Projeto de Redes - Spy
Universidade Federal De Alagoas

Itallo Patrick Castro Alves da Silva
Lucas Buarque de Araujo Barros

O intuito do projeto foi apresentar os conceitos de socket apresentados em aula. Para isso, iniciamos com a ideia de representar um dos ataques mais comuns na área da segurança da informação, o ataque com um Trojan RAT. Como o nome RAT (Remote Access Trojan) sugere, este malware é um programa que dá acesso remoto a um atacante ao computador de uma vítima.

Para isso funcionar, foi desenvolvido a estrutura de cliente e servidor e estruturada uma conexão reversa (A vítima se conecta ao atacante que estará esperando conexões para interagir com elas). Utilizando a arquitetura de sockets, permitimos com que a máquina alvo se comunique diretamente com o atacante, permitindo que ele execute comandos dentro da mesma.

Além disso, foi utilizado o conceito de Threads. Este conceito foi aplicado no projeto para que fosse possível realizar a conexão entre várias vítimas ao mesmo tempo com um servidor de um atacante.

Vale ressaltar, que este projeto foi desenvolvido apenas com o intuito de incentivar o estudo na área de segurança da informação, mais especificamente em segurança ofensiva. Este projeto não incentiva a execução de crimes cibernéticos.

Principais funcionalidades da aplicação:

- Enviar uma mensagem ao computador infectado;
- Tirar uma *screenshot* do computador infectado e a enviar para o servidor;
- Enviar um arquivo para o computador infectado;
- Fazer o download de um arquivo que esteja no computador infectado;
- Ter acesso ao shell do computador infectado;
- Fechar a conexão com o computador infectado;
- Colocar a sessão ativa em segundo plano para interagir com outras sessões sem perder a que já estava ativa anteriormente;

O que poderia ter sido implementado:

- Poderíamos ter implementado a funcionalidade de gerar um executável para que pudesse ser rodado em qualquer computador. Contudo, nosso intuito é apenas exemplificar e usar os conceitos dados em aula.

Dificuldades encontradas no desenvolvimento do projeto:

- A nossa principal dificuldade foi saber quando não estava mais sendo enviados dados de ambos os lados. Contudo, resolvemos esse problema verificando se o servidor não conseguiria mais se comunicar com o cliente após algum comando.
- Em nossos estudos, verificamos que vários RAT's conseguem identificar automaticamente que uma conexão caiu, sem ao menos enviar um comando para checá-la, porém nós não conseguimos implementar essa funcionalidade no período de entrega do projeto.