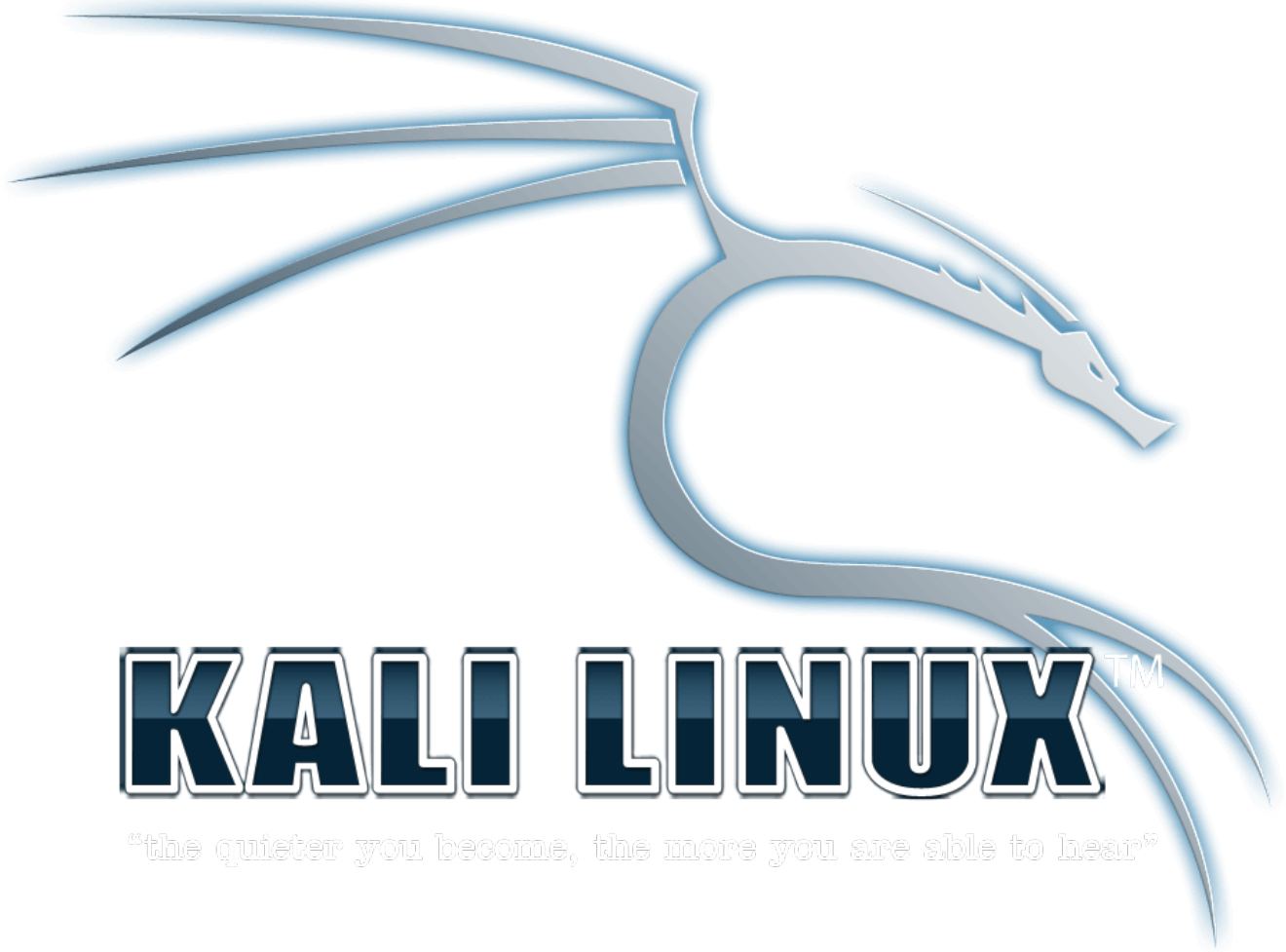
Pentest com Kali Linux



Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email: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:

