**Лабораторная работа по теме № 15. Настройка удаленного доступа в ОС Windows. Сниффинг.**

**Цель:** освоить навык организации удаленного управления по RDP и сниффинга.

**Задачи:**

1. включение и настройка удаленного управления на установленных ранее виртуальных машинах;
2. знакомство со структурой пакетов HTTP с помощью сниффинга.

**Порядок выполнения работы.**

1. Зайдите в «Панель управления», «Система», «Настройка удаленного доступа» и установите переключатель в положение «Разрешить удаленные подключения к этому компьютеру».

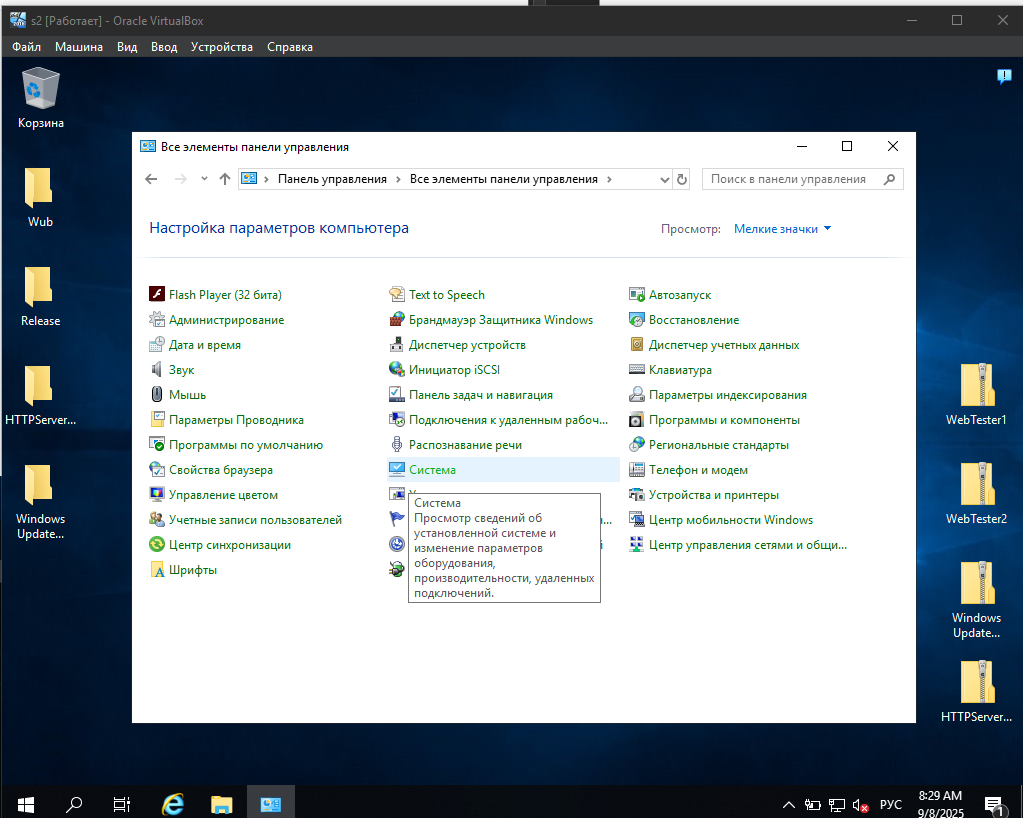


Рисунок 1.1 – Панель управления

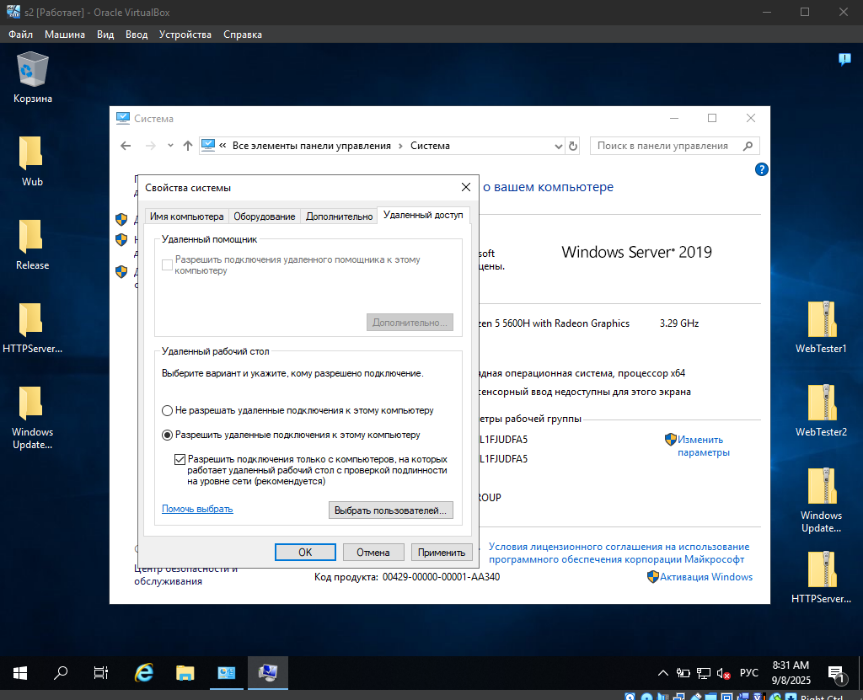


Рисунок 1.2 – Настройка удаленного доступа

1. Зайдите в редактор реестра, откройте раздел HKEY\_LOCAL\_MACHINE\ System\ CurrentControlSet\ Control\ Terminal Server\ WinStations\ RDP-Tcp\ и установите значение параметра PortNumber равным

10000 + <число рождения> \* 100 + <месяц рождения>

10000 + 28 \* 100 + 11 = 12811

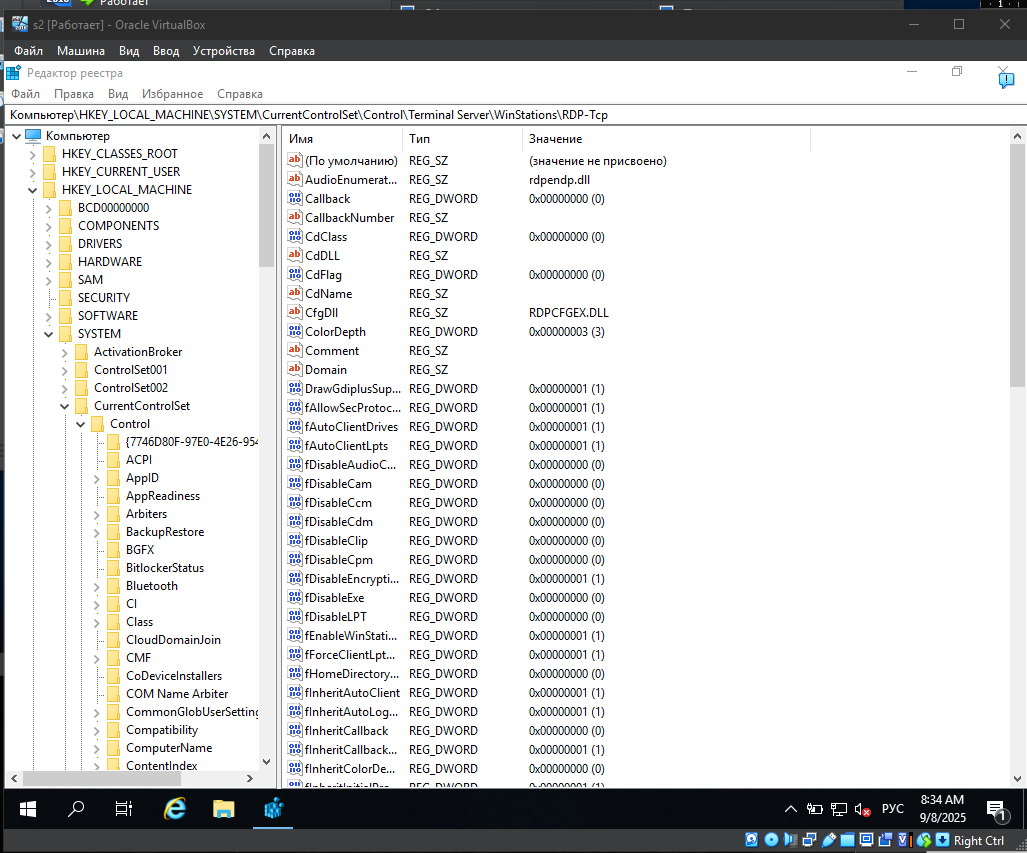


Рисунок 1.3 – Раздел раздел HKEY\_LOCAL\_MACHINE\ System\ CurrentControlSet\ Control\ Terminal Server\ WinStations\ RDP-Tcp\

