Горшков М.А

Студент

Научный руководитель: Уймин А.Г., ст. преподаватель

Российский государственный университет нефти и газа (НИУ) имени И.М. Губкина

АТАКИ НА REMOTEAPP В ИНФРАСТРУКТУРЕ MICROSFT WINDOWS SERVER

Аннотация:

В статье рассматривается проблема обеспечения безопасности при использовании технологии RemoteApp в изолированной инфраструктуре Windows Server 2022 без доменных сервисов. Проанализированы основные угрозы: перебор учётных данных, утечки через буфер обмена и редирект устройств, запуск посторонних процессов. На базе лабораторной среды реализован комплекс защитных мер, включающий фильтрацию по IP-адресам, создание ограниченной группы пользователей, настройку групповых политик и публикацию приложения с помощью RemoteApp Tool. Проведены тесты, подтверждающие эффективность выбранной архитектуры. Сделан вывод о применимости решения в условиях ограниченных ресурсов для построения защищённого удалённого доступа.

Ключевые слова:

RemoteApp, Windows Server 2022, безопасность, изолированная среда, групповая политика, брандмауэр, NAT, удалённый доступ, RDP, защита от утечек данных.

Gorshkov M.A.

Student

Scientific supervisor: Uimin A.G., Senior Lecturer

National University of Oil and Gas «Gubkin University»

ATTACKS ON REMOTEAPP IN MICROSOFT WINDOWS SERVER INFRASTRUCTURE

Abstract:

The article addresses the issue of securing RemoteApp technology deployed in an isolated Windows Server 2022 environment without domain services. Key threats are analyzed, including brute-force attacks, data leakage through clipboard and device redirection, and unauthorized process execution. A laboratory environment was used to implement a set of protection measures: IP address filtering, creation of a restricted user group, configuration of group policies, and application publishing via RemoteApp Tool. A series of tests confirmed the effectiveness of the proposed architecture. The results demonstrate that the solution is applicable in resource-constrained environments for building secure remote access infrastructure.

Keywords:

RemoteApp, Windows Server 2022, security, isolated environment, group policy, firewall, NAT, remote access, RDP, data leakage protection.

RemoteApp – удобный и мощный инструмент, он позволяет запускать серверные приложения на клиентских устройствах как локальные окна. Однако удобство оборачивается рисками, при неправильной настройке RemoteApp становится точкой входа в корпоративную инфраструктуру. Особенно уязвимы инсталляции в изолированных средах без Active Directory, где нет ни централизованного контроля, ни доменных политик, ни мониторинга.

В своей работе я решил проверить можно ли выстроить действительно защищённую RemoteApp-инфраструктуру на базе Windows Server 2022, не выходя за рамки встроенных средств и минимальных ресурсов. Ни VPN, ни SIEM, ни стороннего антивируса – только штатный функционал системы, ручная настройка и чёткое понимание угроз. Результаты оказались интересными.

Основу стенда составила виртуальная машина с Windows Server 2022 (версия 20348.230), развёрнутая в VirtualBox. В качестве клиента использовалась Windows 10 Pro (23H2). Сетевая схема – NAT с пробросом порта RDP (3389) наружу как 33890.

