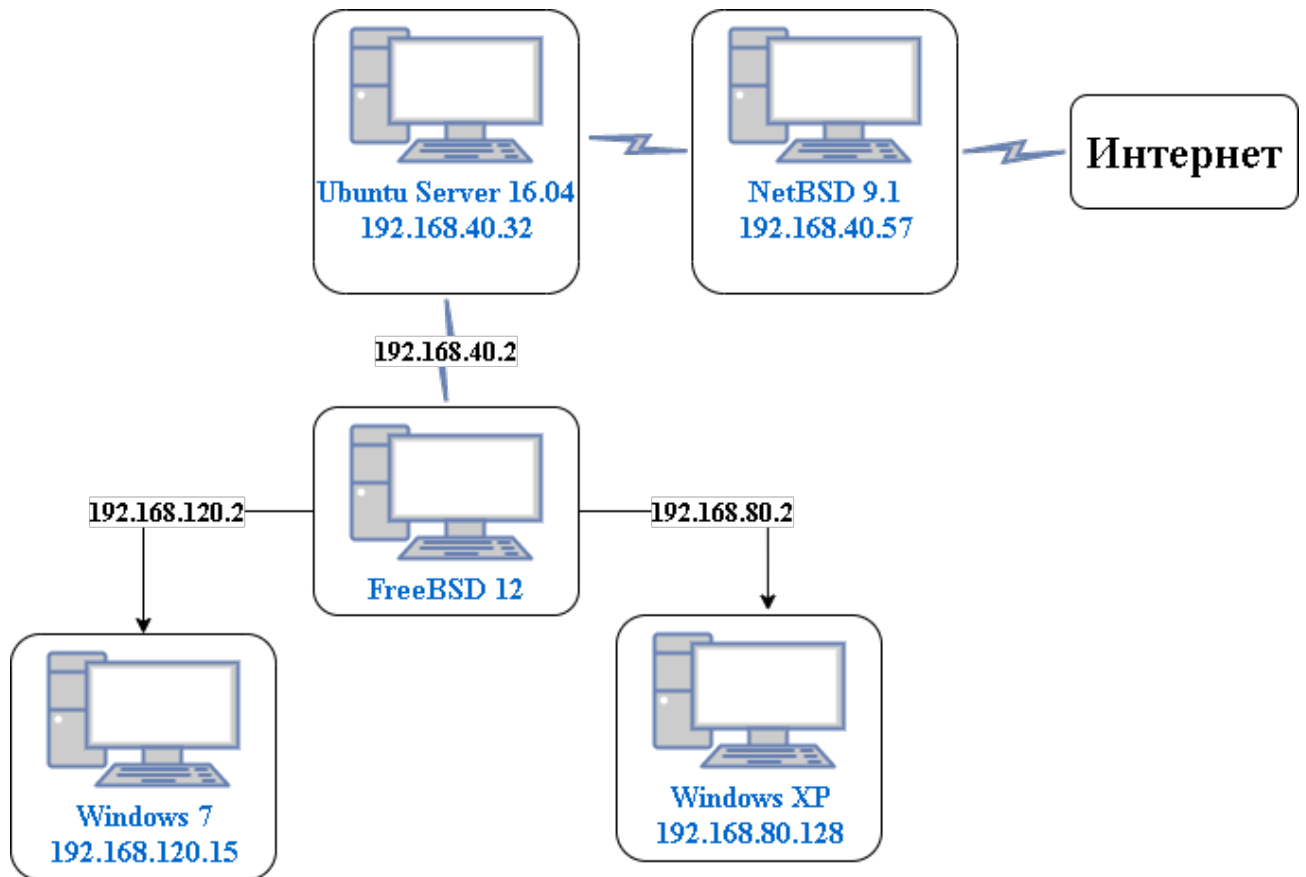


Рисунок 1 - Схема ККС

Тестирование утилит

1. Ifconfig. Отражает список активных сетевых интерфейсов и их параметры

```
user@user-virtual-machine: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

user@user-virtual-machine:~$ ifconfig
ens33    Link encap:Ethernet  HWaddr 00:0c:29:b4:56:39
          inet addr:192.168.40.32  Bcast:192.168.40.255  Mask:255.255.255.0
          inet6 addr: fe80::bb8c:c398:3b5b:6a5b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:56 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9219 (9.2 KB)  TX bytes:7585 (7.5 KB)

lo       Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:4436 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4436 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:329872 (329.8 KB)  TX bytes:329872 (329.8 KB)

user@user-virtual-machine:~$
```

