Remote Shell using RPC

Vuong Bao Son
Nguyen Ngoc Chien
Cao Phuong Linh
Dinh Thuy Hien
Nguyen Hieu Thao

Context

- Introduction
- RPC
- Remote Shell
- Project Architecture

Introduction

- In distributed system, there is a need for controlling computers from distance.
- In the same network, computers can be controlled over a shell, which is called a “remote shell”.
- The network can be LAN or internet.
- The method for establishing the connection is RPC.

RPC

- In distributed computing, a remote procedure call (RPC) is when a computer program causes a procedure (subroutine) to execute in a different address space (commonly on another computer on a shared network).
- This is a form of client–server interaction (caller is client, executor is server), typically implemented via a request–response message-passing system.

Remote Shell

- A shell is a user interface for access to an operating system's services.
- A remote shell is the shell which can controls other computers on a network.
- Direct Remote Shells. A direct remote shell behaves as a server. It works like a ssh or telnet server. The remote user/attacker, connects to a specific port on the target machine and gets automatically access to a shell.
- Reverse Remote Shells. These ones work the other way around. The application running on the target machine connects back (calls back home) to a specific server and port on a machine that belongs to the user/attacker.

Project Architecture

- Our project: using RPC to execute a remote shell.
- Client-server based.
- Communicate over RPC.
- Procedure on server: create shell, kill shell, prompt, run commands (ls, cat, tar, cd…)
- Each client is identified by an unique ID.

Demo