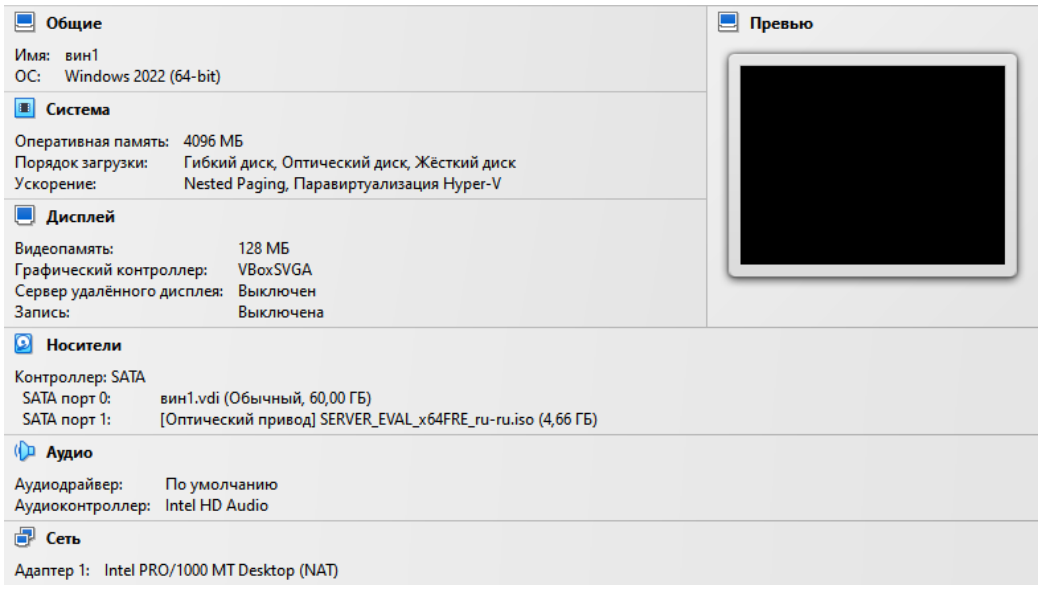

Рисунок 1 – Виртуальная машина Windows Server

Роль RD Session Host установлена через мастер. Веб-интерфейс (RDWeb) развернут, для HTTPS использован самоподписанный сертификат, вручную

импортированный в хранилище доверенных корневых ЦС. Сервер получил имя RDS-SERVER. Обновления и IE ESC отключены – стандартные меры для стабильности.

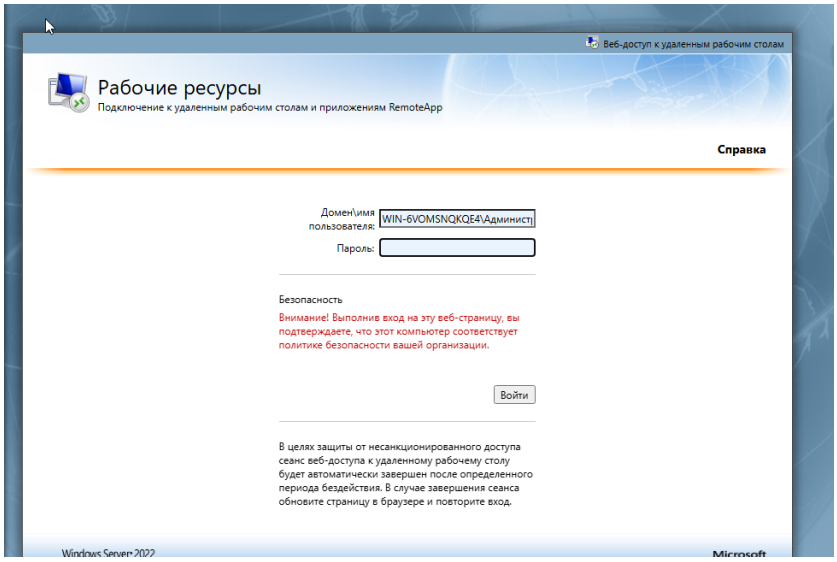

Рисунок 2 – Веб-интерфейс RDWeb

Первый слой – фильтрация по IP. Через брандмауэр Windows разрешил подключения по порту 3389 только с IP хостовой машины. Всё остальное блокируется. Это просто, но эффективно: исключает попытки сканирования и перебора учётных данных.

