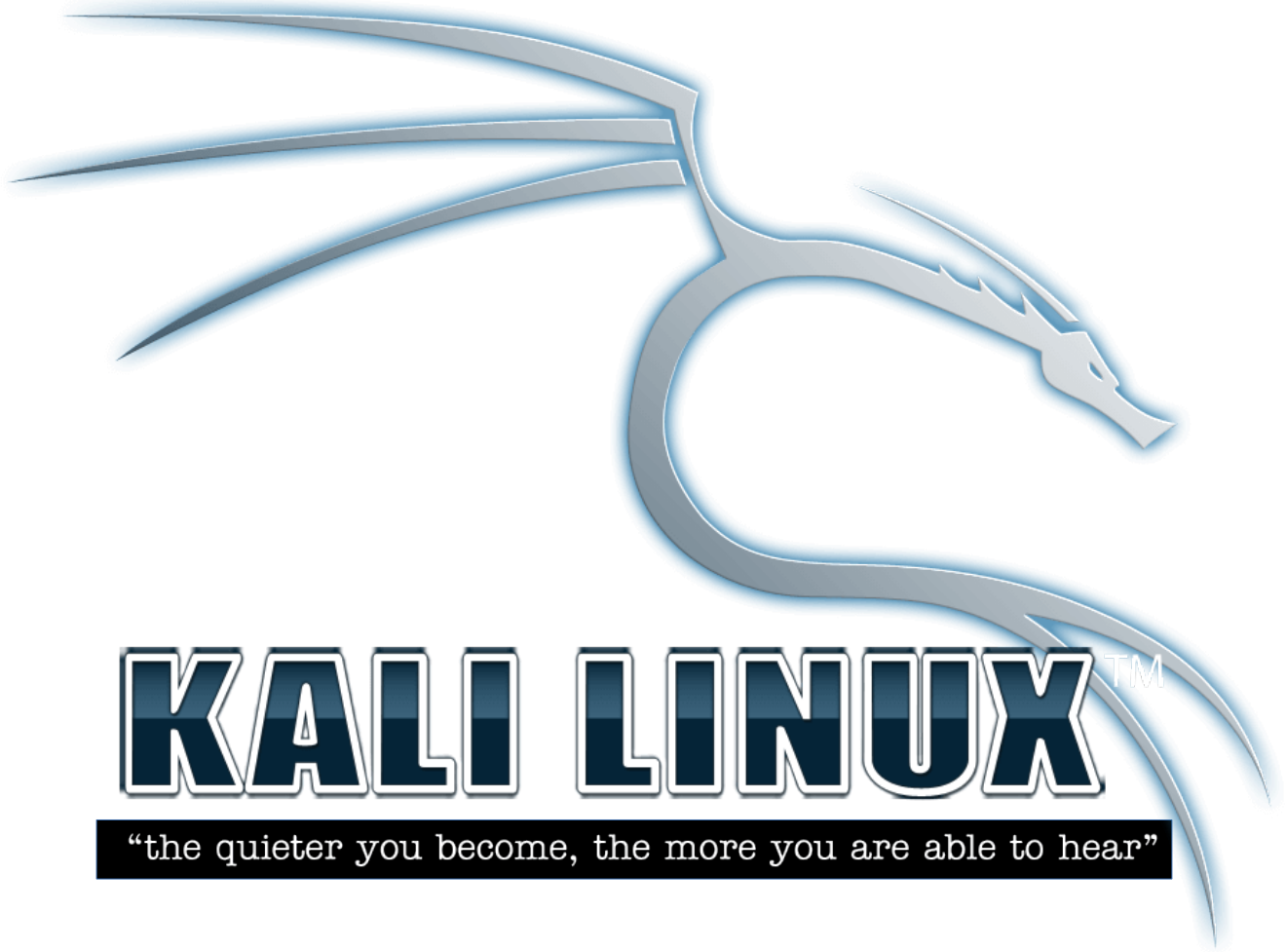
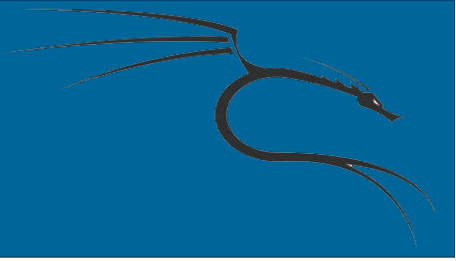
Pentest com Kali Linux





Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Banner com Amap

O Amap é um “primo” do Nmap, e foi projetado especificamente para a finalidade de identificar serviços de rede. Nesta aula, vamos explicar como usar um Amap para executar identificação do serviço. Nosso alvo, será o Metasploitable2.

Banner com Amap

Para executar identificação do serviço em uma única porta, execute o Amap com as especificações de endereço IP e o número da porta:

```
root@KaliLinux:~# amap 192.168.1.196 80
```

Banner com Amap

O Amap também pode ser utilizado para digitalizar uma série sequencial de números de porta usando a notação de traço. Para fazer isso, execute o amap com a especificação de endereço IP e intervalo de portas indicados pelo primeiro número de porta no intervalo, com um traço e, em seguida, o último número da porta no intervalo:

```
root@KaliLinux:~# amap 192.168.1.196 20-30
```

Banner com Amap

Além de identificar todos os serviços que ele pode, ele também gera uma lista no final da saída indicando as portas não identificados. Esta lista não inclui apenas portas abertas que estão executando serviços que não puderam ser identificados, mas também todas as portas fechadas que são examinadas. Embora a saída é controlável quando apenas 10 portos são verificadas, torna-se muito irritante quando intervalos de portas maiores são usados. Para suprimir a informação sobre as portas não identificados, a opção ‘-q’ pode ser usado:

```
root@KaliLinux:~# amap 192.168.1.196 1-100 -q
```

Banner com Amap

Os banners podem ser anexados à saída associado a cada porta usando a opção ‘-b’:

```
root@KaliLinux:~# amap 192.168.1.196 1-100 -qb
```

Banner com Amap

Os *scans* da identificação do serviço em grande número de portas ou varreduras completas sobre todas as 65.536 portas podem ter um tempo excepcionalmente longo se cada sondagem é utilizada em cada serviço. Para aumentar a velocidade da verificação de identificação de serviço, o argumento ‘-1’ pode ser usado para interromper a análise de um determinado serviço depois de ser combinado com uma assinatura:

```
root@KaliLinux:~# amap 192.168.1.196 1-100 -q1
```