Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Identificando com o Python

Vamos agora usar o módulo *scapy* em python para identificarmos os sistemas operacionais de nossos alvos.

Identificando com o 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.
>>> from scapy.all import *
>>> ans = sr1(IP(dst="192.168.1.84”)/ICMP())
>>> if int(ans[IP].ttl) <= 64:
…       print "Host Linux"
```

Identificando com o Python

```
else:
...
    print "Host Windows"
...
>>> ans = sr1(IP(dst="192.168.1.196")/ICMP())
>>> if int(ans[IP].ttl) <= 64:
print "Host is Linux"
... else:
…    print "Host is Windows"
```

Ao enviar as mesmas solicitações, um valor inteiro equivalente do TTL pode ser testado para determinar se é menor ou igual a 64, caso em que, podemos assumir que o dispositivo tem provavelmente um sistema Linux/Unix. Caso contrário, se o valor não é menor ou igual a 64, podemos assumir que o dispositivo provavelmente tem um sistema operacional Windows. Todo esse processo pode ser automatizado usando um script Python executável com o arquivo *ttl_id.py*

root@KaliLinux:~# python ttl_id.py 192.168.1.196