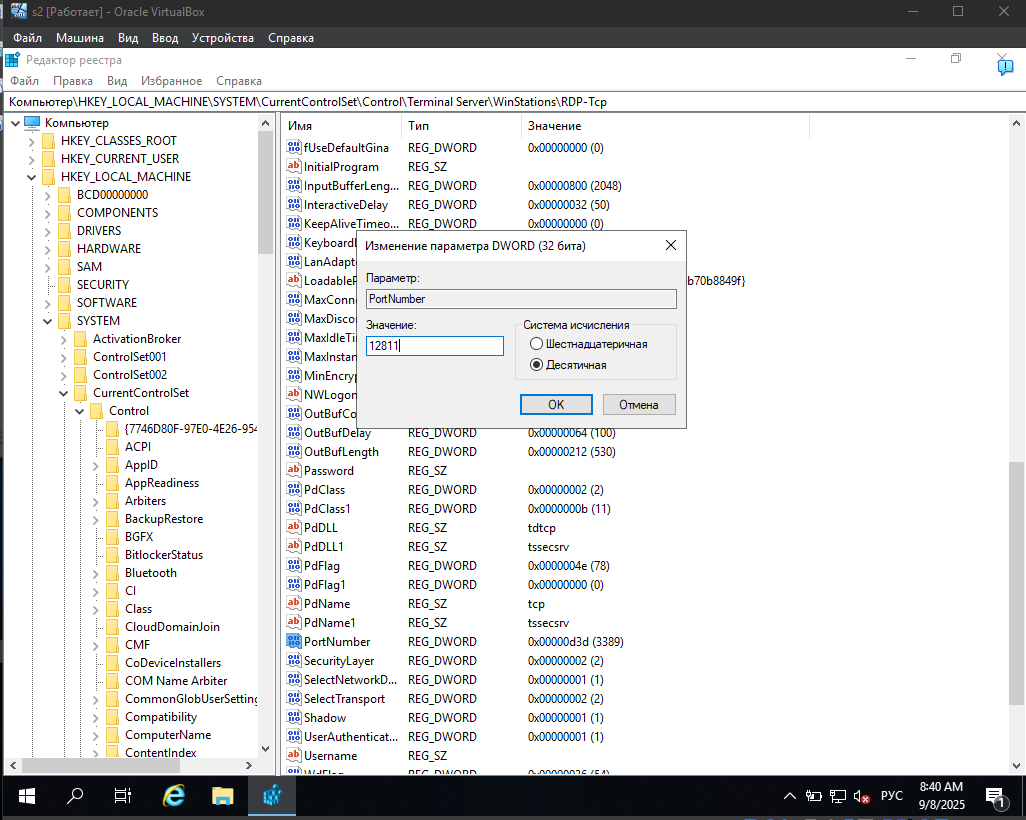


Рисунок 1.4 – Установка значения PortNumber

1. В бранмауэре создайте правило для разрешения входящих подключений на указанный для RDP порт.

