

# Лабораторная работа №2

## Тестирование компьютерной сети на основе TCP/IP



**ПОЛИТЕХ**

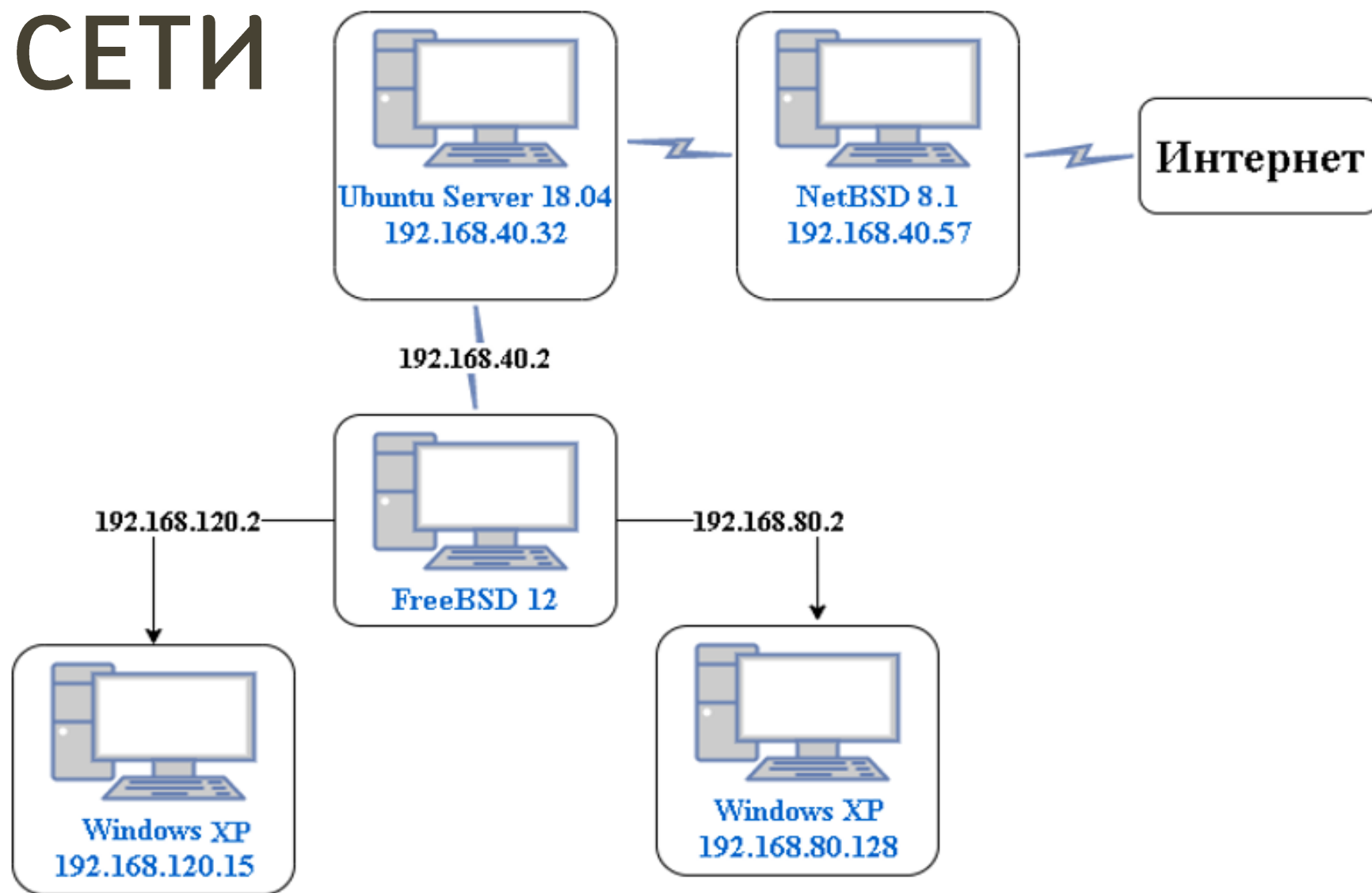
Санкт-Петербургский  
политехнический университет  
Петра Великого