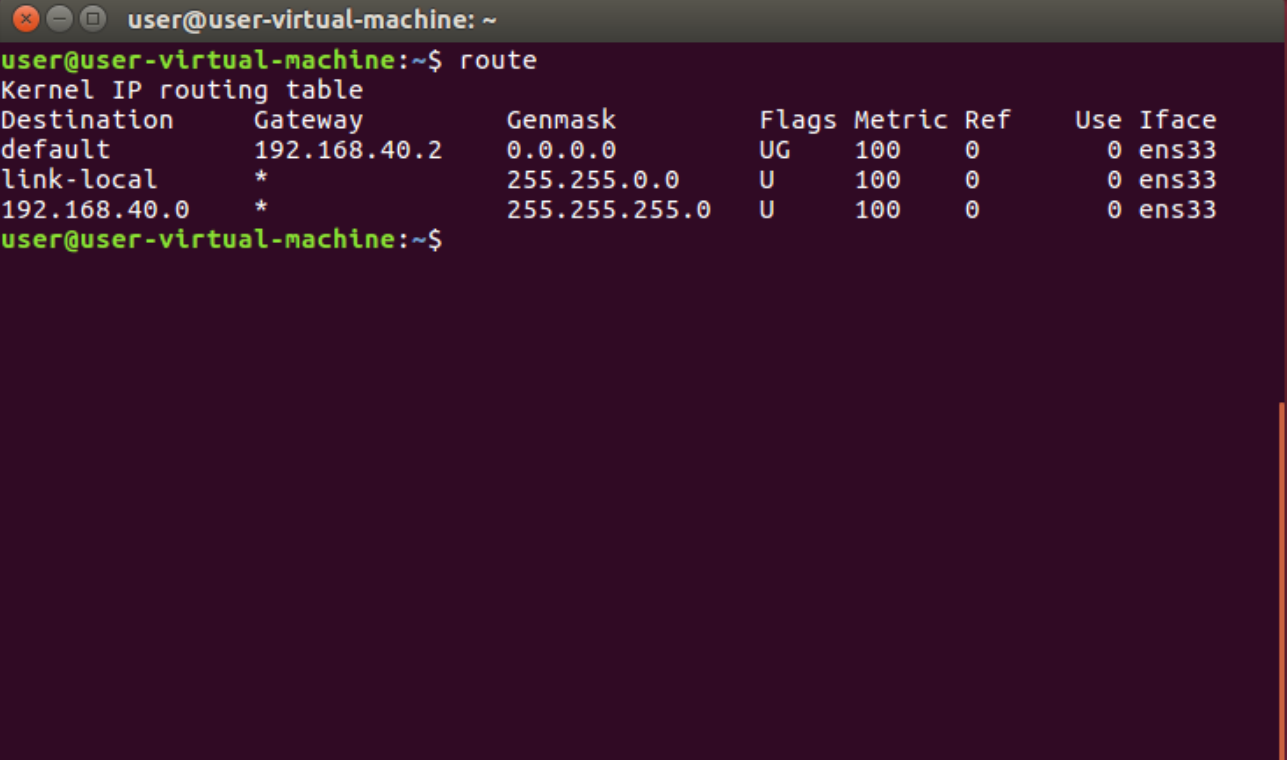
Рисунок 2 - утилита ifconfig

2. Ping. Утилита позволяет проверить наличие доступа к другому компьютеру сети с помощью icmp запросов

```
user@user-virtual-machine: ~
user@user-virtual-machine:~$ ping 192.168.40.2
PING 192.168.40.2 (192.168.40.2) 56(84) bytes of data.
64 bytes from 192.168.40.2: icmp_seq=1 ttl=64 time=0.924 ms
64 bytes from 192.168.40.2: icmp_seq=2 ttl=64 time=0.628 ms
64 bytes from 192.168.40.2: icmp_seq=3 ttl=64 time=0.822 ms
64 bytes from 192.168.40.2: icmp_seq=4 ttl=64 time=0.540 ms
64 bytes from 192.168.40.2: icmp_seq=5 ttl=64 time=0.668 ms
^C
--- 192.168.40.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4033ms
rtt min/avg/max/mdev = 0.540/0.716/0.924/0.140 ms
user@user-virtual-machine:~$
```

