

# 【kali】未安裝工具

## rockyou(seclists)

/usr/share/seclists

```
# 安裝
sudo apt update
sudo apt install -y seclists

cd /usr/share/wordlists
sudo gzip -d rockyou.txt.gz
```

## 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
```

## gobuster

```
# 安裝
sudo apt-get update
sudo apt-get install gobuster

# git hub
# https://github.com/OJ/gobuster
```

## wsgidav

<https://bookstack.treemanou.com/books/treemanoscp/page/smbwsgidav>

```
kali@kali:~$ pip3 install wsgidav
Defaulting to user installation because normal site-packages is not writeable
Collecting wsgidav
  Downloading WsgiDAV-4.0.1-py3-none-any.whl (171 kB)
    _____ 171.3/171.3 KB 1.6 MB/s eta 0:00:00
...
Successfully installed json5-0.9.6 wsgidav-4.0.1
```

## rlwrap

<https://bookstack.treemanou.com/books/treemanoscp/page/terminalrlwrap>

```
# 安裝
sudo apt install rlwrap
# listener 8888
rlwrap -cAr nc -nvlp8888
```

## sshuttle

```
# install
sudo apt install sshuttle

# run at kali
```

```
# kali -> vm1(192.168.50.63 | 10.4.50.63):2222 -> vm2(10.4.50.x)
#
sshuttle -r database_admin@192.168.50.63:2222 10.4.50.0/24 172.16.50.0/24
```

## chisel

```
# 安裝
sudo apt install chisel

# 執行
chisel server --port 8080 --reverse
```

## ncat

```
# 安裝
sudo apt install ncat

# 使用ProxyCommand 執行 ncat
ssh -o ProxyCommand='ncat --proxy-type socks5 \
--proxy 127.0.0.1:1080 %h %p' database_admin@10.4.194.215
```

## linpeas

```
sudo apt-get update

sudo apt-get -y install peass
```

---

🕒 修訂版本 #11  
★ 由 treeman 建立於 17 🇲🇲🇲🇲🇲🇲 2023 11:24:07  
✍ 由 treeman 更新於 26 🇲🇲🇲🇲🇲🇲 2024 01:15:22