Бараев Дамир  
Группа: 3540901/02001

# ЦЕЛИ РАБОТЫ

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

# СХЕМА СЕТИ



## IFCONFIG ДЛЯ ХОСТА UBUNTU (192.168.40.32)

```
baraev@ubuntu:~$ ifconfig
ens33      Link encap:Ethernet  HWaddr 00:0c:29:11:d9:47
            inet addr:192.168.40.32  Bcast:192.168.40.255  Mask:255.255.255.0
            inet6 addr: fe80::859d:e61:125e:9463/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:36 errors:0 dropped:0 overruns:0 frame:0
            TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:4855 (4.8 KB)  TX bytes:7525 (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:19348 errors:0 dropped:0 overruns:0 frame:0
            TX packets:19348 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:1436865 (1.4 MB)  TX bytes:1436865 (1.4 MB)
```

# ПРОСМОТР ТАБЛИЦЫ ARP

```
root@:~ # arp -a
? (192.168.120.2) at 00:0c:29:d1:91:15 on em2 permanent [ethernet]
? (192.168.80.2) at 00:0c:29:d1:91:0b on em1 permanent [ethernet]
? (192.168.40.32) at 00:0c:29:11:d9:47 on em0 expires in 1154 seconds [ethernet]
? (192.168.40.1) at 00:50:56:c0:00:01 on em0 expires in 889 seconds [ethernet]
? (192.168.40.2) at 00:0c:29:d1:91:01 on em0 permanent [ethernet]
? (192.168.40.57) at 00:0c:29:2d:f6:3b on em0 expires in 1154 seconds [ethernet]
```

Команда `arp -a` запускалась на маршрутизаторе FreeBSD

# УТИЛИТА NETSTAT

netstat -r – просмотр  
таблицы  
маршрутизации.

Команда запускалась  
на маршрутизаторе  
FreeBSD.

```
root@:~ # netstat -r
```

```
Routing tables
```

```
Internet:
```

Destination	Gateway	Flags	Netif	Expire
default	192.168.40.57	UGS	em0	
localhost	link#4	UH	lo0	
192.168.40.0/24	link#1	U	em0	
192.168.40.2	link#1	UHS	lo0	
192.168.80.0/24	link#2	U	em1	
192.168.80.2	link#2	UHS	lo0	
192.168.120.0/24	link#3	U	em2	
192.168.120.2	link#3	UHS	lo0	

```
Internet6:
```

Destination	Gateway	Flags	Netif	Expire
::/96	localhost	UGRS	lo0	
localhost	link#4	UH	lo0	
::ffff:0.0.0.0/96	localhost	UGRS	lo0	
fe80::/10	localhost	UGRS	lo0	
fe80::%lo0/64	link#4	U	lo0	
fe80::1%lo0	link#4	UHS	lo0	
ff02::/16	localhost	UGRS	lo0	

# УТИЛИТА NETSTAT

netstat -i – просмотр  
статистики передачи  
пакетов по  
интерфейсам.

Команда запускалась  
на маршрутизаторе  
FreeBSD.

```
root@:~ # netstat -i
```

Name	Mtu	Network	Address	Ipkts	Ierrs	Idrop	Opkts	Oerrs
em0	1500	<Link#1>	00:0c:29:d1:91:01	115	0	0	28	0
em0	-	192.168.40.0/	192.168.40.2	9	-	-	24	-
em1	1500	<Link#2>	00:0c:29:d1:91:0b	55	0	0	0	0
em1	-	192.168.80.0/	192.168.80.2	3	-	-	0	-
em2	1500	<Link#3>	00:0c:29:d1:91:15	55	0	0	0	0
em2	-	192.168.120.0	192.168.120.2	3	-	-	0	-
lo0	16384	<Link#4>	lo0	0	0	0	0	0
lo0	-	localhost	localhost	0	-	-	0	-
lo0	-	fe80::%lo0/64	fe80::1%lo0	0	-	-	0	-
lo0	-	your-net	localhost	0	-	-	0	-