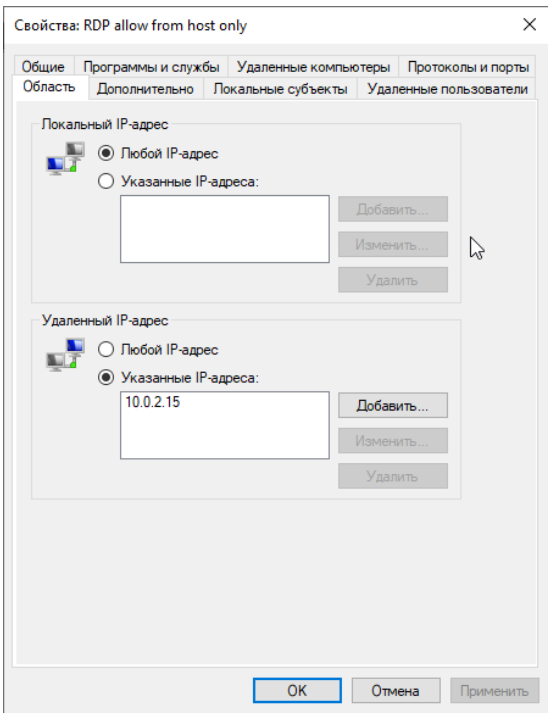

Рисунок 3 – Фильтрация по IP

Проверка показала, что с любого другого IP вход невозможен. Это критически важно, особенно при использовании RemoteApp в публичной NAT-среде без VPN.

Управление доступом через локальные группы

Создал новую группу RemoteAppUsers. Только её участники получают доступ к опубликованному приложению. Это реализация модели RBAC

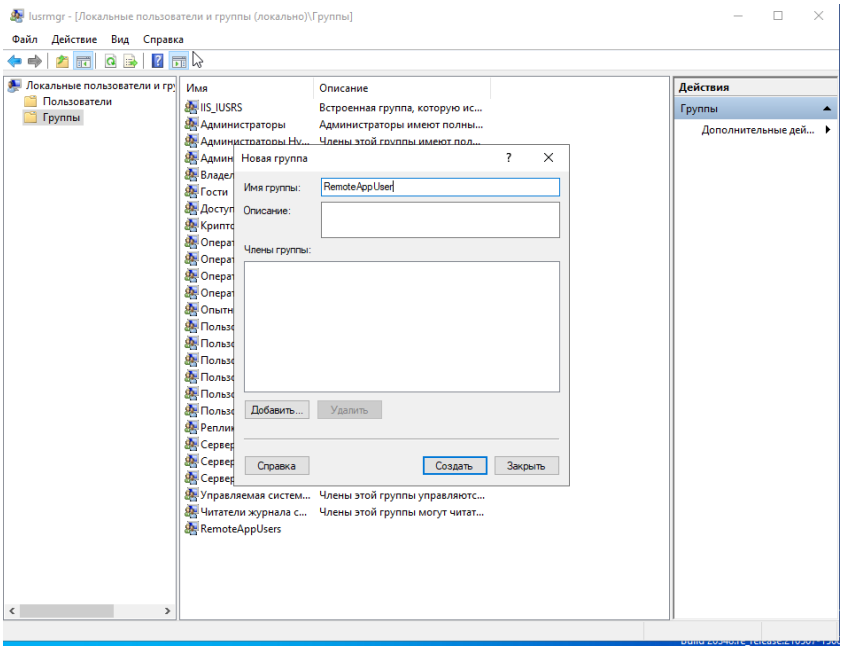

Рисунок 4 – Создание пользовательских групп

Пользователь User2 включён в группу, удалён из всех остальных, включая администраторов и Remote Desktop Users. Он не может запустить сеанс рабочего стола, только строго заданное приложение.

