Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»

Факультет информационных технологий и управления
Кафедра интеллектуальных информационных технологий
Дисциплина «Средства и методы защиты информации в интеллектуальных системах»

ОТЧЁТ
к лабораторной работе №6
на тему
«МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ»

БГУИР 6-05-0611-03 130

Выполнил студент группы 321701
СЕМЕНЯКО Владимир Дмитриевич

_____
(дата, подпись студента)

Проверил
САЛЬНИКОВ Даниил Андреевич

_____
(дата, подпись преподавателя)

Минск 2025

1 ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

а) Создать папку с общим доступом на виртуальной машине с ОС Windows.

б) Настроить брандмауэр, применив различные политики:

– доступ к разделяемому ресурсу разрешен только компьютеру с данным IP-адресом;

– доступ к виртуальной машине разрешен только по заданным портам (например, www или ftp);

– доступ к виртуальной машине разрешен только по заданным портам (например, www или ftp) и только компьютерам с данным IP-адресом (адресами);

– доступ к внешним ресурсам разрешен только конкретным программам;

– конкретной программе разрешен доступ к ресурсам удаленного компьютера с данным IP-адресом по заданному порту;

– запретить запрос входящего эха (ICMP).

Для выполнения задания использовалась операционная система **macOS** с установленной **виртуальной машиной Windows** в среде **UTM** (Universal Turing Machine — программа виртуализации).

2 ВЫПОЛНЕНИЕ РАБОТЫ

На виртуальной машине Windows создана папка *Share*. В свойствах папки на вкладке «Доступ» включён общий доступ и добавлена группа пользователей Everyone с правами чтения и записи.

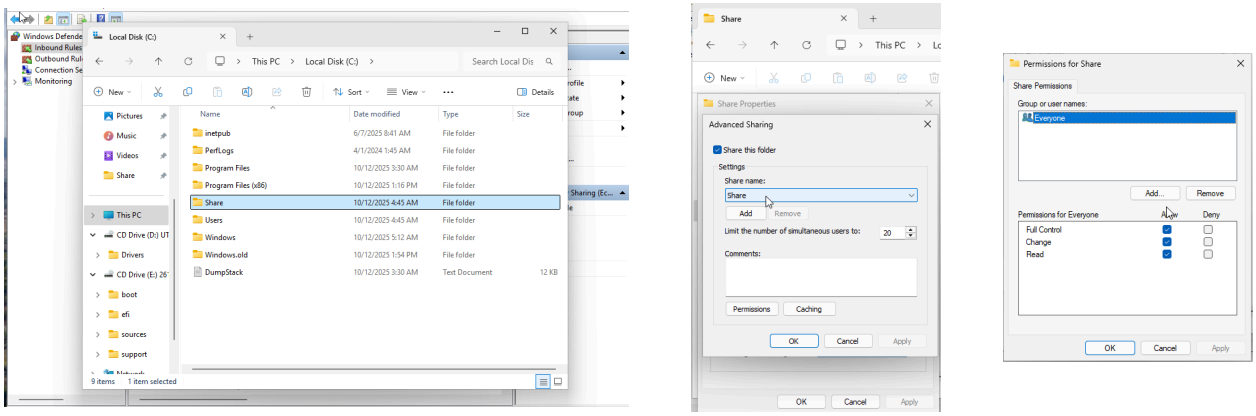

Рисунок 1 – Создание папки Share и настройка доступов

Для доказательства возможности общего доступа к папке Share, запустим на клиенте подключение к ”импровизированному”серверу

