

Санкт-Петербургский политехнический университет Петра Великого

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №4

Курс: **Администрирование компьютерных сетей**

Тема: **Устранение уязвимостей**

---

Студент: **Д.В. Круминьш**

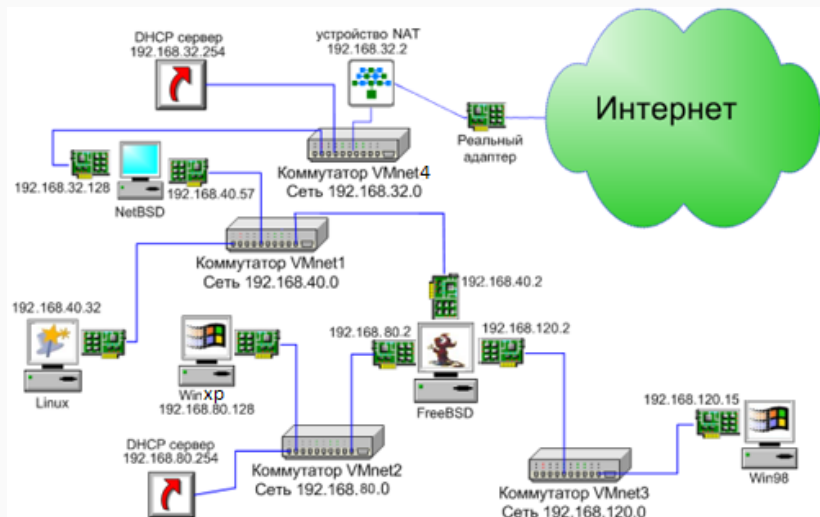
Группа: **13541/3**



Преподаватель: **И.А. Малышев**

1. Устранение найденных уязвимостей хостов в сети.

# Схема компьютерной сети



Ранее были выявлены следующие уязвимости:

- Windows XP (192.168.80.128)
  - сервисом NTP открыт порт 123 по UDP;
  - сервисом RPC Windows открыт порт 135 по TCP;
  - сервисом NBNS открыт порт 137 по UDP;
  - сервисом NetBIOS открыт порт 139 по TCP.
- Windows 98 (192.168.120.15)
  - сервисом NetBIOS-SSN открыт порт 137 по UDP;
  - сервисом NetBIOS открыт порт 139 по TCP.

Устранить данные уязвимости можно следующими способами:

1. установка патчей безопасности;
2. редактирование реестра и системных настроек;
3. настройка межсетевого экрана.

В данном случае будет настроен межсетевой экран, который будет настроен на хосте с FreeBSD.

Внесем следующие настройки в файл `/etc/rc.conf`:

```
firewall_enable="YES"  
firewall_type="/usr/fw_rules/ruleFile"
```

Первой строчкой включается межсетевой экран, а второй файл с фильтрами.

В созданный файл `/usr/fw_rules/ruleFile` внесем следующие строчки:

```
# Windows XP
add deny udp from any to 192.168.80.128 123
add deny tcp from any to 192.168.80.128 135
add deny udp from any to 192.168.80.128 137
add deny tcp from any to 192.168.80.128 139

# Windows 98
add deny udp from any to 192.168.120.15 137
add deny tcp from any to 192.168.120.15 139

# Allow all other packets
add allow in
add allow out
```

Данными правилами были заблокированы пакеты, которые могут использовать уязвимости.

После этого необходимо перезагрузить систему.

В качестве проверки можно использовать утилиту **telnet**. Например, проверим доступность порта 139 до включения экрана:

```
root@FreeBSD:~ # telnet 192.168.80.128 139
Trying 192.168.80.128...
Connected to 192.168.80.128.
Escape character is '^I'.
^CConnection closed_ by foreign host.
```

После включения экрана:

```
root@FreeBSD:~ # telnet 192.168.80.128 135
Trying 192.168.80.128...
^C
```

Как и ожидалось, установить соединение с выбранным портом не удалось.



В данной работе были рассмотрены возможности по устранению уязвимостей ОС.

Наилучшим решением будет являться установка последних патчей безопасности, но это не всегда возможно.

Более оперативным и гибким решением является настройка межсетевого экрана, что и было сделано в данной работе.