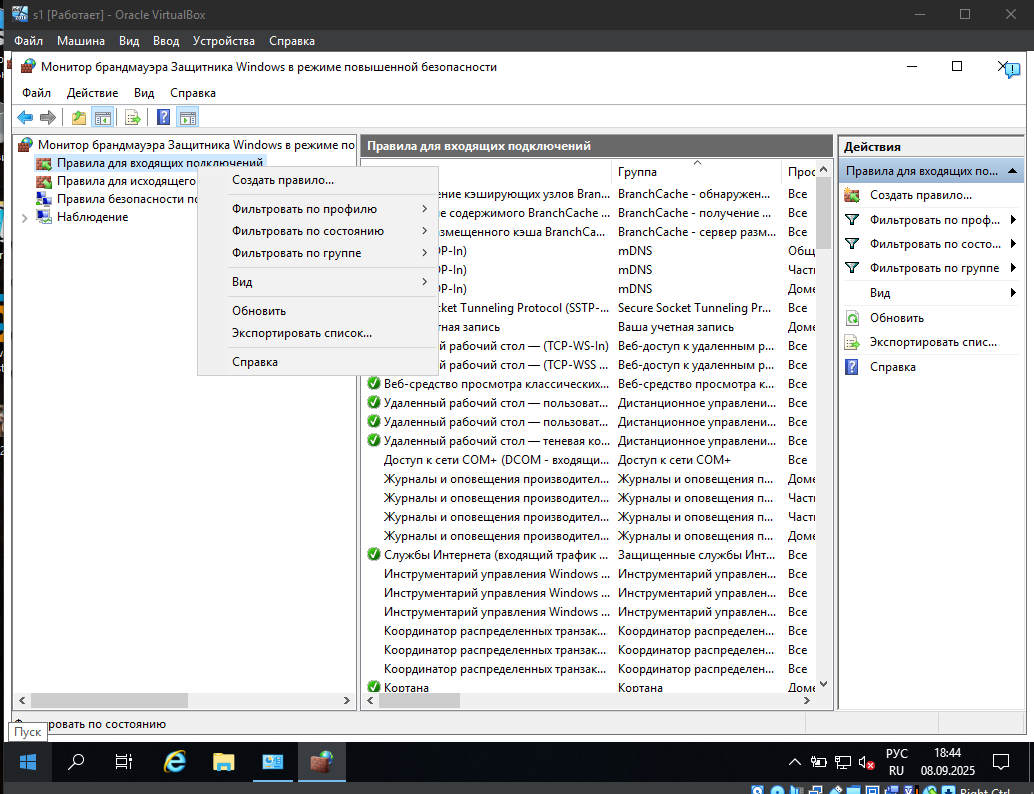


Рисунок 1.5 – Монитор брандмауэра Защитника Windows

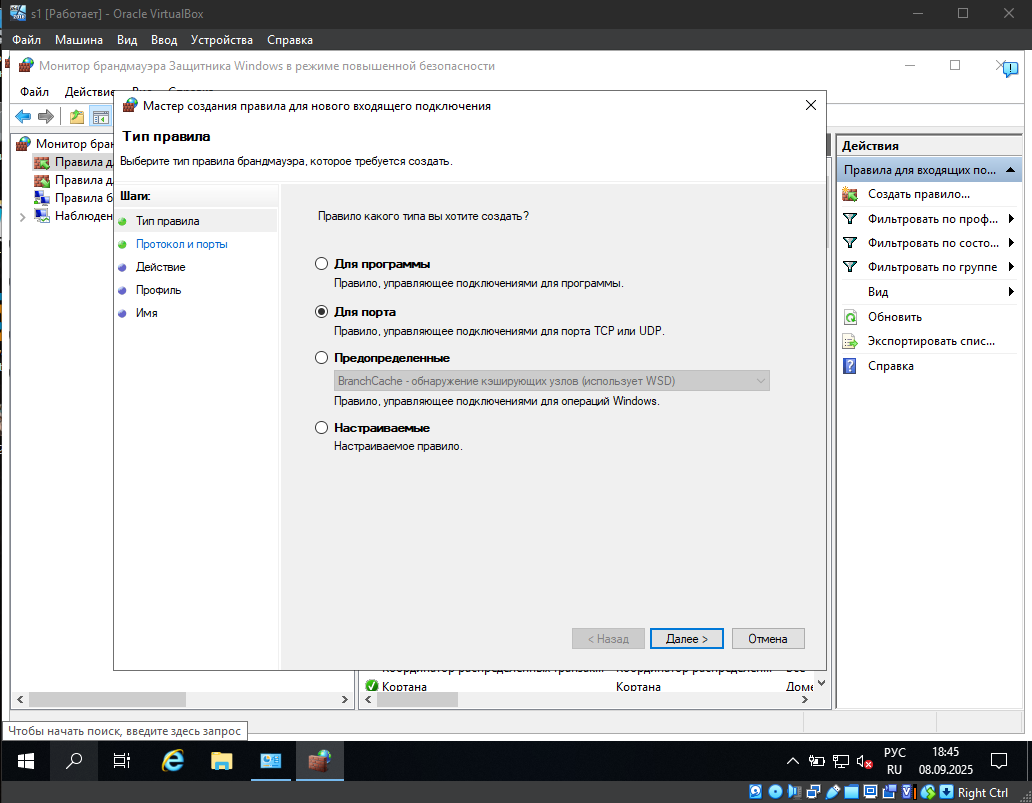


Рисунок 1.6 – Выбор типа правила

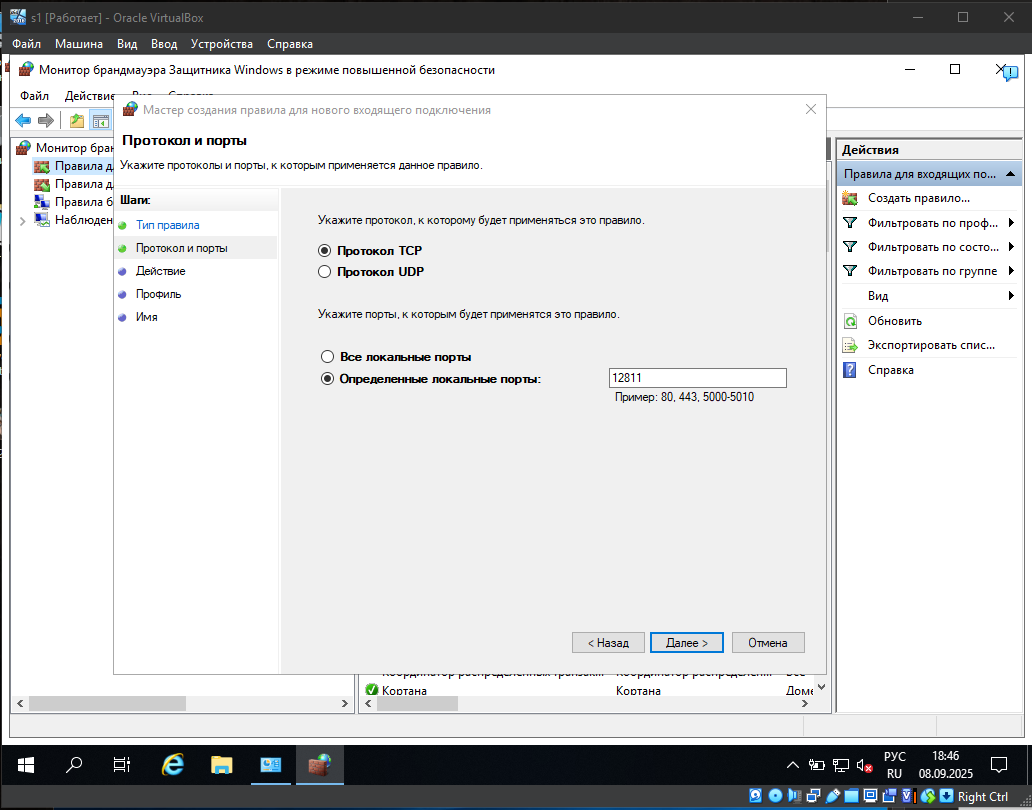


Рисунок 1.7 – Ввод порта

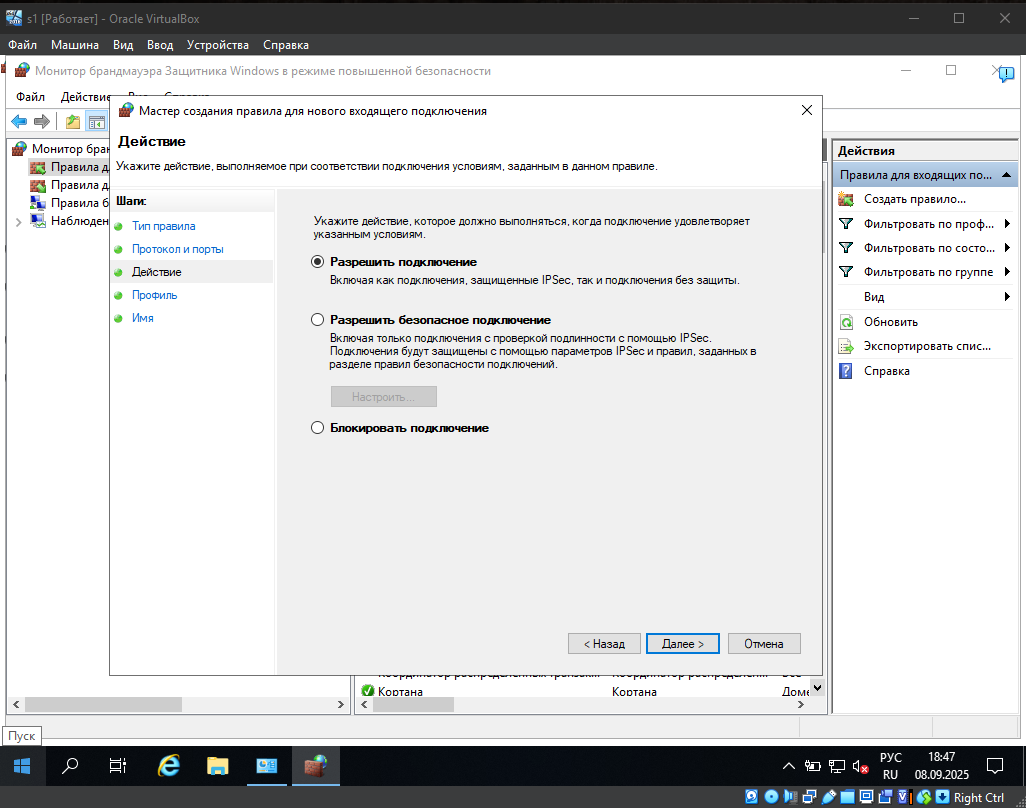


Рисунок 1.8 – Разрешение подключения

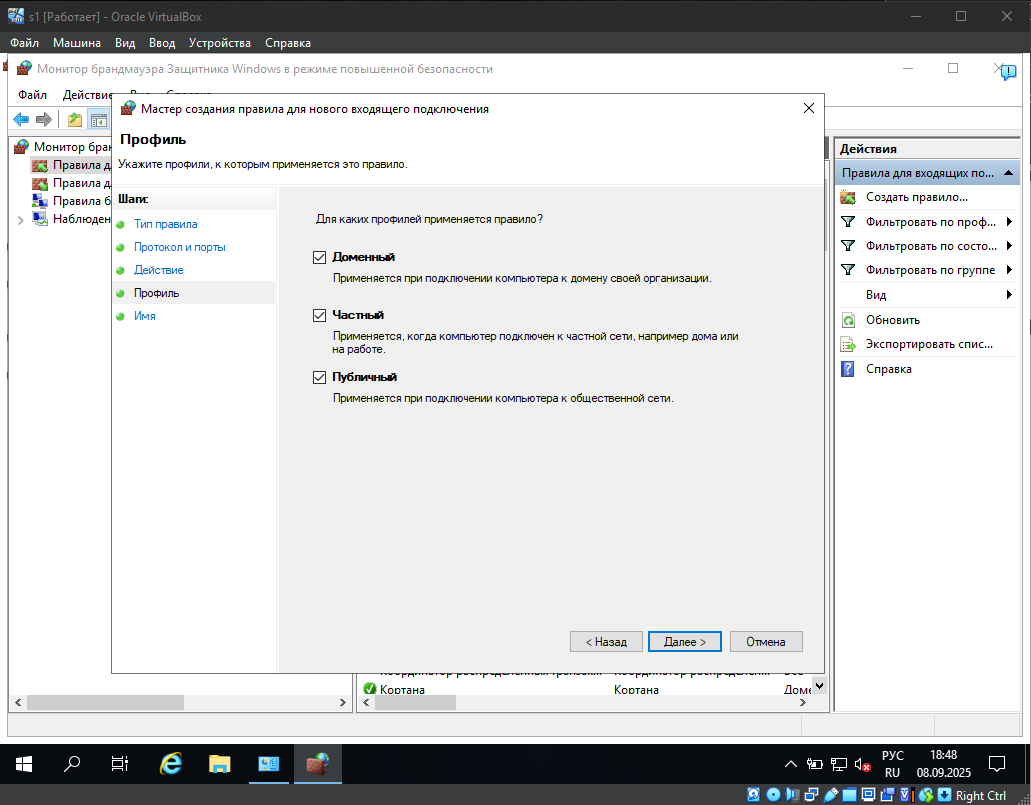


Рисунок 1.9 – Выбор профилей