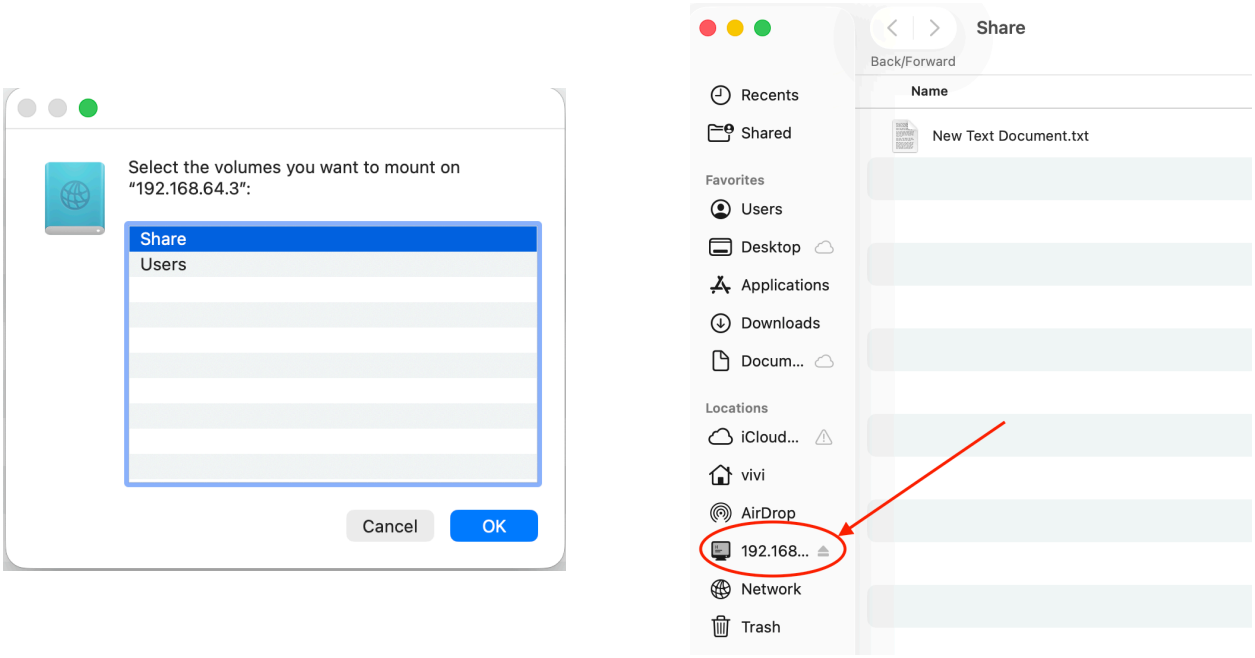

Рисунок 2 – Результат подключения к папке Share со стороны клиента

Далее рассмотрим различные настроенные политики брандмауэра

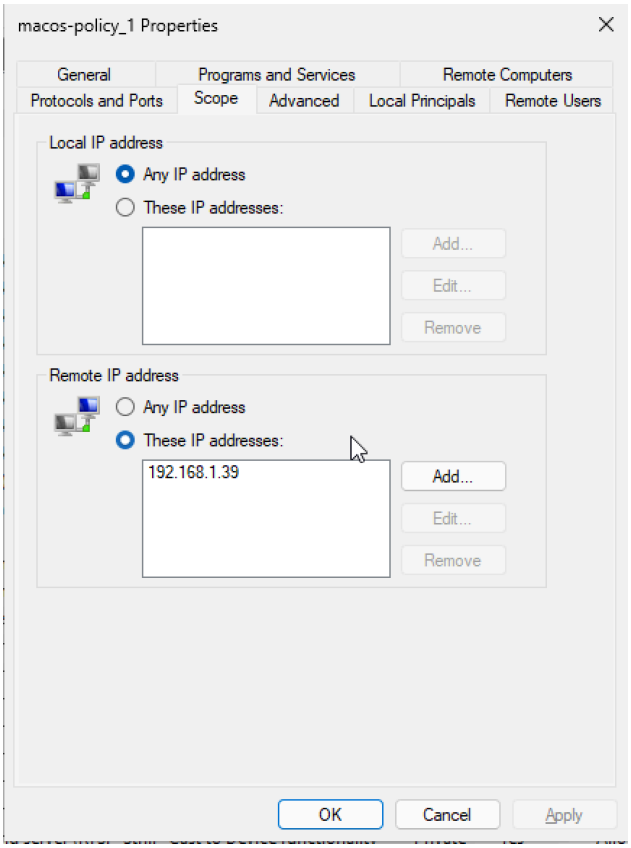

Рисунок 3 – Настройка политики: доступ к разделяемому ресурсу разрешен только компьютеру с указанным IP-адресом

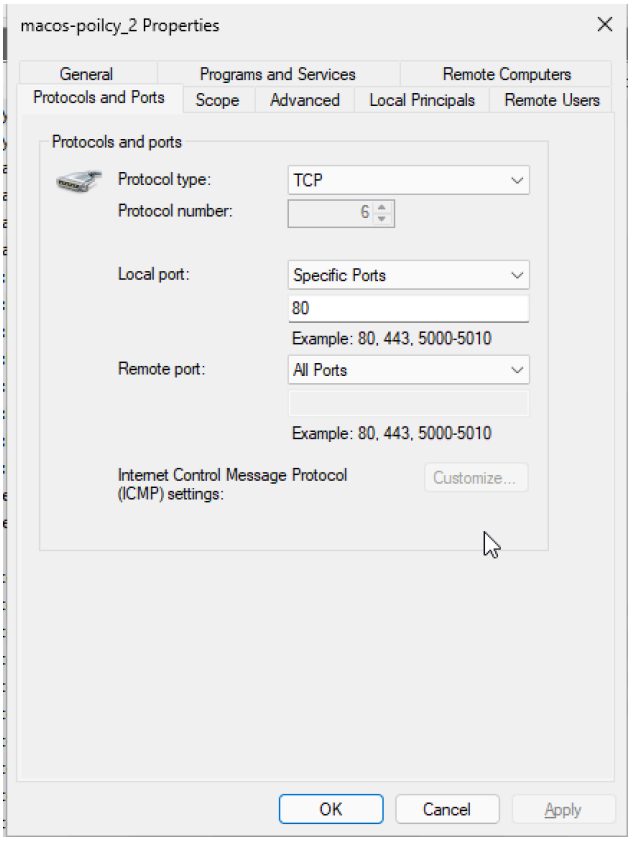

Рисунок 4 – Настройка политики: доступ к виртуальной машине разрешен только по заданным портам

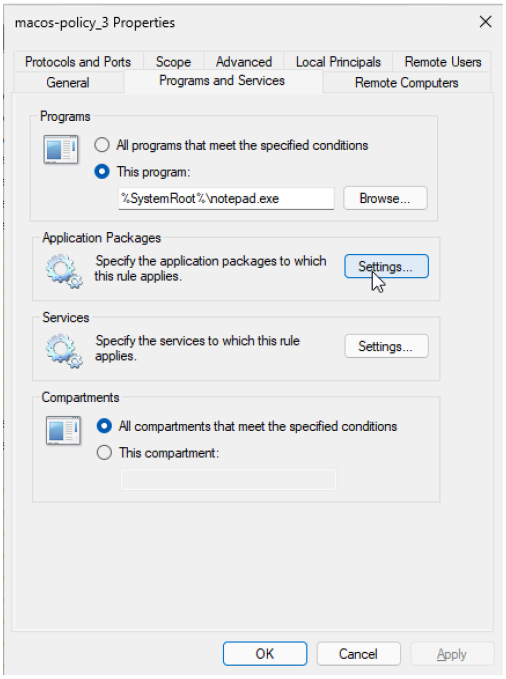

Рисунок 5 – Настройка политики: доступ к внешним ресурсам разрешен только конкретным программам

Для настройки политики запрета запроса эхо, отключим политику ***File and Printer Sharing (Echo Request - ICMPv4-In)***. Результат выполнения представлен на рисунках ниже

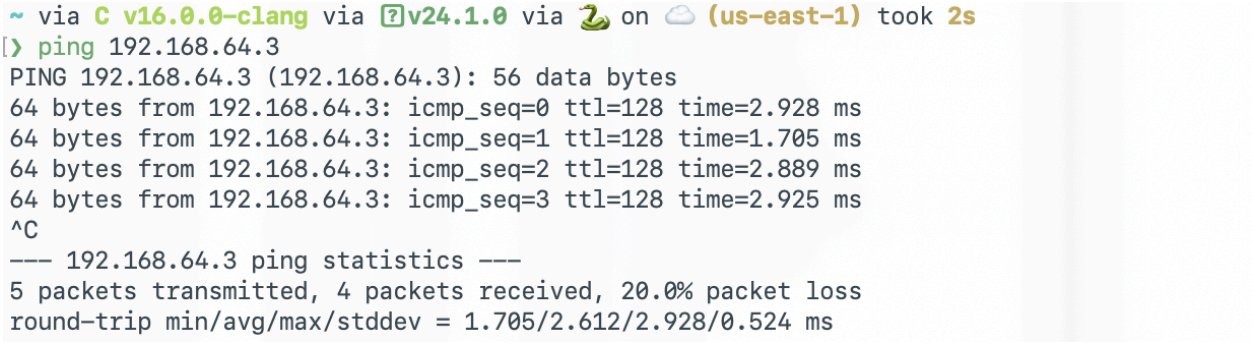

Рисунок 6 – Результат выполнения команды ping до применения политики

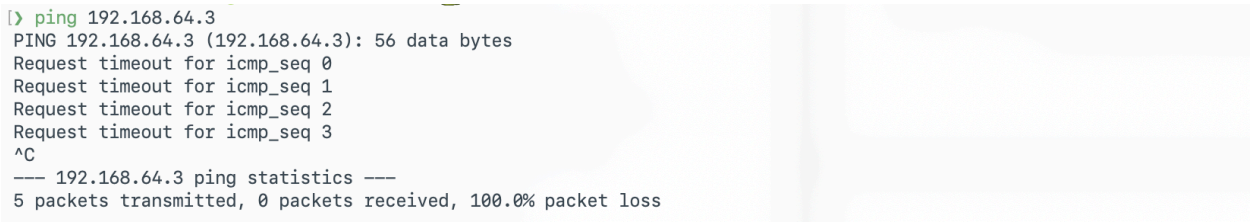

Рисунок 7 – Результат выполнения команды ping после применения политики

ВЫВОД

В ходе лабораторной работы были изучены принципы настройки брандмауэра Windows (firewall — сетевой экран) и применения различных политик безопасности.

Были реализованы следующие политики:

а) ограничение доступа по IP-адресам;
б) фильтрация соединений по портам;
в) создание правил для конкретных программ;
г) блокировка ICMP-запросов.