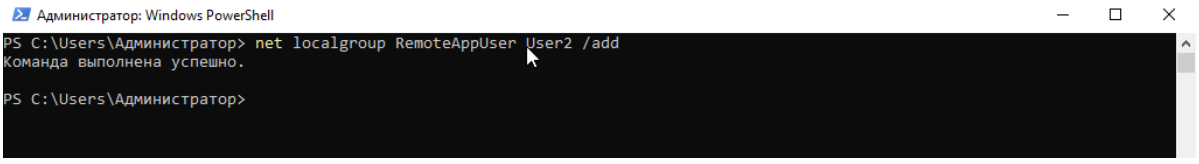

Рисунок 5 – Добавление в группу

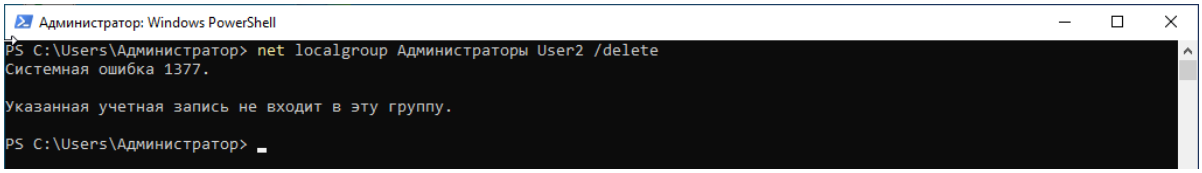

Рисунок 6 – Удаление из группы

Контроль перенаправлений

Редирект буфера обмена, клиентских дисков, COM-портов – всё это отключено через локальные политики (gpedit.msc) и реестр. Это ключевая точка. Без этого любой пользователь может унести данные, просто скопировав их или закинув на локальный диск.

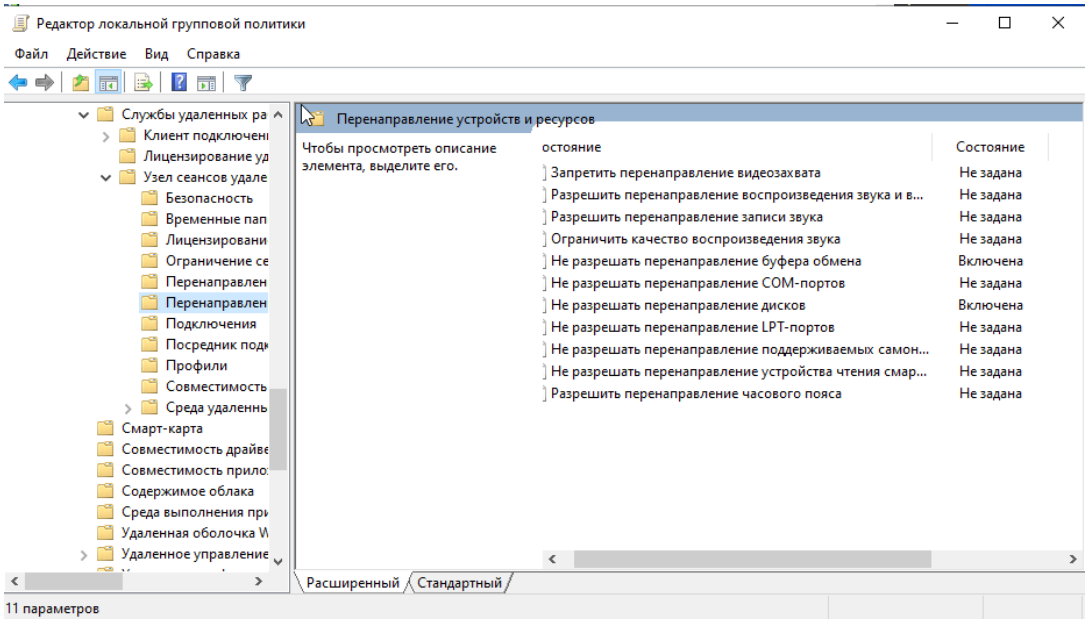

Рисунок 7 – Редактор локальной групповой политики

В реестре выставлены параметры:

fDisableClipboardRedirection = 1

fDisableCdm = 1

Служба TermService перезапущена для немедленного применения.

Публикация приложения и запуск сеанса

Для публикации использовал RemoteApp Tool 6.1.0.0 Простой и рабочий инструмент. Приложение – стандартный notepad.exe. Генерировал .rdp-файл вручную, без использования TSWebAccess. Указан порт 33890, отключены лишние опции.