# УТИЛИТА HOSTNAME

Просмотр и смена хоста для текущего сеанса:

```
baraev@ubuntu:~$ hostname  
ubuntu  
baraev@ubuntu:~$ sudo hostname ubuntuStudent  
[sudo] password for baraev:  
baraev@ubuntu:~$ hostname  
ubuntuStudent
```

Смена имени хоста с сохранением настроек после перезагрузки компьютера (через конфигурационный файл /etc/hostname):

```
baraev@ubuntu:~$ cat /etc/hostname  
ubuntuStudent  
baraev@ubuntu:~$ hostname  
ubuntuStudent
```



# УТИЛИТА TRACERT

Проверка  
доступности хоста  
Ubuntu для  
Windows XP (2) с  
помощью утилиты  
ping.

Определение пути  
пакетов с Windows  
XP (2) до Ubuntu с  
помощью tracert.

```
C:\Documents and Settings\Администратор>ping 192.168.40.32
```

```
Обмен пакетами с 192.168.40.32 по 32 байт:
```

```
Ответ от 192.168.40.32: число байт=32 время=1мс TTL=63
```

```
Ответ от 192.168.40.32: число байт=32 время=1мс TTL=63
```

```
Ответ от 192.168.40.32: число байт=32 время=1мс TTL=63
```

```
Ответ от 192.168.40.32: число байт=32 время=2мс TTL=63
```

```
Статистика Ping для 192.168.40.32:
```

```
Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
```

```
Приблизительное время приема-передачи в мс:
```

```
Минимальное = 1мсек, Максимальное = 2 мсек, Среднее = 1 мсек
```

```
C:\Documents and Settings\Администратор>tracert 192.168.40.32
```

```
Трассировка маршрута к 192.168.40.32 с максимальным числом прыжков 30
```

1	<1 мс	<1 мс	<1 мс	192.168.120.2
2	<1 мс	<1 мс	<1 мс	192.168.40.32

```
Трассировка завершена.
```

# LANSTATE. ЭЛЕМЕНТЫ РАБОТЫ ПРОГРАММЫ

## Шаг 1 из 4. Задание диапазона IP-адресов

В полях "Начальный адрес" и "Конечный адрес" вводятся границы сканирования сети. Для автоматического определения диапазона вашей сети необходимо выбрать текущий сетевой интерфейс.

Интерфейс

AMD PCNET семейство PCI Ethernet адаптеров - Минипорт планировщика пакетов - [192.1 ▼]

