Linux 基礎

Ice1187

Speaker

黃俊嘉 (Ice1187)

- Master’s student at NTU CSIE NSLab
- Member of Balsn CTF Team
- Member of UNDEFINED
- Intern Researcher at CyCraft
- Speaker of CyberSec, SECCON

https://github.com/Ice1187

hcc001202@gmail.com

Course Info

- 簡報連結：https://github.com/Ice1187/My-Slides
- 練習平台：https://github.com/Ice1187/My-CTF-Challenges

什麼是 Linux？

- 自由、開放原始碼的作業系統
- 常用於軟體開發、伺服器維運等
- 擁有許多不同分支：
  - Kali Linux
  - Ubuntu
  - Arch Linux

為什麼要學 Linux？

- 內建許多好用的工具
- 開發者導向，寫程式更方便
- 許多 CTF 現有工具是 Linux only
- ~~簡單的 CTF 題目都是 Linux-based~~

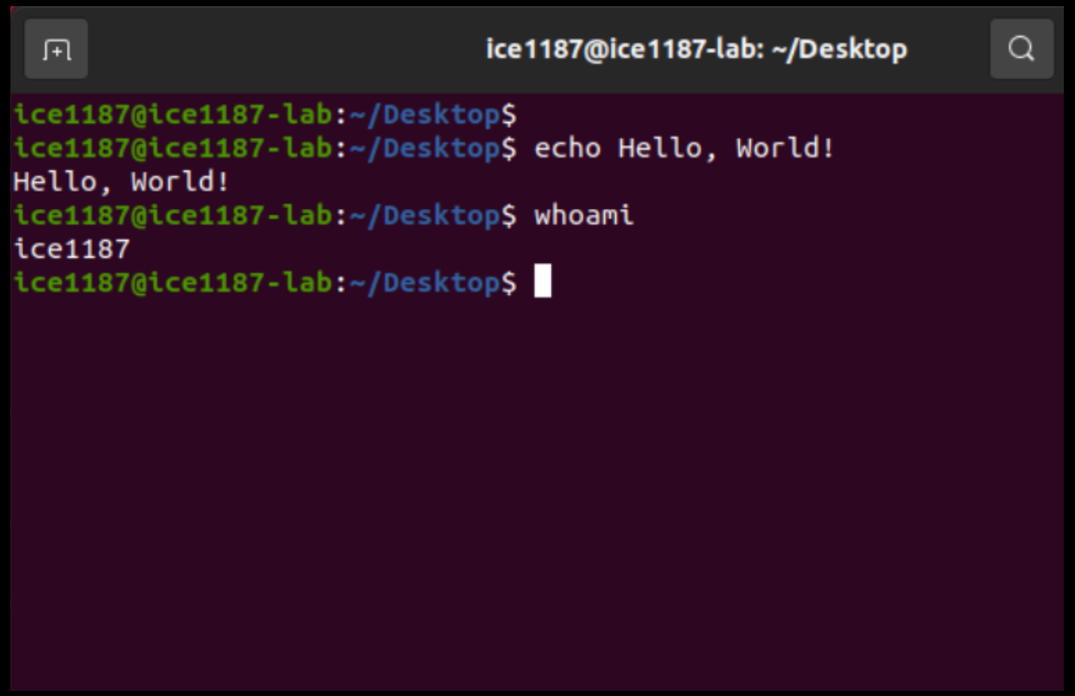
大綱

- Terminal 終端機
- File System 檔案系統
- User & Group 使用者與群組
- File Permission 檔案權限
- Network 網路
- Process
- Editor 編輯器
- Compile & Execute 編譯與執行
- Shell
- ssh 遠端連線
- Compress 壓縮/解壓縮
- Package Manager 套件管理
- Encoding 編碼
- 其他 CTF 常用指令

Terminal 終端機

Terminal 終端機

- Linux 核心功能，類似 Windows 的命令提示字元 cmd.exe
- 透過純文字介面操作電腦
- 為什麼要用 Terminal？
  - 只需要鍵盤
  - 打指令很快
  - 操作自動化

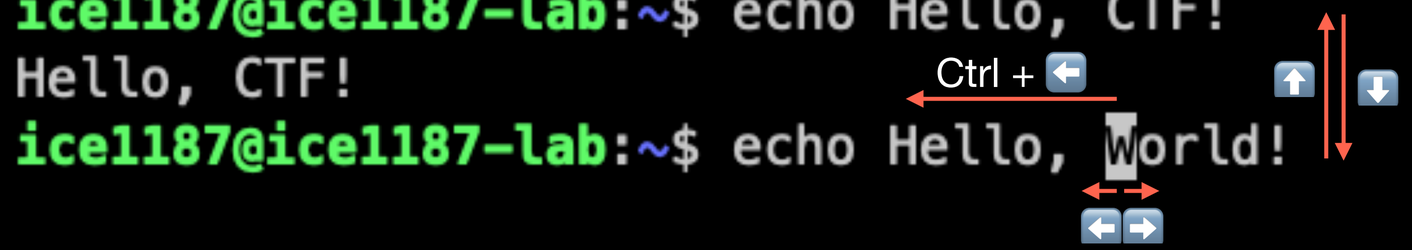


開啟 Terminal


Activities
Terminal
八 21 21:41
ice1187
Trash
1. 右鍵桌面
New Folder
Paste
Show Desktop in Files
Open in Terminal
Change Background...
Display Settings
Settings
2. 點選「Open in Terminal」
ice1187@ice1187-lab: ~/Desktop
ice1187@ice1187-lab:~/Desktop$
3. 開啟終端機

使用方法 — 方向鍵

- 左右鍵 ⬅️➡️
  - 用途：在字元之間移動
- Ctrl + 左右鍵
  - 用途：在字串之間移動
- 上下鍵 ⬆️⬇️
  - 用途：上一個 / 下一個輸入過的指令



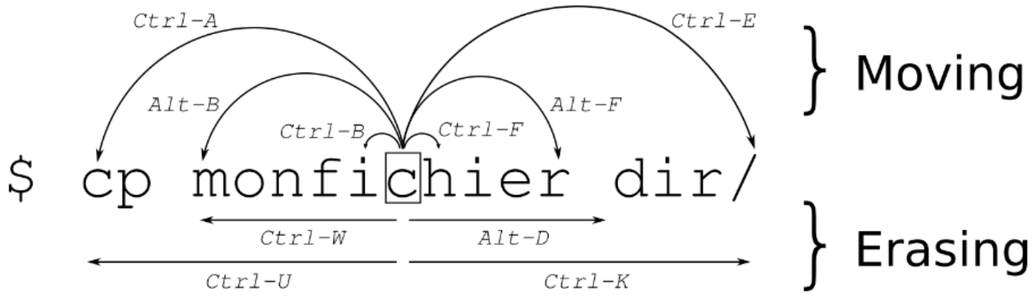
使用方法 — Tab

- 用途：在輸入指令時，按下 Tab 可以自動補完，或是顯示提示
- 自動補完：當輸入的指令有一種可能時觸發
- 顯示提示：當輸入的指令有多種可能時觸發

更多 shortcuts

- 如果想要更快移動與修改指令，可以參考 Bash Shortcuts

Bash Shortcuts



Moving

command	description
ctrl + a	Goto BEGINNING of command line
ctrl + e	Goto END of command line
ctrl + b	move back one character
ctrl + f	move forward one character
alt + f	move cursor FORWARD one word
alt + b	move cursor BACK one word
ctrl + xx	Toggle between the start of line and current cursor position
ctrl +] + x	Where x is any character, moves the cursor forward to the next occurance of x
alt + ctrl +] + x	Where x is any character, moves the cursor backwards to the previous occurance of x

使用方法 — Ctrl+c

- 用途：中斷指令
- 當指令跑到一半，不想繼續執行時，可以用 Ctrl+c 強制中斷指令

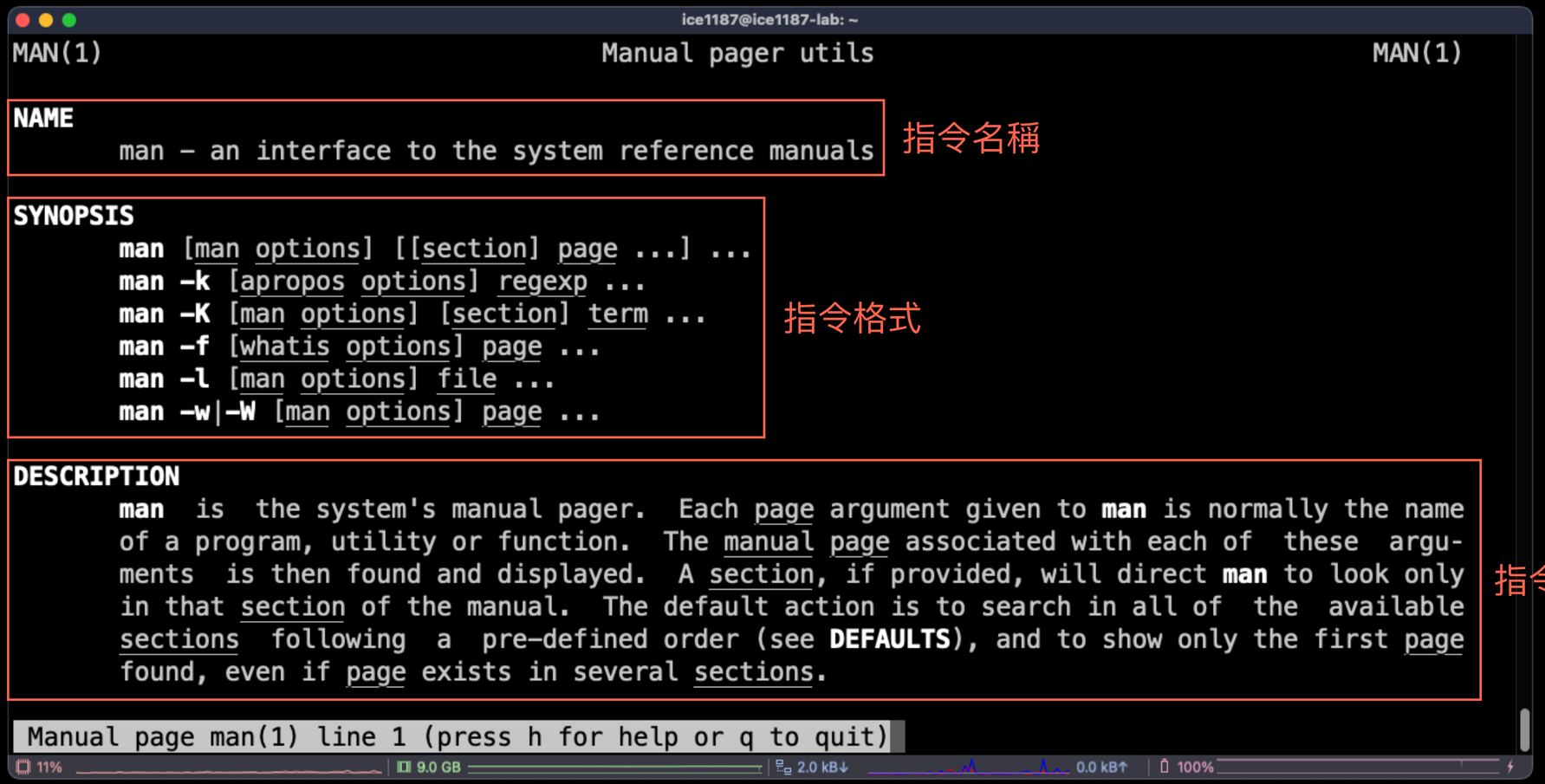
```
ice1187@ice1187-lab:~$ sleep 100
^C
ice1187@ice1187-lab:~$
```

man

- 用途：查看指令或作業系統功能的說明手冊 (**man**ual)
- 上下鍵翻動說明，按 q 退出說明頁面

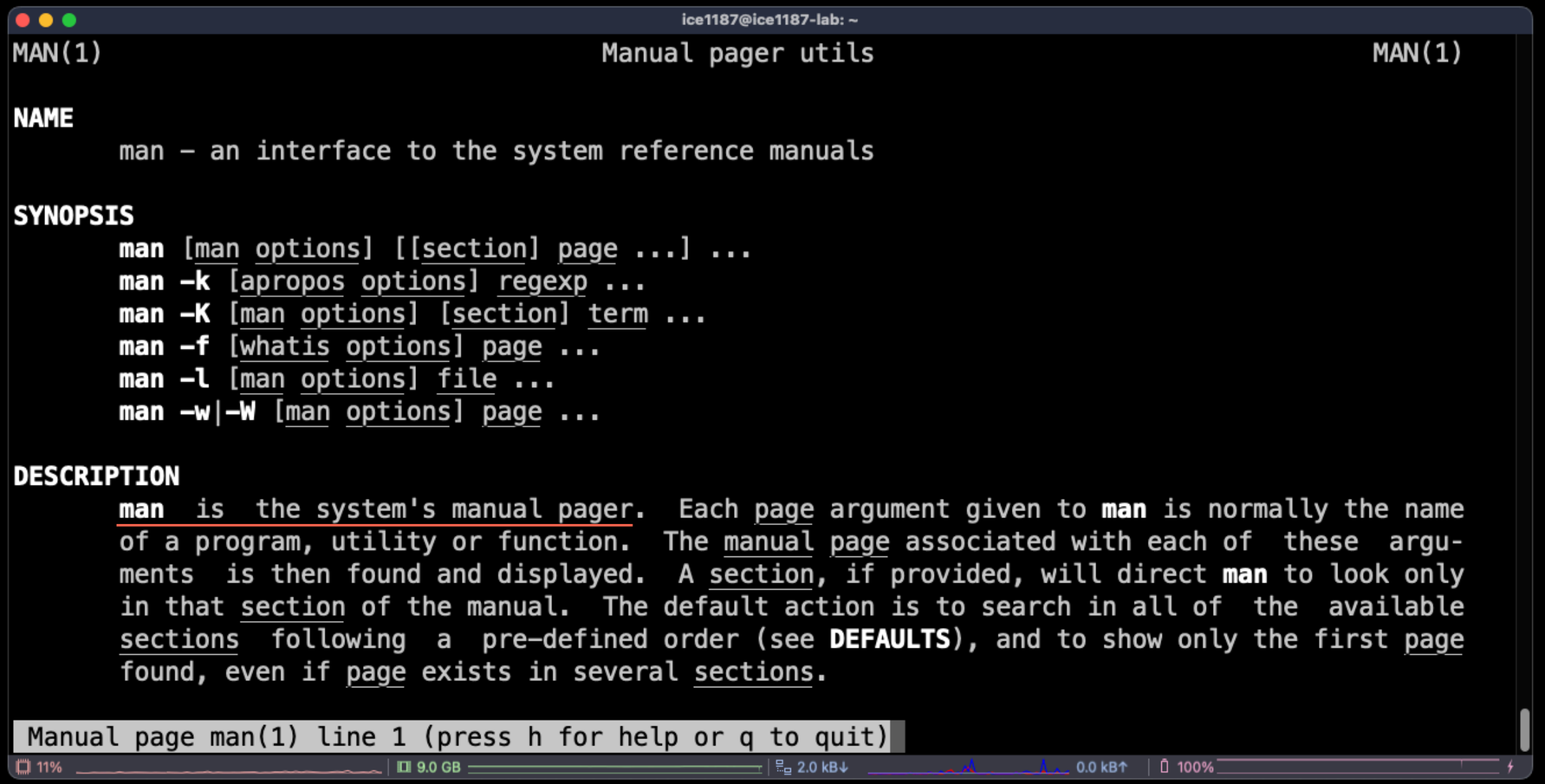
man

- man man


ice1187@ice1187-lab: ~
MAN(1) Manual pager utils MAN(1)
NAME
man - an interface to the system reference manuals
指令名稱
SYNOPSIS
man [man options] [[section] page ...] ...
man -k [apropos options] regexp ...
man -K [man options] [section] term ...
man -f [whatis options] page ...
man -l [man options] file ...
man -w|-W [man options] page ...
指令格式
DESCRIPTION
man is the system's manual pager. Each page argument given to man is normally the name of a program, utility or function. The manual page associated with each of these arguments is then found and displayed. A section, if provided, will direct man to look only in that section of the manual. The default action is to search in all of the available sections following a pre-defined order (see DEFAULTS), and to show only the first page found, even if page exists in several sections.
指令詳細介紹
Manual page man(1) line 1 (press h for help or q to quit)
11% 9.0 GB 2.0 kB↓ 0.0 kB↑ 100%

man

- man man

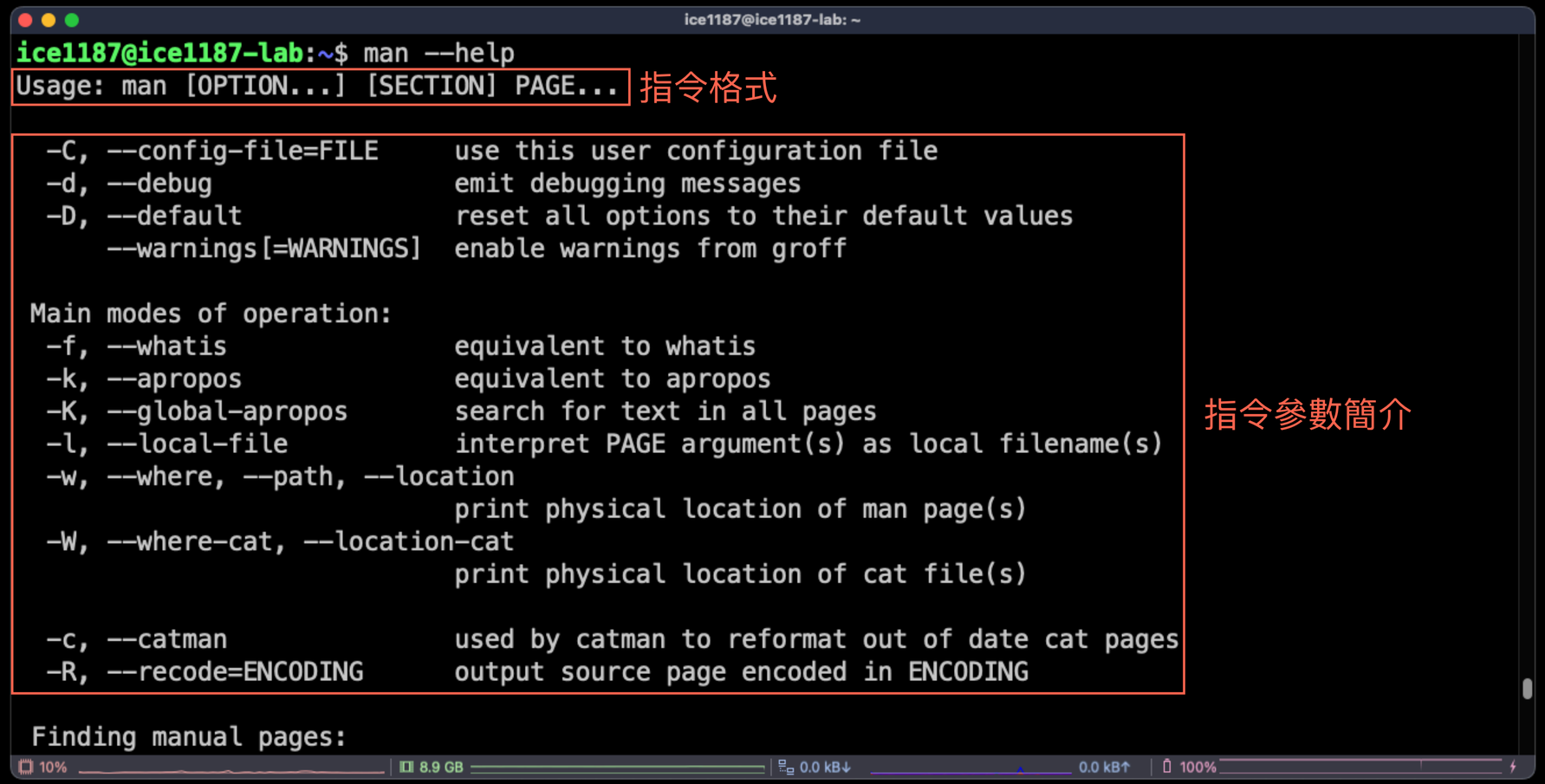

ice1187@ice1187-lab: ~
MAN(1) Manual pager utils MAN(1)
NAME
man - an interface to the system reference manuals
SYNOPSIS
man [man options] [[section] page ...] ...
man -k [apropos options] regexp ...
man -K [man options] [section] term ...
man -f [whatis options] page ...
man -l [man options] file ...
man -w|-W [man options] page ...
DESCRIPTION
man is the system's manual pager. Each page argument given to man is normally the name of a program, utility or function. The manual page associated with each of these arguments is then found and displayed. A section, if provided, will direct man to look only in that section of the manual. The default action is to search in all of the available sections following a pre-defined order (see DEFAULTS), and to show only the first page found, even if page exists in several sections.
Manual page man(1) line 1 (press h for help or q to quit)
11%
9.0 GB
2.0 kB↓
0.0 kB↑
100%

