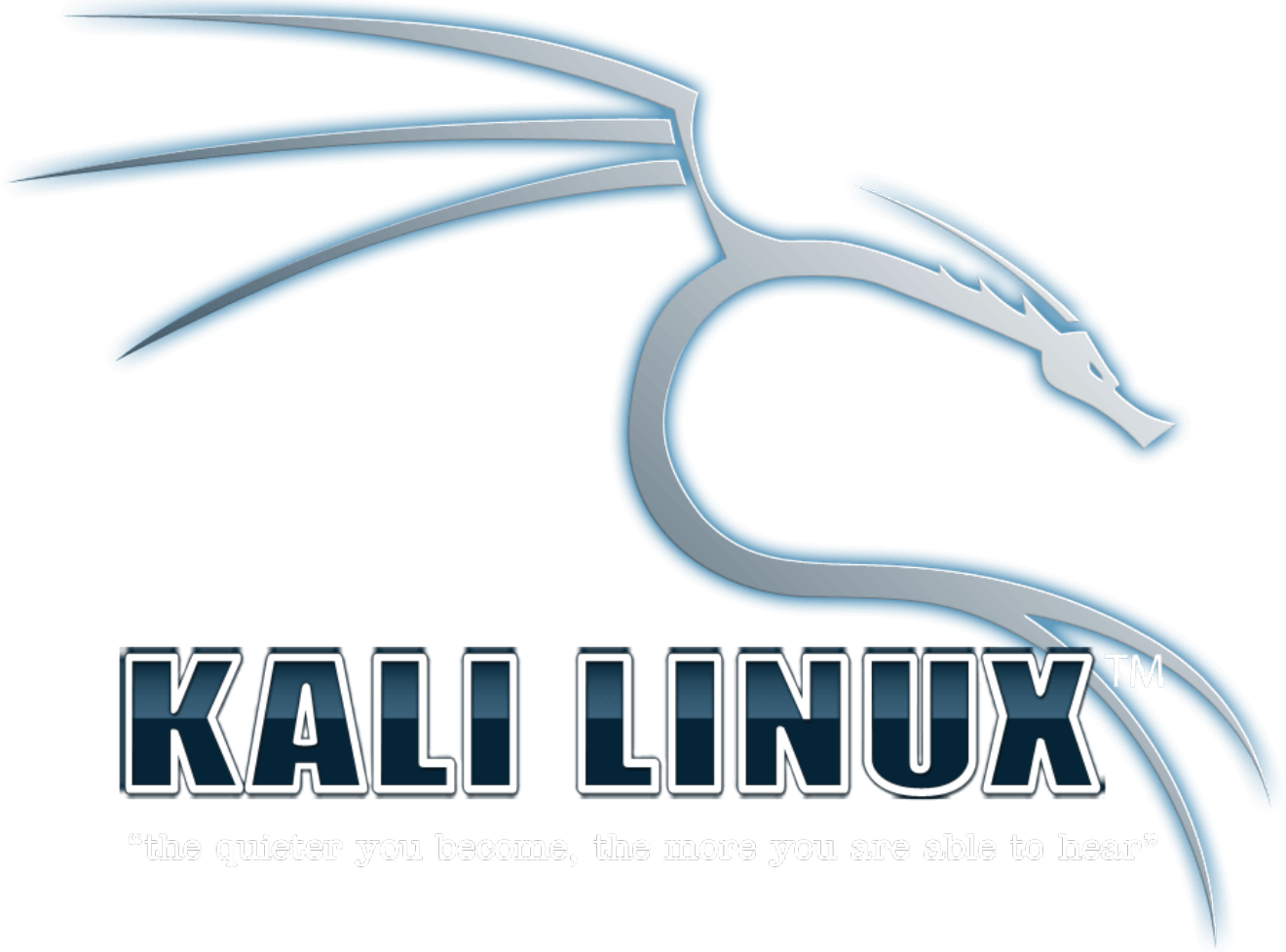
Pentest com Kali Linux



Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Identificar máquinas ativas

Antes de fazer uma *pentest*, primeiro precisamos identificar as máquinas ativas que estão no intervalo da rede de nosso alvo. Uma maneira simples seria através da realização de um *ping* na rede do alvo. Claro, isso pode ser rejeitado ou não por um host, e nós não queremos isso.

Identificar máquinas ativas

Vamos começar o processo de localizar as máquinas ativas. Usando o Nmap podemos encontrar se um *host* está ativa ou não:

```
# nmap -sP 216.27.130.162
```

Podemos também usar Nping (*Nmap suite*), o que nos dá uma visão mais detalhada:

```
# nping --echo-client "public" echo.nmap.org
```

Identificar máquinas ativas

Podemos também enviar alguns dados em hexadecimais para uma porta específica:

```
# nping -tcp -p 445 -data AF56A43D 216.27.130.162
```