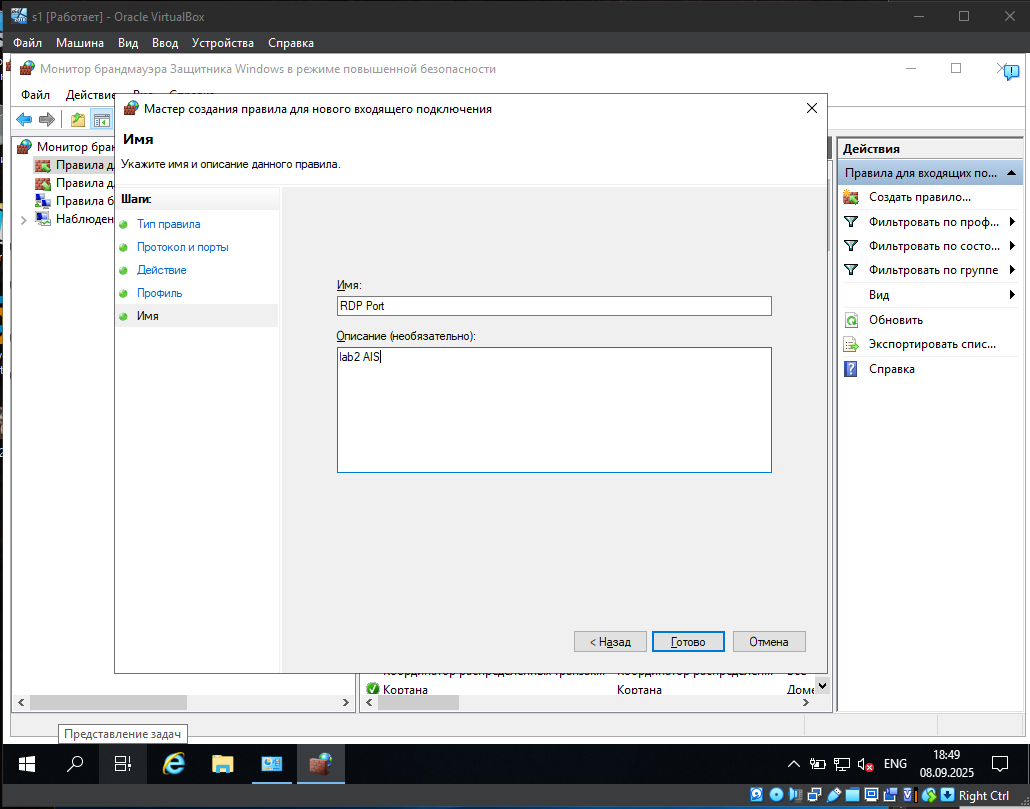


Рисунок 1.10 – Ввод имени и описания правила

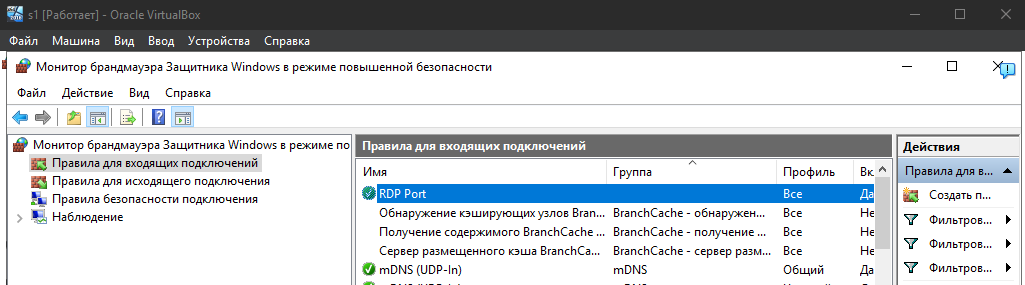


Рисунок 1.11 – Созданное правило в списке

1. Скопируйте на виртуальную машину с файлового сервера по имени «A246K401» или IP-адресам «172.16.0.38» или «172.16.192.252» из папки «!admin\2» установочный пакет «Wireshark-win64-3.2.1.exe» и установите его. Логин: user, пароль: 777.