-h, --help

- 用途：印出指令內建的說明資訊
- 非內建指令沒有 man 說明頁面時很好用
- 此為開發慣例，並非所有指令都有 -h 與 --help

man

- man --help


ice1187@ice1187-lab: ~
ice1187@ice1187-lab:~$ man --help
Usage: man [OPTION...] [SECTION] PAGE...
指令格式
-C, --config-file=FILE use this user configuration file
-d, --debug emit debugging messages
-D, --default reset all options to their default values
--warnings[=WARNINGS] enable warnings from groff
Main modes of operation:
-f, --whatis equivalent to whatis
-k, --apropos equivalent to apropos
-K, --global-apropos search for text in all pages
-l, --local-file interpret PAGE argument(s) as local filename(s)
-w, --where, --path, --location
print physical location of man page(s)
-W, --where-cat, --location-cat
print physical location of cat file(s)
-c, --catman used by catman to reformat out of date cat pages
-R, --recode=ENCODING output source page encoded in ENCODING
指令參數簡介
Finding manual pages:
10%
8.9 GB
0.0 kB↓
0.0 kB↑
100%

指令與參數

- 指令：每個指令都是一個具有特定功能的程式 / 可執行檔
  - man 是一個顯示系統說明手冊的程式
  - sleep 是一個暫停執行 n 秒的程式

指令與參數

- 參數：用於提供指令資訊，沒有特定格式
  - man ls
  - man --help
  - ls -al /home/user

指令與參數

```
grep [OPTION...] PATTERNS [FILE...]
grep [OPTION...] -e PATTERNS ... [FILE...]
```

- 指令格式表達的通用寫法：
  - [OPTION…]：此參數可有可無 (optional)
  - [OPTION…]：此參數可有多個
  - PATTERNS：必要參數

Lab — Read the MANual

Read the MANual

100

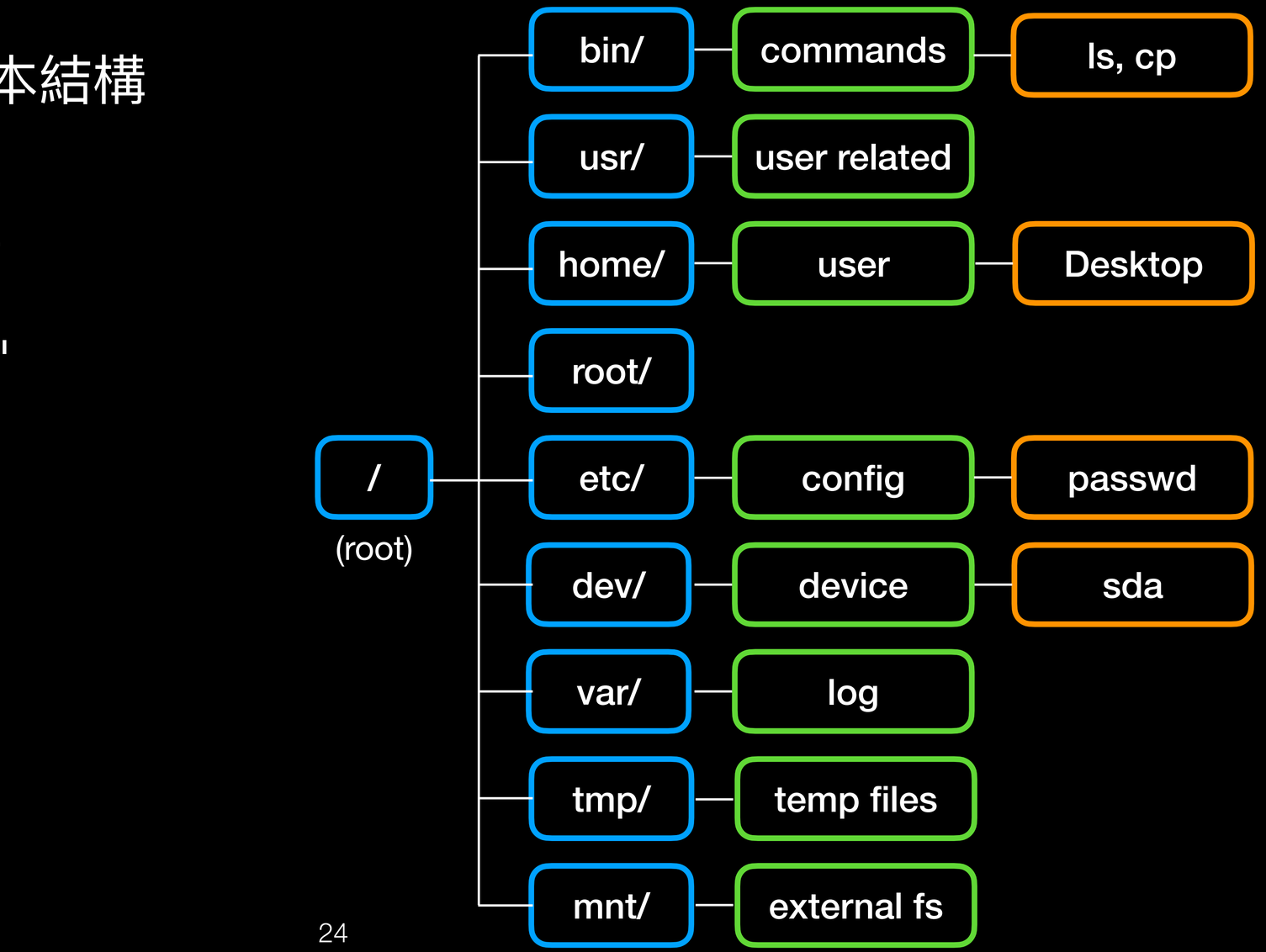
你知道如何查看 Linux 上的 system reference manuals 嗎？請找出 `ls` 指令的 `-a` 參數功能為何。

Flag 格式：`FLAG{descrption of -a option of ls command}`

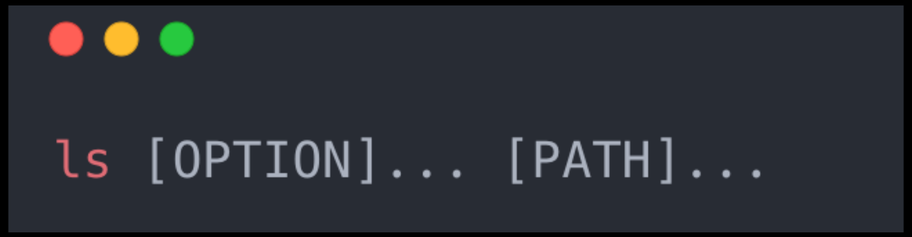
File System 檔案系統

Directory Hierarchy

- Linux 檔案系統的基本結構
- 只是慣例，非強制性
- "Everything is a file."
  - directory
  - device
  - socket
  - …



ls

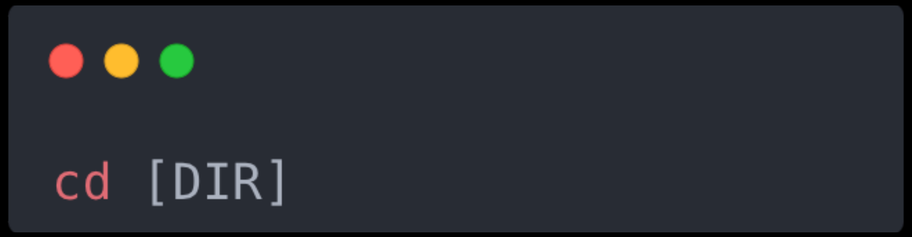


- 用途：列出當前資料夾 / 指定資料夾的檔案
- PATH：用於指定要列出的資料夾，預設為當前資料夾
- OPTION：使用 -al 列出完整資訊（時間、檔案權限、擁有者、隱藏檔案）

ls

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls

┌──(kali㉿kali)-[~/Desktop]
└─$ ls -al
total 8
drwxr-xr-x  2 kali kali 4096 Aug 31 01:44 .
drwxr-xr-x 15 kali kali 4096 Aug 31 02:04 ..
```

cd



- 用途：切換當前資料夾
- DIR：要前往的資料夾，預設為使用者的家目錄
- Tips：使用 - 回到來時的資料夾

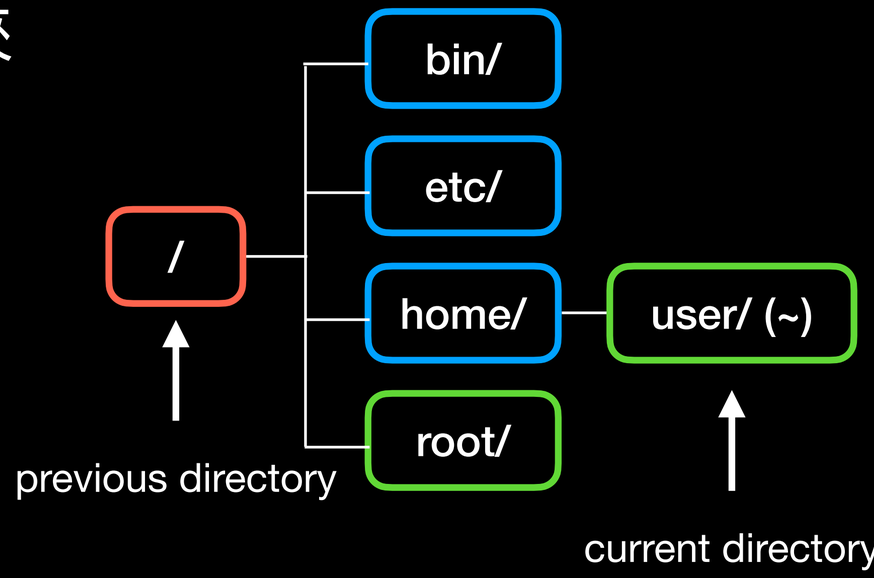
cd

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cd

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ cd -
~
```

. & ..

```
cd .
cd ..
```

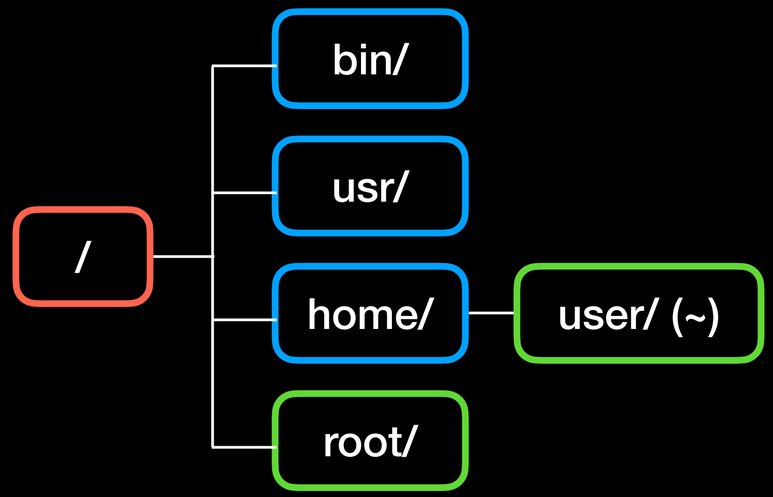
- 用途：. 代表當前資料夾，.. 代表上一層資料夾
  - cd ..
  - ls 相同於 ls .



~ & /

```
cd ~
cd /
```

- 用途：~ 代表使用者的家目錄 (home)；/ 代表根目錄 (root)
  - cd ~
  - ls /
- 名詞：目錄 = 資料夾



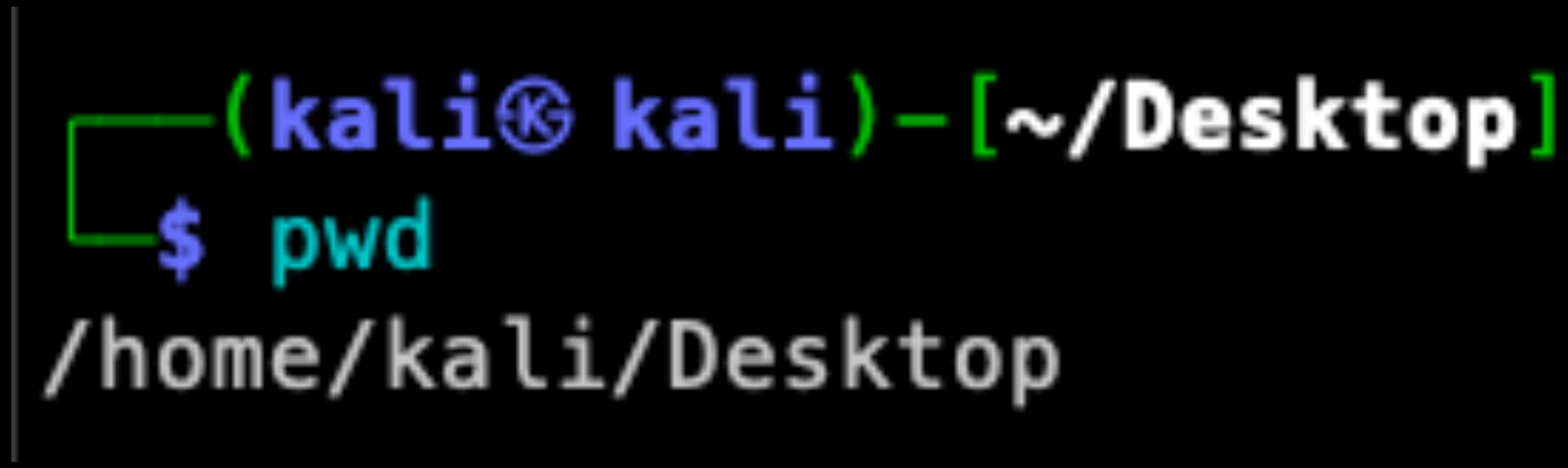
~ & /

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls ~
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l /
total 68
-rw-r--r--   1 root root     0 Aug 31 01:26 0
lrwxrwxrwx   1 root root     7 Aug 31 01:21 bin -> usr/bin
drwxr-xr-x   3 root root  4096 Aug 31 01:41 boot
drwxr-xr-x  17 root root  3200 Aug 31 01:54 dev
drwxr-xr-x 160 root root 12288 Aug 31 01:43 etc
drwxr-xr-x   3 root root  4096 Aug 31 01:41 home
lrwxrwxrwx   1 root root    34 Aug 31 01:21 initrd.img -> boot/initrd.img-
lrwxrwxrwx   1 root root    34 Aug 31 01:21 initrd.img.old -> boot/initrd.
lrwxrwxrwx   1 root root     7 Aug 31 01:21 lib -> usr/lib
lrwxrwxrwx   1 root root     9 Aug 31 01:21 lib32 -> usr/lib32
lrwxrwxrwx   1 root root     9 Aug 31 01:21 lib64 -> usr/lib64
lrwxrwxrwx   1 root root    10 Aug 31 01:21 libx32 -> usr/libx32
drwx------   2 root root 16384 Aug 31 01:21 lost+found
drwxr-xr-x   3 root root  4096 Aug 31 01:21 media
drwxr-xr-x   2 root root  4096 Aug 31 01:21 mnt
drwxr-xr-x   3 root root  4096 Aug 31 01:25 opt
dr-xr-xr-x 184 root root     0 Aug 31 01:43 proc
drwx------   3 root root  4096 Aug 31 01:43 root
drwxr-xr-x  32 root root   840 Aug 31 02:18 run
```

pwd

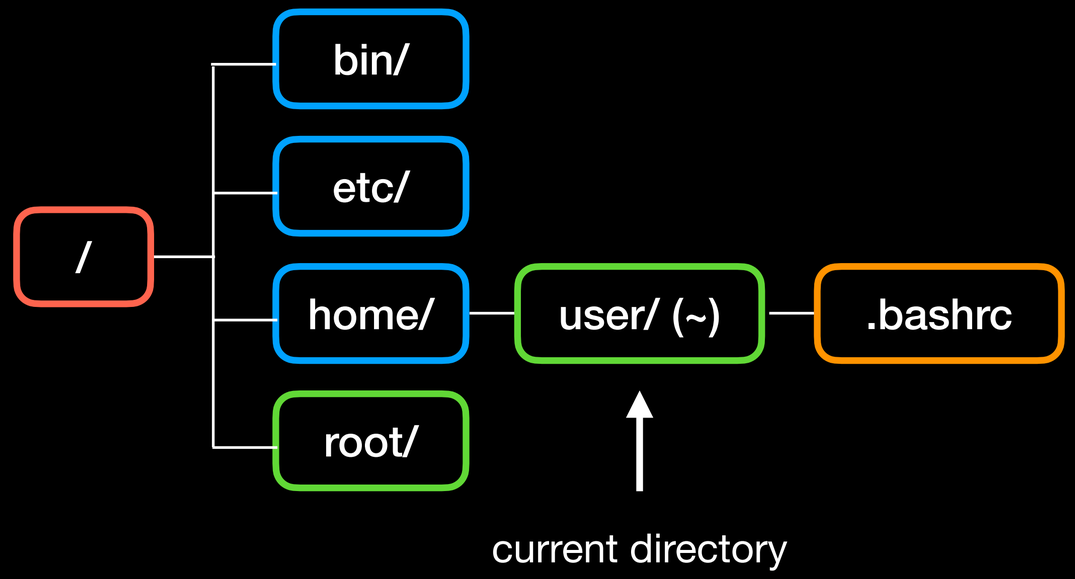
- 用途：顯示當前資料夾的路徑

pwd



相對路徑 v.s. 絕對路徑

- 絕對路徑：從 / 開始指定的路徑，e.g.：/home/user/.bashrc、/etc
- 相對路徑：從當前資料夾開始指定的路徑，e.g.：./.bashrc、../../etc



mkdir

```
mkdir DIR
mkdir -p PATH/TO/CREATE/DIR
```

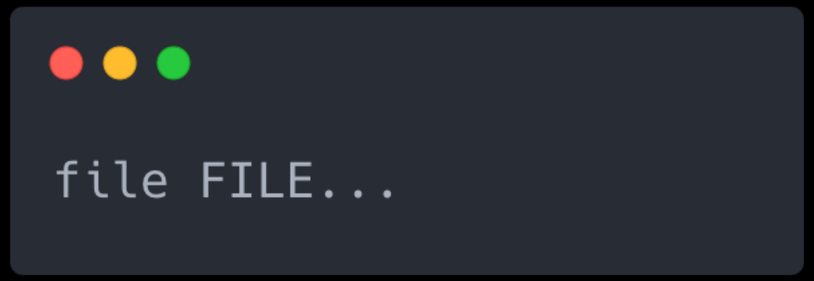
- 用途：建立 DIR 資料夾
- -p：若路徑中的資料夾不存在，則自動建立資料夾
  - 如果 mkdir -p /path/to/create/dir 中的 create/ 不存在，則自動建立 create/

```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  TobeExe  Videos  hello  hello.c

