Criando um Portscan com o Scapy

+ Objetivo: Aprender a montar scripts em python com o scapy

```
#!/usr/bin/python3
import sys
from scapy.all import *

conf.verb = 0

portas = [21,22,23,25,80,443,8080]

pIP = IP(dst=sys.argv[1])
pTCP = TCP(dport=portas,flags="S")
pacote = pIP/pTCP
resp, noresp = sr(pacote)
for resposta in resp:
    porta = resposta[1][TCP].sport
    flag = resposta[1][TCP].flags
    if (flag == "SA"):
        print (f"Porta {porta} aberta")
```

+ Esse conf.verb = 0 serve somente para tornar mais limpa a saída so script

+ No resposta[1], o [1] indica que é o pacote recebido em que estamos fazendo a análise
Se quiséssemos pegar o enviado, bastaria trocar por 0