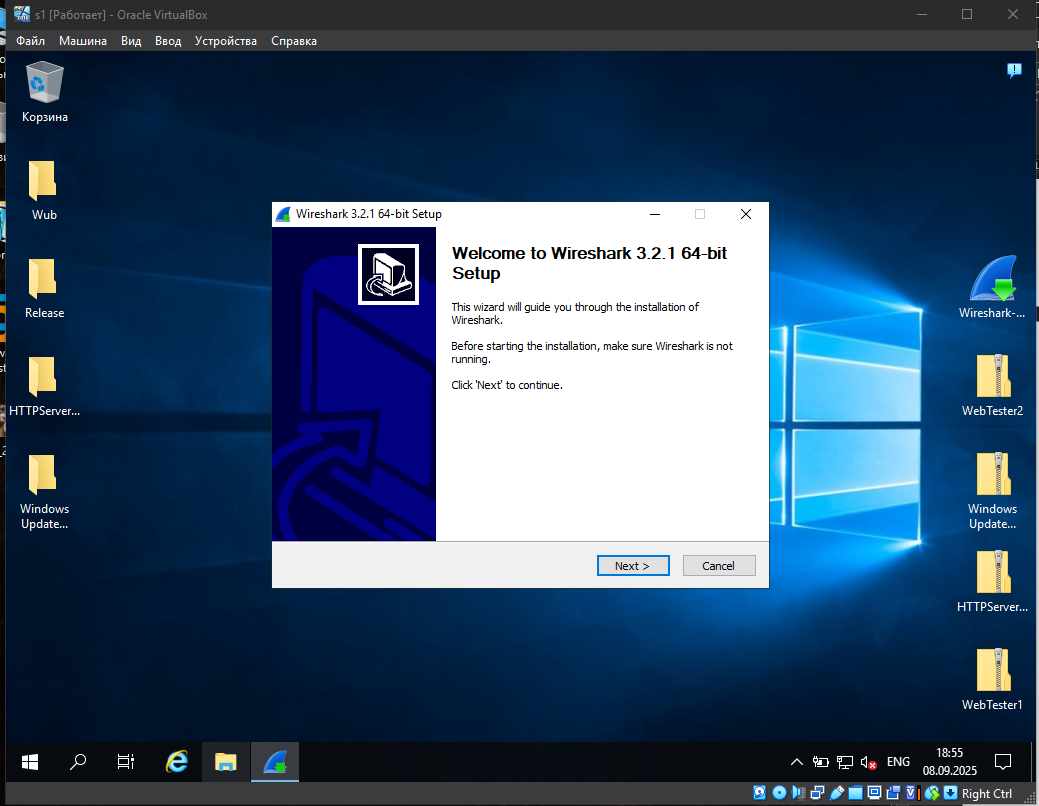


Рисунок 1.12 – Мастер установки Wireshark

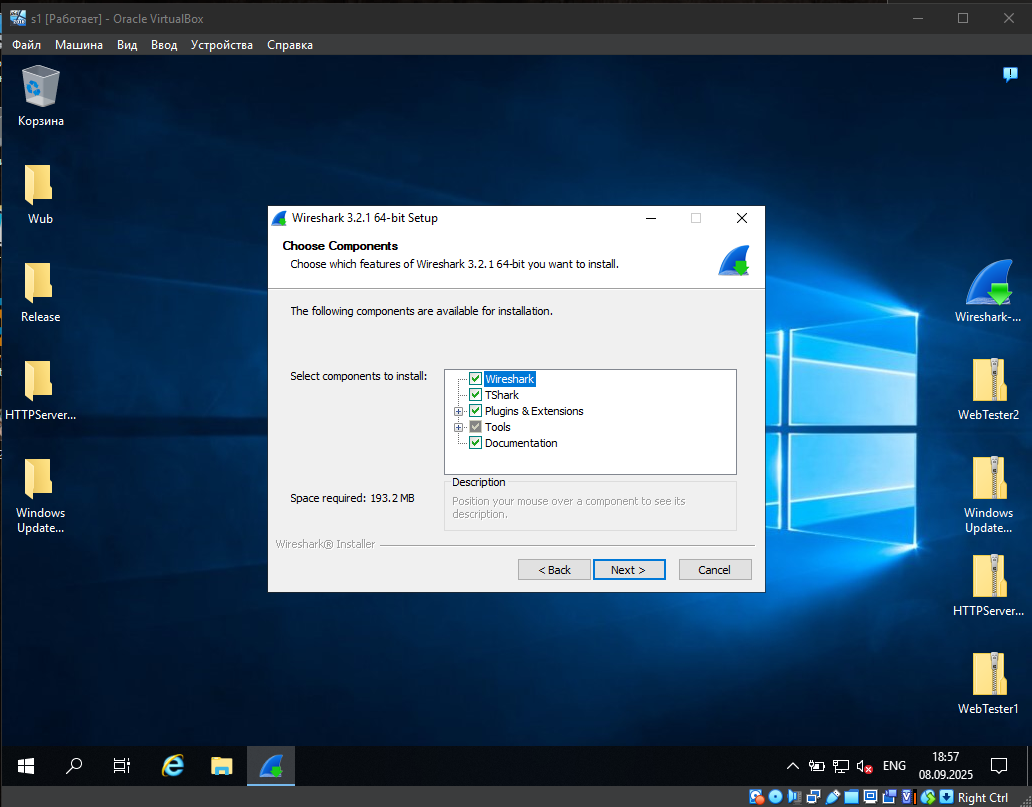


Рисунок 1.13 – Выбор компонентов Wireshark

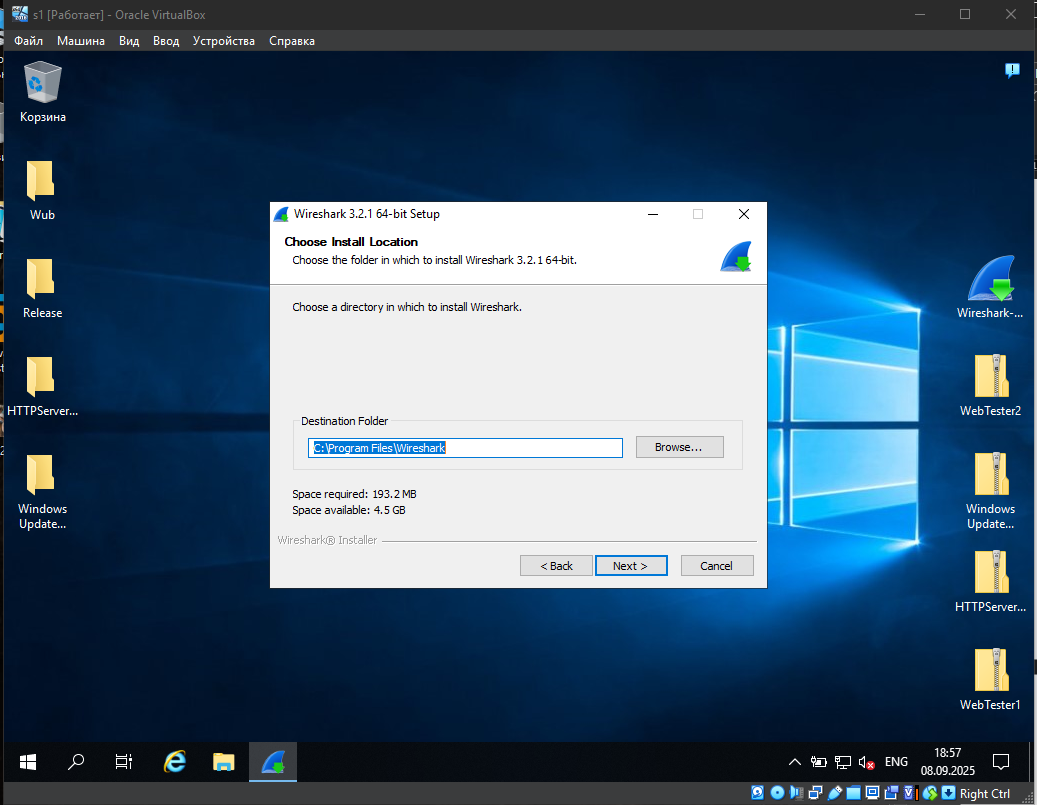


Рисунок 1.14 – Выбор директории установки

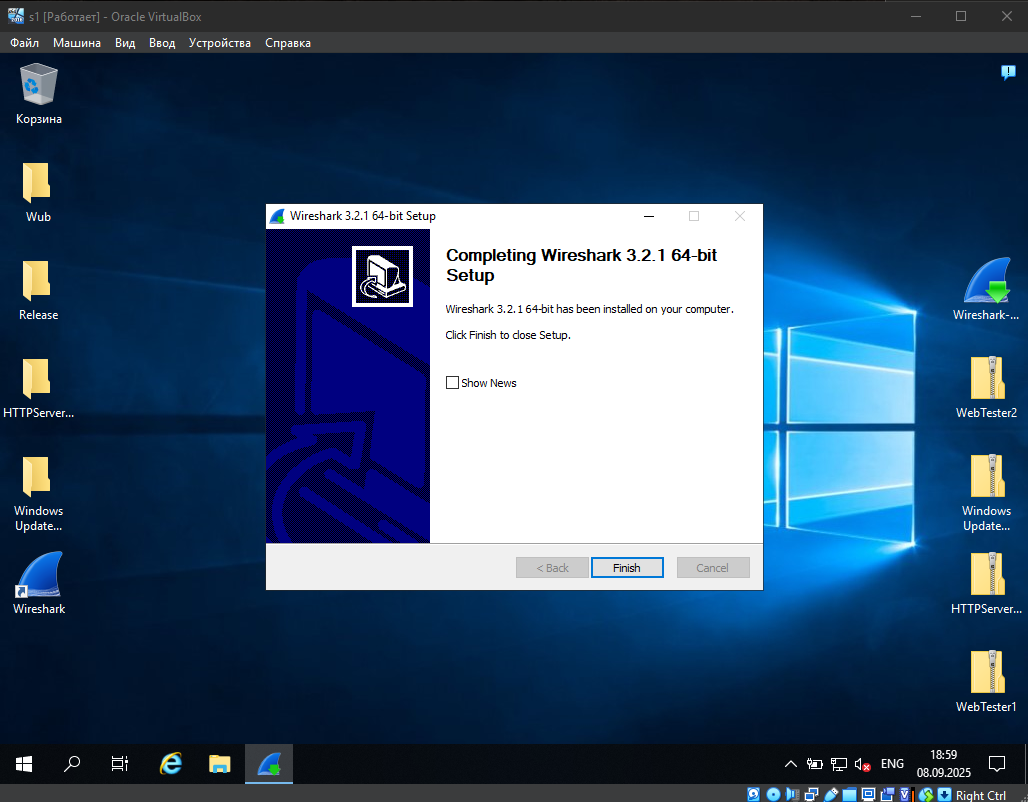


Рисунок 1.15 – Завершение установки

1. Переключите сетевые адаптеры созданных ранее виртуальных машин в режим «Виртуальный адаптер хоста».

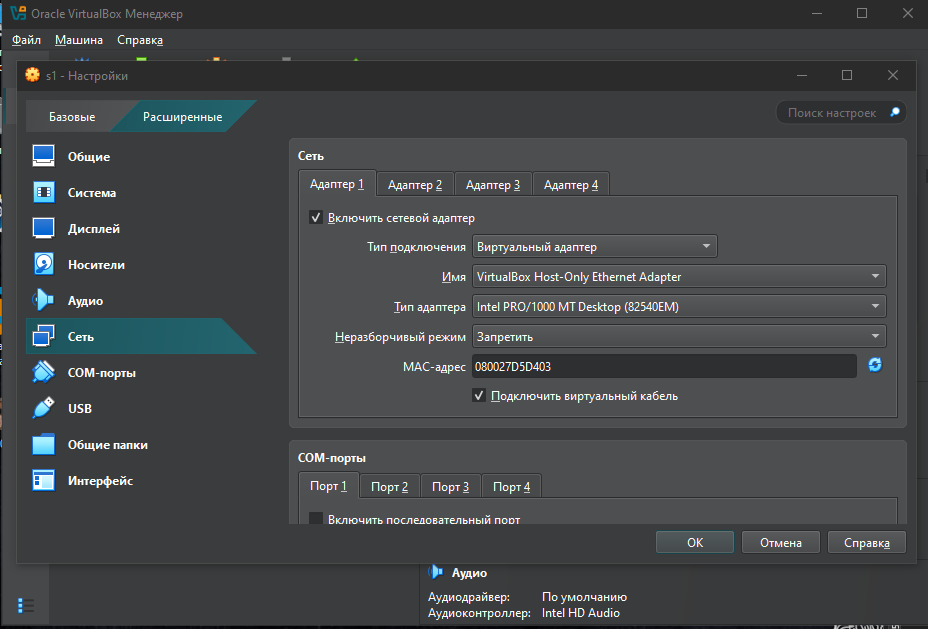


Рисунок 1.16 – Переключение сетевых адаптеров

1. Запустите (перезапустите) виртуальные машины и определите назначенные им IP-адреса.