┌──(kali㉿kali)-[~]
└─$ mkdir myDirectory

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  TobeExe  Videos  hello  hello.c  myDirectory
```

Lab

- 練習熟悉一下～

file



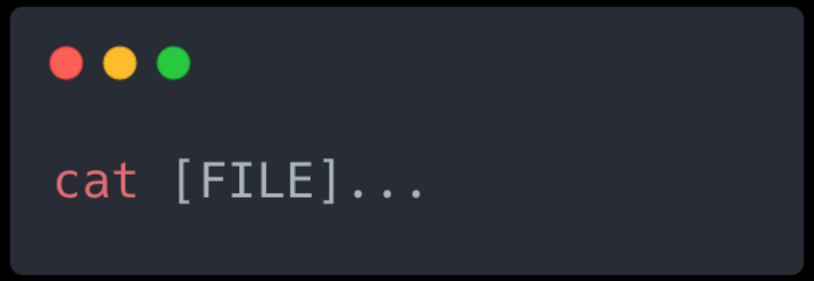
- 用途：顯示 FILE 的檔案格式
- 注意：檔案格式與副檔名 (e.g. document.doc) 無關
- 判斷方式：系統資訊 → magic number → language test

file

```
┌──(kali㉿kali)-[~]
└─$ file Desktop
Desktop: directory

┌──(kali㉿kali)-[~]
└─$ file .bashrc
.bashrc: Unicode text, UTF-8 text

┌──(kali㉿kali)-[~]
└─$ file hello
hello: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked,
2ab9600f2096f833ebb04a985902f6db9, for GNU/Linux 3.2.0, not stripped
```

可執行檔

cat

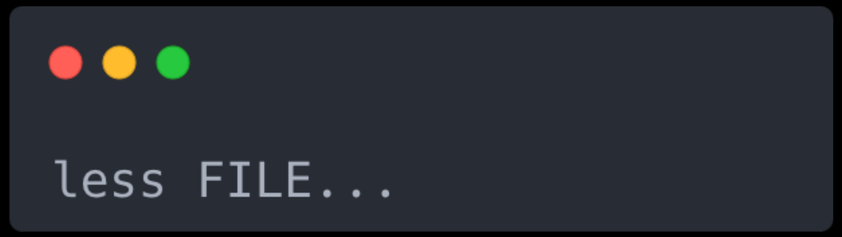


- 用途：顯示檔案內容
- cat .bashrc

cat

```
┌──(kali㉿kali)-[~]
└─$ cat .bashrc
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples

# If not running interactively, don't do anything
case $- in
    *i*) ;;
      *) return;;
esac

# don't put duplicate lines or lines starting with space in the history.
# See bash(1) for more options
HISTCONTROL=ignoreboth
```

less



- 用途：瀏覽檔案內容
- 當前 man 預設的瀏覽工具
- j / k：往下 / 上捲動一行
- f / b：往下 / 上捲動一頁
- /pattern：在檔案中往下搜尋 pattern
- n / shift-n：下 / 上一個搜尋結果
- g：回到檔案開頭
- q：離開

```
LESS(1)                    General Commands Manual                    LESS(1)

NAME
       less - opposite of more

SYNOPSIS
       less -?
       less --help
       less -V
       less --version
       less [-[+]aABcCdeEfFgGiIJKLmMnNqQrRsSuUVwWX~]
            [-b space] [-h lines] [-j line] [-k keyfile]
            [-{oO} logfile] [-p pattern] [-P prompt] [-t tag]
            [-T tagsfile] [-x tab,...] [-y lines] [-[z] lines]
            [-# shift] [+[+]cmd] [--] [filename]...
       (See the OPTIONS section for alternate option syntax with long option names.)

DESCRIPTION
       Less is a program similar to more(1), but it has many more features.  Less does not have to read the
       entire input file before starting, so with large input files it starts up faster than  text  editors
       like  vi(1).   Less uses termcap (or terminfo on some systems), so it can run on a variety of termi-
       nals.  There is even limited support for hardcopy terminals.  (On a hardcopy terminal,  lines  which
       should be printed at the top of the screen are prefixed with a caret.)

       Commands  are  based on both more and vi.  Commands may be preceded by a decimal number, called N in
       the descriptions below.  The number is used by some commands, as indicated.

 Manual page less(1) line 1 (press h for help or q to quit)
```

cp

```
cp [-r] SOURCE DEST
cp SOURCE... DIRECTORY
```

- 用途
  - 複製檔案 SOURCE 為檔案 DEST
  - 複製多個檔案到 DIRECTORY
- -r：複製整個資料夾

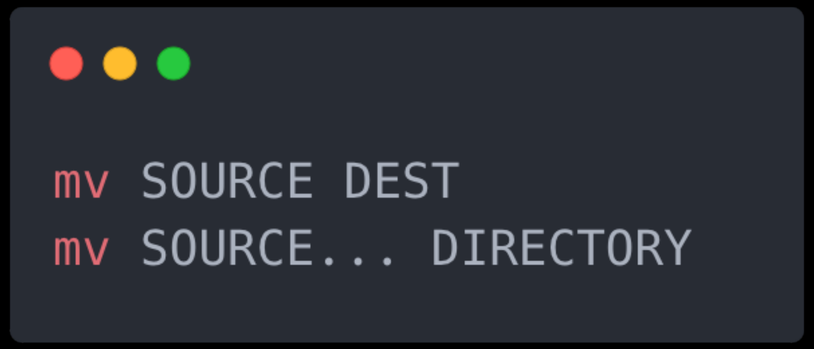
```
┌──(kali㉿kali)-[~/lab]
└─$ ls
a

┌──(kali㉿kali)-[~/lab]
└─$ cat a
This is file 'a'.

┌──(kali㉿kali)-[~/lab]
└─$ cp a b

┌──(kali㉿kali)-[~/lab]
└─$ ls
a  b

┌──(kali㉿kali)-[~/lab]
└─$ cat b
This is file 'a'.
```

Copy file a to file b

```
┌──(kali㉿kali)-[~/lab]
└─$ ls
dir

┌──(kali㉿kali)-[~/lab]
└─$ ls dir
a

┌──(kali㉿kali)-[~/lab]
└─$ cp -r dir dir2

┌──(kali㉿kali)-[~/lab]
└─$ ls
dir  dir2

┌──(kali㉿kali)-[~/lab]
└─$ ls dir2
a
```

Copy directory dir to directory dir2

mv



- 用途：
  - 移動 SOURCE 到 DIRECTORY
  - 將 SOURCE 重新命名為 DEST

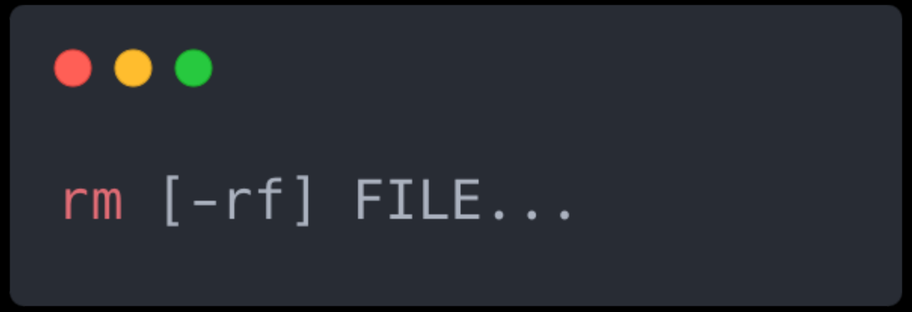
```
┌──(kali㉿kali)-[~/lab]
└─$ ls
a  dir

┌──(kali㉿kali)-[~/lab]
└─$ ls dir

┌──(kali㉿kali)-[~/lab]
└─$ mv a dir/

┌──(kali㉿kali)-[~/lab]
└─$ ls
dir

┌──(kali㉿kali)-[~/lab]
└─$ ls dir
a
```

Move file a into directory dir

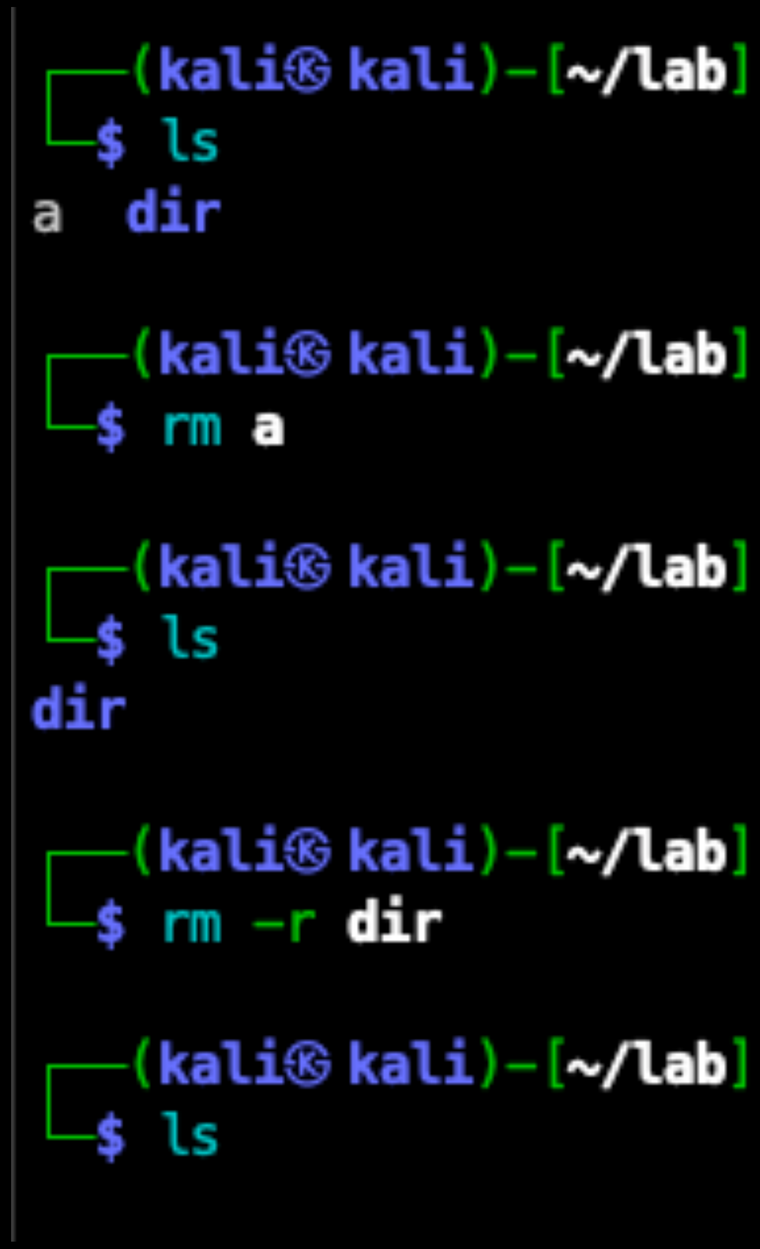
```
┌──(kali㉿kali)-[~/lab]
└─$ ls
a

┌──(kali㉿kali)-[~/lab]
└─$ mv a b

┌──(kali㉿kali)-[~/lab]
└─$ ls
b
```

Rename file a to b

rm

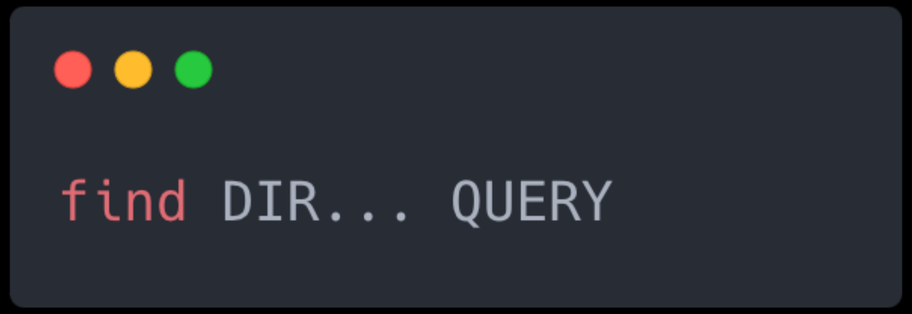


- 用途：刪除檔案 FILE
- -r：遞迴刪除有含內容的資料夾
- -f：無視不存在檔案，不顯示警告直接刪除
- 千萬不要 rm -rf /



Remove file a and directory dir

find



- 用途：在 DIR 資料夾下尋找符合 QUERY 的檔案
- QUERY：
  - -name NAME：檔案名稱
  - -type TYPE：檔案類型
  - 詳細請參考 man find

find

```
┌──(kali㉿kali)-[~]
└─$ find . -name "*rc"
./.dmrc
./.config/xfce4/desktop/icons.screen0-1008x717.rc
./.config/xfce4/desktop/icons.screen.latest.rc
./.config/xfce4/panel/cpugraph-13.rc
./.config/xfce4/panel/genmon-15.rc
./.zshrc
./.bashrc
```

grep

```
grep [-v] PATTERNS FILE...
grep -e PATTERNS FILE...
grep -E PATTERNS FILE...
```

- 用途：印出檔案 FILE 中符合 PATTERNS 的行
- -v：反向匹配，列出不符合 PATTERNS 的行
- -e：使用多次可指定多個可能的 PATTERNS，或是處理開頭為 - 的情況
- -E：將 PATTERNS 視為 extended regex

```
┌──(kali㉿kali)-[~]
└─$ cat text
3742
-3742
1234
1423

┌──(kali㉿kali)-[~]
└─$ grep 3742 text
3742
-3742

┌──(kali㉿kali)-[~]
└─$ grep -v 3742 text
1234
1423

┌──(kali㉿kali)-[~]
└─$ grep -e - text
-3742

┌──(kali㉿kali)-[~]
└─$ grep -e 37 -e 42 text
3742
-3742
1423

┌──(kali㉿kali)-[~]
└─$ grep -E "37|42" text
3742
-3742
1423
```

Lab — Grab the flag

- 下載檔案

1. 右鍵 grab_the_flag 複製檔案連結

2. 輸入 wget "檔案連結"

```
┌──(kali㉿kali)-[~]
└─$ wget http://210.70.138.222/files/b38d2dbd7d2954f8ba4bec9a44da8e0c/grab_the_flag
--2023-09-14 15:15:31--  http://210.70.138.222/files/b38d2dbd7d2954f8ba4bec9a44da8e0c/grab_the_flag
Connecting to 210.70.138.222:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2800028 (2.7M) [application/octet-stream]
Saving to: 'grab_the_flag'

grab_the_flag                                100%[=============================================

2023-09-14 15:15:31 (9.77 MB/s) - 'grab_the_flag' saved [2800028/2800028]
```

Lab — Grab the flag

Grab the flag

100

你知道如何使用 `grep` 指令嗎？請從檔案 `grab_the_flag` 中找出開頭為 `???` 且結尾為 `!!!` 的 flag。

Flag 格式：`FLAG{???_something_in_between_!!!}`

grab_the_flag

User & Group 使用者與群組

User 使用者

- 除了用戶是使用者，許多服務也會建立服務專屬的使用者
- 使用者擁有家目錄、群組等
- 使用者列表位於 /etc/passwd

```
┌──(kali㉿kali)-[~]
└─$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
```

whoami

```
whoami
```

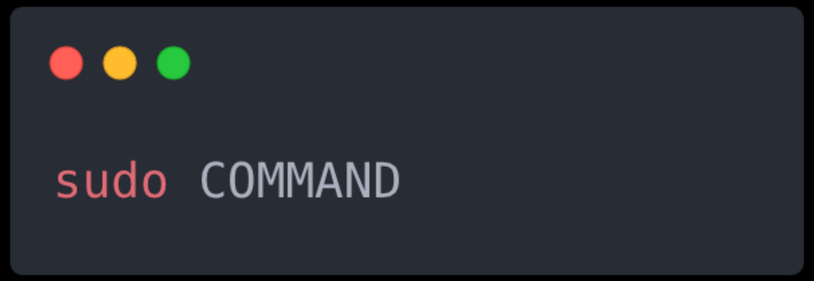
- 用途：顯示使用者名稱

```
┌──(kali㉿kali)-[~]
└─$ whoami
kali
```

Root

- root 是最高權限使用者
- 所有系統操作皆需要 root 授權
  - 安裝程式
  - 開啟、關閉系統服務
  - 修改系統設定
- 雖然很方便，但大多數情況下不應該直接用 root 身份進行操作

sudo



- 用途：使用 root 權限執行指令 COMMAND
- 需輸入當前使用者的密碼
- 使用者須具有 root 權限才能使用 sudo，設定檔位於 /etc/sudoers

sudo

```
┌──(kali㉿kali)-[~]
└─$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied

┌──(kali㉿kali)-[~]
└─$ sudo cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
```

su

- 用途：切換至使用者 USER
- 需輸入該使用者的密碼

su

```
┌──(kali㉿kali)-[~]
└─$ whoami
kali

┌──(kali㉿kali)-[~]
└─$ sudo su root
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# whoami
root
```

Group 群組

- 每個使用者有自己獨立的群組
- 每個使用者可加入多個群組
- 用於管理權限，如：sudoers
- 群組列表位於 /etc/group

```
┌──(kali㉿kali)-[~]
└─$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:kali
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
```

groups

- 用途：查看使用者所屬群組

```
┌──(kali㉿kali)-[~]
└─$ groups
kali adm dialout cdrom floppy sudo audio dip video plugdev netdev wireshark bluetooth scanner kaboxer
```

id

- 用途：查看使用者的名稱、UID 和所屬群組

```
┌──(kali㉿kali)-[~]
└─$ id
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),
44(video),46(plugdev),109(netdev),119(wireshark),121(bluetooth),137(scanner),141(kaboxer)
```

Lab — What can Super User DO

What can SUper DO

100

你知道遇到 Permission denied 的時候是出了什麼問題嗎？請找出檔案 `/etc/shadow` 的第一行內容為何。

Flag 格式： `FLAG{first line of /etc/shadow}`

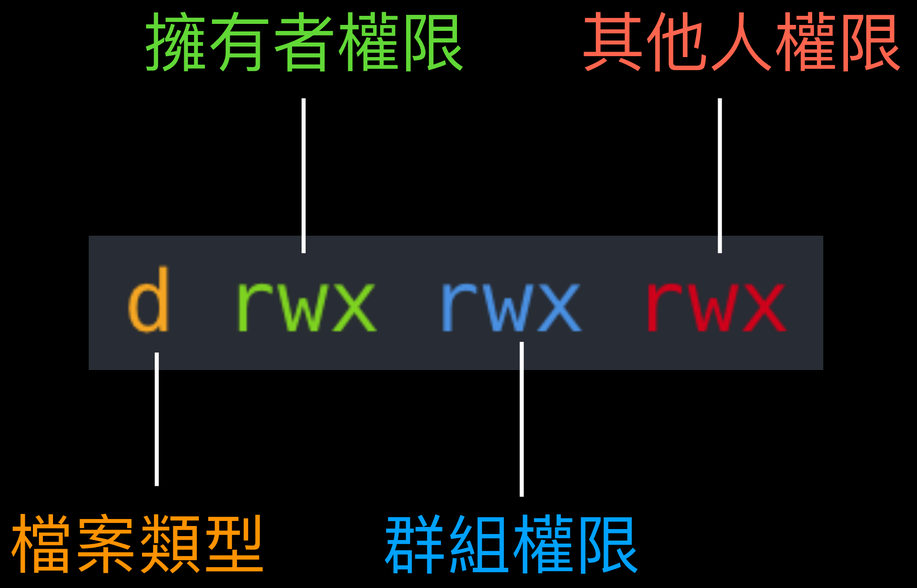
File Permission 檔案權限

