

【PortScan】Masscan

Masscan是網路大規模的連接埠掃描儀。它可以在5分鐘內掃描整個互聯網，每秒從一台機器上傳輸1000萬個資料包（和掃描者的頻寬有關，掃描速率高容易誤報）

<https://github.com/robertdavidgraham/masscan>

```
$ sudo ./masscan MACHINE_IP/24 -p443
$ sudo ./masscan MACHINE_IP/24 -p80,443
$ sudo ./masscan MACHINE_IP/24 -p22-25
$ sudo ./masscan MACHINE_IP/24 --top-ports 100

$ sudo ./masscan -p80,443,8000-9000 182.92.106.58
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-03-28 06:16:32 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [1003 ports/host]
Discovered open port 8894/tcp on 182.92.106.58
Discovered open port 80/tcp on 182.92.106.58
Discovered open port 8896/tcp on 182.92.106.58
```

還是同樣偵測**80,443,8000至9000**之間的連接埠開放情況，新增參數rate（速度/速率）設定時要考慮自己的頻寬，不是越高越好，太高會出現漏報，頻寬和速率設定參考

```
rate=1000000 (1M)
rate=100000 (100K)
rate=50000 (50K)
```

```
$ sudo ./masscan -p80,443,8000-9000 182.92.106.58 --rate=10000
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-03-28 07:00:01 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [1003 ports/host]
Discovered open port 80/tcp on 182.92.106.58
Discovered open port 8894/tcp on 182.92.106.58
Discovered open port 8896/tcp on 182.92.106.58
```

🕒 修訂版本 #2

★ 由 treeman 建立於 29 🌟🌟🌟 2024 02:54:27

✍ 由 treeman 更新於 29 🌟🌟🌟 2024 03:04:10