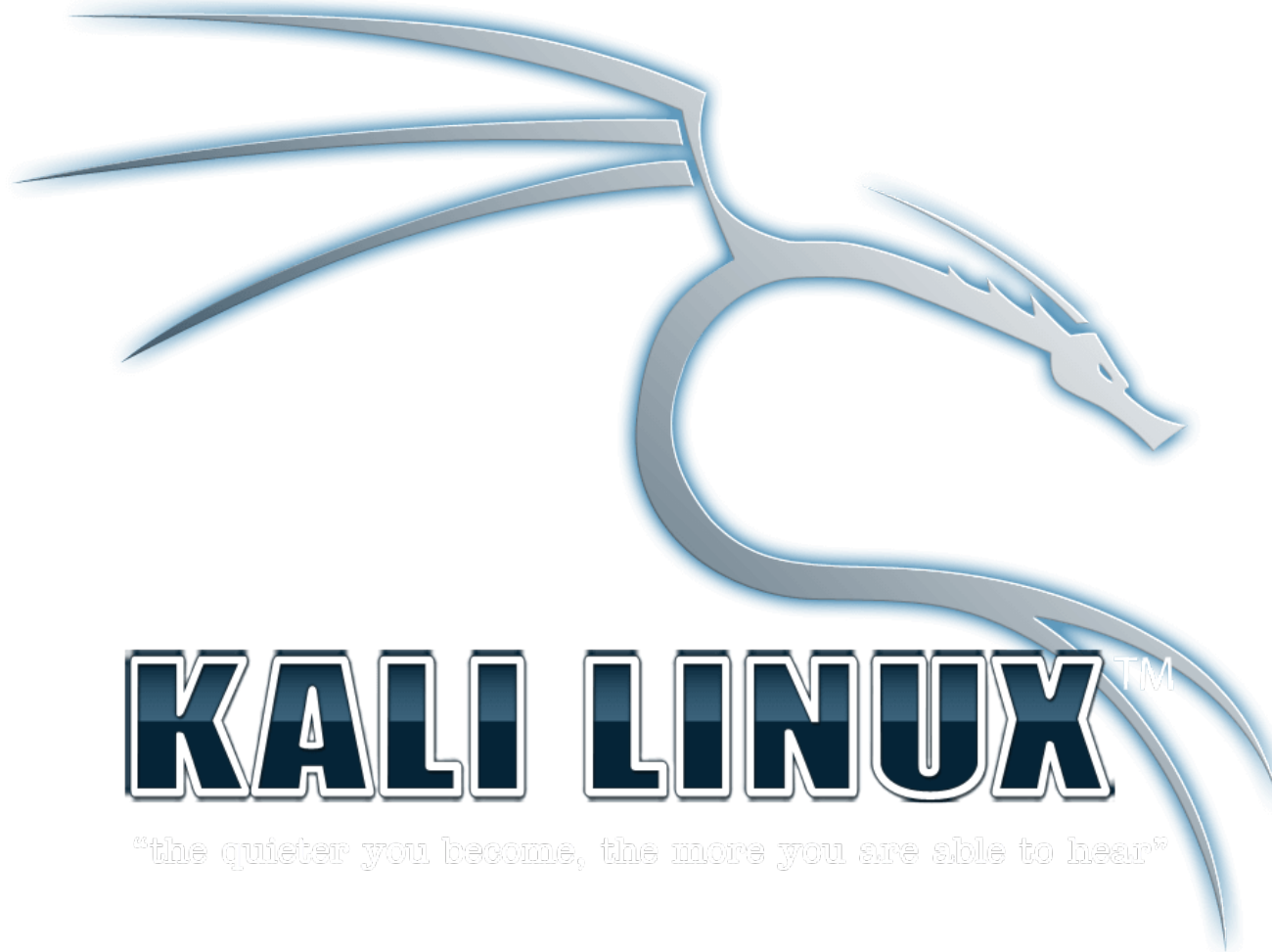


# Pentest com Kali Linux





**Instrutor: Vitor Mazuco**

**<http://facebook.com/vitormazuco>**

**Email: [vitor.mazuco@gmail.com](mailto:vitor.mazuco@gmail.com)**

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



## Usando o DNSenum

Nessa aula vamos usar o DNSenum para a enumeração de DNS. Para iniciar uma enumeração de DNS, abra o terminal e digite o seguinte comando:

```
# cd /usr/bin
```

```
# ./dnsenum --enum testedeurl.com.br
```



## Usando o DNSenum

Devemos obter uma saída com informações como, servidor de nomes, o servidor(es) e-mail, e, se tivermos sorte, uma transferência de zona:

# Usando o DNSenum

```
root@kali:~# dnsenum --enum megainput.com
dnsenum.pl VERSION:1.2.2
Warning: can't load Net::Whois::IP module, whois queries disabled.

----- megainput.com -----

Host's addresses:
-----
megainput.com 14400 IN A 69.165.173.136

Name Servers:
-----
ns3.dreamhost.com 8303 IN A 69.33.216.216
ns2.dreamhost.com 7883 IN A 208.66.40.221
ns1.dreamhost.com 8023 IN A 69.33.206.206

Mail (MX) Servers:
-----
ALT1.ASPMX.L.GOOGLE.com 238 IN A 173.194.74.27
ALT2.ASPMX.L.GOOGLE.com 71 IN A 173.194.75.27
ASPMX2.GOOGLEMAIL.com 81 IN A 173.194.74.27
ASPMX3.GOOGLEMAIL.com 123 IN A 173.194.75.26
ASPMX4.GOOGLEMAIL.com 241 IN A 74.125.138.26
ASPMX5.GOOGLEMAIL.com 85 IN A 173.194.70.27
ASPMX.L.GOOGLE.com 175 IN A 74.125.114.27
```

Trying Zone Transfers and getting Bind Versions:



Existem algumas opções adicionais que podem ser executados utilizando o DNSenum e eles incluem o seguinte:

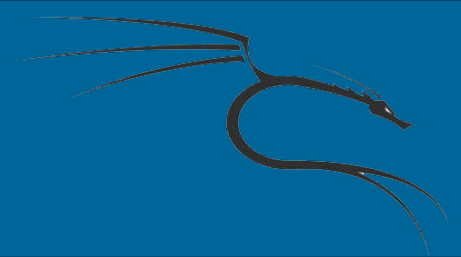
- -- threads [numero] permite definir quantos processos será executado de uma só vez
- -r permite ativar pesquisas recursivas
- -d permite definir o tempo de atraso em segundos entre solicitações de WHOIS



## Usando o DNSenum

- `-o` permite especificar o local de saída
- `-w` permite-nos para permitir que as consultas do

WHOIS

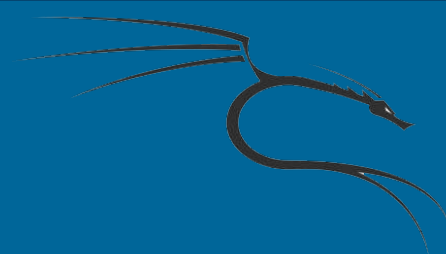


Para executar uma verificação feroz de domínio com uma ferramenta que leva várias técnicas para encontrar todos os endereços IP e nomes de *host* usados por um alvo que pode emitir o seguinte comando:

```
#cd /usr/bin
```

```
# fierce -dns sitedainternet.com
```





Para realizar a mesma operação, mas com uma *wordlist*,  
digite o seguinte comando:

```
# fierce -dns sitedainternet.com -wordlist hosts.txt  
  
-file /tmp/output.txt
```