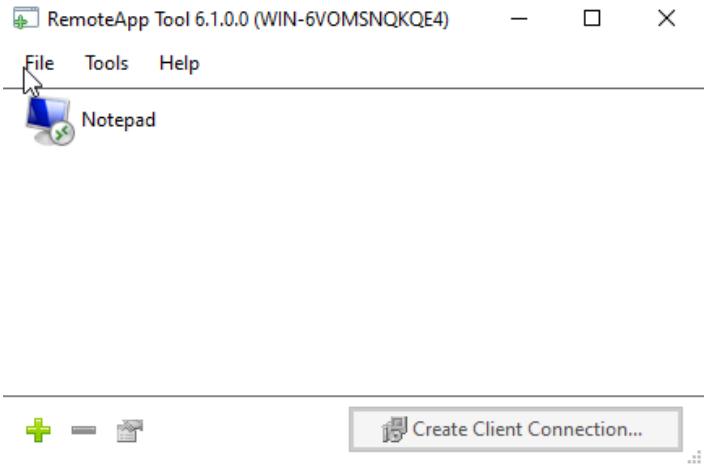

Рисунок 8 – RemoteApp Tool 6.1.0.0

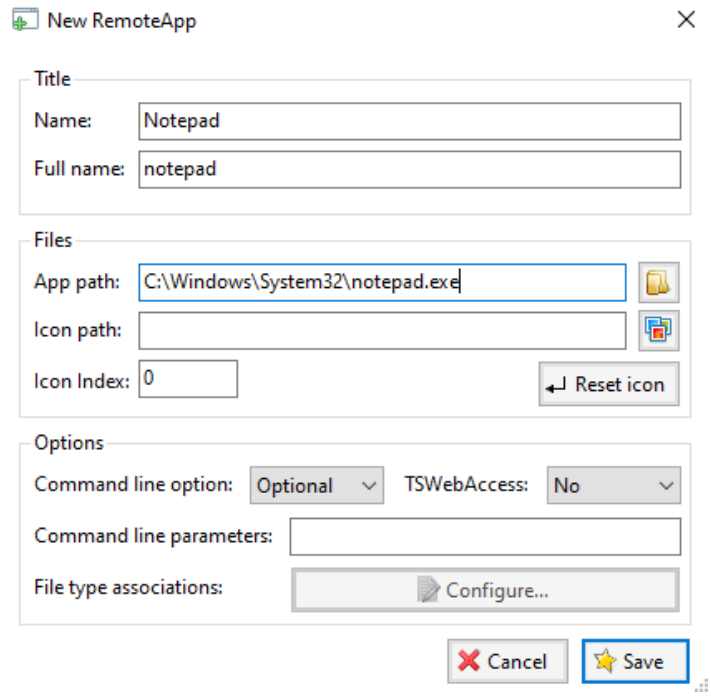

Рисунок 9 – New RemoteApp

Файл передан на хост, запуск через mstsc. Подключение от имени User2 успешно, но запускается только блокнот – ни рабочего стола, ни оболочки.

Проверка изоляции:

- Буфер обмена не работает – скопированный с хоста текст не вставляется.
- Редирект дисков отсутствует – в Notepad доступны только серверные папки.
- CMD, PowerShell, Explorer – не запускаются даже через уловки с диалогом «Сохранить как».
- Пользователь вне RemoteAppUsers – получает отказ в доступе.

