Python para Pentesters (V)

Introdução: Python

```
#!/usr/bin/python
# comentario
print "KairWne"
ip = raw_input("Digite o IP: ") #string
porta = input("Digite a porta: ") #inteiro
ver = 1.1

print "Scan versao: ",ver
print "Varrendo host: ",ip,"na porta",porta
```

Trabalhando com Argumentos

```
#!/usr/bin/python
import sys
print "Varrendo o host:",sys.argv[1],"na porta",sys.argv[2]
```

```
#!/usr/bin/python
import os
print "Verificando portas abertas"
os.system("netstat -nlvp")
```

Condições e Repetições

```
#!/usr/bin/python
#codicoes
import sys

if len(sys.argv) <= 2:
  print "Modo de uso: script.py 10.1.1.1 80"

else:
  print "Varrendo host:",sys.argv[1],"na porta",sys.argv[2]
```

```
#!/usr/bin/python
#repeticoes

for ip in range(1,255):
  print "Varrendo IP: 192.168.0.%s" %ip
```

Trabalhando com sockets

```
#!/usr/bin/python

import socket,sys

ip = sys.argv[1]
porta = int(sys.argv[2])

meusocket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
res = meusocket.connect_ex((ip,porta))

if (res == 0):
  print "Porta Aberta"
else:
  print "Porta Fechada"
```

Criando um portscan em Python

```
#!/usr/bin/python

import socket,sys

for porta in range(1..65535):
  meusocket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
  if meusocket.connect_ex((sys.argv[1],porta)) == 0:
    print "Host-",sys.argv[1],"Porta",porta,"[ABERTA]"
    meusocket.close()
```

Banner Grabbing em Python

```
#!/usr/bin/python

import socket

ip = raw_input("Digite o ip:")
porta = input("Digite a porta:")
```

```
meusocket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
meusocket.connect((ip,porta))
banner = meusocket.recv(1024)
print(banner)
```

```
#!/usr/bin/python3

import socket

def banner(ip, port):
    s = socket.socket()
    s.connect((ip, int(port)))
    s.settimeout(5)
    print(s.recv(1024))

def main():
    ip = input("Please enter the IP: ")
    port = str(input("Please enter the port: "))
    banner(ip, port)

main()
```

Interagindo com Serviços

```
#!/usr/bin/python
import socket,sys

print "Interagindo com FTP SERVER"

ip = raw_input("Digite o IP:")
porta = 21

meusocket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
meusocket.connect_ex((ip,porta))
banner = meusocket.recv(1024)
print banner

print "Enviando usuario"
meusocket.send("USER kairwne\r\n")
banner = meusocket.recv(1024)
print banner

print "Enviando senha"
meusocket.send("PASS kairwne\r\n")
banner = meusocket.recv(1024)
print banner
```

Criando um DNS Resolver em Python

```
import socket,sys

host = sys.argv[1]

print host,"--->",socket.gethostbyname(host)
```

Trabalhando com WEB

```
#!/usr/bin/python
import requests

site = requests.get("http://site.com.br/")
status = site.status_code

if (status == 200):
  print "Pagina Existe"
else:
  print "Pagina Nao Existe"
```

```
import urllib
site = urllib.urlopen("site")
server = site.info()

print "o servidor esta rodando"
print server["server"]
```