Cyber Security Tool
Port Scan by Python

郭益華

GitHub

撰寫一般的port掃描程式

portScanner.py portScanner_threaded.py

portScanner.py > ...

```python
import socket
import time

startTime = time.time()


if __name__ == '__main__':
    target = input('Enter the host to be scanned: ')

    t_IP = socket.gethostbyname(target) # 將主機名稱轉換成ipv4地址
    print ('Starting scan on host: ', t_IP)

# 掃描常見的端口
    for i in range(50, 500): #可自行更改
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        conn = s.connect_ex((t_IP, i))

        if(conn == 0) :
            print ('Port %d: OPEN' % (i,))
            s.close()
print('Time taken:', time.time() - startTime)
```

測試

可觀察到掃描所花費的時間為 918 秒，大約為15分鐘，效率較差

```
PS C:\Users\jerry\Desktop\mastercourse\dataEngineer\PythonforHackers\networkprogram\portScanbyPython> python portScanner
.py
Enter the host to be scanned: localhost
Starting scan on host:  127.0.0.1
Port 135: OPEN
Port 445: OPEN
Time taken: 918.5217776298523
```

使用分散式架構撰寫port掃描程式

portScanner_threaded.py > threader

```python
import socket
import time
import threading
from queue import Queue


socket.setdefaulttimeout(0.25)
print_lock = threading.Lock()
target = input('Enter the host to be scanned: ')
t_IP = socket.gethostbyname(target) # 將主機名稱轉換成ipv4地址
print ('Starting scan on host: ', t_IP)

def portscan(port):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    try:
        con = s.connect((t_IP, port))
        with print_lock:
            print(port, 'is open')
        con.close()
    except:
        pass
```

```python
def threader():
    while True:
        worker = q.get()
        portscan(worker)
        q.task_done()

q = Queue()
startTime = time.time()
for x in range(100):
    t = threading.Thread(target=threader)
    t.daemon = True
    t.start()

# 掃描常見的端口
for worker in range(50, 500): #可自行更改
    q.put(worker)
    q.join()
print('Time taken:', time.time() - startTime)
```

測試

可觀察到掃描所花費的時間為 117 秒，大約為2分鐘，效率大幅提升

```
PS C:\Users\jerry\Desktop\mastercourse\dataEngineer\PythonforHackers\networkprogram\portScanbyPython> python .\portScanner_threaded.py
Enter the host to be scanned: localhost
Starting scan on host:  127.0.0.1
135 is open
445 is open
Time taken: 117.67755365371704
```

兩者比較

使用分散式的方式可以大幅提升port掃描的效率

```
PS C:\Users\jerry\Desktop\mastercourse\dataEngineer\PythonforHackers\networkprogram\portScanbyPython> python portScanner
.py
Enter the host to be scanned: localhost
Starting scan on host:  127.0.0.1
Port 135: OPEN
Port 445: OPEN
Time taken: 918.5217776298523
PS C:\Users\jerry\Desktop\mastercourse\dataEngineer\PythonforHackers\networkprogram\portScanbyPython> python .\portScann
er_threaded.py
Enter the host to be scanned: localhost
Starting scan on host:  127.0.0.1
135 is open
445 is open
Time taken: 117.67755365371704
```

End