```
┌──(kali㉿kali)-[~]
└─$ ls -al
total 132
drwxr-xr-x 15 kali kali  4096 Aug 31 05:41 .
drwxr-xr-x  3 root root  4096 Aug 31 01:41 ..
-rw-------  1 kali kali     0 Aug 31 01:44 .ICEauthority
-rw-------  1 kali kali    49 Aug 31 01:44 .Xauthority
-rw-r--r--  1 kali kali   220 Aug 31 01:41 .bash_logout
-rw-r--r--  1 kali kali  5551 Aug 31 01:41 .bashrc
-rw-r--r--  1 kali kali  3526 Aug 31 01:41 .bashrc.original
drwxr-xr-x  5 kali kali  4096 Aug 31 02:04 .cache
drwxr-xr-x 12 kali kali  4096 Aug 31 02:04 .config
-rw-r--r--  1 kali kali    35 Aug 31 02:03 .dmrc
-rw-r--r--  1 kali kali 11759 Aug 31 01:41 .face
lrwxrwxrwx  1 kali kali     5 Aug 31 01:41 .face.icon -> .face
drwx------  3 kali kali  4096 Aug 31 01:44 .gnupg
drwxr-xr-x  3 kali kali  4096 Aug 31 01:41 .java
```

檔案權限　檔案擁有者　檔案所屬群組

File Permission 檔案權限

- 檔案類型
  - -：一般檔案
  - d：目錄
  - l：連結檔



- 權限
  - r： readable 可讀
  - w：writeable 可寫
  - x：executable 可執行

File Permission 檔案權限

```
-rw-r--r-- 1 ice1187 ice1187  184 Aug 29 11:51 hello.c
-rwxr-xr-x 1 ice1187 ice1187  17K Aug 29 11:51 hello
```

- 擁有者 ice1187：可讀 / 可寫 / 可執行
- 屬於 ice1187 群組的使用者：可讀 / 可執行
- 其他使用者：可讀 / 可執行
- 不同檔案格式，其預設的權限不同：
  - hello.c 原始碼不可執行；hello 執行檔可執行

chmod

```
chmod MODE FILE...
```

- 用途：改變檔案 FILE 的檔案權限為 MODE
- MODE
  - 用數字表示：r / w / x = 4 / 2 / 1
    - rwxr-x-r-x = 755
    - rwxrw-r-- = 764
  - 用 +- 增減權限：
    - 使用 +r / +w / +x 增加權限
    - 使用 -r / -w / -x 刪除權限

```
ice1187@ice1187-lab:/tmp$
ice1187@ice1187-lab:/tmp$ ls hello
-rwxr-xr-x 1 ice1187 ice1187 17K Aug 31 20:05 hello
ice1187@ice1187-lab:/tmp$ chmod 764 hello
ice1187@ice1187-lab:/tmp$ ls hello
-rwxrw-r-- 1 ice1187 ice1187 17K Aug 31 20:05 hello
```

Change file permission from rwxr-xr-x (755) to rwxrw-r-- (764)

```
ice1187@ice1187-lab:/tmp$ wget 127.0.0.1:8000/hello
--2023-08-31 20:06:03--  http://127.0.0.1:8000/hello
Connecting to 127.0.0.1:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16744 (16K) [application/octet-stream]
Saving to: ‘hello’

hello                   100%[============================>]  16.35K  --.-KB/s    in 0s

2023-08-31 20:06:03 (184 MB/s) - ‘hello’ saved [16744/16744]

ice1187@ice1187-lab:/tmp$ ls hello
-rw-r--r-- 1 ice1187 ice1187 17K Aug 31 20:05 hello
ice1187@ice1187-lab:/tmp$ chmod +x hello
ice1187@ice1187-lab:/tmp$ ls hello
-rwxr-xr-x 1 ice1187 ice1187 17K Aug 31 20:05 hello
```

Add executable permission (+x) to downloaded file

Lab — Give me flag

Give me flag

100

你知道如何執行一個下載來的檔案嗎？

Flag 格式：`FLAG{...}`

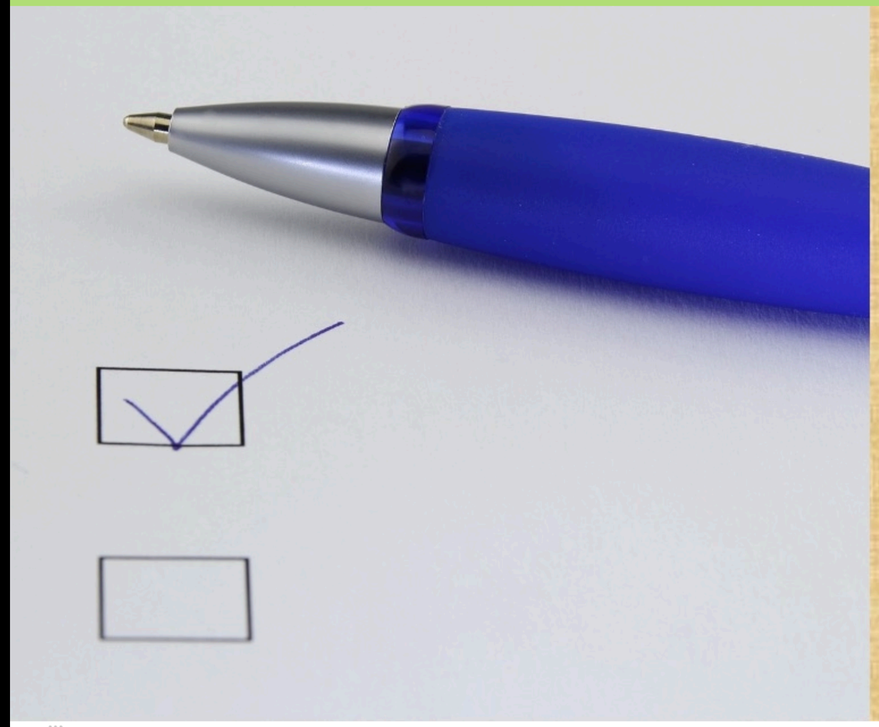
give_me_flag

Network 網路

國立台南一中 臺南第一高級中學
TAINAN FIRST SENIOR HIGH SCHOOL

::: 網站導覽 / 相關連結 / English / AA /

最新消息 | 學生專區 | 行政處室 | 專案計劃 | 教職專區 | 公開資訊 | 關於本校



111學年度
學習歷程檔案勾選
112年9月14日截止

學生訊息 | 教職員訊息 | 升學資訊 | 考試資訊

社團活動組	置頂	公告：9/14(四)–9/18(一)高一轉社辦理事宜	2023–09–14
生活輔導組	置頂	112年國家防災日地震避難掩護演練注意事項	2023–09–13

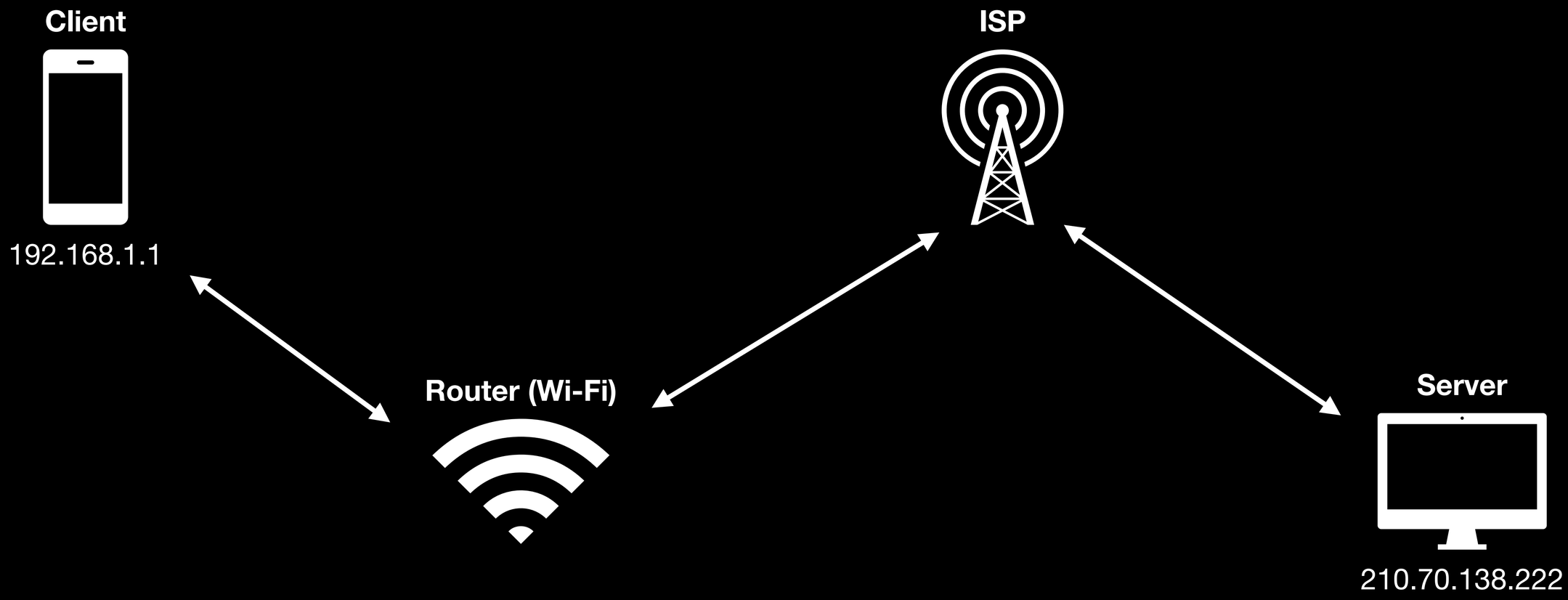
https://www.tnfsh.tn.edu.tw/

How Internet Works — IP

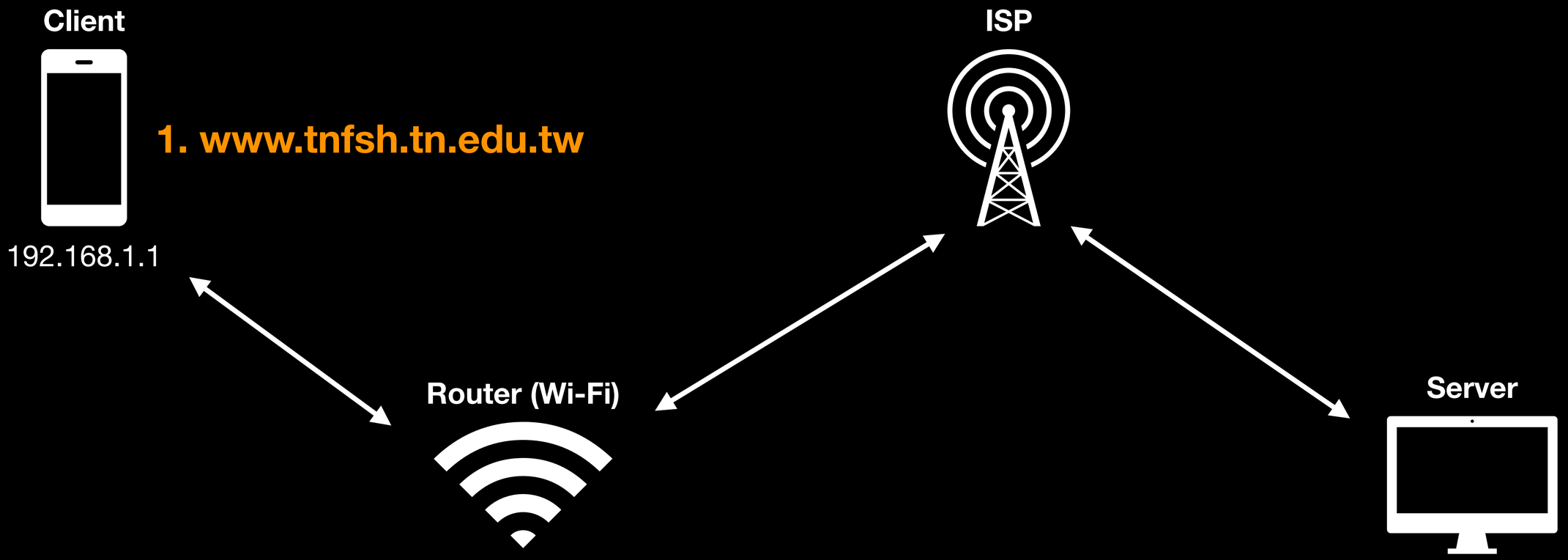
https://www.tnfsh.tn.edu.tw/index.html

https://www.tnfsh.tn.edu.tw:443/index.html

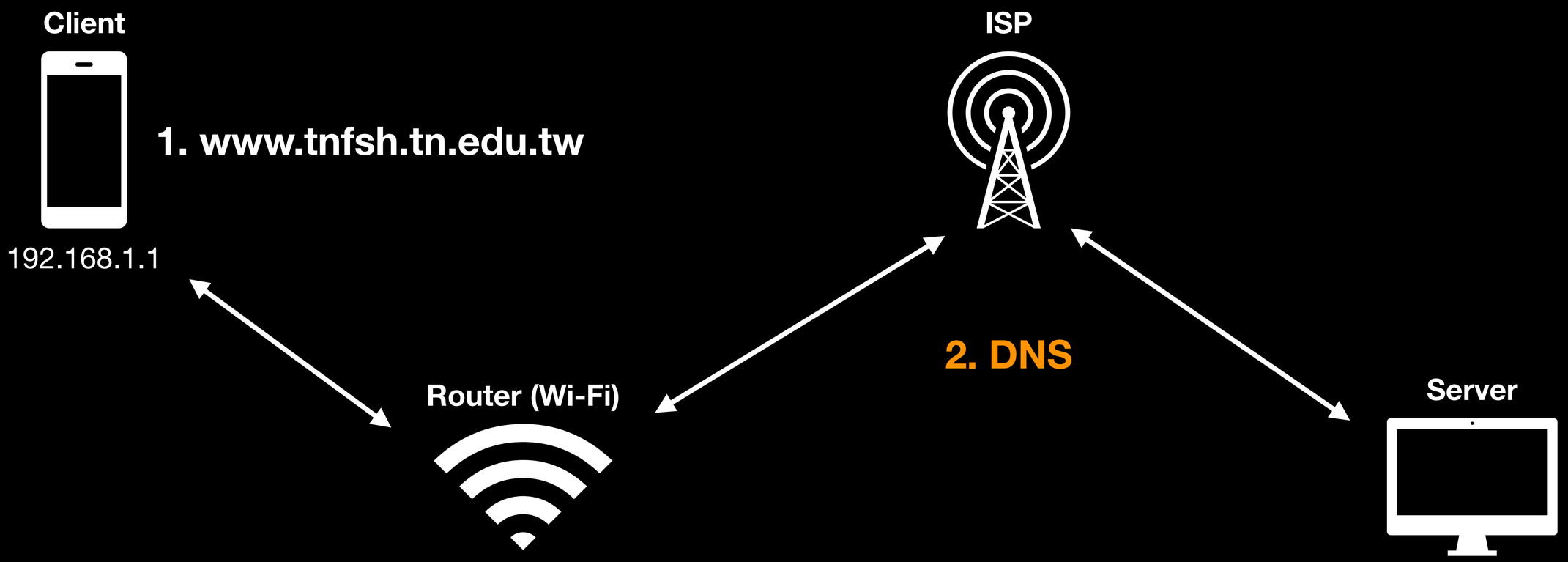
How Internet Works — IP



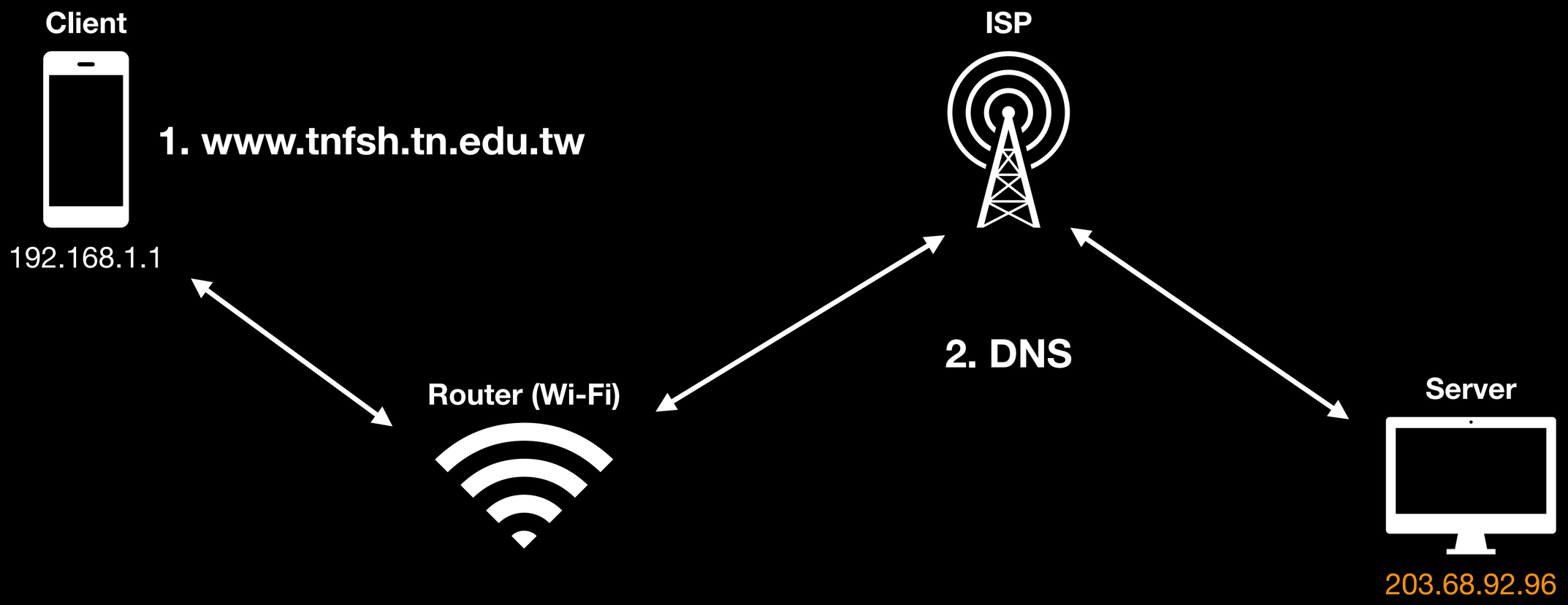
How Internet Works — IP



How Internet Works — IP



How Internet Works — IP



How Internet Works — Port

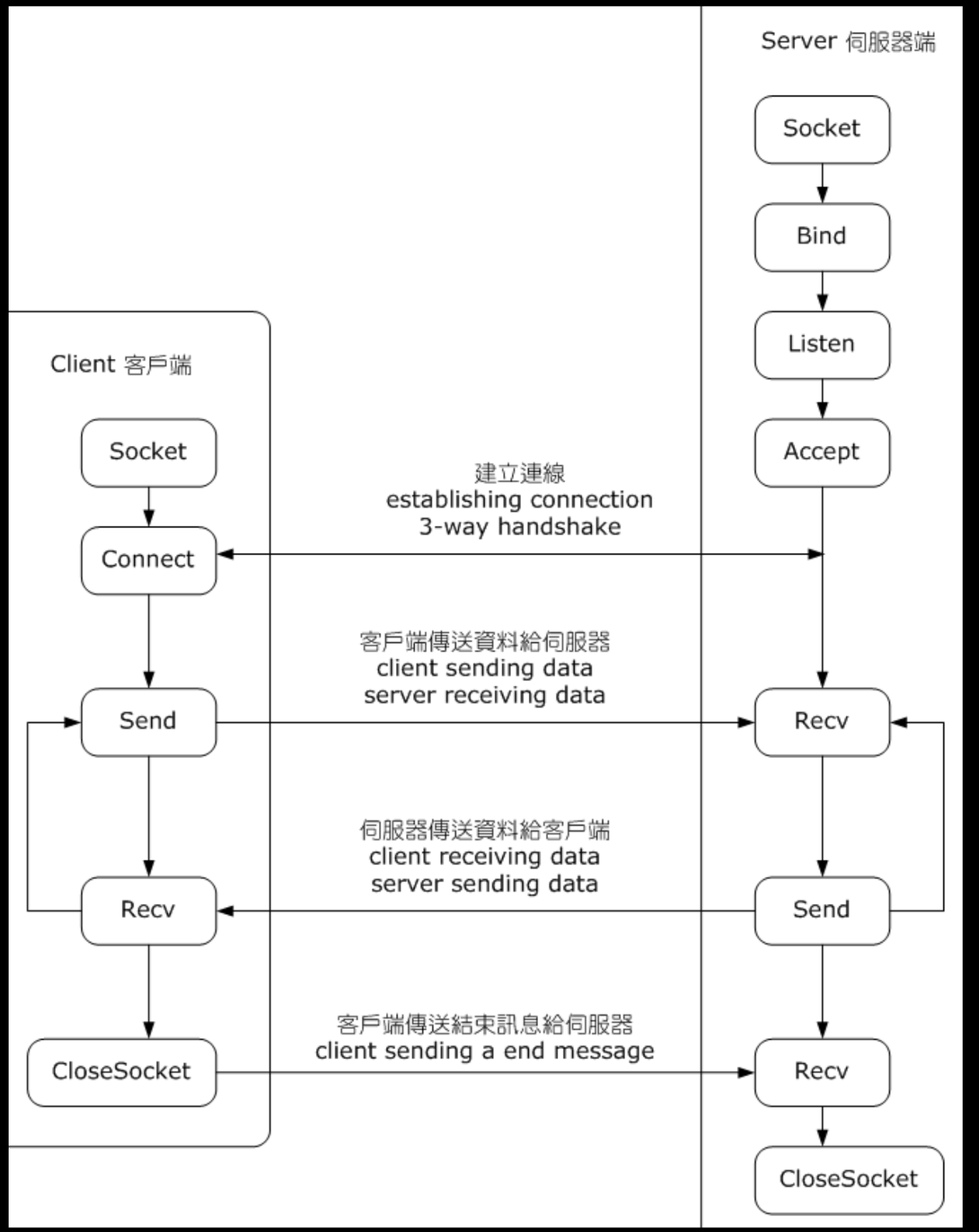
https://www.tnfsh.tn.edu.tw/index.html

https://www.tnfsh.tn.edu.tw:443/index.html

https://203.68.92.96:443/index.html

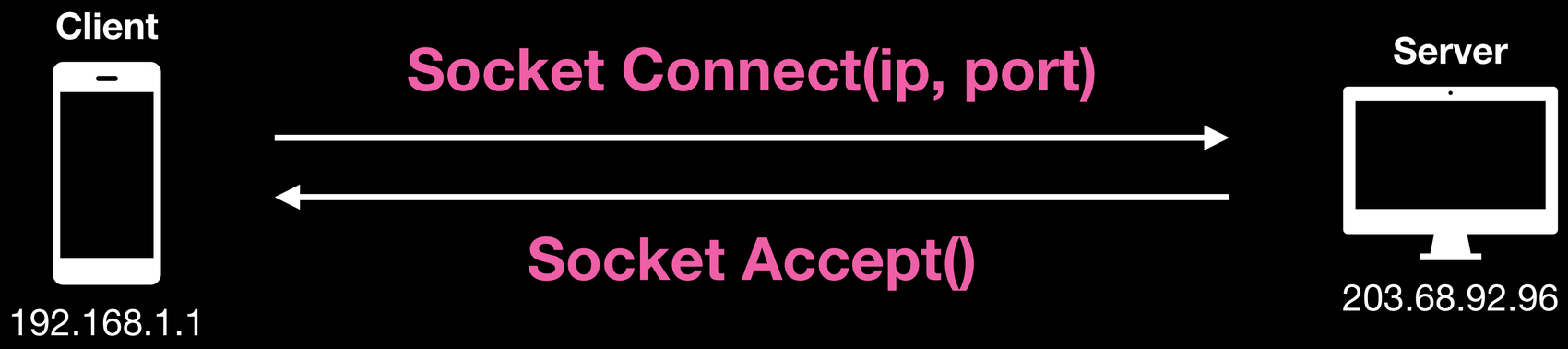
Socket & TCP

- Client
  - Connect：嘗試建立連線
  - Send/Recv：傳送/接收資料
- Server
  - Bind：綁定 ip
  - Listen：監聽 port
  - Accept：接受建立連線

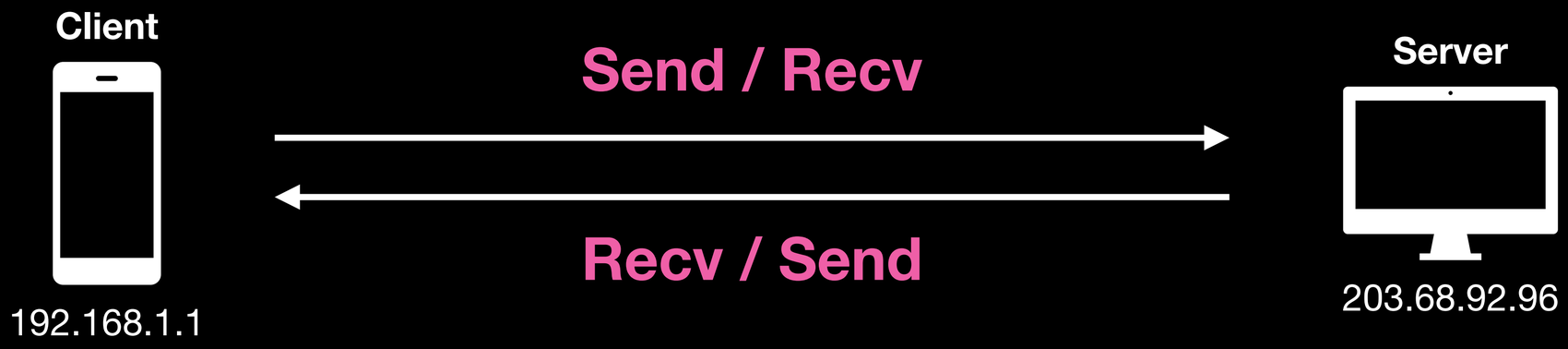


Img src: https://en.wikipedia.org/wiki/Berkeley_sockets

How Internet Works — Port



How Internet Works — Port



How Internet Works — Port

