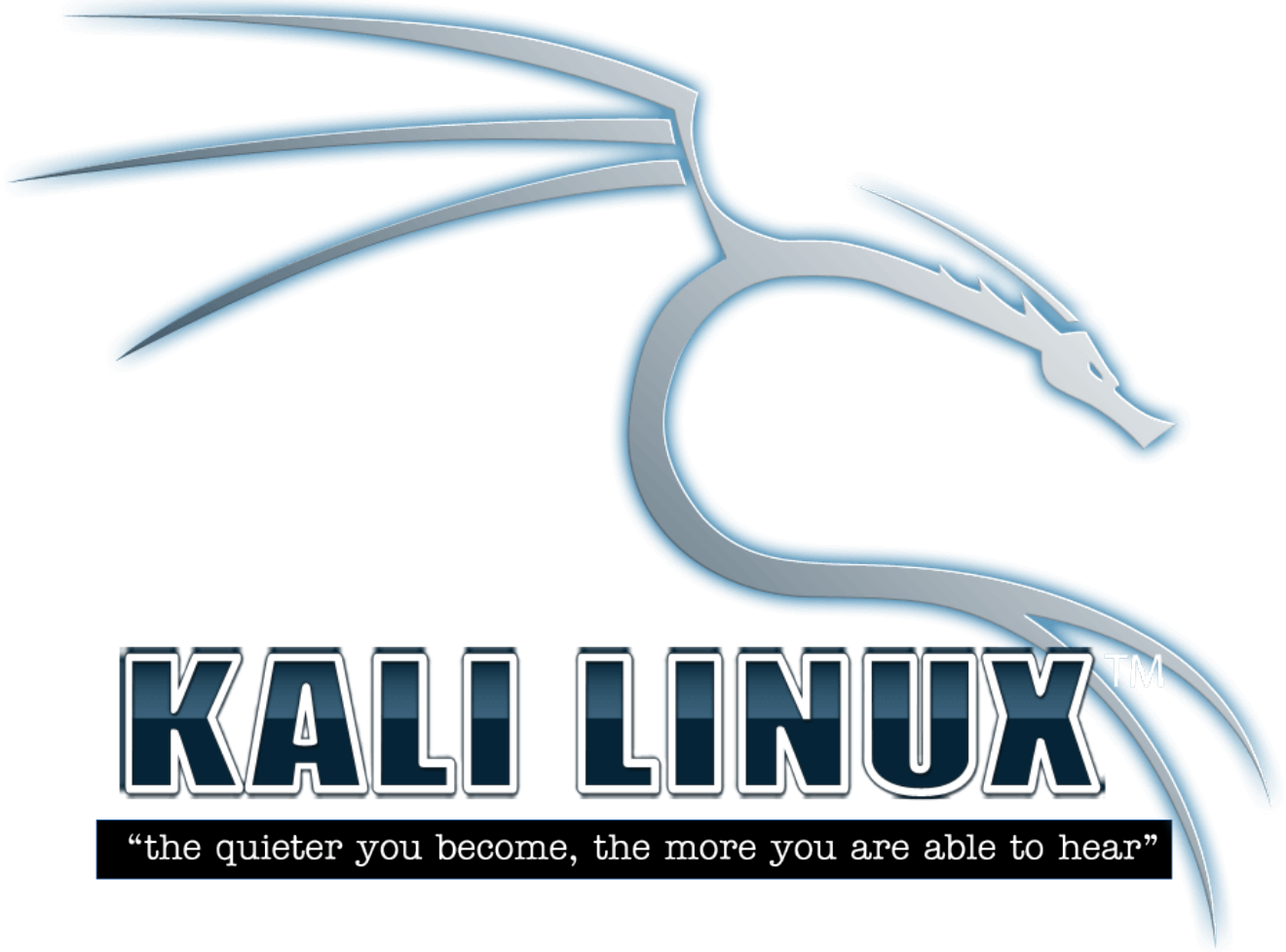
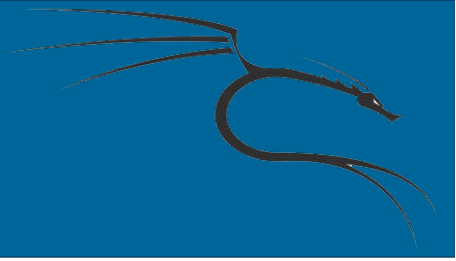
Pentest com Kali Linux





Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Metasploit Console (MSFCONSOLE)

Nesta aula, vamos examinar o Console do Metasploit (msfconsole). O **msfconsole** é usado principalmente para gerenciar o banco de dados do Metasploit, gerenciar sessões, e configurar e lançar módulos do Metasploit. Essencialmente, para efeitos de exploração, o **msfconsole** vai ficar conectado a um host de modo que você pode lançar suas façanhas contra ela.