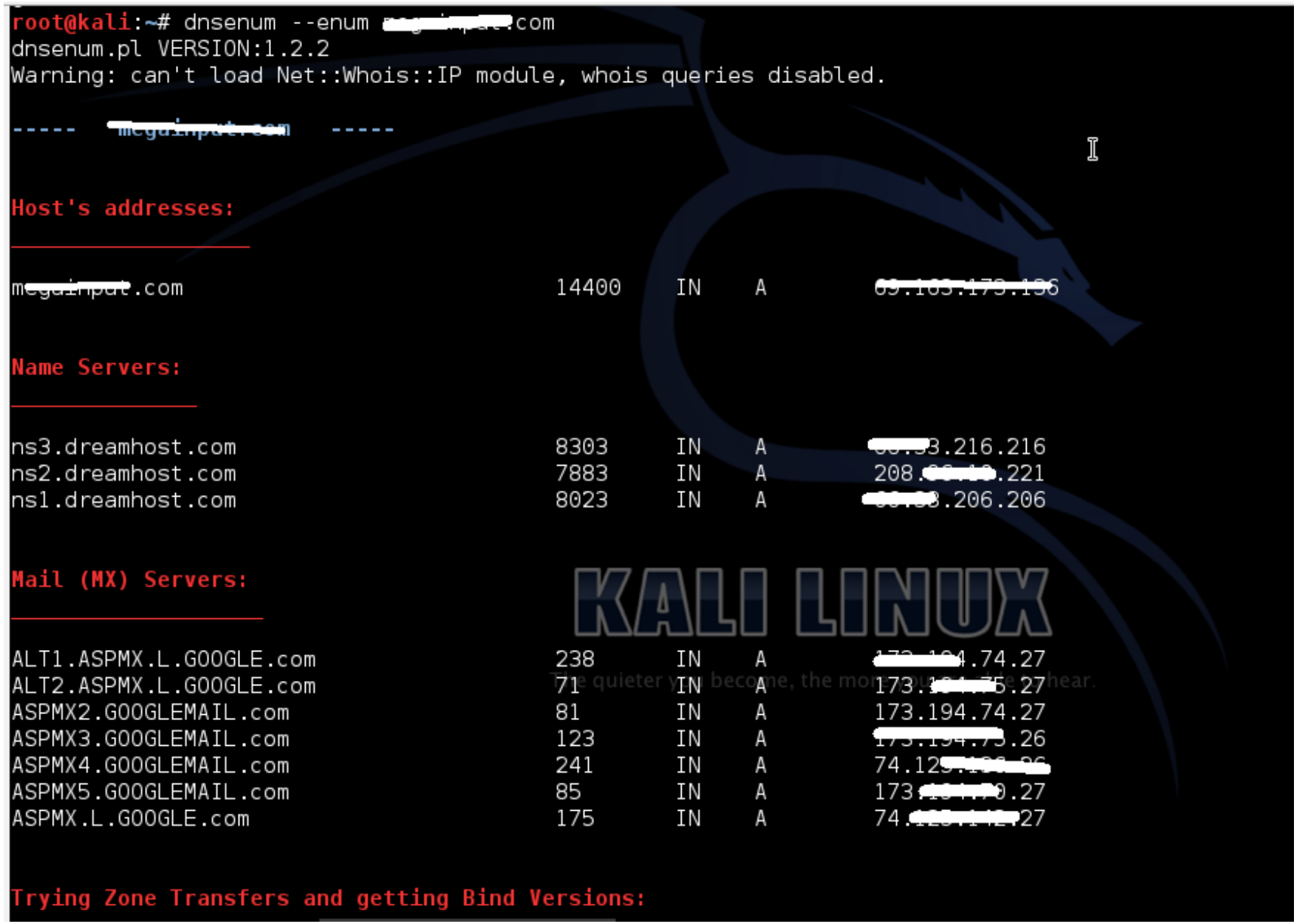
```
# cd /usr/bin

# ./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



Usando o DNSenum

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

Usando o DNSenum

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
```

Usando o DNSenum

Para realizar a mesma operação, mas com uma *wordlist*,

digite o seguinte comando:

```
# fierce -dns sitedainternet.com -wordlist hosts.txt

-file /tmp/output.txt
```