5. nmap

Wednesday, November 4, 2020 8:05 AM

Nmap es un potente escáner de puertos que permite identificar puertos abiertos, cerrados o filtrados, así como programar rutinas para encontrar posibles vulnerabilidades en un host determinado.

```
import nmap

# take the range of ports to
# be scanned
begin = 78
end = 80

# assign the target ip to be scanned to
# a variable
target = '148.234.5.206'

# instantiate a PortScanner object
scanner = nmap.PortScanner()

for i in range(begin,end+1):

    # scan the target port
    res = scanner.scan(target,str(i))

    # the result is a dictionary containing
    # several information we only need to
    # check if the port is opened or closed
    # so we will access only that information
    # in the dictionary
    res = res['scan'][target]['tcp'][i]['state']

    print(f'port {i} is {res}.')
```