Metasploit Console (MSFCONSOLE)

Alguns comandos comuns que você vai usar quando interagir com o console são:

help: Ele permitir que você veja o arquivo de ajuda para o comando que você está tentando executar

use module : Ele permite-lhe começar a configurar o módulo que você escolheu

set optionname module : Ele permite que você defina as várias opções para um determinado módulo

exploit : Este comando lança o módulo de exploração

Metasploit Console (MSFCONSOLE)

run : Este comando lança uma não-exploração do módulo

search module : Este comando permite-lhe procurar um módulo individual

exit : Ele sai do ***msfconsole***

Se caso, você não tenha um arquivo, você pode criar em:

/usr/share/metasploit-framework/data/john/wordlists/password.lst

E a lista de *password.lst*, você pode baixar em:

https://raw.githubusercontent.com/aircrack-ng/aircrack-ng/master/test/password.lst

Ou em algum outro site da internet

Nessa parte, vamos usar o Módulo ***John The Ripper,*** no qual usa para identificar senhas fracas que foram adquiridos como arquivos hash (pilhagem) ou hashes LANMAN/NTLM (hashdump). O objetivo deste módulo é encontrar senhas triviais em um curto espaço de tempo. Para quebrar senhas complexas ou usar grandes listas de palavras, *John the Ripper* deve ser usado fora do Metasploit. Esta versão inicial apenas lida com credenciais LM/NTLM de *hashdump* e usa a lista de palavras e regras padrão.

Metasploit Console (MSFCONSOLE)

Vamos começar nossa exploração do msfconsole:

1. Abra um prompt de comando.

2. Inicie o *msfconsole* usando o seguinte comando:

 # msfconsole

3. Procure todos os módulos Linux disponíveis usando o comando de busca. Isto é sempre uma boa idéia para procurar o nosso módulo de cada vez que quiser executar uma ação. A principal razão disto é que entre as várias as versões do Metasploit, o caminho para o módulo pode ter mudado:

Metasploit Console (MSFCONSOLE)

 # search linux

```
nd Shell, Find Tag Inline
   payload/linux/x86/shell_reverse_tcp                                normal     Linux Comma
nd Shell, Reverse TCP Inline
   payload/linux/x86/shell_reverse_tcp2                               normal     Linux Comma
nd Shell, Reverse TCP Inline - Metasm Demo
   post/linux/gather/checkvm                                          normal     Linux Gathe
r Virtual Environment Detection
   post/linux/gather/enum_configs                                     normal     Linux Gathe
r Configurations
   post/linux/gather/enum_network                                     normal     Linux Gathe
r Network Information
   post/linux/gather/enum_protections                                 normal     Linux Gathe
r Protection Enumeration
   post/linux/gather/enum_system                                      normal     Linux Gathe
r System and User Information
   post/linux/gather/enum_users_history                               normal     Linux Gathe
r User History
   post/linux/gather/enum_xchat                                       normal     Linux Gathe
r XChat Enumeration
   post/linux/gather/hashdump                                         normal     Linux Gathe
r Dump Password Hashes for Linux Systems
   post/linux/gather/mount_cifs_creds                                 normal     Linux Gathe
r Saved mount.cifs/mount.smbfs Credentials
   post/linux/gather/pptpd_chap_secrets                               normal     Linux Gathe
r PPTP VPN chap-secrets Credentials
   post/linux/manage/download_exec                                    normal     Linux Manag
e Download and Exececute
   post/multi/manage/sudo                                             normal     Multiple Li
nux / Unix Post Sudo Upgrade Shell
   post/windows/manage/pxexploit                                      normal     Windows Mar
age PXE Exploit Server


msf > 
```

Metasploit Console (MSFCONSOLE)

Use o módulo John the Ripper Linux Password Cracker com o comando:

msf > use auxiliary/analyze/jtr_linux

```
msf > use auxiliary/analyze/jtr_linux
msf auxiliary(jtr_linux) >
```

5. Mostrar as opções disponíveis para o módulo usando o seguinte comando:

msf auxiliary(jtr_linux) > *show options*

```
msf auxiliary(jtr_linux) > show options

Module options (auxiliary/analyze/jtr_linux):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Crypt      false            no        Try crypt() format hashes(Very Slow)
   JOHN_BASE                   no        The directory containing John the Ripper (src, run, doc)
   JOHN_PATH                   no        The absolute path to the John the Ripper executable
   Munge      false            no        Munge the Wordlist (Slower)
   Wordlist                    no        The path to an optional Wordlist

msf auxiliary(jtr_linux) >
```

6. Agora que temos uma lista de opções que podem ser executados para este módulo, podemos definir as opções individuais usando o comando set. Vamos definir a opção JOHN_PATH:

set JOHN_PATH /usr/share/metasploit-framework/data/john/wordlists/password.lst

7. E por último, rode o comando para dar um exploid:

msf auxiliary(jtr_linux) > *exploit*