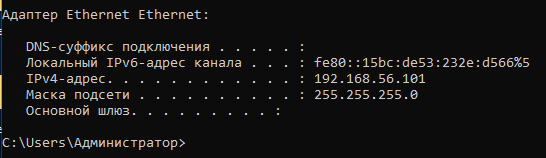


Рисунок 1.17 – IP-адрес первой виртуальной машины

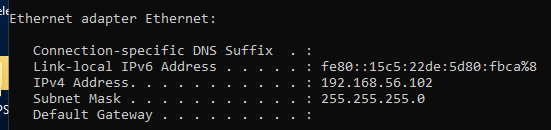


Рисунок 1.18 – IP-адрес второй виртуальной машины

1. Включите захват пакетов с помощью Wireshark на виртуальной машине.

Жмем на заголовок Capture, открывается новое окошко, затем выбираем Ethernet, затем Start.

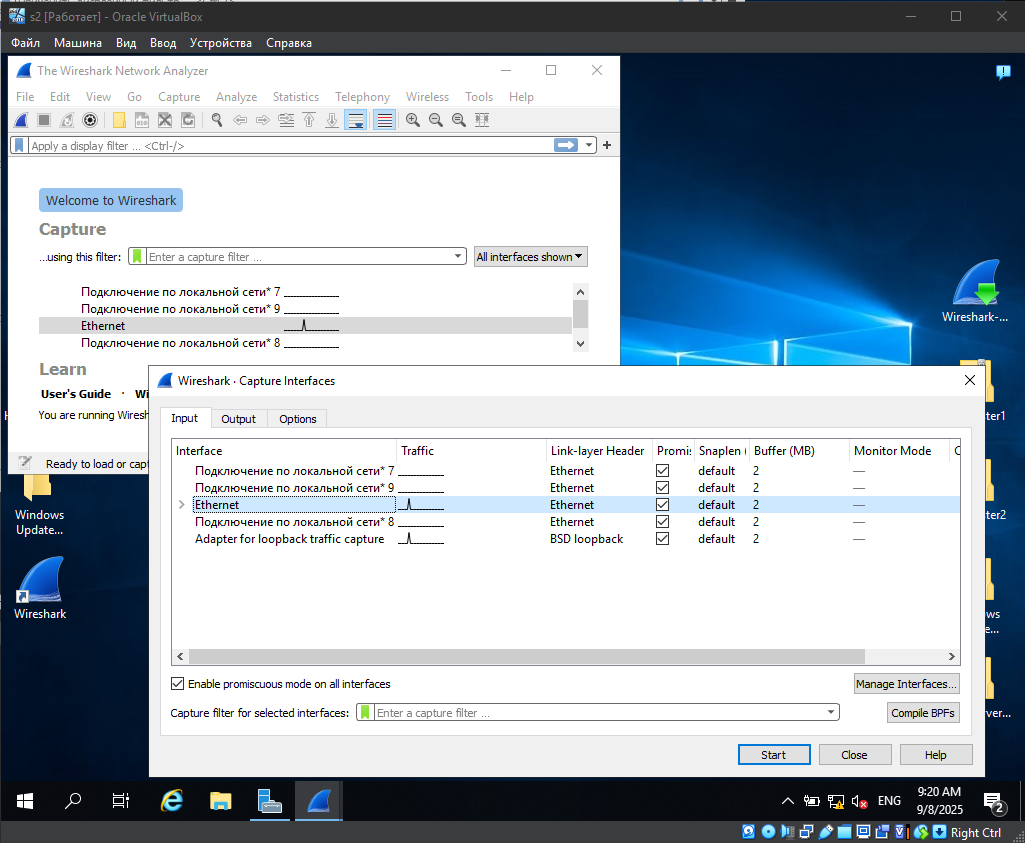


Рисунок 1.19 – Включение захвата

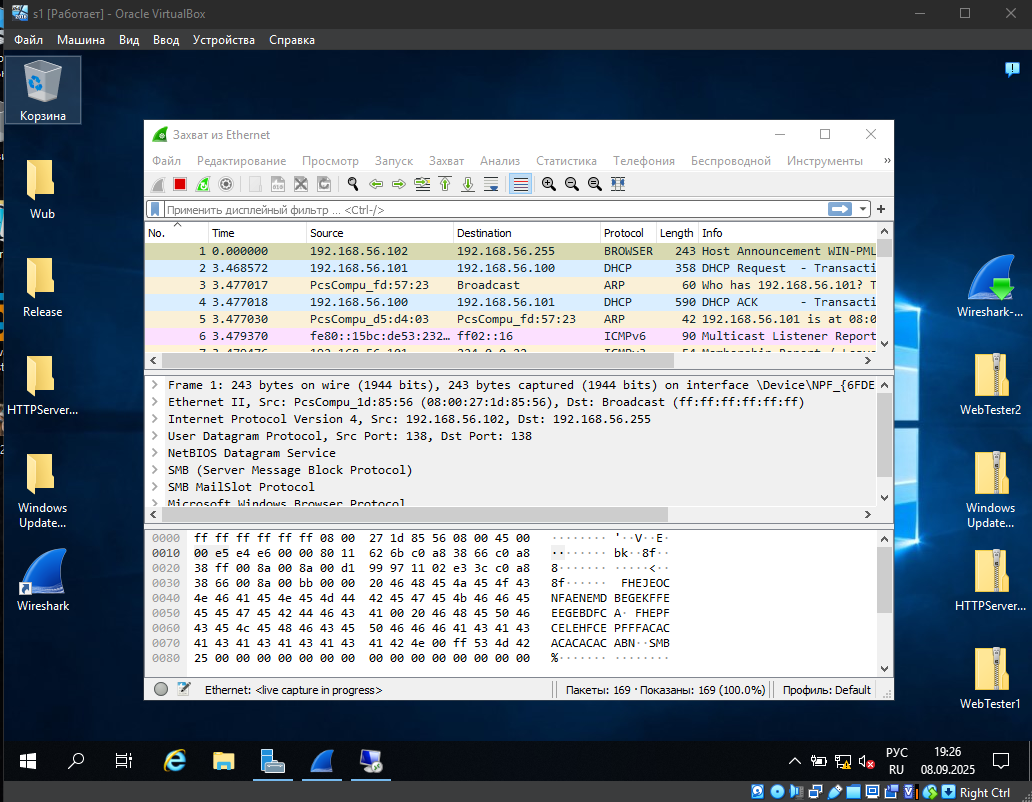


Рисунок 1.20 – Вид окна Захват из Ethernet

1. Подключитесь с помощью приложения «Подключение к удаленному рабочему столу» физической машины по IP-адресу и порту к виртуальной машине.