Начальный адрес

192 168 120 1



Конечный адрес

192 168 120 254

Добавить



Диапазоны

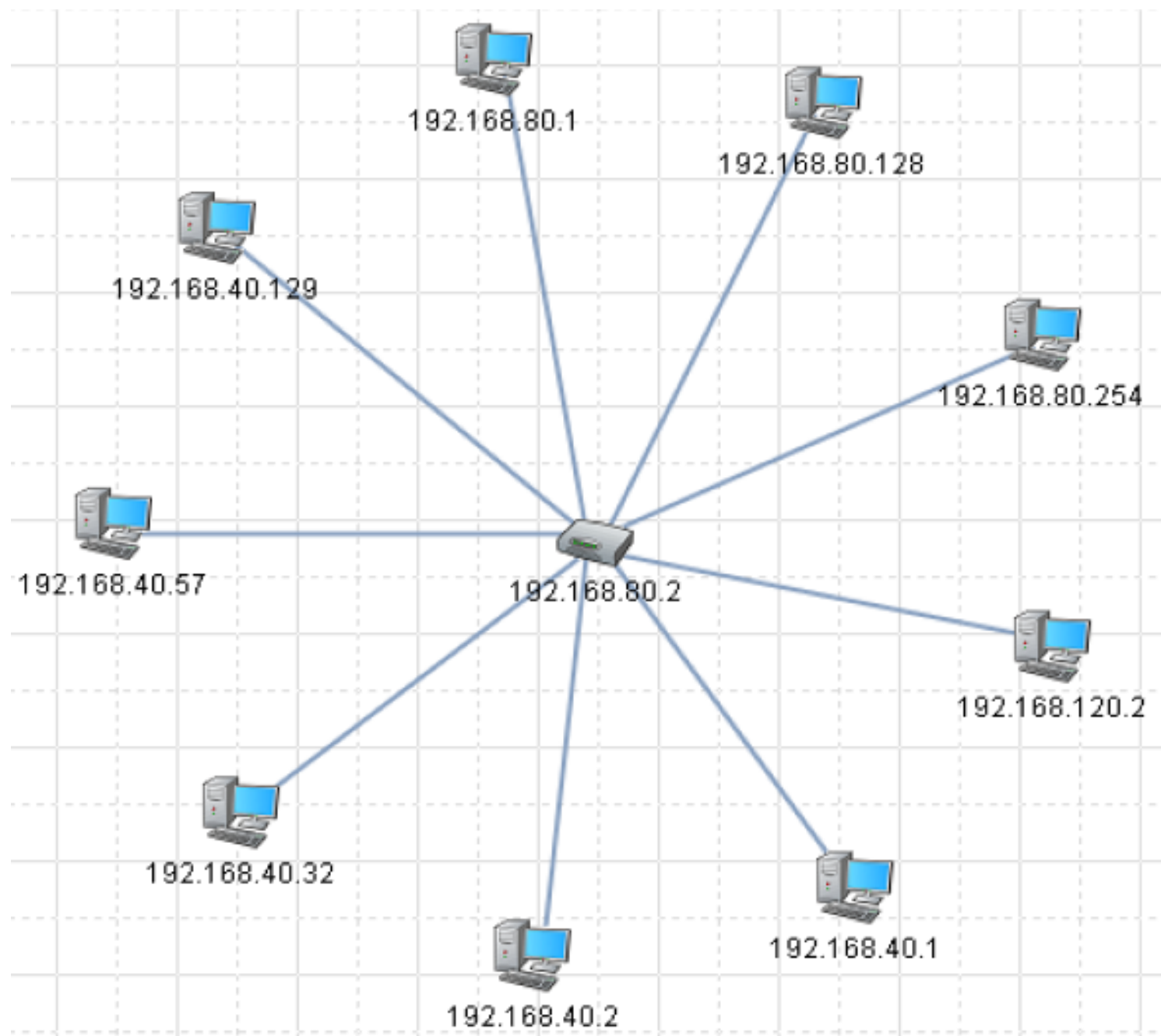
- ☒ 192.168.80.1 - 192.168.80.254
- ☒ 192.168.40.1 - 192.168.40.254
- ☒ 192.168.120.1 - 192.168.120.254

# LANSTATE. ЭЛЕМЕНТЫ РАБОТЫ ПРОГРАММЫ


Шаг 3 из 4. Поиск и отбор компьютеров для помещения на карту









IP-адрес	MAC-адрес	Производитель адаптера	DNS-имя	Тип устройства	Принтер	SNMP-агент	Найден по...
<input checked="" type="checkbox"/> 192.168.40.1	00-50-56-C0-00-01	[VMWare, Inc.]	OPTIMUSGANG	Компьютер	-	-	ICMP
<input checked="" type="checkbox"/> 192.168.40.2				Компьютер	-	-	ICMP
<input checked="" type="checkbox"/> 192.168.40.32				Компьютер	-	-	ICMP
<input checked="" type="checkbox"/> 192.168.40.57				Компьютер	-	-	ICMP
<input checked="" type="checkbox"/> 192.168.40.129				Компьютер	-	-	ICMP
<input checked="" type="checkbox"/> 192.168.80.1	00-50-56-C0-00-02	[VMWare, Inc.]	OPTIMUSGANG	Компьютер	-	-	ICMP
<input checked="" type="checkbox"/> 192.168.80.2	00-0C-29-D1-91-...	[VMware, Inc.]		Роутер	-	-	ICMP
<input checked="" type="checkbox"/> 192.168.80.128	00-0C-29-4F-1D-...	[VMware, Inc.]	baraev-c0d64be...	Компьютер	-	-	ICMP
<input checked="" type="checkbox"/> 192.168.80.254	00-50-56-E0-E8-...	[VMWare, Inc.]		Компьютер	-	-	ARP
<input checked="" type="checkbox"/> 192.168.120.2				Компьютер	-	-	ICMP

