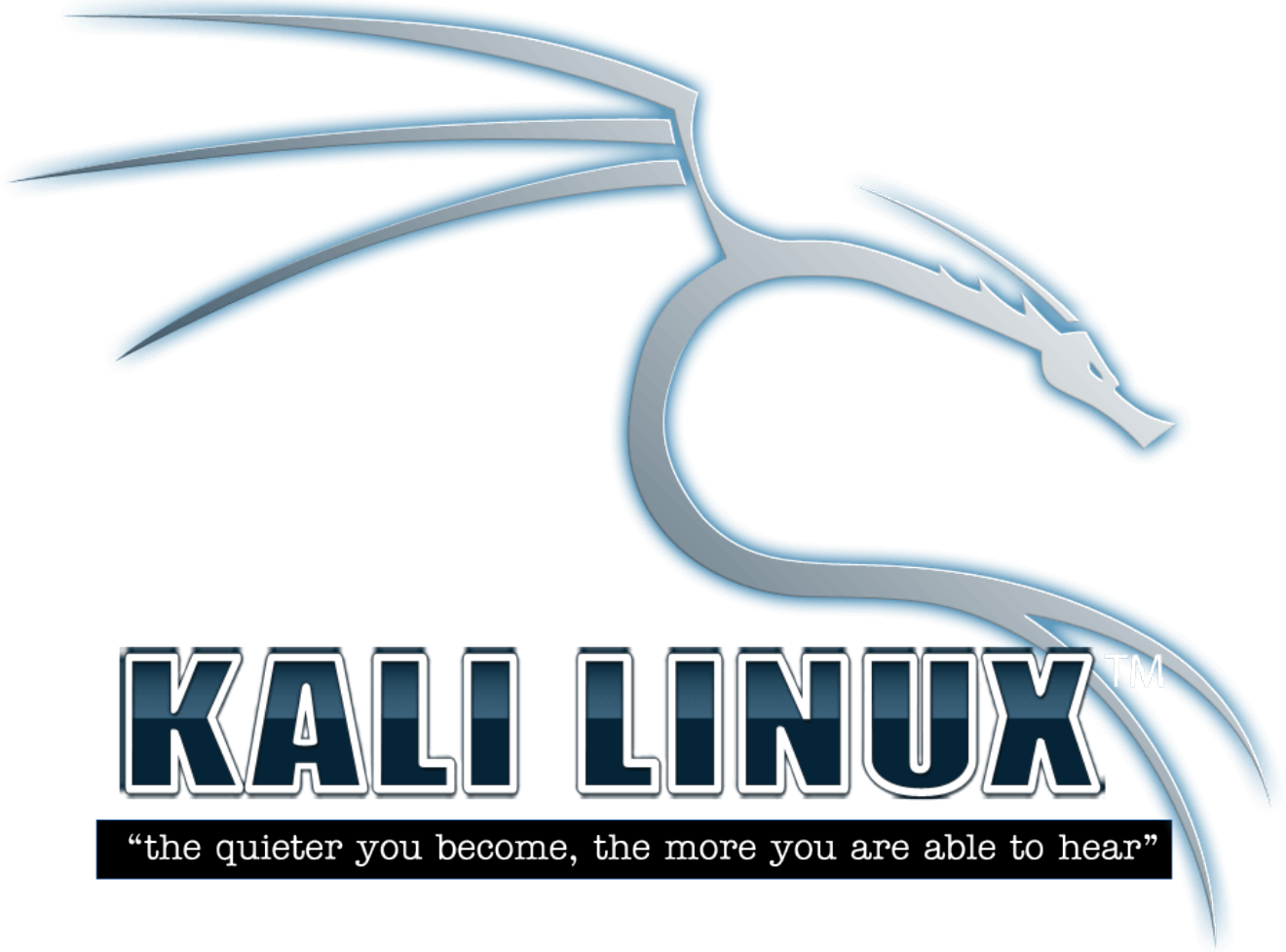
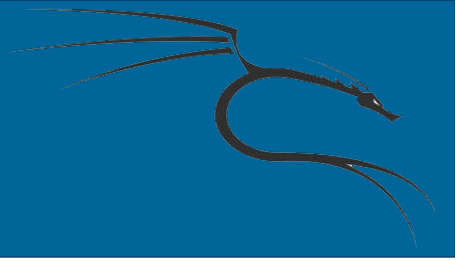
Pentest com Kali Linux





Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Banner com Python

O módulo de soquete em Python pode ser usado para conectar a serviços de rede que funcionam em portas remotas. Esta aula irá demonstrar como usar o Python para adquirir a banners de serviços, a fim de identificar os serviços associados com as portas abertas em um sistema de destino.

Vamos usar um máquina Metasploitable2 para ver o nosso alvo.

Banner com Python

```
root@kali:~# python
Python 2.7.3 (default, Jan 2 2016, 16:53:07) [GCC 4.7.2] on
linux2 Type "help", "copyright", "credits" or "license" for more
information.
>>> import socket
>>> bangrab = socket.socket(socket.AF_INET,
socket.SOCK_STREAM)
>>> bangrab.connect(("192.168.1.193", 21))
```

Banner com Python

```
>>> bangrab.recv(4096)
'220 (vsFTPd 2.3.4)\r\n'
>>> bangrab.close()
>>> exit()
```

No exemplo fornecido, um novo socket é criado com o nome bangrab. O argumento AF_INET é usado para indicar que o encaixe que vai linkar um endereço em IPv4 e o argumento SOCK_STREAM é usado para indicar que o transporte TCP é o que será usado. Uma vez que o socket é criado, a função *connect* pode ser usado para inicializar uma ligação. No exemplo, o socket *bangrab* está conectado à porta 21 no host remoto Metasploitable2 no 192.168.1.193.

Após a ligação, a função *recv* pode ser usado para receber o conteúdo do serviço ao qual o soquete está conectado. Supondo que há informação disponível, ele será impresso como saída. Aqui, podemos ver o banner fornecido pelo serviço FTP em execução no servidor do Metasploitable2. Finalmente, a função *close* pode ser usado para terminar graciosamente a conexão com o serviço remoto. Se tentar se conectar com um serviço que não está aceitando conexões, um erro será devolvido pelo interpretador do Python:

Banner com Python

```
root@KaliLinux:~# python Python 2.7.3 (default, Jan
2 2016, 16:53:07) [GCC 4.7.2] on linux2 Type "help",
"copyright", "credits" or "license" for more information.
>>> import socket
>>> bangrab = socket.socket(socket.AF_INET,
socket.SOCK_STREAM)
```

Banner com Python

```
>>> bangrab.connect(("192.168.1.193", 443))
Traceback (most recent call last):
File "<stdin>", line 1, in <module>
File "/usr/lib/python2.7/socket.py", line 224, in meth
return getattr(self._sock,name)(*args)
socket.error: [Errno 111] Connection refused
>>> exit()
```

Banner com Python

Se for feita uma tentativa para conectar a porta TCP 443 no sistema Metasploitable2, um erro será retornado indicando que a conexão foi recusada. Isso ocorre porque não há nenhum serviço em execução neste porta remota. No entanto, mesmo quando não há serviços em execução em uma porta de destino, isso não significa que um banner serviço irá necessariamente estar disponíveis.