```
┌──(kali㉿kali)-[~]
└─$ nc 127.0.0.1 11187
AAAAAAABBBBBBBB
Hello, World!
1234567890
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 11187
listening on [any] 11187 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 49298
AAAAAAABBBBBBBB
Hello, World!
1234567890
```

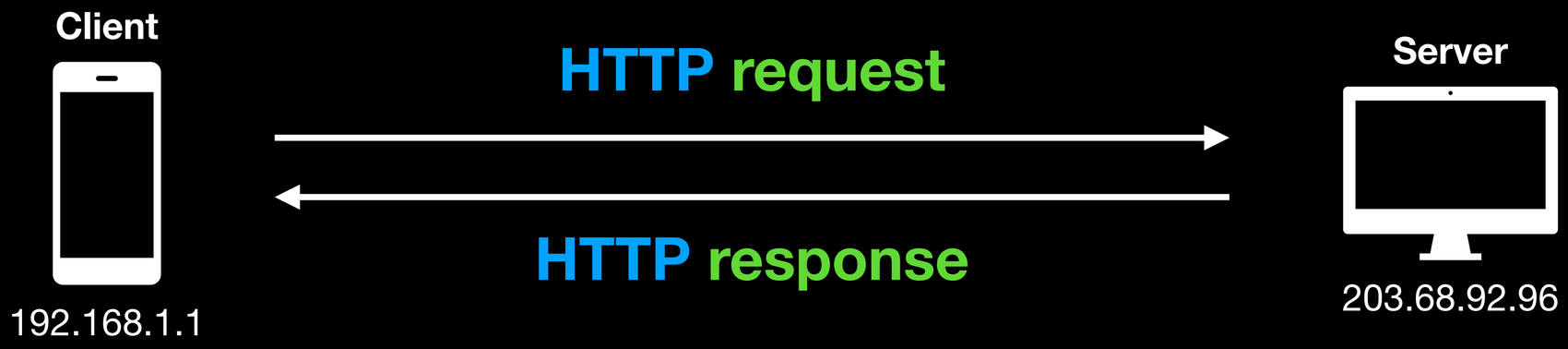
How Internet Works — Content

https://www.tnfsh.tn.edu.tw/index.html

https://www.tnfsh.tn.edu.tw:443/index.html

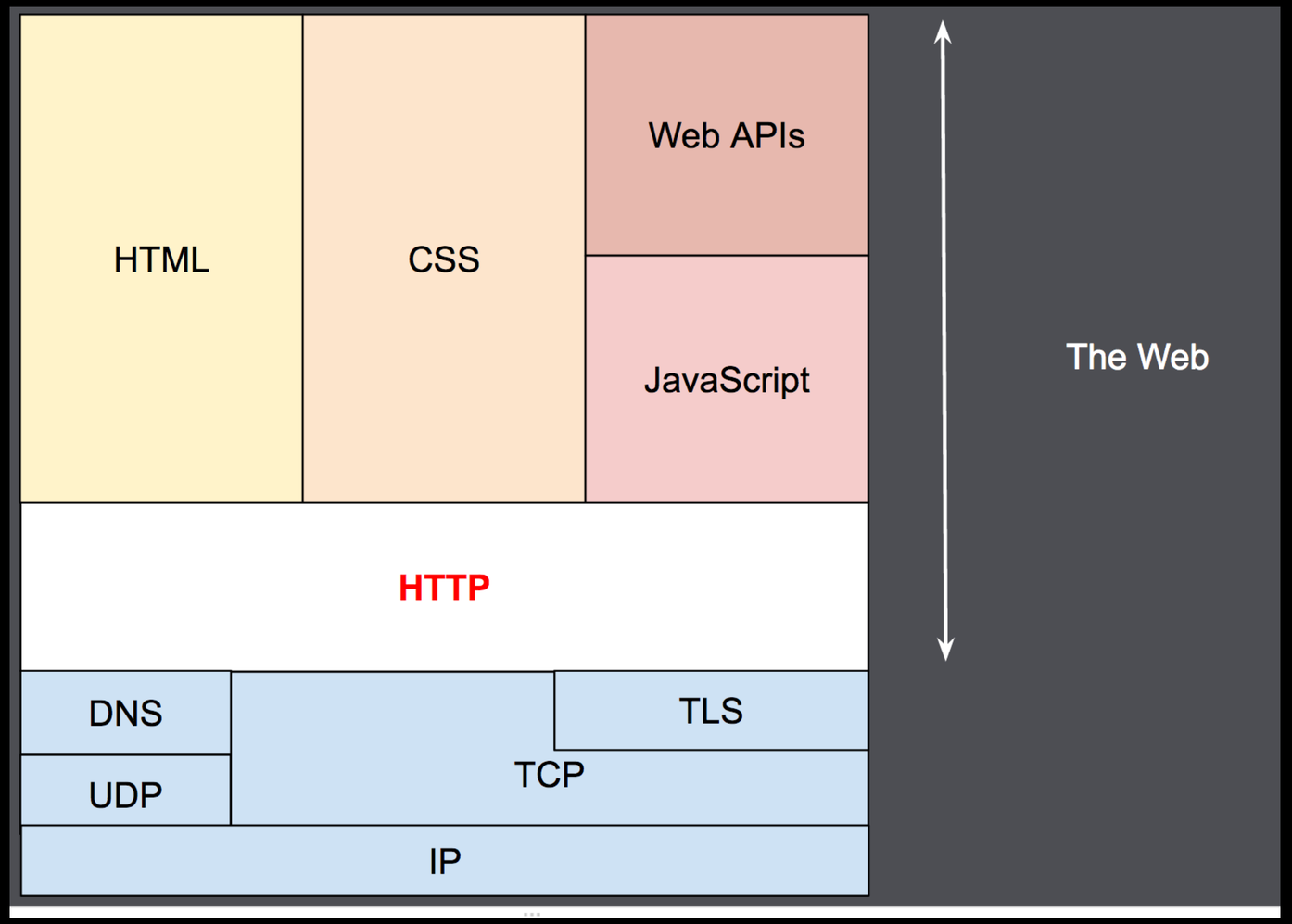
https://203.68.92.96:443/index.html

How Internet Works — Content



HTTP

- 一種網路傳輸協定 (protocol)



Img Src: https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview

HTTP Request / Response

```
GET / HTTP/1.1
Host: developer.mozilla.org
Accept-Language: fr
```

```
HTTP/1.1 200 OK
Date: Sat, 09 Oct 2010 14:28:02 GMT
Server: Apache
Last-Modified: Tue, 01 Dec 2009 20:18:22 GMT
ETag: "51142bc1-7449-479b075b2891b"
Accept-Ranges: bytes
Content-Length: 29769
Content-Type: text/html

<!DOCTYPE html>… (here come the 29769 bytes of the requested web page)
```

Img Src: MDN — An overview of HTTP

ip

- 用途：顯示網卡 address、設定網卡
- CTF 應用：基礎網路管理功能
- ip Command Cheat Sheet by Red Hat

```
┌──(kali㉿kali)-[~]
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether be:ba:f6:f2:eb:0e brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.54/24 brd 192.168.10.255 scope global dynamic noprefixroute eth0
       valid_lft 4142sec preferred_lft 4142sec
    inet6 fe80::bcba:f6ff:fef2:eb0e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

netstat

- 用途：查看 listen port 與運行 process / program
- 查看運行 process / program 需要 sudo
- CTF 應用：基礎網路管理功能、查看網路服務

```
┌──(kali㉿kali)-[~]
└─$ netstat -alnp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:12345           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8000            0.0.0.0:*               LISTEN      321725/python3
tcp        0      0 0.0.0.0:11187           0.0.0.0:*               LISTEN      321825/nc
tcp        0    932 192.168.10.54:22        192.168.2.2:55982       ESTABLISHED -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 192.168.10.54:68        192.168.10.254:67       ESTABLISHED -
raw6       0      0 :::58                   :::*                    7           -
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name     Path
unix  2      [ ACC ]     STREAM     LISTENING     12665    -                    /run/systemd/userdb/io.systemd.DynamicUser
unix  2      [ ACC ]     STREAM     LISTENING     12666    -                    /run/systemd/io.system.ManagedOOM
unix  2      [ ]         DGRAM                    12677    -                    /run/systemd/journal/syslog
unix  2      [ ACC ]     STREAM     LISTENING     12679    -                    /run/systemd/fsck.progress
unix  17     [ ]         DGRAM      CONNECTED     12683    -                    /run/systemd/journal/dev-log
```

curl

```
curl --user user:pswd URL
curl  [--cookie COOKIE] --data DATA URL
curl -X POST -H HEADER URL
```

- 用途：對 HTTP(S) 網站發 request
- 功能多元，詳見 man curl
- CTF 應用：Request 網頁內容、自動化腳本

```
┌──(kali㉿kali)-[~]
└─$ curl https://www.tnfsh.tn.edu.tw/

<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" lang="zh-tw">

<head>

    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <meta name="format-detection" content="telephone=no" />
    <title>臺南第一高級中學</title>

    <link href="css/bootstrap.css" rel="stylesheet" type="text/css" />
    <link rel="stylesheet" href="Content/df_js/OwlCarousel/owl.carousel.css" />
    <link rel="stylesheet" href="Content/df_js/OwlCarousel/owl.theme.default.css" />
    <link rel="stylesheet" href="css/font-awesome.css" />
    <link href="css/in_style.css" rel="stylesheet" type="text/css" />
    <link href="css/in_rwd.css" rel="stylesheet" type="text/css" />
    <link href="css/font-awesome.css" rel="stylesheet" />
    <link rel="shortcut icon" href="favicon.ico" />
    <link rel="icon" href="images/favicon.ico" type="image/x-icon" />
    <link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />
    <meta property="og:site_name"      content="臺南第一高級中學" />
<meta property="og:image"          content="https://www.tnfsh.tn.edu.tw/images/og.jpg" />
<meta property="og:title"          content="(臺南第一高級中學)" />
<meta property="og:description"      content="臺南第一高級中學" />
```

wget

```
wget [--continue, --header HEADER] URL
```

- 用途：從 HTTP(S) 網站下載檔案
- 有許多參數，詳見 man wget
- CTF 應用：下載 CTF 題目、下載檔案

```
┌──(kali㉿kali)-[~]
└─$ wget http://120.114.62.217/TobeExe
--2023-09-01 00:06:03--  http://120.114.62.217/TobeExe
Connecting to 120.114.62.217:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7348 (7.2K)
Saving to: 'TobeExe'

TobeExe                                    100%[=============================>

2023-09-01 00:06:03 (1.42 GB/s) - 'TobeExe' saved [7348/7348]


┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  TobeExe
```

nc

```
nc HOST PORT
nc -lvnp [-k] [-e PROGRAM] PORT
```

- 用途： 對 TCP/UDP port 進行網路連線
- -k：持續保持 listen
- CTF 應用：與 pwn 題目互動、於 local 架設題目、彈 reverse shell
- 注意：nc 有兩個版本，其中一個沒有 -e，需要安裝 netcat 或 ncat 指令

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 11187
listening on [any] 11187 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 45698
0. Hello
1. Say Hi~~~~
```

```
┌──(kali㉿kali)-[~]
└─$ nc 127.0.0.1 11187
0. Hello
1. Say Hi~~~~
```

```
┌──(kali㉿kali)-[~]
└─$ nc -e ./hello -klvnp 11187
listening on [any] 11187 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 44172
```

```
┌──(kali㉿kali)-[~]
└─$ nc 127.0.0.1 11187
100
Hello, World!
Input is 100
```

Python HTTP Server

```
python3 -m http.server [PORT]
```

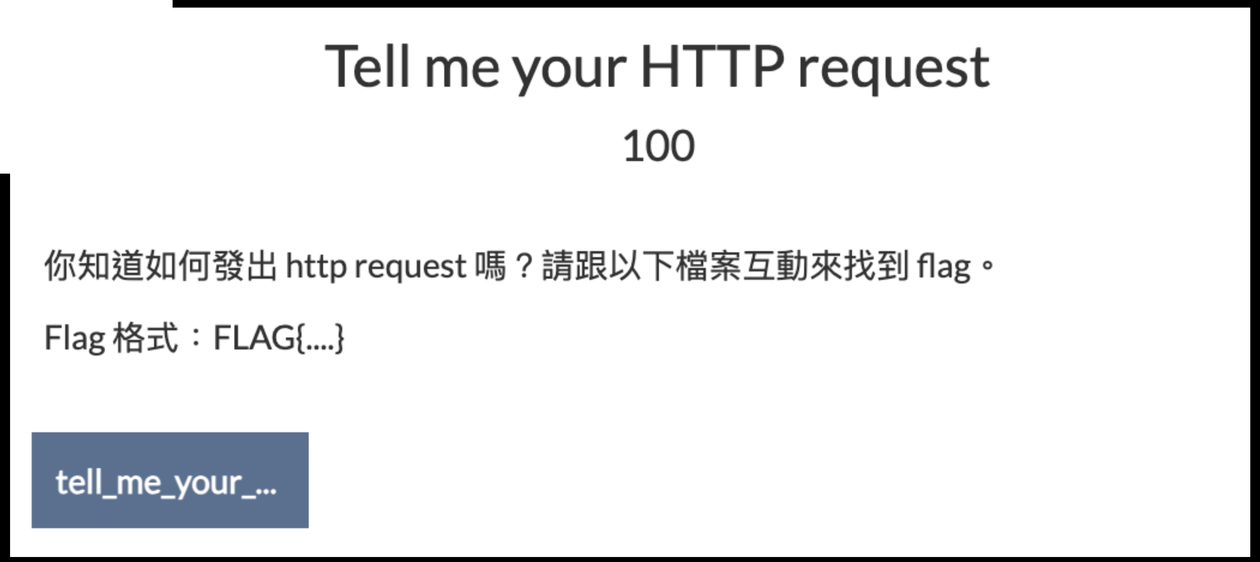
- 用途：架設臨時的 HTTP server
- PORT：指定 listen port，預設為 8000
- CTF 應用：接收 request、傳檔案 (？

```
┌──(kali㉿kali)-[~]
└─$ python3 -m http.server 11187
Serving HTTP on 0.0.0.0 port 11187 (http://0.0.0.0:11187/) ...
127.0.0.1 - - [01/Sep/2023 02:13:12] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [01/Sep/2023 02:13:49] code 404, message File not found
127.0.0.1 - - [01/Sep/2023 02:13:49] "GET /from_nc HTTP/1.1" 404 -
```

