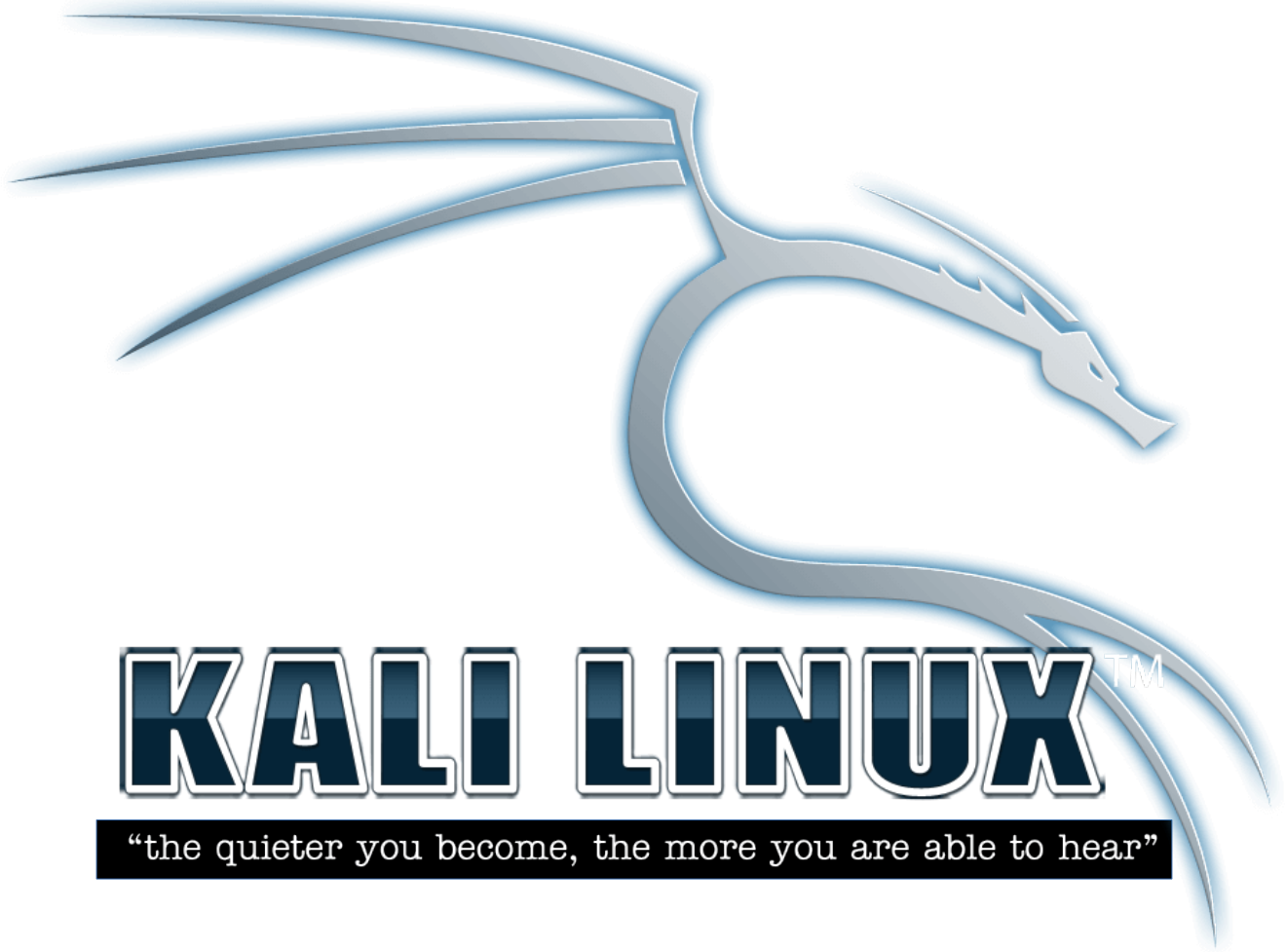
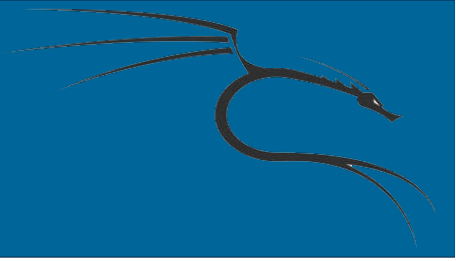
Pentest com Kali Linux





Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Criando WL com Crunch

Tem inúmeras wordlists na internet, como no projeto http://wordlist.sourceforge.net, mas as vezes queremos wordlists com senhas que tenham números e com uma quantidade determinada de caracteres.

Ex: no mínimo de 6 e máximo 8 caracteres que tenha números, ou muitas vezes que comecem com uma determinada string e que seja seguida por cinco números.

Criando WL com Crunch

Essas combinações de wordlists, todas podem ser geradas com o app Crunch, que já vem instalado no Kali Linux.

Criando WL com Crunch

Você pode usar a seguinte string:

crunch [quant_minima] [quant_maxima] [caracteres] wordlist.txt

crunch 6 8 0123456789 -o /tmp/numerica.txt

Criando WL com Crunch

Se você especificar a opção -o a geração da lista não será mostrada no terminal, geralmente enquanto está se aprendendo a utilizar o comando é bom deixar sem a opção -o para que possa ver se o que está sendo gerado é o que realmente quer.

Criando WL com Crunch

Temos outras possibilidade de criação:

```
# crunch 9 9 0123456789 -t admin@@@@ -o /tmp/wordlist.admin.txt
```

Criando WL com Crunch

O arquivo charset.lst tem como meta, suavizar o seu trabalho oferecendo listas com caracteres pré-definidos, para que não seja necessário especificar de forma manual todos os caracteres que quer colocar em sua nova wordlist.

Criando WL com Crunch

O charset.lst fornece os seguintes blocos de caracteres:

- **lalpha**: somente letras minúsculas;
- **ualpha**: somente letras maiúsculas;
- **lalpha-numeric**: letras minúsculas e números;
- **ualpha-numeric**: letras maiúsculas e números;
- **lalpha-numeric-all-space**: letras minúsculas, números e caracteres especiais mais o espaço;

Criando WL com Crunch

Continuando...

- **ualpha-numeric-all-space**: letras maiúsculas, números e caracteres especiais mais o espaço;
- **mixalpha**: letras minúsculas e maiúsculas;
- **mixalpha-numeric-all-space**: letras minúsculas, maiúsculas, números, caracteres especiais e espaço.

Criando WL com Crunch

Vamos ao nosso exemplo:

```
# crunch 4 4 -f /usr/share/crunch/charset.lst mixalpha -o /tmp/wordlist.lst
```