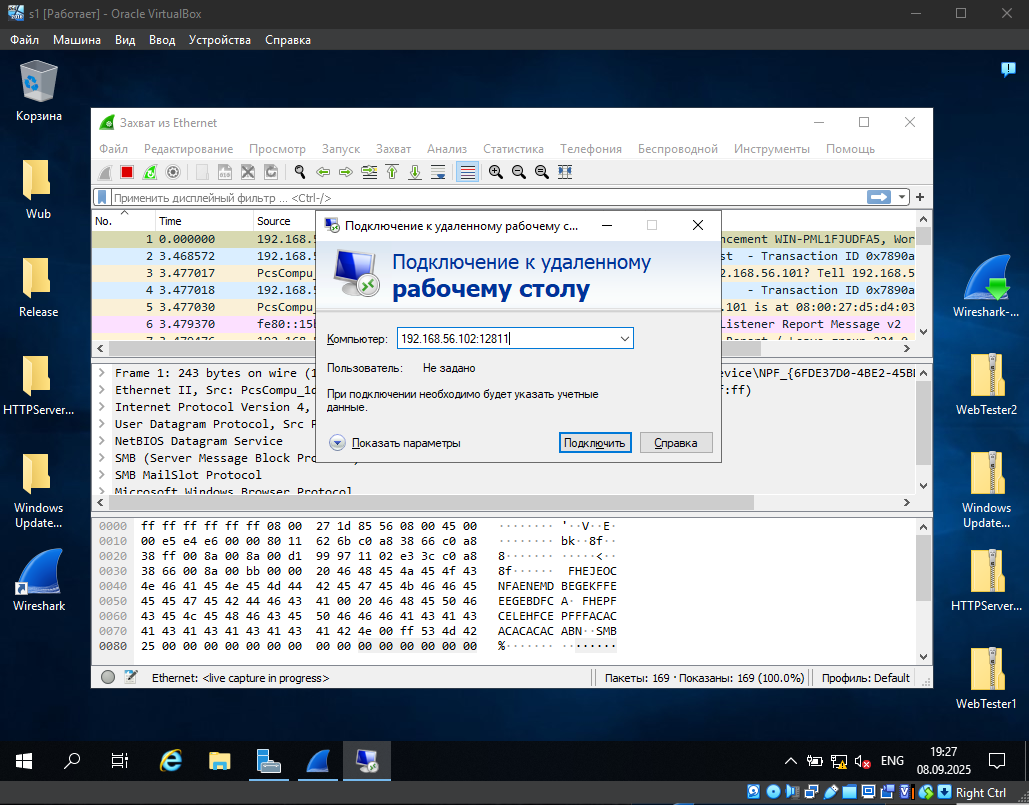


Рисунок 1.21 – Подключение к рабочему столу

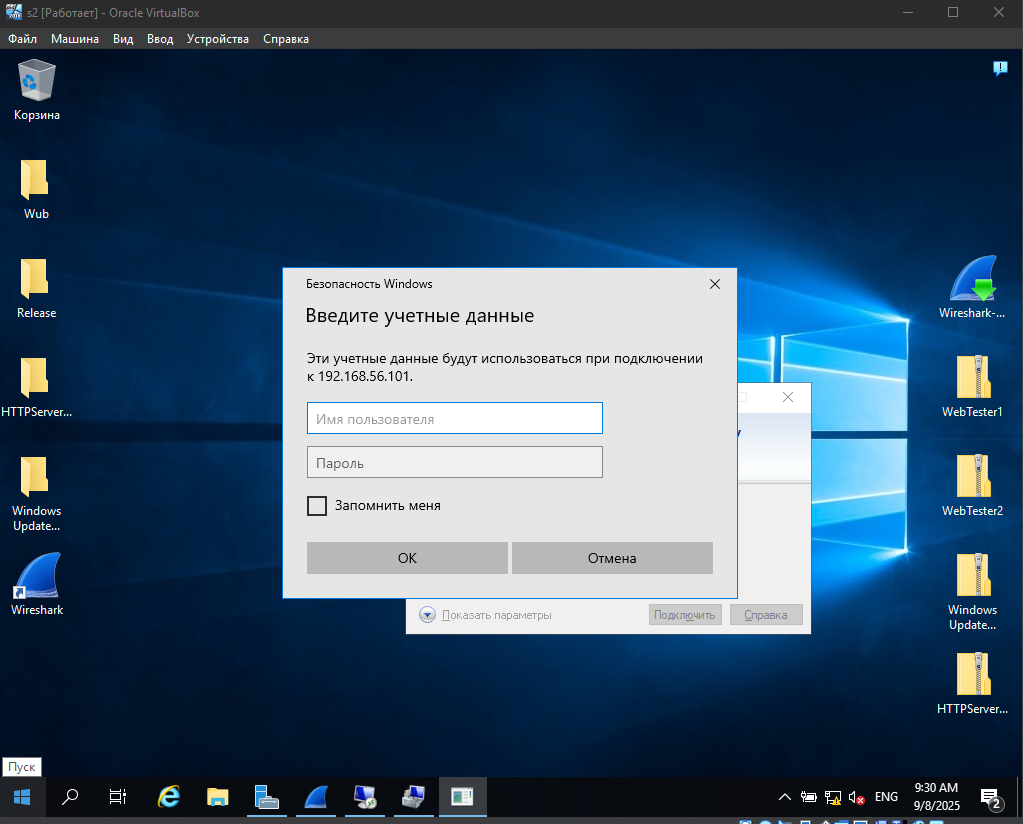


Рисунок 1.22 – Ввод пароля

Во время ввода пароля выскочит окошко о том, что необходимо сменить пароль при первом входе, меняем, пробуем заново.

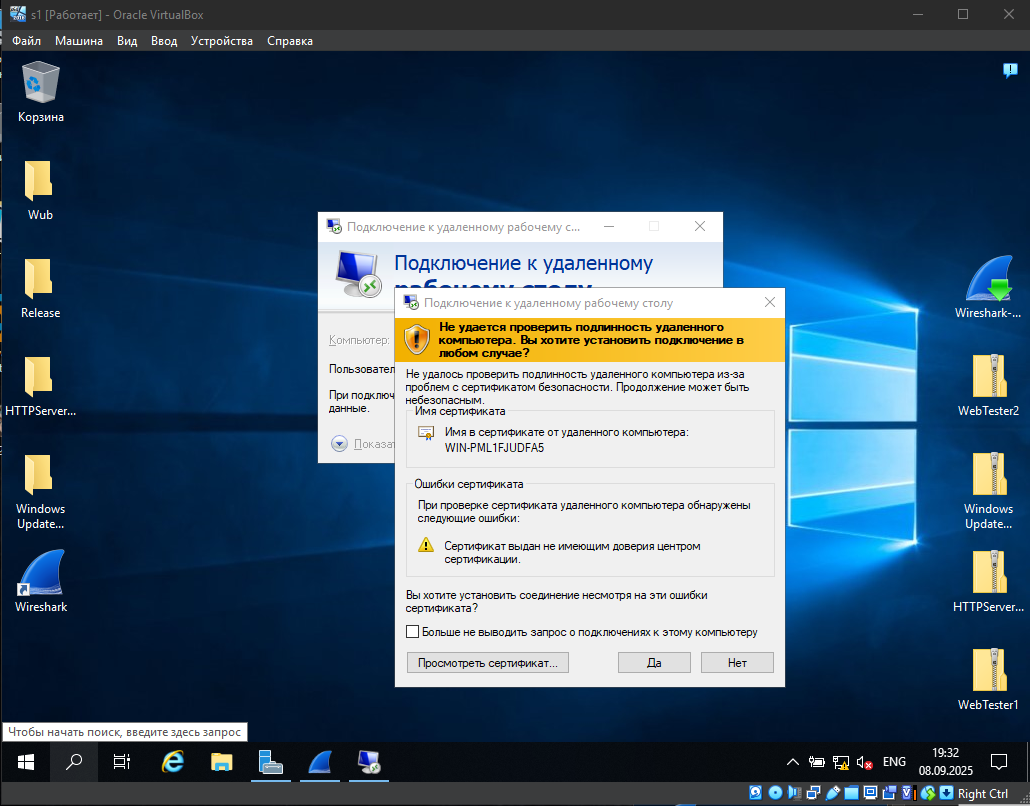


Рисунок 1.23 – Установка подключения

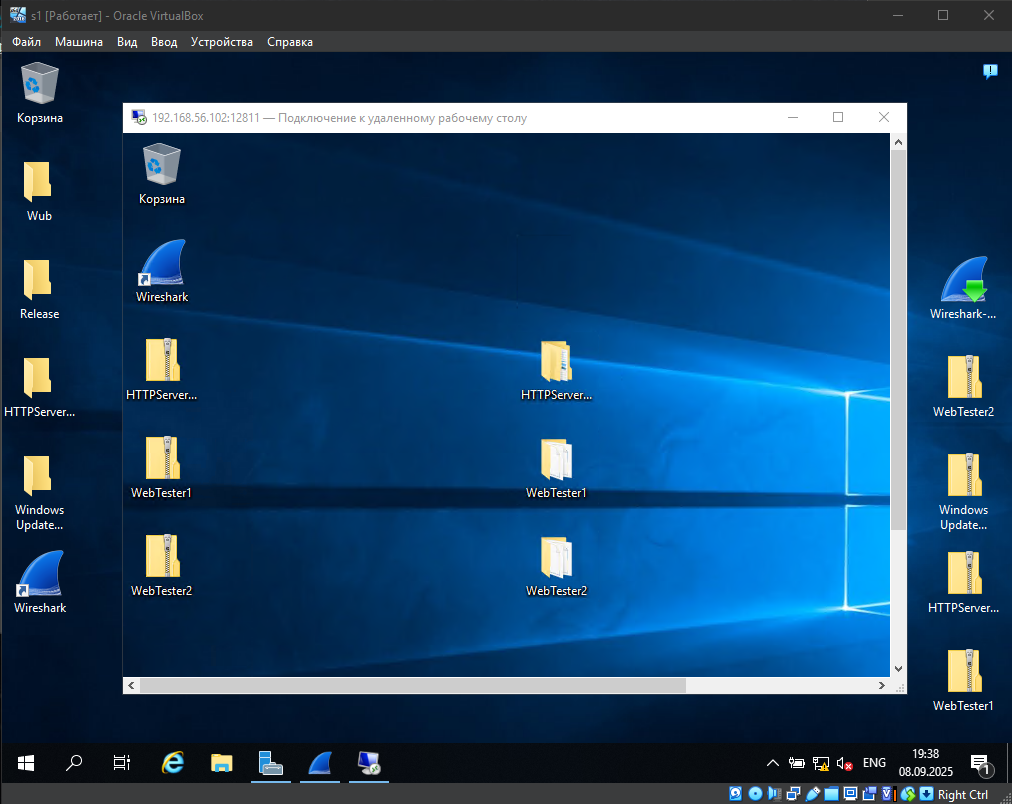


Рисунок 1.24 – Удаленный рабочий стол

1. Запустите и откройте учебные веб-приложения из лабораторной работы №1, нажмите обе кнопки.

