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

Выполнил: Потоцкий Д.А.

Группа: 221702

Проверила: Крищенович В.А.

Минск 2024

Лабораторная работа №6

МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ

**Задание:** 1) Создать папку с общим доступом на одной из виртуальных машин.

2) Настроить брандмауэр, применив различные политики:

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

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

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

г) доступ к внешним ресурсам разрешен только конкретным программам;

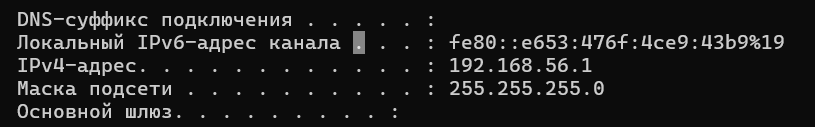
д) конкретной программе разрешен доступ к ресурсам удаленного

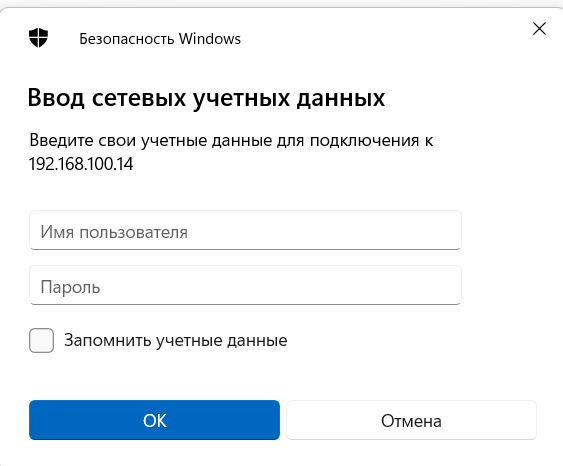
компьютера с данным IP-адресом по заданному порту;

е) запретить запрос входящего эха (ICMP).

3) Оформить отчет, подтверждающий применение указанных политик.

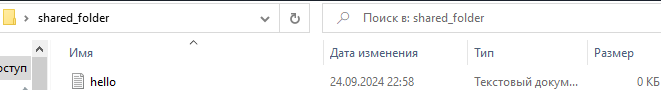
**Ход работы:**  
**а) Доступ к разделяемому ресурсу разрешён только компьютеру с определённым IP-адресом**   
Для начала, в настройках виртуальной машины выберем тип сети Bridge. Это позволит виртуальной машине получать IP-адрес из той же сети, что и основной ПК с Windows 11.

Далее получим IP-адрес виртуальной машины с помощью команды ipconfig  
  
Затем настроим брандмауэр для управления доступом к общему ресурсу по IP-адресу. Для этого нам необходимо открыть бранмауэр, во входящих правилах выбрать “создать новое правило”. Тип правила “Для порта”. Это означает, что правило будет касаться управления соединениями по определённому порту. Далее мы выбираем тип протокола TCP и в поле “Определённые локальные порты” необходимо ввести значение 445 (это порт, используемый для доступа к общим папкам через протокол SMB). Затем в окне “Применить это правило только для этих IP-адресов” в поле “Удалённые IP-адреса” необходимо выбрать опцию “Эти IP-адреса”.

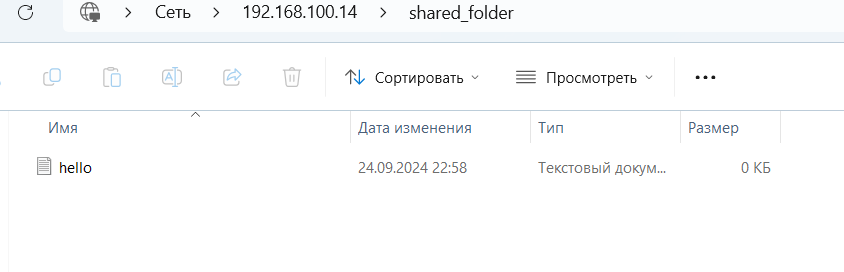
Нажимаем кнопку **“**Добавить**”** и вводим IP-адрес виртуальной машины, который мы узнали с помощью команды ipconfig. Если всё настроено верно, у нас появится следующее окно  


Здесь необходимо ввести информацию о пользователе виртуальной машины, после чего можно увидеть все данные, которые содержатся в данной папке

Содержимое папки на виртуальной машине:



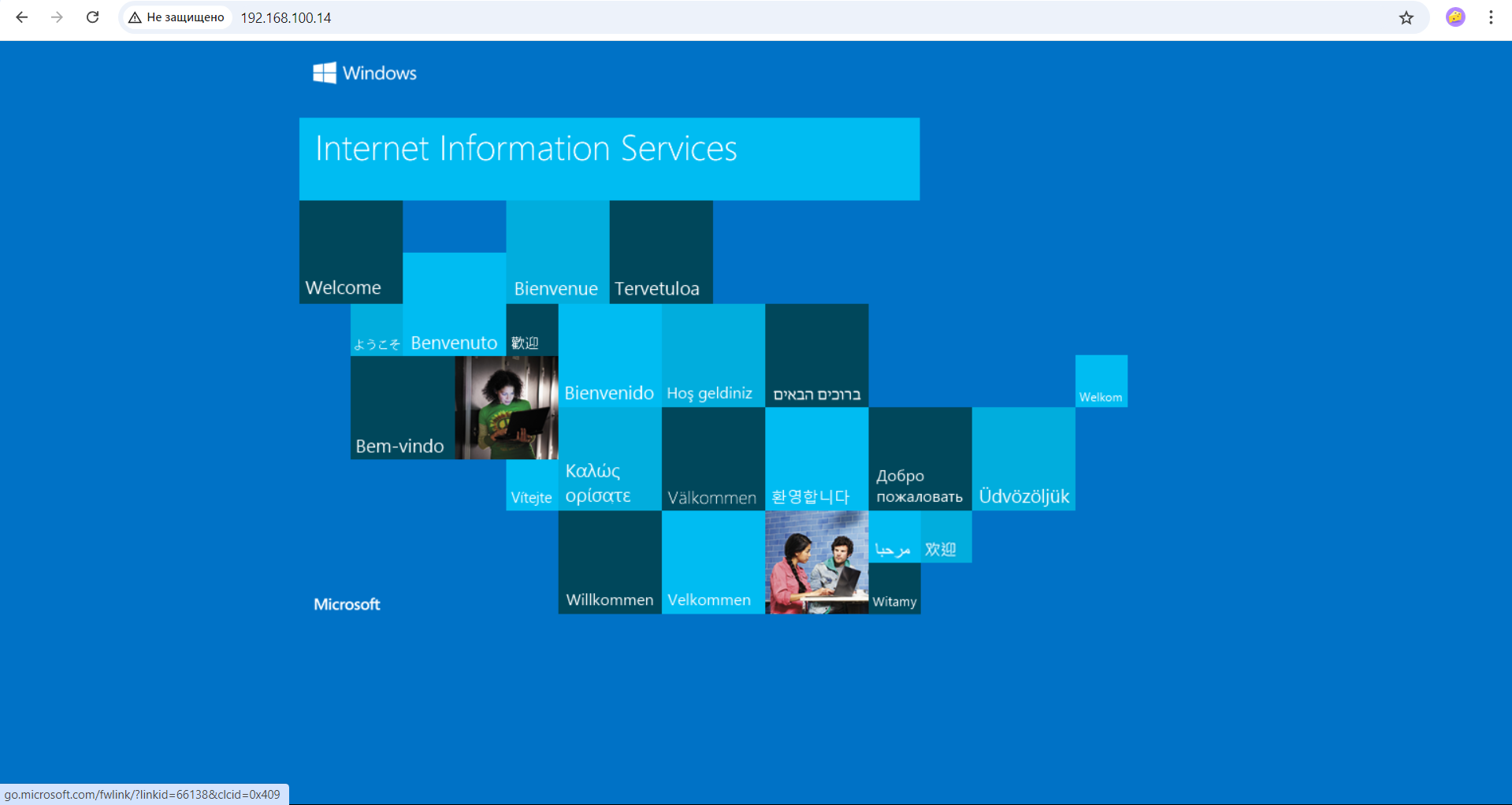
Содержимое папки на основном ПК:

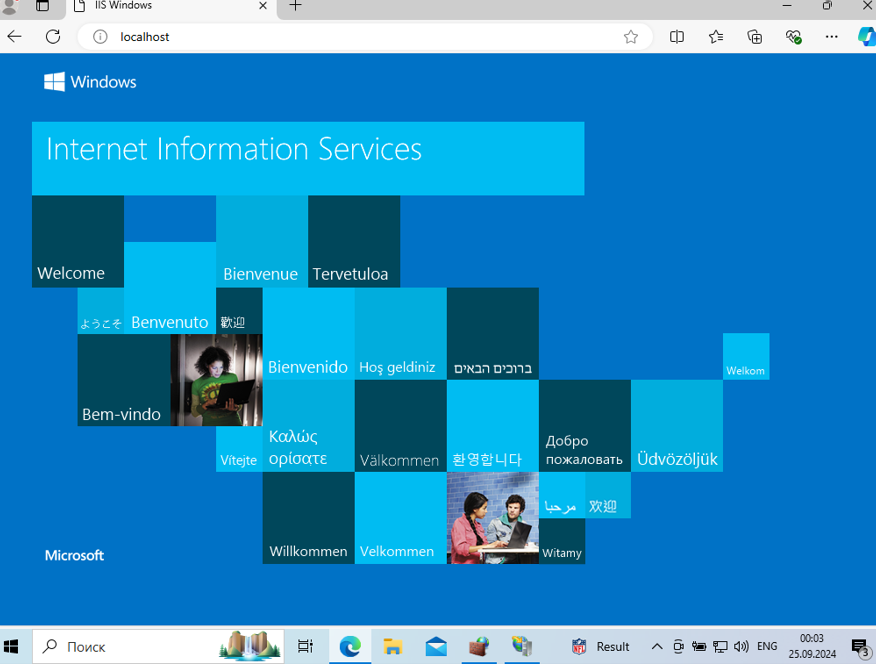
  
**б) доступ к виртуальной машине разрешен только по заданным портам (например, www или ftp);**

Для создания правила доступа по портам нам необходимо сделать следующее

* Нажать на “Создать правило” в правом меню.
* Выбрать “Для порта” и нажать “Далее”.
* Выбрать “TCP” и ввести “80”.
* Нажать “Далее”, выбрать “Разрешить подключение” и нажать “Далее”.
* Выбрать нужные профили (Домен, Частный, Общедоступный) и нажать “Далее”.
* Назвать правило (например, "HTTP Port 80") и нажать “Готово”.

Доступ к сайту с основного ПК:



Доступ к сайту с виртуальной машины:  


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

В данном случае мы применим комбинацию правил, полученных в пункте а) и б), результат будет такой же, как и в пункте б)

**г) доступ к внешним ресурсам разрешен только конкретным программам;**

Для создания данного правила необходимо выбрать “создать правило” в “правилах для исходящего подключения”, выбрать “для программы”, затем указать путь, по которому расположена исполняемая программа. В случае, если всё выполнено верно, то мы получим результат, аналогичный пункту б)

**д) конкретной программе разрешен доступ к ресурсам удаленного**

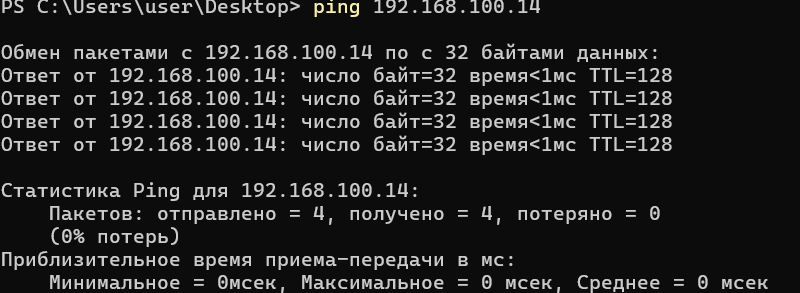
**компьютера с данным IP-адресом по заданному порту;**

Для создания данного правила нам необходимо повторить алгоритм пункта г), только вместо “правила для исходящего подключения” выбрать “правила для входящего подключения”. Данное правило необходимо применять вместе с правилами a) и б). В случае корректной работы мы увидим результат, аналогичный пункту б)

**е) запретить запрос входящего эха (ICMP).**

Для выполнения данной задачи необходимо ввести команду   
*netsh advfirewall firewall add rule name="Block ICMP" protocol=ICMPV4 dir=in action=block*

После чего запрос входящего эха будет запрещён  
Запрос входящего эха до введения команды:



Запрос входящего эха после введения команды:

