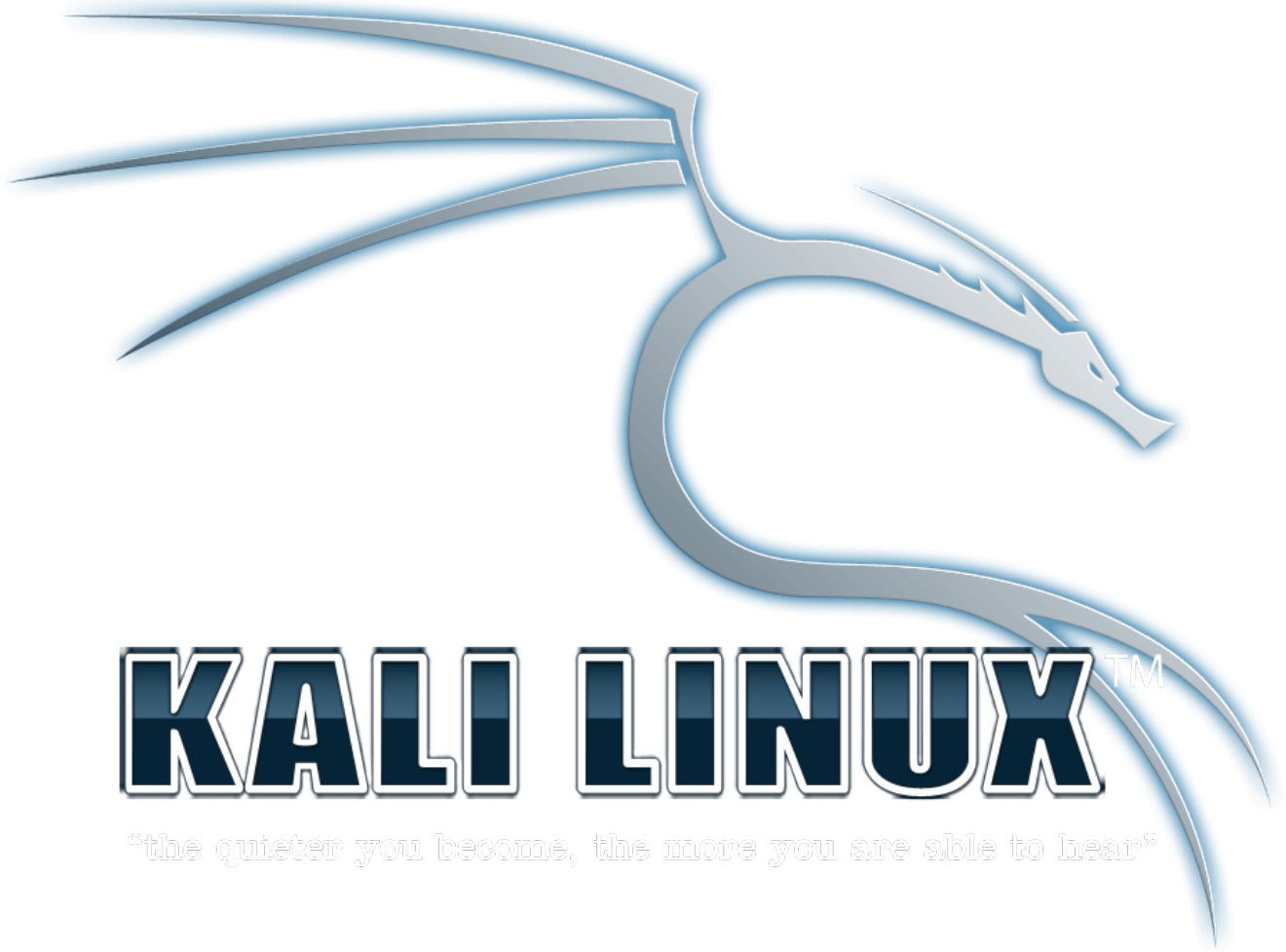
Pentest com Kali Linux



Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Encontrar portas ativas

Com o conhecimento do intervalo da rede da vítima e as máquinas ativas, vamos prosseguir com o processo de varredura de portas para buscar portas TCP e UDP abertas e seus pontos de acesso.

** O servidor web Apache deve ser iniciado a fim de completar essa aula.

Encontrar portas ativas

Vamos começar o processo de encontrar as portas abertas abrindo com o comando:

```
# nmap 192.168.1.101
```

Nós também podemos especificar explicitamente as portas para verificar (neste caso, estamos especificando 1000 portas):

```
# nmap -p 1-1000 192.168.1.101
```

Encontrar portas ativas

Ou especificar o Nmap para verificar toda a rede da organização pela porta TCP 22(SSH):

```
# nmap -p 22 192.168.1.*
```

Ou saída o resultado para um formato especificado:

```
# nmap -p 22 192.168.1.* -oG /tmp/nmap-targethost-tcp445.txt
```

Encontrar portas ativas

Nesta aula usamos o Nmap para escanear *hosts* de destino em nossa rede para determinar quais portas estão abertas.

Encontrar portas ativas

E mais, ainda possui o Zenmap, para usar o nmap com interface gráfica!