# LANSTATE. КАРТА СЕТИ




# XSPIDER. ЗАДАНИЕ ХОСТОВ ДЛЯ СКАНИРОВАНИЯ

[-]  Сканируемые хосты ( 8 )


-  192.168.40.1
-  192.168.40.2
-  192.168.40.32
-  192.168.40.57
-  192.168.40.129
-  192.168.80.1
-  192.168.80.2
-  192.168.80.128










**Добавить диапазон адресов**

 Начальный IP адрес  
192 . 168 . 120 . 1

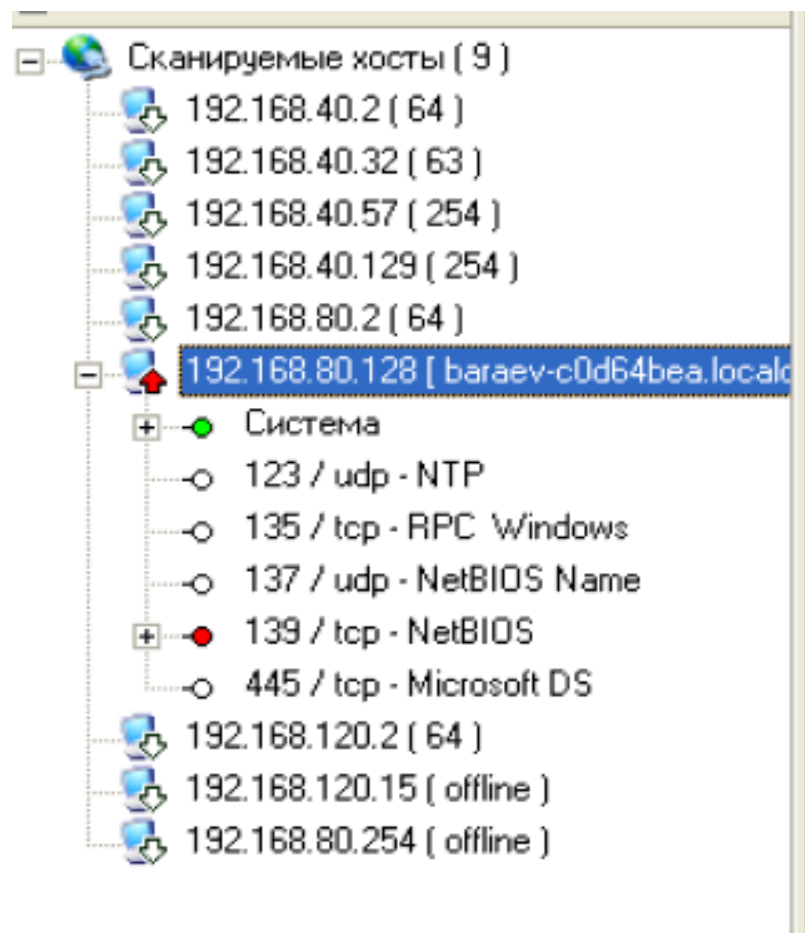
Конечный IP адрес  
192 . 168 . 120 . 254

☒ Добавлять только активные хосты

[-]  Сканируемые хосты ( 9 )

-  192.168.40.2
-  192.168.40.32
-  192.168.40.57
-  192.168.40.129
-  192.168.80.2
-  192.168.80.128
-  192.168.120.2
-  192.168.120.15
-  192.168.80.254

# XSPIDER. РЕЗУЛЬТАТЫ СКАНИРОВАНИЯ



Хост

**192.168.80.128**

## Информация

Имя хоста (полученное при обратном DNS запросе):	<b>baraev-c0d64bea.localdomain</b>
---	------------------------------------

