Министерство образования и науки Российской Федерации

Санкт-Петербургский Политехнический Университет Петра Великого

—

Институт компьютерных наук и кибербезопасности

ЛАБОРАТОРНАЯ РАБОТА № 1

«Удаленный файловый менеджер с имперсонацией клиента»

1. по дисциплине «Безопасность современных информационных технологий»
2. Выполнил
3. студент гр. 5151004/10101 Веремейчук Я.Ю.

<подпись>

1. Преподаватель
2. асс. преподавателя Соловей Р.С.

<подпись>

1. Санкт-Петербург
2. 2023
3. Цель работы

Получить навыки работы с механизмом удаленного вызова процедур (RPC).

1. Задача

Написать программу-сервер и программу-клиент, работающие под Windows 7-11. Сервер должен предоставлять доступ локальным и удаленным клиентам к файлам в своей файловой системе.

1. Ход работы

Для начала был создан интерфейс RPC. Он должен описывать функции, которые будет реализовывать клиент-серверное приложение.

Чтобы создать интерфейс, необходимо запустить командную строку от имени администратора, перейти в папку C:\Program Files (x86)\Windows Kits\10\bin\10.0.19041.0\x64 и ввести команду uuidgen –i –oInterfaceRPC.idl.

Изображение выглядит как текст, снимок экрана, Шрифт, диаграмма

Автоматически созданное описание

Рисунок – Процесс создания интерфейса

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Автоматически созданное описание

Рисунок – Создание интерфейса

Далее были прописаны прототипы функций, которые требуются по заданию.

Затем хост и гостевая система были настроены.

На обеих системах необходимо найти «Службы» и установить тип запуска Автоматическая для «Локатора удаленного вызова процедур (RPC)», «Модуля запуска процессов DCOM-сервера» и «Удаленного вызов процедур (RPC)».

Изображение выглядит как текст, программное обеспечение, снимок экрана, веб-страница

Автоматически созданное описание

Рисунок – Настройка окружения

Далее для хостовой системы были добавлены два пользователя (без учетных записей Microsoft).

Изображение выглядит как текст, снимок экрана, круг

Автоматически созданное описание

Рисунок – Другие пользователи

Затем на хосте была создана новая папка для настроек доступа пользователей.

Изображение выглядит как текст, программное обеспечение, веб-страница, Значок на компьютере

Автоматически созданное описание

Рисунок – Выбор пользователей

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок – Настройка разрешений для пользователей

Затем был написал код для клиента и сервера. Был получен exe-файл для сервера и скопирован в папку, для которой был настроен доступ пользователям. Exe-файл для клиента был собран на гостевой системе.

В коде сервера были прописаны функции, которые представляют собой удаленные процедуры, доступные для вызова по сети.

* GetLoginPass: Проверяет учетные данные пользователя, выполняя вход в систему.
* PreDownloadFile: Получает размер файла перед его скачиванием.
* DownloadFile: Скачивает файл с сервера.
* UploadFile: Загружает файл на сервер.
* RemoveFile: Удаляет файл с сервера.
* LogOut: Завершает сеанс пользователя и закрывает его обработчик.

В функции main выполняются следующие действия:

* Инициализируется сервер RPC с помощью RpcServerUseProtseqEp, указывая протокол, порт и другие параметры.
* Регистрируется сервер RPC с помощью RpcServerRegisterIf2, указывая интерфейс, обработчик безопасности и другие параметры.
* Запускается прослушивание сервера RPC с использованием RpcServerListen, которое блокирует выполнение программы и ожидает удаленных вызовов процедур.

В коде клиента функция main выполняет следующие шаги:

* Создает строковый дескриптор (szStringBinding), который представляет строку, описывающую, как подключиться к удаленному серверу. Для этого используется функция RpcStringBindingCompose, которая формирует строку с указанием протокола (ncacn\_ip\_tcp), IP-адреса сервера и порта (в данном случае 192.168.56.1 и 9000).
* После формирования строки дескриптор строки преобразуется в явный байндинг (hBinding) с использованием функции RpcBindingFromStringBinding. Это позволяет клиенту совершать вызов удаленных процедур на сервере.
* Затем клиент запрашивает у пользователя логин и пароль, которые будут использоваться для аутентификации на сервере.
* После завершения операций клиент освобождает ресурсы, такие как строковый дескриптор и явный байндинг, с использованием функций RpcStringFree и RpcBindingFree.

Ниже будут отображены различные сценарии взаимодействия сервера и клиента.

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Рисунок – Работа сервера

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание

Рисунок – Чтение файла пользователем 1

Изображение выглядит как текст, снимок экрана, Шрифт, дизайн

Автоматически созданное описание

Рисунок – Попытка загрузки файла пользователем 1

Изображение выглядит как текст, программное обеспечение, Мультимедийное программное обеспечение, Графическое программное обеспечение

Автоматически созданное описание

Рисунок – Загрузка файла пользователем 2



Рисунок – Отказ в доступе для пользователя 2

1. Контрольные вопросы
2. В чем различия между statefull и stateless серверами?

Stateful серверы сохраняют состояние клиентских сессий между запросами, в то время как stateless серверы не сохраняют состояния и обрабатывают каждый запрос независимо. Stateful серверы могут быть сложнее в управлении и масштабировании, но позволяют сохранять информацию о клиентах между запросами. Statelessness делает серверы более легкими в масштабировании и отказоустойчивости.

1. Что такое имперсонация?

Имперсонация (impersonation) – это процесс, при котором один пользователь (обычно с административными или привилегированными правами) временно принимает и использует идентификацию и права доступа другого пользователя (обычно менее привилегированного) для выполнения определенных задач или операций.

1. Что такое LPC? чем этот механизм отличается от RPC?

LPC (Local Procedure Call) – это механизм взаимодействия между процессами или компонентами, выполняющимися в пределах одной и той же системы (локально). Он обычно используется в операционных системах, чтобы процессы или потоки могли вызывать функции или процедуры в других процессах на той же машине. Взаимодействие между процессами осуществляется на том же уровне привилегий, что и вызывающий процесс. RPC (Remote Procedure Call) – вызов процедур между процессами на разных машинах через сеть.

1. Выводы

В ходе работы были получены навыки работы с механизмом удаленного вызова процедур (RPC).