

САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО

КАФЕДРА КОМПЬЮТЕРНЫХ СИСТЕМ И ПРОГРАММНЫХ ТЕХНОЛОГИЙ

Отчёт по лабораторной работе №4

Курс: «Администрирование компьютерных сетей»

Тема: «Устранение уязвимостей»

Выполнил студент:

Ерниязов Тимур Ертлеуевич

Группа: 13541/2

Проверил:

Малышев Игорь Алексеевич

Санкт-Петербург
2019 г.

Содержание

1	Лабораторная работа №4	2
1.1	Цели работы	2
1.2	Выполнение работы	2

Лабораторная работа №4

1.1 Цели работы

1. Устранение найденных уязвимостей хостов в сети.

1.2 Выполнение работы

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.

На узле с FreeBSD, внесем следующие строчки в файл **/etc/rc.conf**:

```
1 firewall_enable="YES"
2 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:

```
1 # Windows XP
2 add deny udp from any to 192.168.80.128 123
3 add deny tcp from any to 192.168.80.128 135
4 add deny udp from any to 192.168.80.128 137
5 add deny tcp from any to 192.168.80.128 139
6
7 # Windows 98
8 add deny udp from any to 192.168.120.15 137
9 add deny tcp from any to 192.168.120.15 139
10
11 # Allow all other packets
12 add allow in
13 add allow out
```

Данными правилами были заблокированы пакеты, которые могут использовать уязвимости. Применения правил идет сверху вниз, поэтому остальные пакеты проигнорируют правила для узлов с уязвимостями и к ним будут применены правила типа **add allow in** или **add allow out** то есть пропуск всех исходящих и входящих пакетов.

После этого, для применения правил, необходимо перезагрузить систему.

В качестве проверки можно использовать утилиту **telnet**.

Например команда **telnet 192.168.80.128 135** успешно установит соединение с уязвимым портом до включения межсетевого экрана. После включения, как и ожидается, соединение установить не получится, что говорит о невозможности использовать данный порт как уязвимость.

Вывод

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.