

# 【PortScan】rustscan

Rustscan (只做udp 掃描)

**RustScan** 是一個用於快速、輕量級端口掃描的開源工具，使用 Rust 編程語言開發。它的目標是提供快速且高效的端口掃描，同時提供友好的用戶界面和一些有用的功能。以下是一些 **RustScan** 的主要特點和用途：

1. **快速的端口掃描**：**RustScan** 被設計為快速的端口掃描工具，能夠在短時間內掃描大量端口。
2. **高效的並行處理**：工具使用多線程和並行處理來提高效能，可以充分利用多核處理器，加速掃描速度。
3. **端口範圍設定**：用戶可以指定要掃描的端口範圍，以便針對特定需求進行掃描。
4. **版本檢測**：**RustScan** 可以嘗試識別目標端口上運行的服務的版本信息，這有助於更好地理解目標系統。
5. **輸出格式選擇**：工具允許用戶選擇不同的輸出格式，包括易於閱讀的文本格式和 JSON 格式。
6. **主機存活檢測**：除了端口掃描，**RustScan** 還可以執行主機存活檢測，以確定目標主機是否可訪問。
7. **自定義選項**：用戶可以使用各種自定義選項來調整掃描行為，以滿足其需求。

**RustScan** 是一個適用於滲透、漏洞探測、安全評估和網絡監視的實用工具。它的速度和效能使其成為許多安全專業人員的首選，並且易於使用，即使是初學者也可以快速上手。使用時應謹慎，確保在合法和授權的範圍內使用，並遵循法律和道德準則。

<https://github.com/RustScan/RustScan>

## #安裝

```
wget https://github.com/RustScan/RustScan/releases/download/2.0.1/rustscan_2.0.1_amd64.deb
sudo dpkg -i rustscan_2.0.1_amd64.deb
```

```
rustscan -a 192.168.203.151 -u 5000 -t 8000 --scripts none
```

```
# -a ip
```

```
# -u buffer (thread)
```

```
# -t timeout (minisec)
```

```
# rustscan + nmap
```

```
rustscan -a 192.168.203.151 -u 5000 -t 8000 --scripts -- -n -Pn -sVC
```

```
—(kali㉿kali)-[~]
```

```
└─$
```

```
nmap -n -sn -T4 192.168.202.0/24 -oG - | grep "Up" | awk '{print $2}' | tee ips.txt
```

```
192.168.202.6
```

```
192.168.202.8
```

```
> ports.txt
```

```
for i in $(cat ips.txt); do rustscan -a $i -u 5000 -t 5000 -g -- | awk '{gsub("->", ""); gsub("\\"[\\]", ""); print $1,$2}' | tee -a ports.txt ;done
```

```
192.168.202.6 22,80
```

```
192.168.202.8 22,25
```

```
sudo nmap -sS 192.168.202.6 -p22,80 --script http-headers,http-title
```

```
PORT      STATE SERVICE
```

```
22/tcp    open  ssh
```

```
80/tcp    open  http
```

```
| http-headers:
```

```
| Date: Tue, 07 Nov 2023 14:59:11 GMT
```

```
| Server: Apache/2.4.41 (Ubuntu)
```

```
| Last-Modified: Tue, 07 Nov 2023 12:34:33 GMT
```

```
| ETag: "d1-6098f315f9180"
```

```
| Accept-Ranges: bytes
```

```
| Content-Length: 209
```

```
| Vary: Accept-Encoding
```

```
| Connection: close
```

```
| Content-Type: text/html
```

```
|
```

```
|_ (Request type: HEAD)
```

```
|_ http-title: Under Construction
```

```
—(kali㉿kali)-[~]
```

```
└─$ curl http://192.168.202.6/
```

```
<html>
  <head>
    <title>Under Construction</title>
  </head>
  <body>
    Flag: OS{e9482a10e325a046a90b76cbf1d4e443}
    This site is still under construction, please come back later.
  </body>
</html>
```

使用方式：rustscan [標誌] [選項] [-- <命令>...]

標誌：

- accessible 可訪問模式。關閉對屏幕閱讀器產生不良影響的功能
- g, --greppable 可grep模式。僅輸出端口信息，不包括Nmap信息。適用於grep或輸出到文件
- h, --help 顯示幫助信息
- n, --no-config 是否忽略配置文件
- top 使用前1000個常見端口
- V, --version 顯示版本信息

選項：

- a, --addresses <addresses>... 要掃描的CIDR、IP或主機的逗號分隔列表
- b, --batch-size <batch-size> 端口掃描的批量大小，它會增加或減慢掃描速度，取決於操作系統的文件打開限制。如果設置為65535，將同時掃描所有端口。  
但是，您的操作系統可能不支持這一點 [默認值：4500]
- p, --ports <ports>... 要掃描的端口的逗號分隔列表。例如：80,443,8080
- r, --range <range> 端口範圍，格式為起始-結束。例如：1-1000
- scan-order <scan-order> 要執行的掃描順序。"serial"選項將按升序掃描端口，而"random"選項將隨機掃描端口 [默認值：serial] [可能的值：Serial、Random]
- scripts <scripts> 運行所需腳本的[] [默認值：default] [可能的值：None、Default、Custom]
- t, --timeout <timeout> 端口被視為關閉之前的超時時間（毫秒） [默認值：1500]
- tries <tries> 端口被視為關閉之前的嘗試次數。如果設為0，rustscan會將其更正為1 [默認值：1]
- u, --ulimit <ulimit> 自動提高ULIMIT值，以提供您提供的值

參數：<command>... 要運行的腳本參數。要使用-A參數，請在RustScan的參數末尾使用'-- -A'。

例如：'rustscan -T 1500 127.0.0.1 -- -A -sC'。

此命令會自動添加-Pn -vvv -p \$PORTS參數到nmap。

對於像--script '(safe and vuln)' 這樣的參數，請用引號括住 ""(safe and vuln)""。

☺修訂版本 #6

★由 treeman 建立於 7 🍀Q🍀@🍀🍀 2023 00:54:11

🔪由 treeman 更新於 7 🍀@🍀🍀 2024 19:30:26