```
┌──(kali㉿kali)-[~]
└─$ curl 127.0.0.1:11187
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
html4/strict.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html
<title>Directory listing for /</title>
</head>
<body>
<h1>Directory listing for /</h1>
<hr>
<ul>
<li><a href=".bash_logout">.bash_logout</a></li>
<li><a href=".bashrc">.bashrc</a></li>
```

```
┌──(kali㉿kali)-[~]
└─$ nc 127.0.0.1 11187
GET /from_nc HTTP/1.1
User-Agent: nc/ice1187

HTTP/1.0 404 File not found
Server: SimpleHTTP/0.6 Python/3.10.5
Date: Fri, 01 Sep 2023 06:13:49 GMT
Connection: close
Content-Type: text/html;charset=utf-8
Content-Length: 469

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
        "http://www.w3.org/TR/html4/strict.dtd">
<html>
    <head>
```

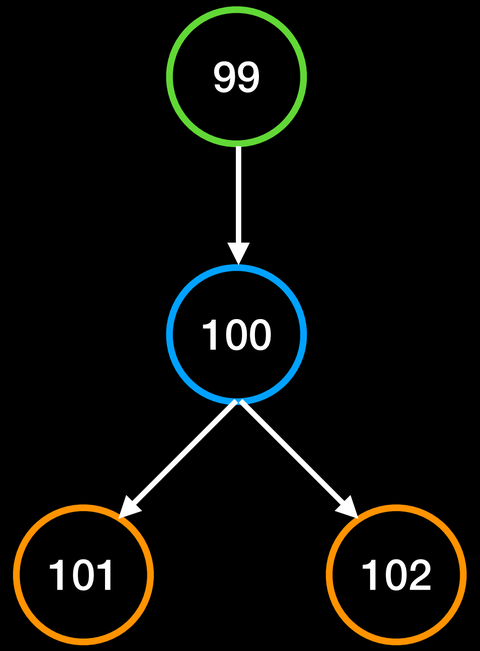
Lab — Tell me your (http) request



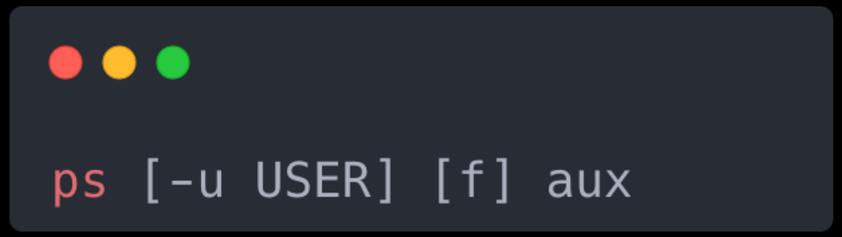
Process

Process

- 常見翻譯：進程、行程、程序
- 建議直接叫 process，較不易搞混
- 每個 process 都有唯一的 Process ID (PID)
- Process / Parent Process / Child Process



ps



- 用途：查看 process，類似 Windows 的工作管理員
- -u：指定 user
- f：以樹形顯示
- 參數繁雜，有無 dash 功能不一定相同，詳見 man ps

```
┌──(kali㉿kali)-[~]
└─$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.5 102544 12072 ?        Ss   Aug31   0:01 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    Aug31   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   Aug31   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   Aug31   0:00 [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I<   Aug31   0:00 [netns]
root           7  0.0  0.0      0     0 ?        I<   Aug31   0:00 [kworker/0:0H-events_highpri]
root           9  0.0  0.0      0     0 ?        I<   Aug31   0:01 [kworker/0:1H-events_highpri]
root          10  0.0  0.0      0     0 ?        I<   Aug31   0:00 [mm_percpu_wq]
root          11  0.0  0.0      0     0 ?        I    Aug31   0:00 [rcu_tasks_kthread]
root          12  0.0  0.0      0     0 ?        I    Aug31   0:00 [rcu_tasks_rude_kthread]
root          13  0.0  0.0      0     0 ?        I    Aug31   0:00 [rcu_tasks_trace_kthread]
root          14  0.0  0.0      0     0 ?        S    Aug31   0:01 [ksoftirqd/0]
root          15  0.0  0.0      0     0 ?        I    Aug31   0:09 [rcu_preempt]
root          16  0.0  0.0      0     0 ?        S    Aug31   0:00 [migration/0]
root          18  0.0  0.0      0     0 ?        S    Aug31   0:00 [cpuhp/0]
root          20  0.0  0.0      0     0 ?        S    Aug31   0:00 [kdevtmpfs]
root          21  0.0  0.0      0     0 ?        I<   Aug31   0:00 [inet_frag_wq]
```

```
┌──(kali㉿kali)-[~]
└─$ ps -u kali fu
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
kali      741996  0.0  0.3  18696  7060 ?        S    04:24   0:00 sshd: kali@pts/1
kali      741997  0.0  0.3  10676  6332 pts/1    Ss   04:24   0:00  \_ -zsh
kali      744446  0.0  0.1  10116  3208 pts/1    R+   04:34   0:00      \_ ps -u kali fu
kali         608  0.0  1.3 268692 26812 ?        Ssl  Aug31   0:00 xfce4-session
kali         665  0.0  0.0   8008   848 ?        Ss   Aug31   0:00  \_ /usr/bin/ssh-agent x-session-manager
kali         708  0.0  2.1 404884 43528 ?        Sl   Aug31   0:59  \_ xfwm4
kali         732  0.0  1.4 231548 29472 ?        Sl   Aug31   0:00  \_ xfsettingsd
kali         741  0.0  2.4 476120 48860 ?        Sl   Aug31   0:01  \_ xfce4-panel
kali         757  0.0  2.5 409632 52396 ?        Sl   Aug31   0:01  |   \_ /usr/lib/x86_64-linux-gnu/xfce4/p
kali         760  0.1  1.6 201936 33708 ?        Sl   Aug31   5:07  |   \_ /usr/lib/x86_64-linux-gnu/xfce4/p
kali         761  0.0  1.3 341168 26724 ?        Sl   Aug31   0:00  |   \_ /usr/lib/x86_64-linux-gnu/xfce4/p
kali         762  0.0  1.4 359084 29688 ?        Sl   Aug31   2:55  |   \_ /usr/lib/x86_64-linux-gnu/xfce4/p
kali         763  0.0  2.3 602088 47564 ?        Sl   Aug31   0:40  |   \_ /usr/lib/x86_64-linux-gnu/xfce4/p
kali         764  0.0  2.2 334144 44804 ?        Sl   Aug31   0:00  |   \_ /usr/lib/x86_64-linux-gnu/xfce4/p
kali         765  0.0  2.3 399868 46892 ?        Sl   Aug31   0:00  |   \_ /usr/lib/x86_64-linux-gnu/xfce4/p
kali         766  0.0  2.2 399708 44796 ?        Sl   Aug31   0:00  |   \_ /usr/lib/x86_64-linux-gnu/xfce4/p
kali         745  0.0  2.6 485636 54168 ?        Sl   Aug31   0:00  \_ Thunar --daemon
kali         754  0.0  2.8 475512 57144 ?        Sl   Aug31   0:01  \_ xfdesktop
kali         785  0.0  0.5 236892 10708 ?        Sl   Aug31   0:00  \_ xiccd
```

kill

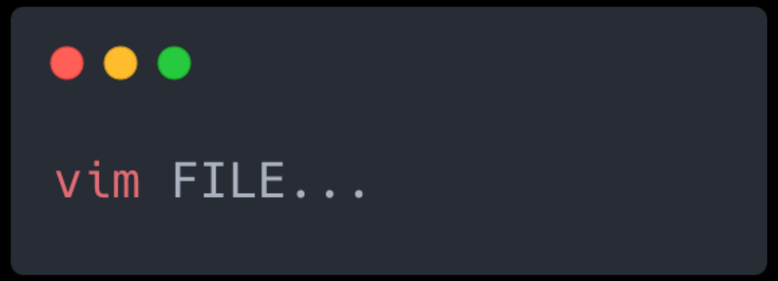
```
kill [-SIGKILL] PID...
```

- 用途：傳送 signal 到指定 process，通常用於強制結束 process
- 預設傳送 TERM (terminate) signal
- -SIGKILL：傳送 KILL signal
- TERM v.s. KILL：是否讓 process 執行必要的結束程序

```
┌──(kali㉿kali)-[~]
└─$ sleep 100000 &
[1] 748156

┌──(kali㉿kali)-[~]
└─$ ps u
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
kali        6025  0.0  0.3  14080  7336 pts/0    Ss+  Aug31   0:01 /usr/bin/zsh
kali      741997  0.1  0.3  10676  6400 pts/1    Ss   04:24   0:01 -zsh
kali      748156  0.0  0.0   5416   736 pts/1    SN   04:47   0:00 sleep 100000
kali      748168  0.0  0.1   9960  3236 pts/1    R+   04:47   0:00 ps u

┌──(kali㉿kali)-[~]
└─$ kill 748156

[1]  + terminated  sleep 100000
┌──(kali㉿kali)-[~]
└─$ ps u
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
kali        6025  0.0  0.3  14080  7336 pts/0    Ss+  Aug31   0:01 /usr/bin/zsh
kali      741997  0.1  0.3  10676  6400 pts/1    Ss   04:24   0:01 -zsh
kali      748228  0.0  0.1   9960  3276 pts/1    R+   04:47   0:00 ps u
```

Editor 編輯器

vim



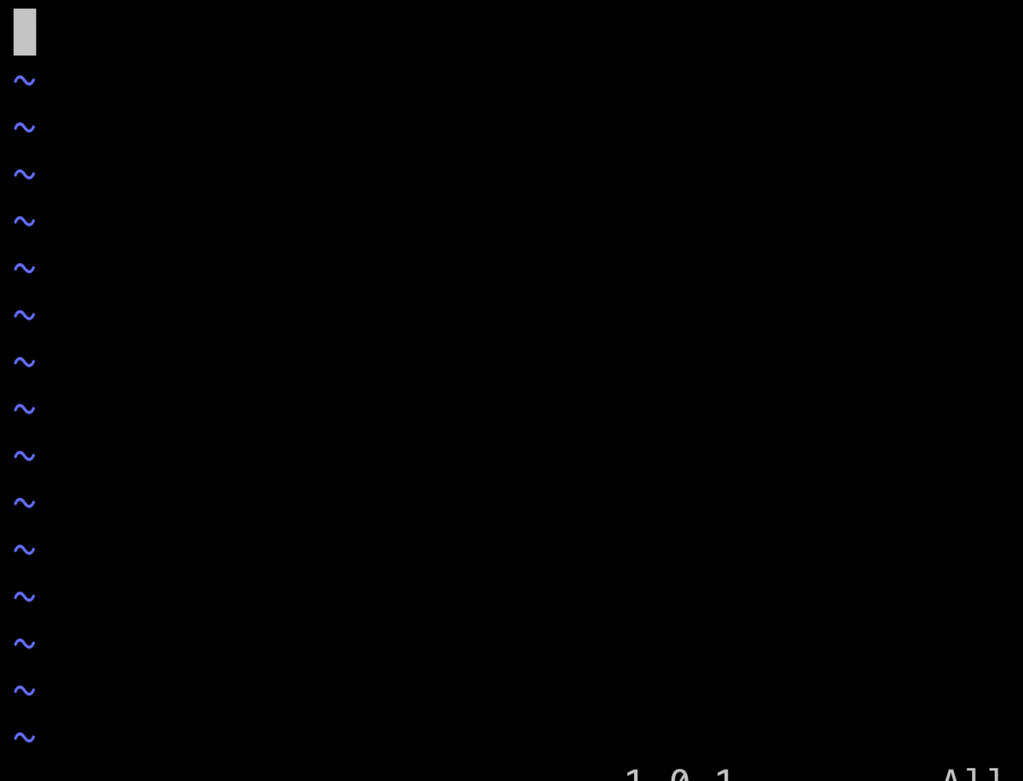
- ~~最難最複雜~~、最快最好用的編輯器
- 分成三種模式：指令模式、插入模式、可視模式
- 注意當前所在的模式！

插入模式

- 指令模式按 i 進入插入模式
- 左下角顯示 INSERT 表示為插入模式
- ↑↓←→：上下左右移動
- Esc：回到指令模式

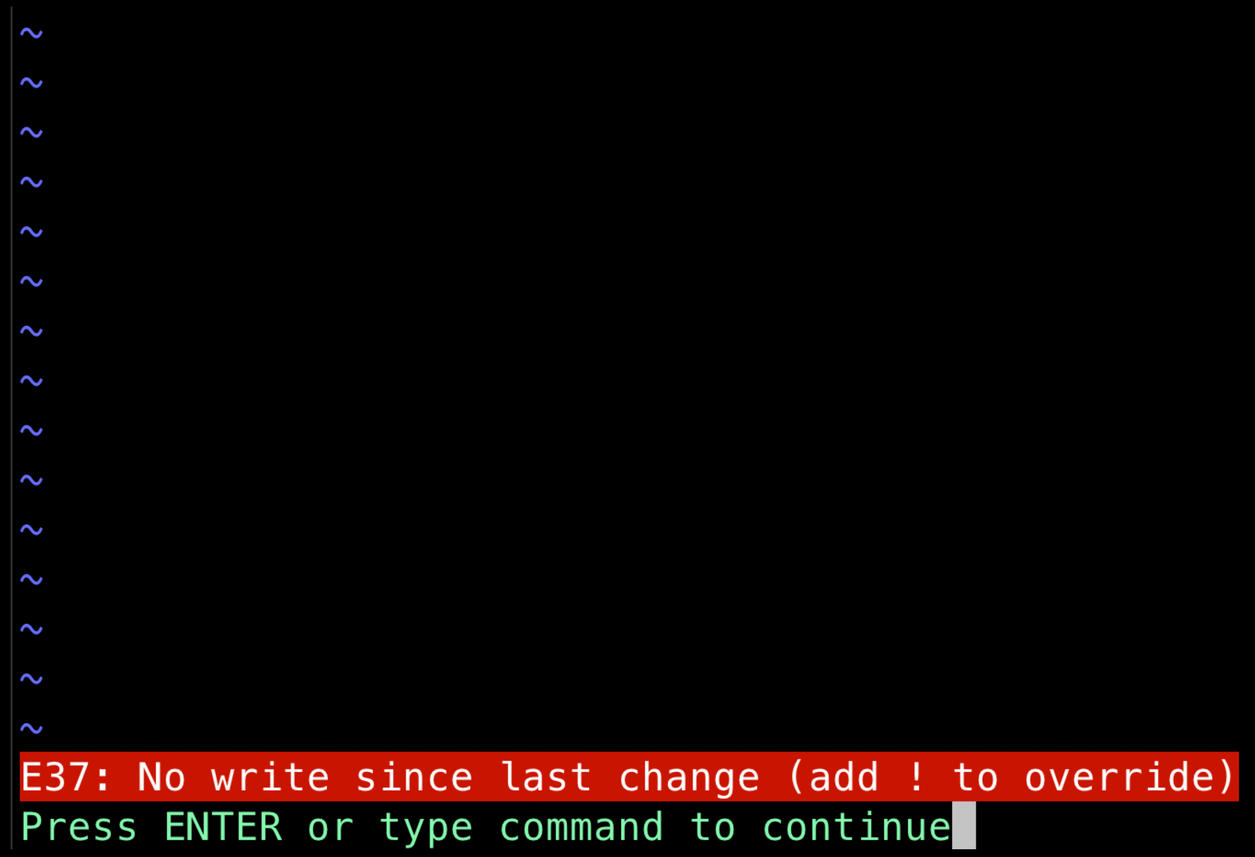
指令模式

- i：進入插入模式
- h / j / k / l：鼠標往左 / 下 / 上 / 右移動
- :：輸入指令
  - w：寫入存檔
  - q：退出
- u / ctrl+r：undo / redo



No write since last change

- 編輯後沒有存檔就退出
- :wq 寫入並退出
- :q! 放棄編輯並退出



Found a swap file

- .swp 是編輯暫存檔
- 刪除 .{filename}.swp

```
E325: ATTENTION
Found a swap file by the name ".hello.c.swp"
          owned by: kali   dated: Sun Sep 03 03:08:29 2023
         [cannot be read]
While opening file "hello.c"
             dated: Sun Sep 03 03:07:17 2023

(1) Another program may be editing the same file.  If this is the case,
    be careful not to end up with two different instances of the same
    file when making changes.  Quit, or continue with caution.
(2) An edit session for this file crashed.
    If this is the case, use ":recover" or "vim -r hello.c"
    to recover the changes (see ":help recovery").
    If you did this already, delete the swap file ".hello.c.swp"
    to avoid this message.

Swap file ".hello.c.swp" already exists!
[O]pen Read-Only, (E)dit anyway, (R)ecover, (D)elete it, (Q)uit, (A)bort:
```

Compile & Execute 編譯與執行

Compile — gcc

```
gcc -o OUTPUT_FILE source.c source.h
```

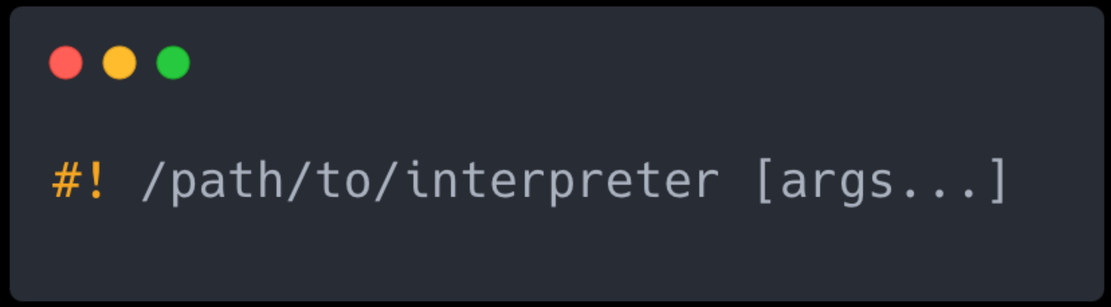
- 用途：編譯程式
- CTF 應用：自學組語、編譯題目、寫腳本
- 如何關閉保護機制，請參考「拜託別 Pwn 我啦！ - Protection 保護機制」

Execution 執行

```
./file_to_execute arg0 arg1 arg2
/path/to/file_to_execute
```

- 用途：執行檔案
- 注意：檔案需要有執行權限才能執行，下載的檔案有時需要先 chmod +x
- 任何檔案只要有執行權限皆可執行，例如：Python script、文字檔

Shebang #!



- 用途：指定執行該檔案 FILE 的 interpreter (直譯器)
- 實際執行指令：
  - /path/to/interpreter [args…] FILE

```
┌──(kali㉿kali)-[~]
└─$ cat ls.ls
#! /usr/bin/ls /home/kali

┌──(kali㉿kali)-[~]
└─$ ls -l ls.ls
-rwxr-xr-x 1 kali kali 26 Sep 10 03:50 ls.ls

┌──(kali㉿kali)-[~]
└─$ ./ls.ls
./ls.ls

/home/kali:
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  TobeExe  Videos  err.sh
```

為什麼平常下的指令不用加 ./ 或用絕對路徑？

PATH 環境變數

- "The search path for commands. It is a colon-separated list of directories in which the shell looks for commands." — *man bash*
- PATH 環境變數中儲存了許多資料夾，shell 會從這些資料夾中找尋指令
- 範例：
  - PATH: /usr/local/sbin, /usr/local/bin, /usr/bin
  - CMD: ls
  - 從 /usr/local/sbin 依序搜尋 ls，直到找到 /usr/bin/ls

```
┌──(kali㉿kali)-[~]
└─$ echo $PATH
/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games

┌──(kali㉿kali)-[~]
└─$ whereis ls
ls: /usr/bin/ls /usr/share/man/man1/ls.1.gz
```

Lab

- 練習用 vim 寫出 hello_world.c，並編譯和執行起來

