Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

As versões mais recentes do Metasploit usa uma ferramenta gráfica chamado *Armitage*. A compreensão da Armitage é importante porque em última análise, faz a sua utilização do Metasploit mais fácil, fornecendo informações para você de forma visual. Ela engloba o *Console Metasploit* e, usando suas capacidades de conexão, permite que você veja mais de uma sessão do terminal.

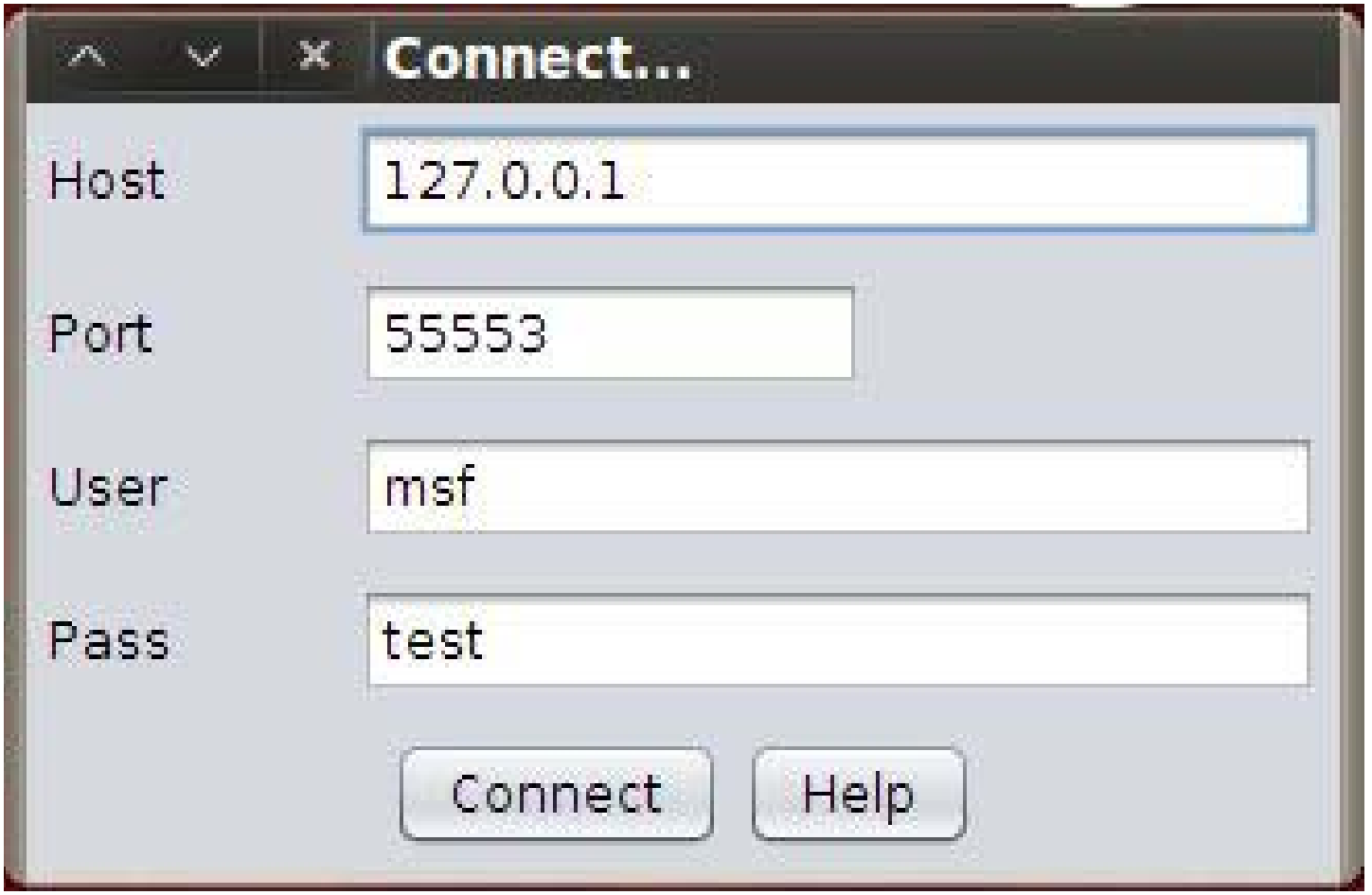
Usando o Mastering Armitage

Para abrir, você pode ir em **Exploitation Tools > Armitage**

Ou digitar no comando a palavra # **armitage**

** Só que antes de usar o **armitage**, digite o comando # ***msfdb init*** para criar o banco de dados!!

Usando o Mastering Armitage

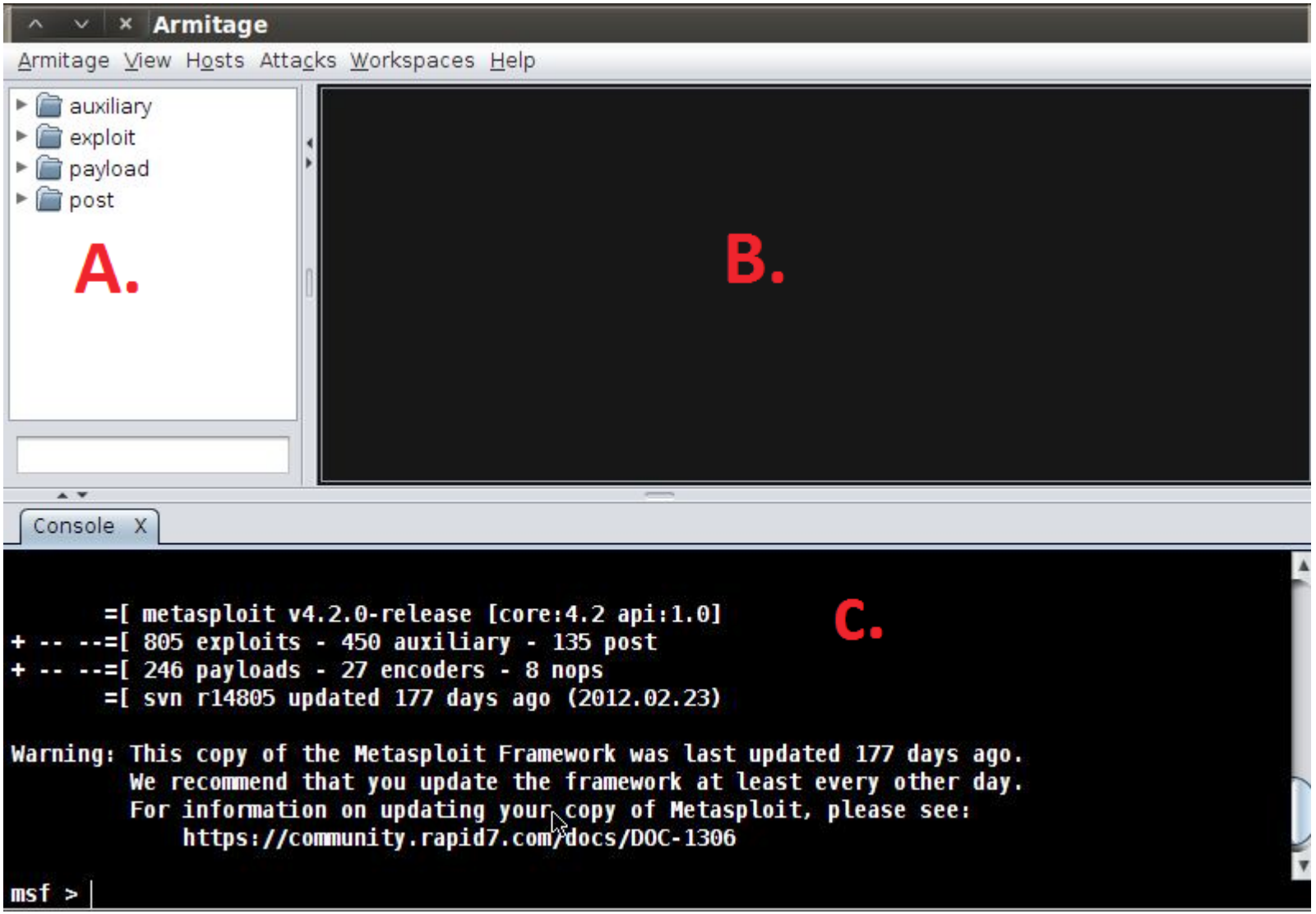

Connect...
Host
127.0.0.1
Port
55553
User
msf
Pass
test
Connect
Help

O Armitage, pode levar um tempo para se conectar ao Metasploit. Enquanto isso acontece, você pode ver a janela de notificação o seguinte. Não se assuste. Ele vai embora, uma vez Armitage é capaz de se conectar. No início Metaspoit? tela, clique em Sim(YES):


Start Metasploit?
A Metasploit RPC server is not running or not accepting connections yet. Would you like me to start Metasploit's RPC server for you?
No
Yes

Então, ele vai abrir a tela principal do Armitage. Vamos agora discutir as três regiões seguintes na tela principal (marcado como A., B. e C.):

Usando o Mastering Armitage



A: Esta região apresenta os módulos pré-configurados. Você pode procurar os módulos utilizando o espaço abaixo na lista de módulos.

B: Esta região apresenta os seus alvos ativos que são capazes de executar os nossos exploits contra eles.

C: Esta região apresenta vários separadores do Metasploit, permitindo múltiplas sessões do Meterpreter ou um terminal para ser executado e exibidos simultaneamente.