Время отклика:	<b>&lt; 1 мсек</b>
----------------	--------------------

TTL:	<b>128</b>
------	------------

## Параметры сканирования

Начало сканирования:	<b>14:55:28 30.04.2021</b>
----------------------	----------------------------

Время сканирования:	<b>00:03:01</b>
---------------------	-----------------

Версия:	<b>7.7 Demo Build 3100</b>
---------	----------------------------

Профиль:	<b>Default.prf</b>
----------	--------------------

# XSPIDER. СПИСОК УЯЗВИМОСТЕЙ

Уязвимость	Хост	Порт	Сервис
удаленное управление реестром	192.168.80.128	139 / tcp	NetBIOS
неочищаемая виртуальная память	192.168.80.128	139 / tcp	NetBIOS
слабое шифрование	192.168.80.128	139 / tcp	NetBIOS
LanManager и OS	192.168.80.128	139 / tcp	
MAC-адрес	192.168.80.128	139 / tcp	NetBIOS
Scheduler Service	192.168.80.128	139 / tcp	NetBIOS
Windows XP Professional ( Service Pack 3 )	192.168.80.128		
автозапуск	192.168.80.128	139 / tcp	NetBIOS
версия Internet Explorer	192.168.80.128	139 / tcp	NetBIOS
версия Windows	192.168.80.128	139 / tcp	NetBIOS
список программного обеспечения	192.168.80.128	139 / tcp	NetBIOS

# XSPIDER. ОПИСАНИЕ УЯЗВИМОСТИ

## Описание уязвимости

↑ удаленное управление реестром



Серьезная уязвимость

### Удаленное управление реестром

#### Описание

Эта уязвимость существует только в том случае, если Вы не являетесь Администратором на проверяемом хосте.

Возможен полный доступ к реестру хоста.

#### Решение

Отключить возможность удаленного управления реестром.



# УТИЛИТА IPERF

Iperf запущена на хосте Ubuntu (192.168.40.32) как сервер.

Измеряется пропускная способность канала между хостами Ubuntu и Windows XP (192.168.80.128)

```
baraev@ubuntuStudent:~$ iperf -s
-----
Server listening on TCP port 5001
TCP window size: 128 KByte (default)
-----
[  4] local 192.168.40.32 port 5001 connected with 192.168.80.128 port 49402
[ ID] Interval          Transfer        Bandwidth
[  4]  0.0-10.1 sec    49.1 MBytes    45.4 Mbits/sec
```

# УТИЛИТА IPERF

Iperf запущена на Windows XP (192.168.80.128) как клиент.

Измеряется пропускная способность канала между хостами Ubuntu и Windows XP (192.168.80.128)

```
C:\Documents and Settings\Администратор\Рабочий стол>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 192.168.80.128 port 1039 connected with 192.168.40.32 port 5001
[ ID] Interval           Transfer     Bandwidth
[  3]  0.0-10.1 sec   49.1 MBytes  45.4 Mbits/sec
C:\Documents and Settings\Администратор\Рабочий стол>
```

# ВЫВОДЫ

1. Произведено тестирование сети, эмуляция которой проводилась в лабораторной работе №1.
2. Получена информация о сетевых интерфейсах для хоста Ubuntu (192.168.40.32) с помощью утилиты `ifconfig`.
3. Получена динамическая таблица MAC-адресов элементов сети с помощью утилиты `arp`.
4. Получена таблица маршрутизации для хоста Ubuntu и статистика передачи пакетов для всех интерфейсов хоста с помощью утилиты `netstat`.
5. Получено и изменено имя хоста с помощью утилиты `hostname`.
6. Произведена проверка доступности хостов сети при помощи утилиты `ping`, а также получен путь пакетов по сети с помощью утилиты `tracert`.
7. Построена карта сети с помощью программы LANState.
8. Выявлен список уязвимостей сети с помощью программы Xspider.
9. Получена пропускная способность канала между хостами Ubuntu и Windows XP с помощью утилиты `iperf`, пропускная способность составляет 45.4 Мбит/сек.