```c
#include <stdio.h>

int main(void) {
        printf("Hello, World!\n");
        return 0;
}
```

```
┌──(kali㉿kali)-[~]
└─$ vim hello_world.c

┌──(kali㉿kali)-[~]
└─$ gcc hello_world.c -o hello_world

┌──(kali㉿kali)-[~]
└─$ ./hello_world
Hello, World!
```

Shell

What is Shell

- Shell 是人與作業系統互動的介面

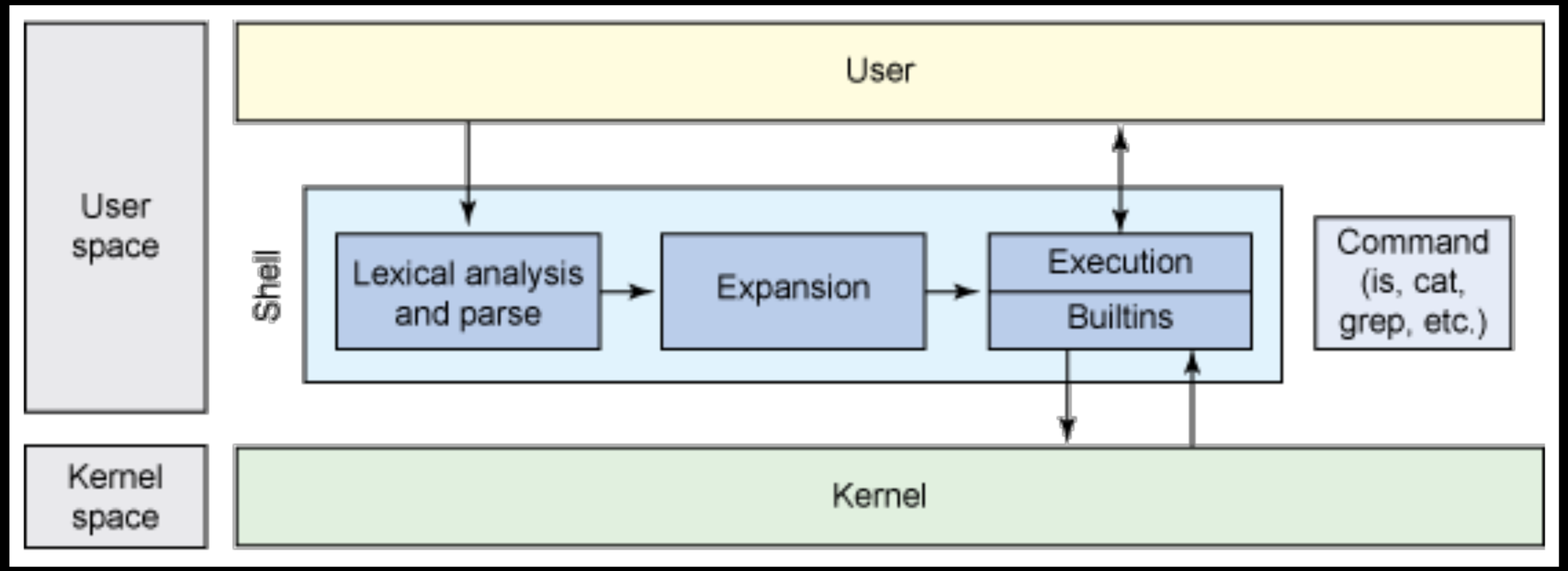
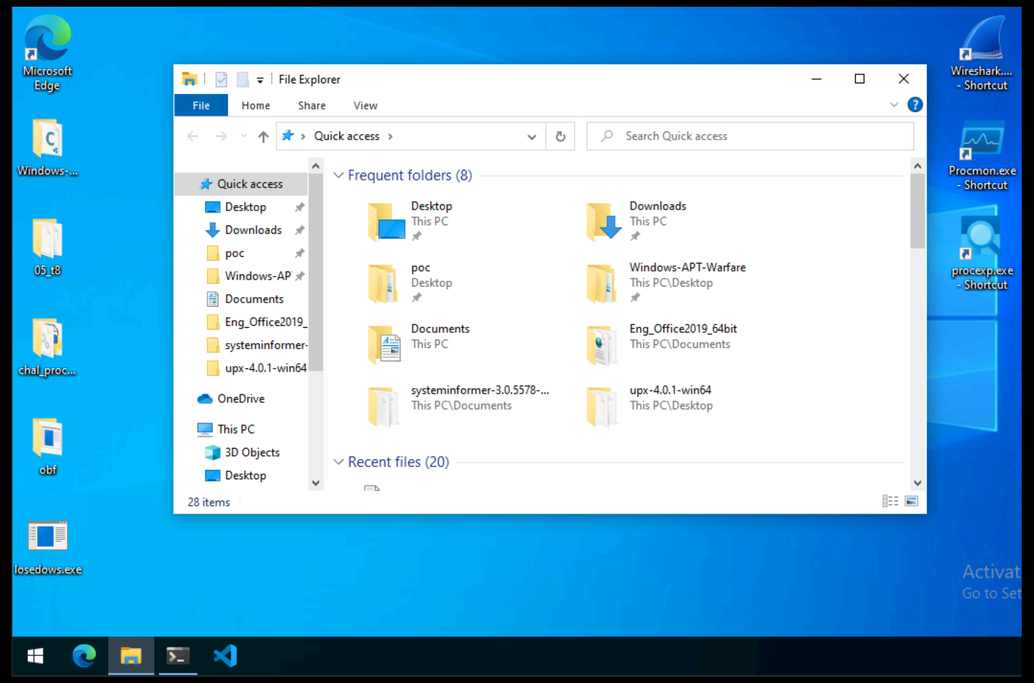


Image src: https://developer.ibm.com/tutorials/l-linux-shells/

What is Shell

- Shell 是人與作業系統互動的介面
  - 圖形化介面 – Windows Shell
  - 文字指令介面 – bash, zsh, fish



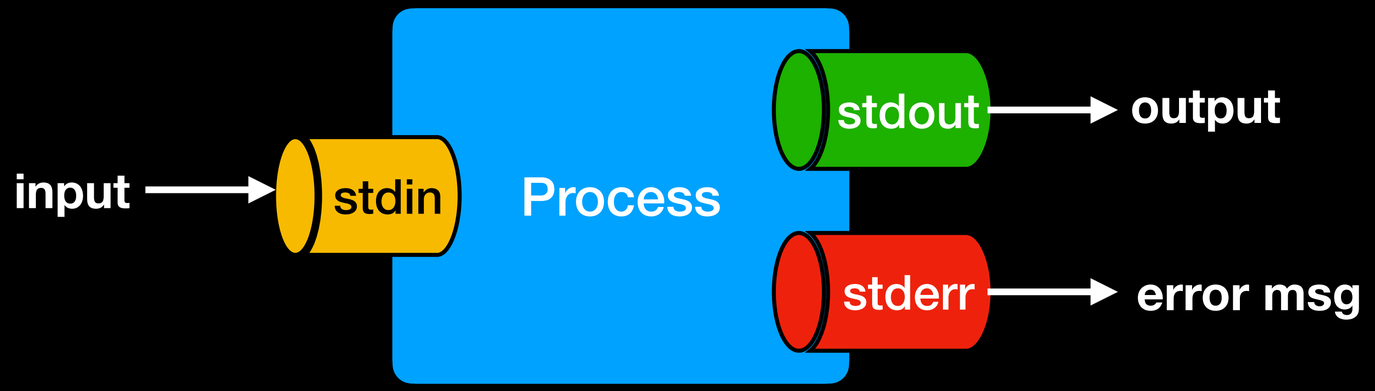

```
┌──(kali㉿kali)-[~]
└─$ echo $SHELL
/usr/bin/zsh
```

Shell

- Shell 有很多種，常見的預設為 bash, zsh
- Shell 的主要功能：
  - Command-line interpreter
    - execute program、pipe、redirect、substitution
  - Modify environment variable
  - Scripting

stdin, stdout, stderr

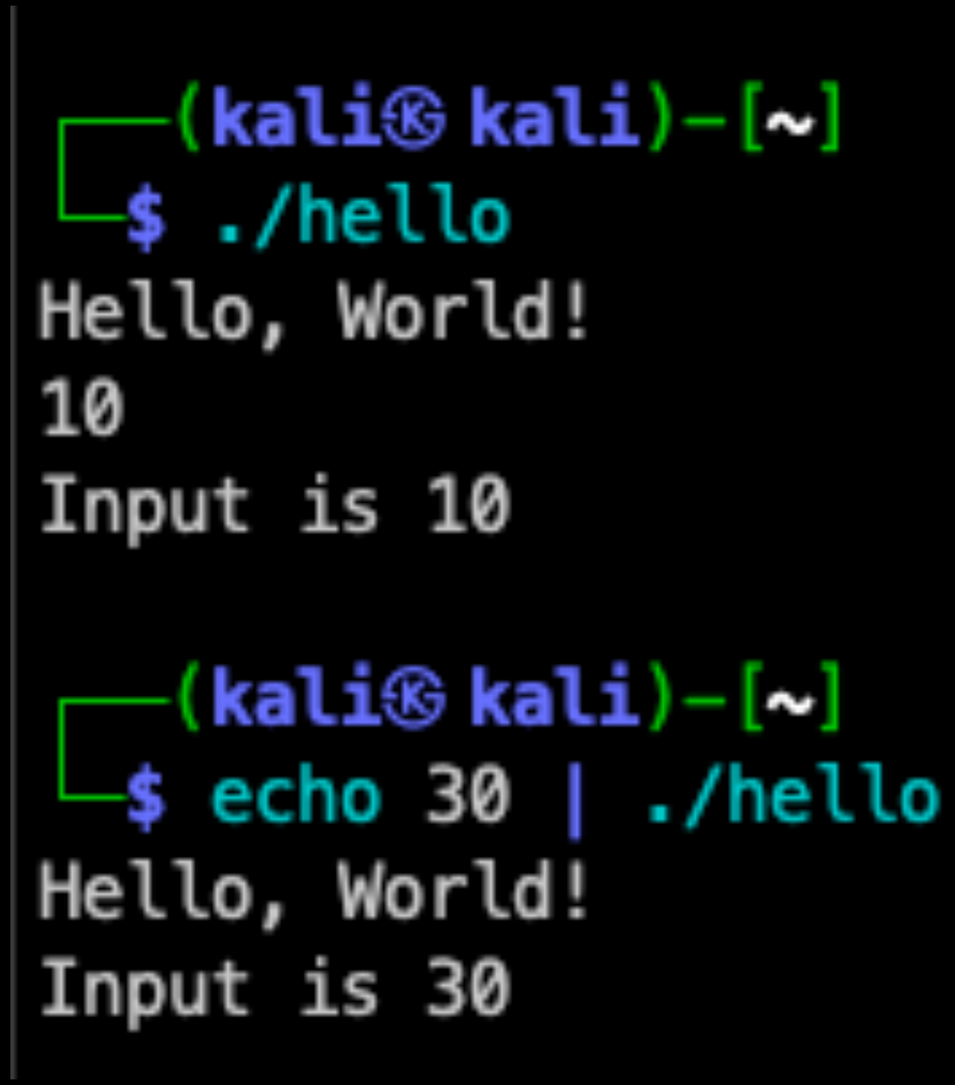
- Linux process 的三個標準輸入/輸出口
- stdin：標準輸入
- stdout：標準輸出
- stderr：標準錯誤輸出



Pipe 管道

```
command_A | command_B
```

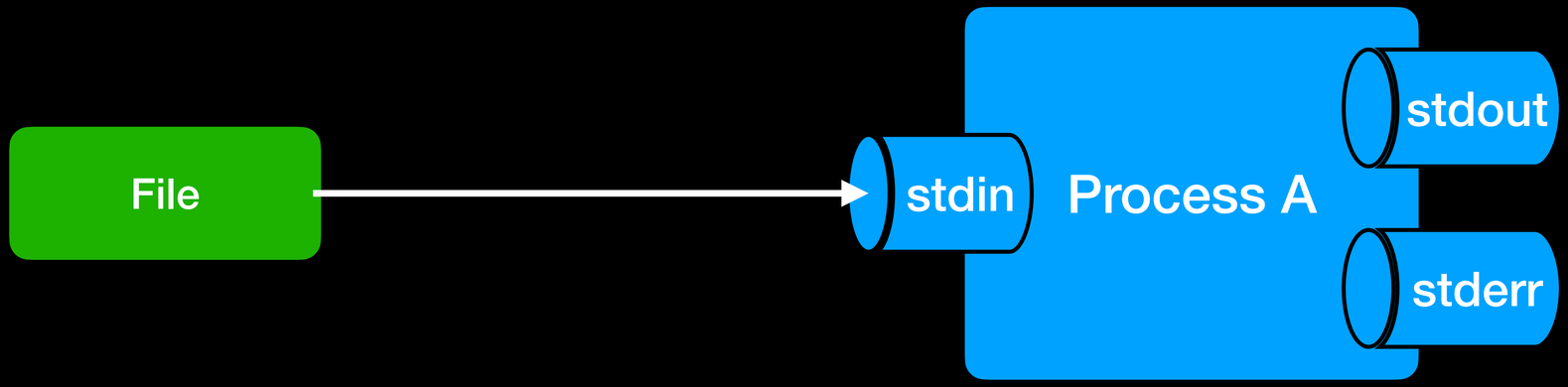
- 用途：將 command A 的 stdout 傳入 command B 的 stdin


(kali㉿kali)-[~]
$ ./hello
Hello, World!
10
Input is 10
(kali㉿kali)-[~]
$ echo 30 | ./hello
Hello, World!
Input is 30

Redirect 重導向

```
command < file
```

- 用途：將 file 的內容傳入 command 的 stdin

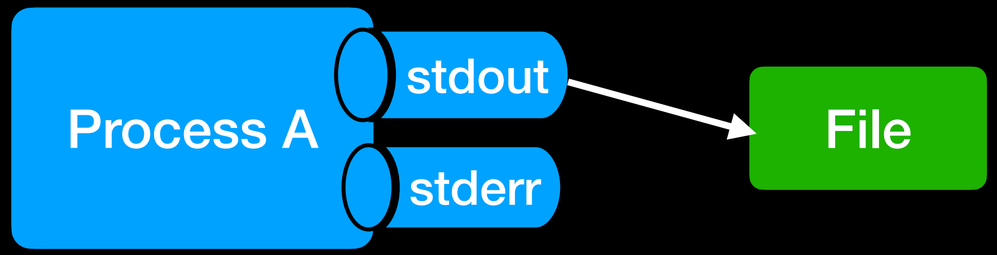


```
┌──(kali㉿kali)-[~]
└─$ cat < hello.c
#include <stdio.h>

int main(void) {
        int a;
        printf("Hello, World!\n");

        scanf("%d", &a);
        printf("Input is %d\n", a);

        return 0;
}
```

Redirect 重導向

```
command > file
command 2> file
command &> file
```

- 用途：將 command 的 stdout/stderr 傳入 file
  - >：stdout 傳入 file



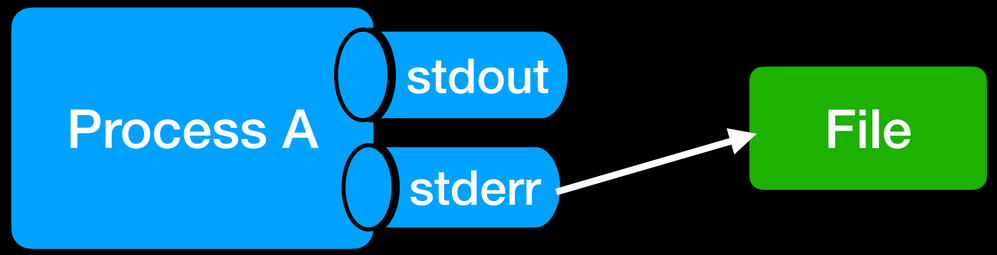
>：stdout 傳入 file

```
┌──(kali㉿kali)-[~]
└─$ ls -l hello non_exist > a
ls: cannot access 'non_exist': No such file or directory

┌──(kali㉿kali)-[~]
└─$ cat a
-rwxr-xr-x 1 kali kali 16208 Sep  1 02:00 hello
```

Redirect 重導向

```
command > file
command 2> file
command &> file
```

- 用途：將 command 的 stdout/stderr 傳入 file
  - >：stdout 傳入 file
  - 2>：stderr 傳入 file



2>：stderr 傳入 file

```
┌──(kali㉿kali)-[~]
└─$ ls -l hello non_exist 2> a
-rwxr-xr-x 1 kali kali 16208 Sep  1 02:00 hello

┌──(kali㉿kali)-[~]
└─$ cat a
ls: cannot access 'non_exist': No such file or directory
```

為什麼 2> 是 stderr？

- "Everything is a file."
- stdin, stdout, stderr 被當作檔案來處理，對應的 file descriptor (fd)：
  - stdin：fd = 0
  - stdout：fd = 1
  - stderr：fd = 2

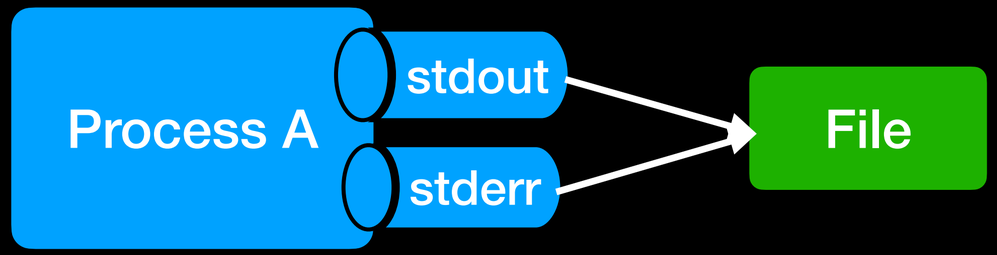
```
┌──(kali㉿kali)-[~]
└─$ sleep 10000
Write to stdout of sleep
```

```
┌──(kali㉿kali)-[~]
└─$ ps -u | grep "sleep 1000"
kali     3299410  0.0  0.0   5472   896 pts/3    S+   11:59   0:00 sleep 10000

┌──(kali㉿kali)-[~]
└─$ ls /proc/3299410/fd
0  1  2

┌──(kali㉿kali)-[~]
└─$ echo "Write to stdout of sleep" >  /proc/3299410/fd/1
```

Redirect 重導向