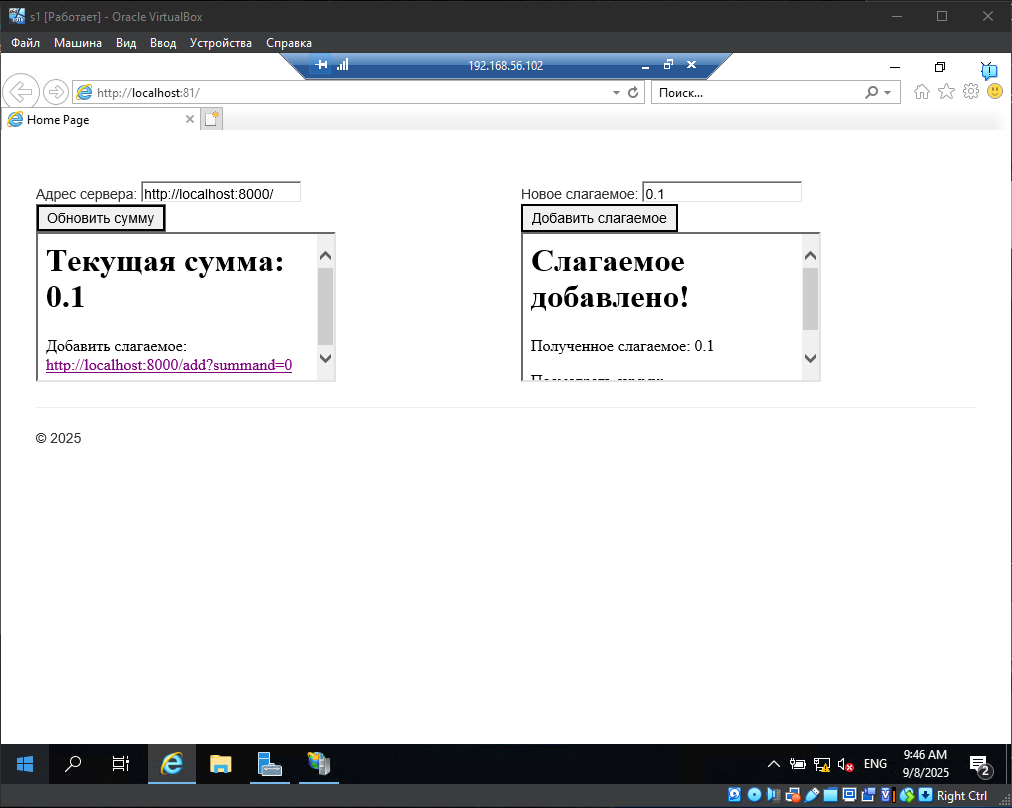


Рисунок 1.25 – Веб-приложения на удаленном рабочем столе

1. Остановите захват пакетов в Wireshark, выполните фильтрацию захваченных пакетов путем ввода «http» в строку фильтрации.

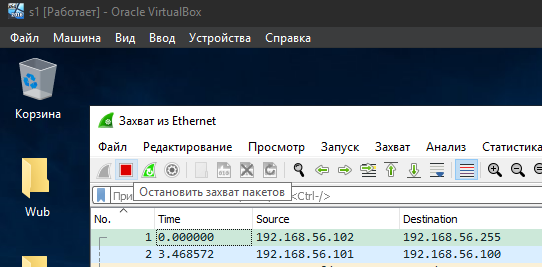


Рисунок 1.26 – Остановка захвата пакетов

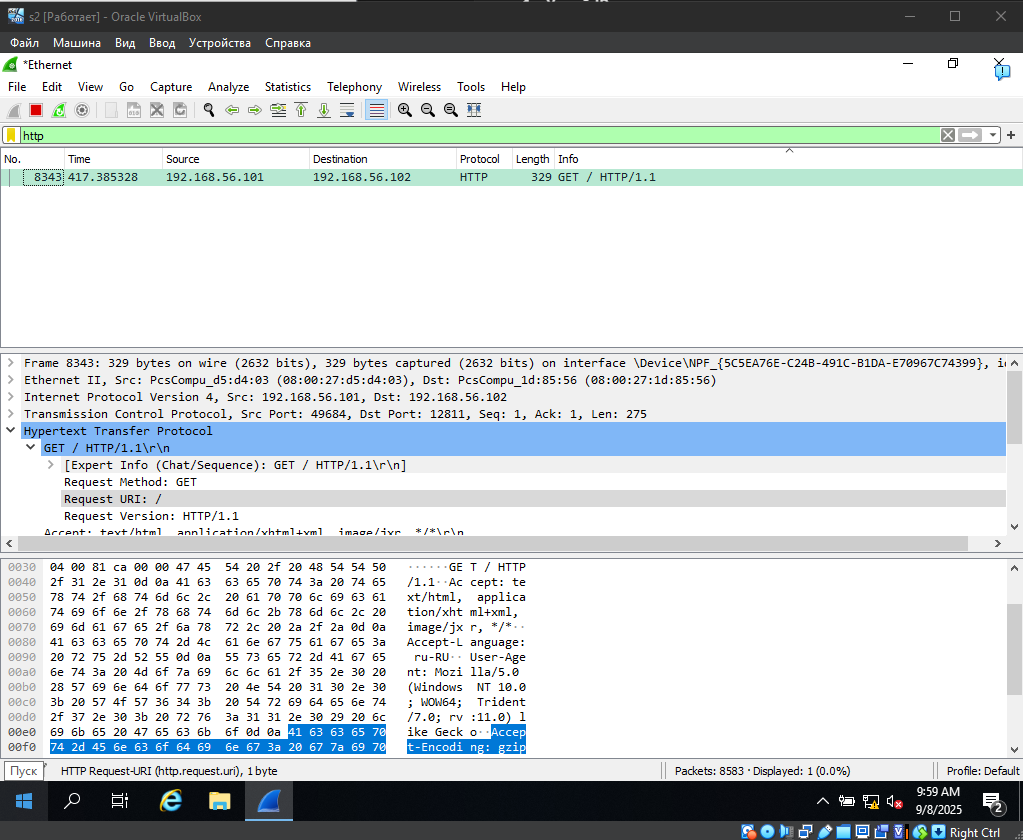


Рисунок 1.27 – Фильтрация http-пакетов

1. Ознакомьтесь со структурой HTTP-пакетов и порядком отправки запросов и получения ответов в веб-приложениях.

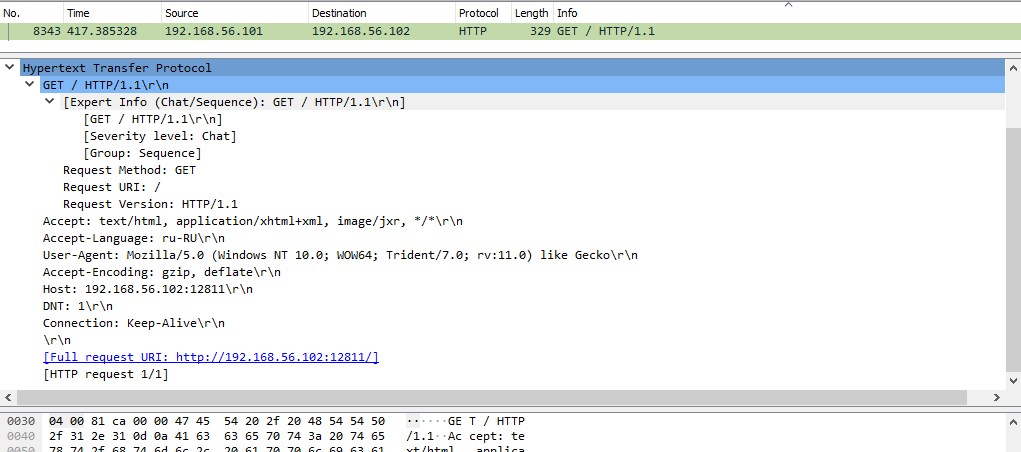


Рисунок 1.28 – Структура http-пакетов

**Порядок защиты лабораторной работы.**

1. Зайдите с физической машины на виртуальную по RDP.
2. Продемонстрируйте захватываемые при работе с веб-приложениями из лабораторной работы №1 пакеты в Wireshark.
3. Опишите структуру и виды http-пакетов.