Рисунок 3 - утилита ping

3. Route. Показывает таблицу ip-маршрутизации



```
user@user-virtual-machine: ~
user@user-virtual-machine:~$ route
Kernel IP routing table
Destination      Gateway         Genmask        Flags Metric Ref    Use Iface
default          192.168.40.2   0.0.0.0        UG    100    0      0 ens33
link-local       *              255.255.0.0    U     100    0      0 ens33
192.168.40.0     *              255.255.255.0  U     100    0      0 ens33
user@user-virtual-machine:~$
```

Рисунок 4 - утилита route

4. Arp. Протокол ARP сканирует локальную сеть и устанавливает соответствия между логическим сетевым адресом и физическим адресом. Утилита имеет множество флагов, например. Запуск команды “arp -a” выдаст подключенные хосты в BSD стиле.

```
user@user-virtual-machine: ~  
user@user-virtual-machine:~$ arp  
Address          HWtype  HWaddress      Flags Mask    Iface  
192.168.40.57     ether   00:0c:29:03:85:6f  C           ens33  
192.168.40.2      ether   00:0c:29:fc:8b:59  C           ens33  
user@user-virtual-machine:~$
```

Рисунок 5 - утилита arp

5. Hostname

```
user@user-virtual-machine: ~  
user@user-virtual-machine:~$ hostname  
user-virtual-machine  
user@user-virtual-machine:~$
```

Рисунок 6 - утилита hostname

6. Netstat. Позволяет получить в режиме реального времени информацию о состоянии сетевых соединений, а также статистические данные и таблицу маршрутизации

```
user@user-virtual-machine: ~
user@user-virtual-machine:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags   Type       State             I-Node  Path
unix  2      [ ]     DGRAM                    19363    /run/systemd/cgroups-agent
unix  2      [ ]     DGRAM                    28207    /run/user/1000/systemd/notify
unix  2      [ ]     DGRAM                    19368    /run/systemd/journal/syslog
unix  7      [ ]     DGRAM                    19370    /run/systemd/journal/socket
unix 13      [ ]     DGRAM                    19385    /run/systemd/journal/dev-log
unix  3      [ ]     DGRAM                    19362    /run/systemd/notify
unix  3      [ ]     STREAM      CONNECTED          25096    /run/systemd/journal/stdout
unix  3      [ ]     STREAM      CONNECTED          31584    @/tmp/dbus-HUAUY11T4h
unix  3      [ ]     STREAM      CONNECTED          29432
unix  3      [ ]     STREAM      CONNECTED          28870
unix  3      [ ]     STREAM      CONNECTED          28816    @/tmp/dbus-g0gBH3NtAd
unix  3      [ ]     STREAM      CONNECTED          28807    /var/run/dbus/system_bus_socket
```

Рисунок 7 - утилита netstat

7. Iperf. Утилита предназначенная для тестирования пропускной способности. Была поставлена на Ubuntu с помощью команды `sudo apt-get install iperf`. После чего узнали версию поставленной утилиты с помощью команды `iperf -version`, поставили такую же версию ПО на WinXP и произвели тестирование утилиты


```
user@user-virtual-machine: ~
user@user-virtual-machine:~$ iperf -s
-----
Server listening on TCP port 5001
TCP window size: 128 KByte (default)
-----
[  4] local 192.168.40.32 port 5001 connected with 192.168.40.2 port 43567
[ ID] Interval      Transfer    Bandwidth
[  4]  0.0-10.1 sec  41.4 MBytes  34.3 Mbits/sec
```

Рисунок 8 - утилита iperf(ubuntu)

```
Командная строка
C:\Documents and Settings\Администратор\Рабочий стол\iperf-2.0.5-win32>iperf -c
192.168.40.32
-----
Client connecting to 192.168.40.32, TCP port 5001
TCP window size: 64.0 KByte (default)
-----
[  3] local 192.168.120.15 port 1035 connected with 192.168.40.32 port 5001
[ ID] Interval      Transfer    Bandwidth
[  3]  0.0-10.1 sec  41.4 MBytes  34.5 Mbits/sec
C:\Documents and Settings\Администратор\Рабочий стол\iperf-2.0.5-win32>_
```

Рисунок 9 - утилита iperf(winxp)

8. Сканирование уязвимостей сети. Поиск уязвимостей в сети осуществлялось через программу XSpider. Результаты поиска показали, что все обнаруженные уязвимости связаны с хостом Windows XP

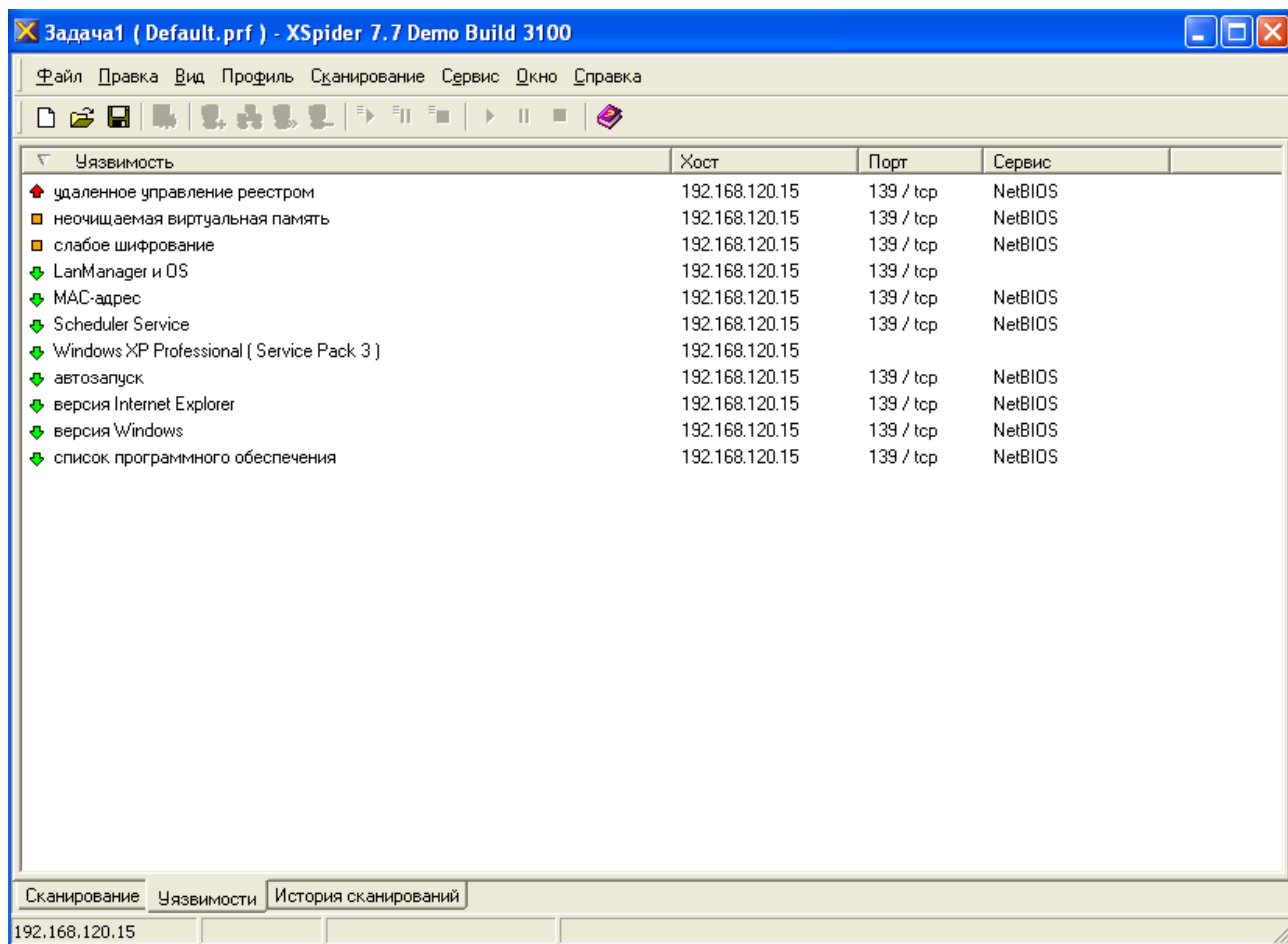


Рисунок 10 - найденные уязвимости

9. Карта сети. Карта строилась в программе 10-Страйк: Схема Сети.