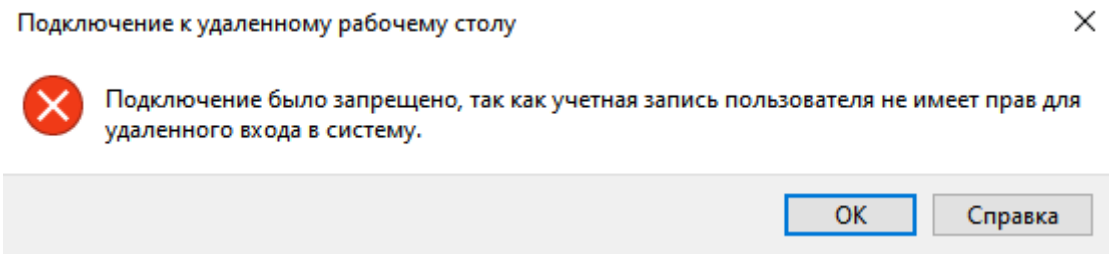

Рисунок 10 – Подключение к удаленному рабочему столу

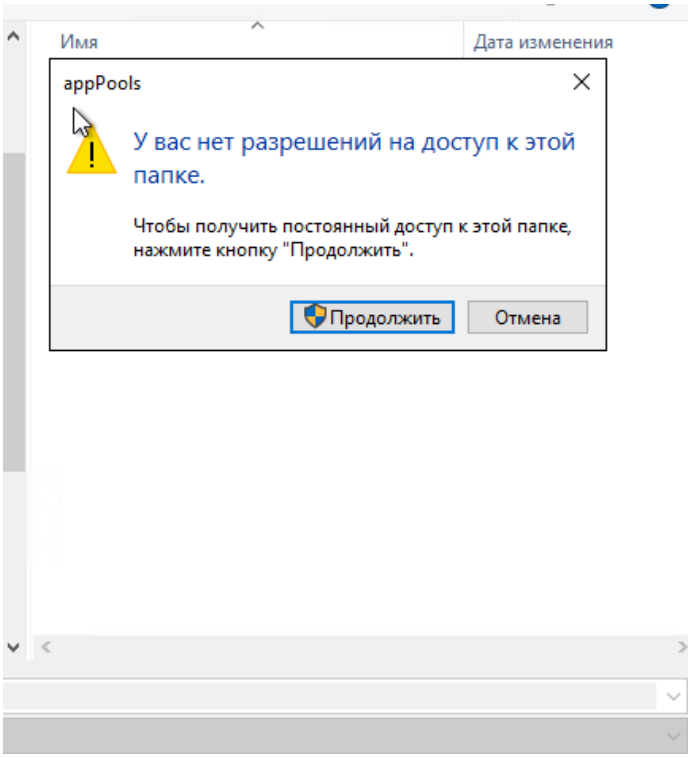

Рисунок 11 – Нет доступа к папке

Таблица 1 – Сводка механизмов защиты

Механизм	**Назначение**	**Тип угроз**
Фильтрация IP	Только доверенный клиент	Brute-force, сканирование
Группы пользователей	Только авторизованные пользователи	Повышение привилегий
GPO + реестр	Отключение обмена данными	Утечка данных
RemoteApp Tool	Ограничение сеанса одним приложением	Запуск произвольного кода

В ходе исследования установлено, что технология RemoteApp, применяемая в изолированной среде Windows Server 2022 без доменной инфраструктуры, подвержена ряду существенных угроз, включая несанкционированный доступ, утечки данных через буфер обмена и устройства, а также запуск стороннего кода. Практическая реализация комплекса защитных мер показала, что даже без использования внешних программных или аппаратных решений возможно добиться высокого уровня изоляции и контроля. В частности, эффективными мерами оказались: фильтрация входящего трафика по IP-адресам средствами Windows Firewall, разграничение прав доступа с помощью локальных групп пользователей, отключение опасных механизмов перенаправления через групповые политики и публикация строго ограниченного набора приложений через RemoteApp Tool. Результаты тестирования подтвердили надёжность предложенной архитектуры, обеспечивающей выполнение принципов минимизации прав и устойчивости к типовым атакам на RDP-сервисы.

Список используемых источников

1. Уймин, А. Г. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование: практикум / А. Г. Уймин. — СПб.: Лань, 2024. — 116 с. — ISBN 978-5-507-48647-2.

2. ФСТЭК России. Приказ от 11 февраля 2013 г. № 17 «Об утверждении требований по защите информации». — [Электронный ресурс]. — URL: https://fstec.ru (дата обращения: 28.04.2025).

3. Microsoft. Windows Server 2022. Обзор. – [Электронный ресурс]. – URLL: https://www.microsoft.com/ru-ru/evalcenter/evaluate-windows-server-2022

4. VirtualBox. Powerful open source virtualization. – [Электронный ресурс]. – URL: https://www.virtualbox.org/

5. Microsoft. Скачать Windows 10. – [Электронный ресурс]. – URL: https://www.microsoft.com/ru-ru/software-download/windows10

6. Microsoft. Настройка веб-клиента удаленного рабочего стола для пользователей 2025. – [Электронный ресурс]. – URL: https://learn.microsoft.com/ru-ru/windows-server/remote/remote-desktop-services/remote-desktop-web-client-admin