Санкт-Петербургский политехнический университет Петра Великого
Институт компьютерных наук и технологий

Кафедра компьютерных систем и программных технологий

Отчет о лабораторной работе №4

Курс: Администрирование компьютерных сетей

Тема: Устранение уязвимостей

Выполнил студент группы 13541/3 _____ Д.В. Круминьш
(подпись)

Преподаватель _____ И.А. Малышев
(подпись)

Санкт-Петербург
2018 г.

1 Цели работы

1. Устранение найденных уязвимостей хостов в сети.

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**:

```
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. Применения првил 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** тоесть 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.