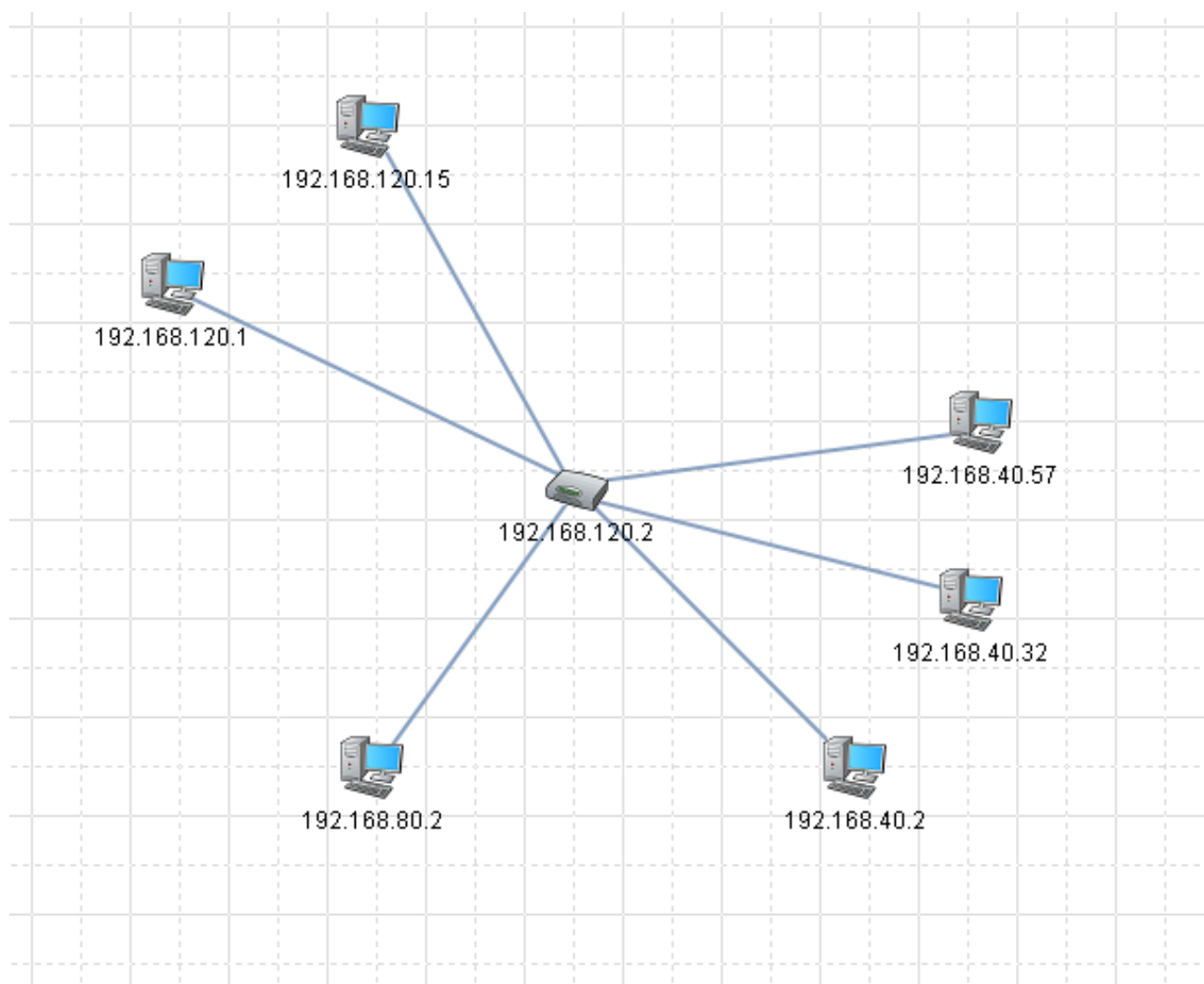


Рисунок 11 - карта сети

Вывод

- Существует множество разного рода полезных утилит и программ для мониторинга и настройки сети;
- Утилиты, которые были использованы в ходе лабораторной работе, были выбраны из-за их главного достоинства – большой функционал, а именно большое количество флагов для разных типов запросов;
- Приложения для мониторинга и анализа сети имеют как преимущества, так и недостатки;
- Были обнаружены уязвимости, связанные с хостом на Windows XP.