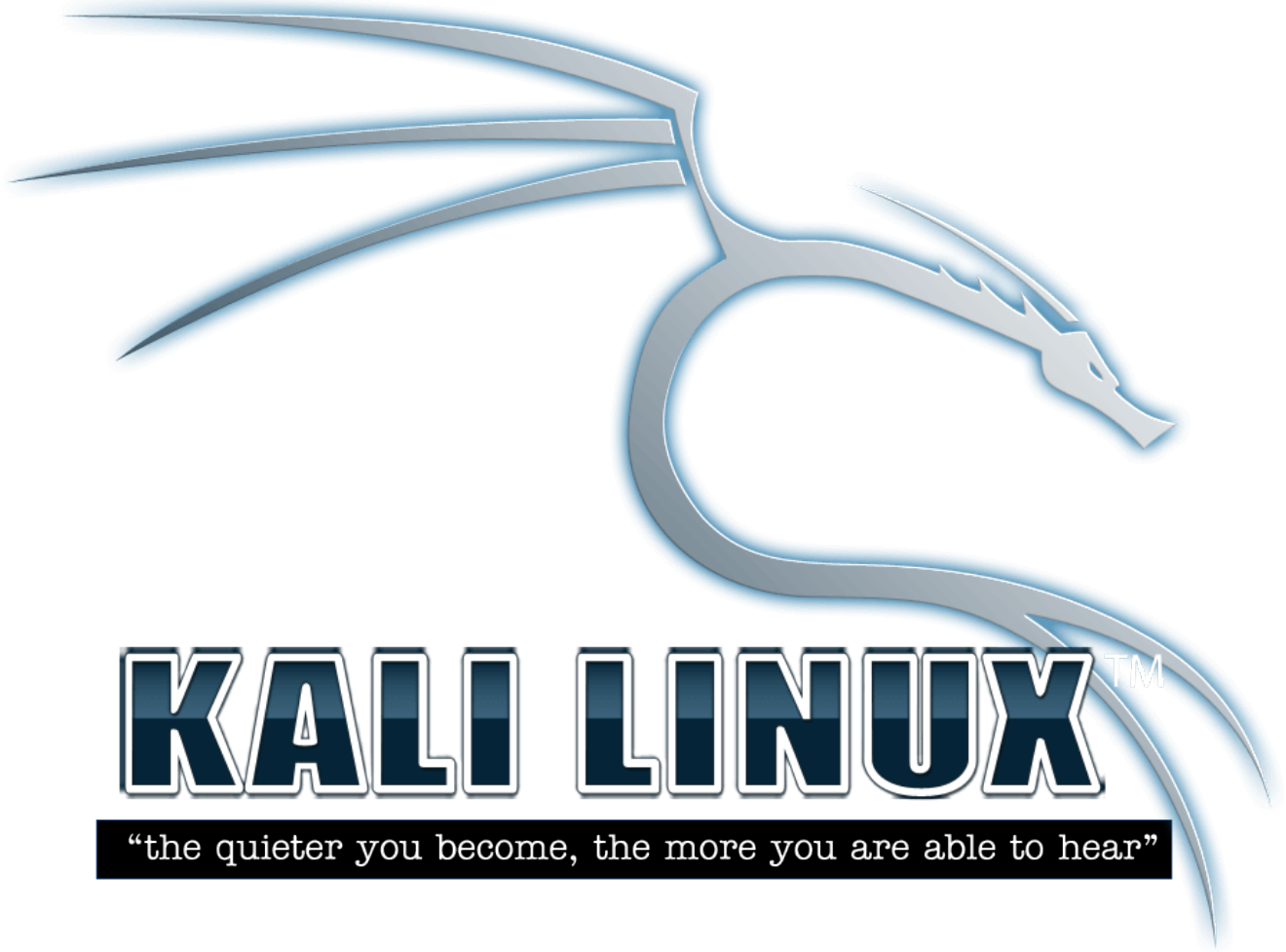
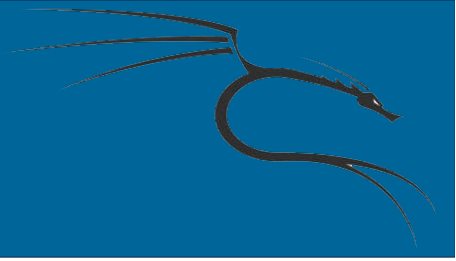
Pentest com Kali Linux





Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Netcat

Netcat é o canivete suíço para hackers e administrador de rede. Como tal, você pode usá-lo para abrir conexões TCP e UDP entre duas máquinas sobre qualquer porta que deseja. Ele também pode ser usado como uma ferramenta de verificação de portas, semelhante ao nmap. Além disso, ele pode ser usado para encaminhamento de porta, proxy, servidor web simples, e deixando um backdoor aberto para o hacker.

Netcat

Vamos agora usar o Netcat para escanear as portas de um IP. Por exemplo, podemos verificar todos as portas até 1000, emitindo este comando:

```
# netcat -z -v 192.168.1.196 1-1000
```

Junto com a opção -z, temos também a opção -v para o netcat fornecer informações mais detalhada.

No entanto, a digitalização vai muito mais rápido se você souber o endereço IP que você precisa. Em seguida, você pode usar a opção -n para especificar que você não precisa para resolver o endereço IP usando DNS:

```
# netcat -z -n -v 192.168.1.196 1-1000
```

Em uma máquina, você pode usar o netcat para escutar uma porta específica para conexões. Nós podemos fazer isso, fornecendo o parâmetro -l e escolher uma porta:

```
# netcat 192.168.1.196 4444
```

Ou usar o

```
# nc -vn 192.168.1.196 22
```

Netcat é capaz de verificar as bandeiras de esses serviços, porque os serviços são configurados para auto-divulgar essas informações quando um serviço cliente se conecta a eles. A prática de serviços e versões de auto-revelação era comumente usado no passado para garantir aos clientes que ligam que eles estão se conectando ao seu destino pretendido.

Como desenvolvedores estão se tornando mais conscientes da segurança, esta prática está se tornando menos comum. No entanto, ainda não é incomum você achar um servidor mal desenvolvidos ou mais velho que podem fornecem muita informação sob os banners de serviços.