```
command > file
command 2> file
command &> file
```

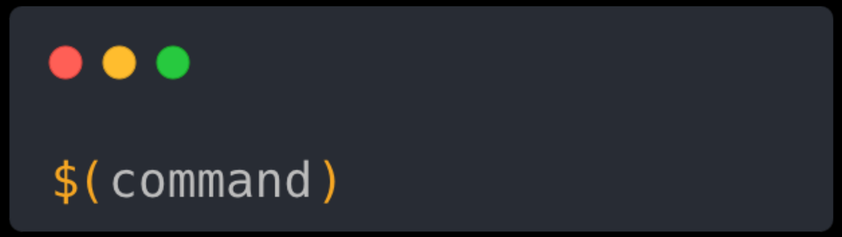
- 用途：將 command 的 stdout/stderr 傳入 file
  - >：stdout 傳入 file
  - 2>：stderr 傳入 file
  - &>：stdout 與 stderr 傳入 file



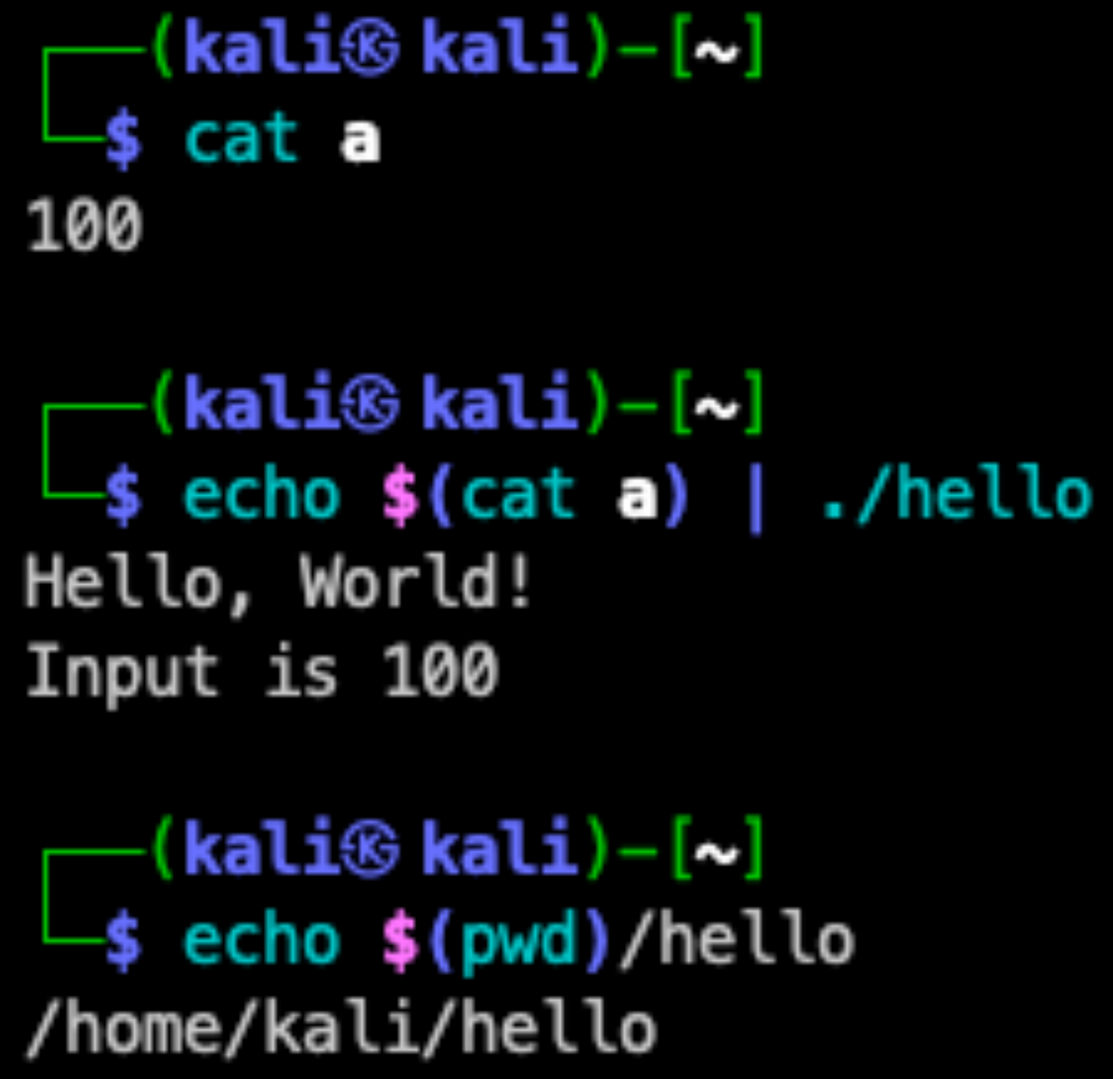
&>：stdout 與 stderr 傳入 file

```
┌──(kali㉿kali)-[~]
└─$ ls -l hello non_exist &> a

┌──(kali㉿kali)-[~]
└─$ cat a
ls: cannot access 'non_exist': No such file or directory
-rwxr-xr-x 1 kali kali 16208 Sep  1 02:00 hello
```

Command Substitution 指令替換



- 用途：將 command 的 output 作為指令的一部分
- 常見範例：$(pwd)/file_A 快速取得當前檔案 file_A 的絕對路徑
- 以上 bash 功能的詳細介紹可參考：man bash

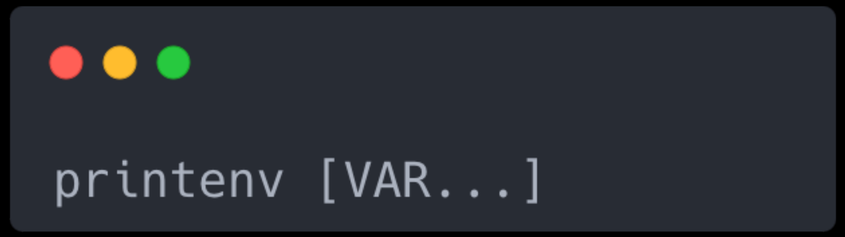

(kali㉿kali)-[~]
$ cat a
100
(kali㉿kali)-[~]
$ echo $(cat a) | ./hello
Hello, World!
Input is 100
(kali㉿kali)-[~]
$ echo $(pwd)/hello
/home/kali/hello

Environment Variable 環境變數

- 以 KEY=value 形式表示
- 另一組傳遞給程式的參數，類似於 argv
- 前述 PATH 即為其中一項環境變數

```
#include <unistd.h>

int execve(const char *pathname, char *const _Nullable argv[],
           char *const _Nullable envp[]);
```

printenv



- 用途：列出環境變數
- VAR：指令要列出的環境變數，預設為所有

```
┌──(kali㉿kali)-[~]
└─$ printenv
LC_TERMINAL_VERSION=3.4.20
LC_CTYPE=UTF-8
LC_TERMINAL=iTerm2
USER=kali
LOGNAME=kali
HOME=/home/kali
PATH=/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
SHELL=/usr/bin/zsh
TERM=xterm-256color
XDG_SESSION_ID=2237
XDG_RUNTIME_DIR=/run/user/1000
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
XDG_SESSION_TYPE=tty
XDG_SESSION_CLASS=user
MOTD_SHOWN=pam
COMMAND_NOT_FOUND_INSTALL_PROMPT=1
POWERSHELL_UPDATECHECK=Off
POWERSHELL_TELEMETRY_OPTOUT=1
DOTNET_CLI_TELEMETRY_OPTOUT=1
LANG=en_US.UTF-8
SSH_CLIENT=192.168.2.2 61501 22
SSH_CONNECTION=192.168.2.2 61501 192.168.10.54 22
SSH_TTY=/dev/pts/1
SHLVL=1
PWD=/home/kali
```

修改環境變數

- 用途：將傳遞給 command 的環境變數 ENV_VAR 的值修改為 VALUE
- CTF 應用：使用 LD_PRELOAD 或 LD_LIBRARY_PATH 做 hook

```
┌──(kali㉿kali)-[~]
└─$ PAGER=more man man
man: can't set the locale; make sure $LC_* and $LANG are correct
MAN(1)                    Manual pager utils                    MAN(1)

NAME
       man - an interface to the system reference manuals

SYNOPSIS
       man [man options] [[section] page ...] ...
       man -k [apropos options] regexp ...
       man -K [man options] [section] term ...
       man -f [whatis options] page ...
       man -l [man options] file ...
       man -w|-W [man options] page ...

DESCRIPTION
       man  is  the system's manual pager.  Each page argument given to
       man is normally the name of a program, utility or function.  The
       manual  page  associated  with  each  of these arguments is then
       found and displayed.  A section, if provided, will direct man to
       look  only in that section of the manual.  The default action is
       to search in all of the available sections following  a  pre-de-
       fined  order  (see  DEFAULTS),  and  to show only the first page
       found, even if page exists in several sections.

       The table below shows the section numbers of the manual followed
--More--
```

Change the pager of man to more

Bash Scripting

- Bash 有自己的 grammar，可以視做一種程式語言
- 常用於操作自動化
- 執行方式：
  - 將指令寫入 script.sh，然後以 bash script.sh 執行
  - shebang
- 語法請參考 Bash Scripting Cheatsheet

Lab — You know how to set env var!

You know how to set environment variables

100

你知道如何對單一 process 設定環境變數嗎？設置環境變數 `GIVE_ME_FLAG` 後執行附件程式來得到 flag！

Flag 格式：`FLAG{...}`

ssh 遠端管理

ssh

- 於非安全網路環境中建立安全連線的網路傳輸協定
- 常用於遠端管理、傳輸檔案等
- 支援密碼、非對稱式加密身份驗證

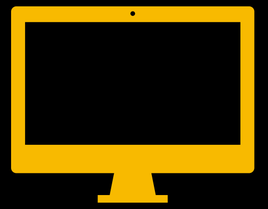
非對稱式加密

1. 使用者產生公鑰、私鑰

公鑰

私鑰

使用者



伺服器

非對稱式加密

非對稱式加密

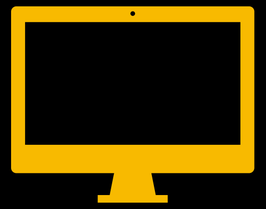
非對稱式加密

非對稱式加密

5. 檢查使用者回傳的驗證訊息是否正確

私鑰

使用者



伺服器

公鑰

非對稱式加密

生成公私鑰 — ssh-keygen

```
ssh-keygen [-t ed25519 | rsa]
```

- 用途：產生一副公鑰、私鑰
- -t：選擇非對稱式加密演算法
- 預設儲存位置：
  - 公鑰：~/.ssh/id_{algo}.pub
  - 私鑰：~/.ssh/id_{algo}

傳送公鑰 — ssh-copy-id

```
ssh-copy-id [-p PORT] user@host
```

- 用途：將本地的公鑰複製到 host 伺服器的 user 使用者底下
- -p：指定 ssh 伺服器監聽的 port，預設為 22
- 公鑰儲存於伺服器該使用者的 ~/.ssh/authorized_keys 內，也可以手動複製

遠端連線 — ssh

```
ssh [-v] [-p PORT] [-i priv_key_file] user@host
```

- 用途：遠端連線至 host 伺服器的 user 使用者
- -v：印出連線時的 debug 資訊
- -p：指定 ssh 伺服器監聽的 port，預設為 22
- -i：指定身份驗證使用的私鑰

遠端傳送檔案 — scp

```
scp [-v] [-r] [-P PORT] source destination
```

- 用途：在遠端與本地傳送檔案
- 將檔案從 source 複製至 destination
- 本地檔案格式：相對路徑或絕對路徑
- 遠端檔案格式：user@host:[path/to/file]

- -r：複製整個資料夾
- -P：指定 ssh 監聽的 port
- -v：印出 debug 資訊

Lab

- 嘗試使用 public key 驗證連線到某台有 ssh service 的機器
- ssh 遠端連線
  1. 輸入 ssh user@host
  2. 輸入 yes (第一次連線)
  3. 輸入密碼

```
ice1187@ice1187-lab:~$ ssh kali@192.168.10.54
The authenticity of host '192.168.10.54 (192.168.10.54)' can't be established.
ECDSA key fingerprint is SHA256:8zdkRD0LT+3OxfnIPLP5E5Qlum0monS6DDQOTATb5JU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.10.54' (ECDSA) to the list of known hosts.
kali@192.168.10.54's password:
Linux kali 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali6 (2022-07-07) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Sep 15 04:32:27 2023 from 192.168.2.2
┌──(kali㉿kali)-[~]
└─$
```

Compress 壓縮/解壓縮

7z

```
7z a output.7z FILE...
7z l output.7z
7z x output.7z
```

- 7z 支援多種壓縮演算法，多數壓縮檔都可用 7z 解開
- a：壓縮 (archive)
- l：列出壓縮檔內容 (list)
- x：解壓縮

zip

```
zip output.zip [-r DIR] FILE...
unzip [-l] output.zip
```

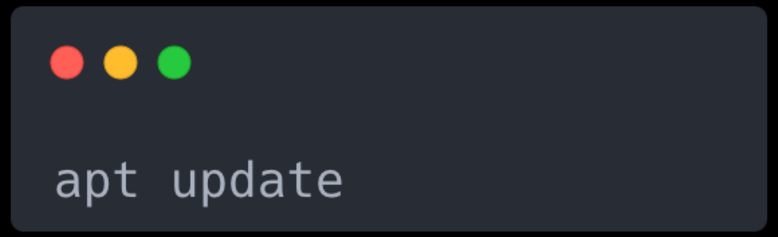
- output.zip 在 FILE... 前面
- -r：壓縮整個資料夾
- -l：列出壓縮檔內容
- 更多壓縮/解壓縮指令請參考「GNU / Linux 各種壓縮與解壓縮指令」

Package Manager 套件管理

Package Manager 套件管理

- 安裝、解除安裝、更新套件，並自動管理 dependency 和 conflict 等
- 程式語言的套件管理器：
  - Python — pip
  - Node.js — npm
- 作業系統也有套件管理器：pacman、yum、apt、dpkg

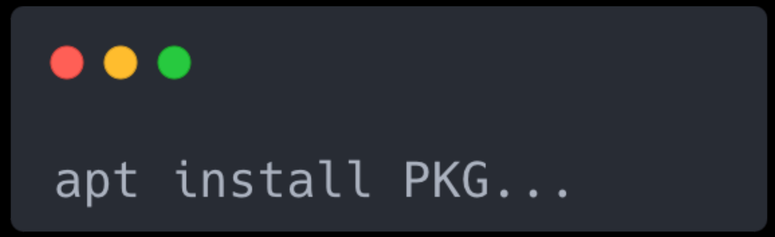
apt update



- 用途：從網路下載最新的套件資訊至本地套件資料庫 (a.k.a 更新套件資料庫)
- apt 多數功能皆仰賴套件資訊，無法安裝、升級時，可能需要先 update
- 套件管理屬於系統操作，需要加上 sudo

```
┌──(kali㉿kali)-[~]
└─$ apt update
Reading package lists... Done
E: Could not open lock file /var/lib/apt/lists/lock - open (13: Permission denied)
E: Unable to lock directory /var/lib/apt/lists/
W: Problem unlinking the file /var/cache/apt/pkgcache.bin - RemoveCaches (13: Permission denied)
W: Problem unlinking the file /var/cache/apt/srcpkgcache.bin - RemoveCaches (13: Permission denied)

┌──(kali㉿kali)-[~]
└─$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.cs.nycu.edu.tw/kali kali-rolling InRelease [41.2 kB]
Get:2 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 Packages [19.4 MB]
Get:3 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 Contents (deb) [45.6 MB]
Get:4 http://kali.cs.nycu.edu.tw/kali kali-rolling/contrib amd64 Packages [115 kB]
Fetched 65.1 MB in 14s (4780 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1834 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

apt install



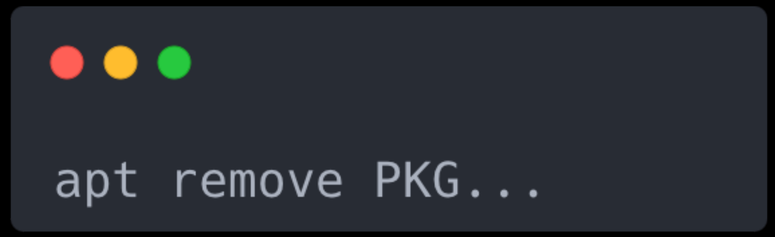
- 用途：安裝、更新套件
  - 安裝套件 PKG
  - 更新現有套件 PKG

```
┌──(kali㉿kali)-[~]
└─$ docker
Command 'docker' not found, but can be installed with:
sudo apt install docker.io
sudo apt install podman-docker

┌──(kali㉿kali)-[~]
└─$ sudo apt install docker.io
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  cgroupfs-mount containerd criu libapt-pkg-perl libcommon-sense-perl libcrypt-ssleay-perl libdbd-mariadb-
  liblist-moreutils-xs-perl liblocale-gettext-perl libmodule-find-perl libmodule-scandeps-perl libnet-dbus
  libsort-naturally-perl libstring-crc32-perl libterm-readkey-perl libtext-charwidth-perl libtext-iconv-pe
Suggested packages:
  containernetworking-plugins docker-doc aufs-tools btrfs-progs debootstrap rinse rootlesskit xfsprogs zfs
  libterm-readline-gnu-perl | libterm-readline-perl-perl libtap-harness-archive-perl
The following NEW packages will be installed:
  cgroupfs-mount containerd criu docker.io libintl-perl libintl-xs-perl libmodule-find-perl libmodule-scar
The following packages will be upgraded:
  libapt-pkg-perl libcommon-sense-perl libcrypt-ssleay-perl libdbd-mariadb-perl libdbi-perl libfcgi-perl l
  libnet-dns-sec-perl libnet-libidn-perl libnet-ssleay-perl libsocket6-perl libstring-crc32-perl libterm-r
24 upgraded, 15 newly installed, 0 to remove and 1803 not upgraded.
Need to get 79.0 MB of archives.
After this operation, 320 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libapt-pkg-perl amd64 0.1.40+b2 [69.2 kB]
Get:2 http://kali.cs.nycu.edu.tw/kali kali-rolling/main amd64 libxml-parser-perl amd64 2.46-4 [201 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 libunicode-linebreak-perl amd64 0.0.20190101-1+b5
```

```
┌──(kali㉿kali)-[~]
└─$ apt list vim
Listing... Done
vim/kali-rolling 2:9.0.1672-1 amd64 [upgradable from: 2:8.2.4793-1]
N: There is 1 additional version. Please use the '-a' switch to see it

┌──(kali㉿kali)-[~]
└─$ sudo apt install vim
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  vim-common vim-runtime vim-tiny xxd
```

```
┌──(kali㉿kali)-[~]
└─$ apt list vim
Listing... Done
vim/kali-rolling,now 2:9.0.1672-1 amd64 [installed]
```

apt remove



- 用途：解除安裝套件（保留部分使用者設定）
- 使用 apt purge 移除使用者設定

Lab — Install Docker

- 練習安裝 Docker

```
┌──(kali㉿kali)-[~]
└─$ docker

Usage:  docker [OPTIONS] COMMAND

A self-sufficient runtime for containers

Options:
      --config string      Location of client config files (default "/home/kali/.docker")
  -c, --context string     Name of the context to use to connect to the daemon (overrides DOCKER_HOST env
  -D, --debug              Enable debug mode
  -H, --host list          Daemon socket(s) to connect to
  -l, --log-level string   Set the logging level ("debug"|"info"|"warn"|"error"|"fatal") (default "info")
      --tls                Use TLS; implied by --tlsverify
      --tlscacert string   Trust certs signed only by this CA (default "/home/kali/.docker/ca.pem")
      --tlscert string     Path to TLS certificate file (default "/home/kali/.docker/cert.pem")
      --tlskey string      Path to TLS key file (default "/home/kali/.docker/key.pem")
      --tlsverify          Use TLS and verify the remote
  -v, --version            Print version information and quit
```

Encoding 編碼

ASCII

- 字母如何在電腦中被表示？

ASCII可顯示字元（共95個）

二進位	十進位	十六進位	圖形	二進位	十進位	十六進位	圖形	二進位	十進位	十六進位	圖形
0010 0000	32	20	(space)	0100 0000	64	40	@	0110 0000	96	60	`
0010 0001	33	21	!	0100 0001	65	41	A	0110 0001	97	61	a
0010 0010	34	22	"	0100 0010	66	42	B	0110 0010	98	62	b
0010 0011	35	23	#	0100 0011	67	43	C	0110 0011	99	63	c
0010 0100	36	24	$	0100 0100	68	44	D	0110 0100	100	64	d
0010 0101	37	25	%	0100 0101	69	45	E	0110 0101	101	65	e
0010 0110	38	26	&	0100 0110	70	46	F	0110 0110	102	66	f
0010 0111	39	27	'	0100 0111	71	47	G	0110 0111	103	67	g
0010 1000	40	28	(	0100 1000	72	48	H	0110 1000	104	68	h
0010 1001	41	29	)	0100 1001	73	49	I	0110 1001	105	69	i
0010 1010	42	2A	*	0100 1010	74	4A	J	0110 1010	106	6A	j

Img Src: https://zh.wikipedia.org/zh-tw/ASCII

Hex & Binary

- Hex 十六進位
  - 通常以 0x 開頭表示
  - 0123456789abcdef
  - 每兩個數字剛好一個 byte
- Binary 二進位
  - 通常以 0b 開頭表示

0x10 = 28 = 0b11100

0x100 = 256 = 0b100000000

Base64 編碼

- 一種由英文大小寫、數字和 +/= 組成 binary-to-text 編碼
- 功能：使 binary 檔案 (圖片、執行檔) 得以在純文字管道中進行傳輸
- 特徵：結尾為 = 或 ==

Source	Text (ASCII)	M			a																		
	Octets	77 (0x4d)							97 (0x61)														
Bits		0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	0						
Base64 encoded	Sextets	19							22							4				Padding			
	Character	T							W							E				=			
	Octets	84 (0x54)							87 (0x57)							69 (0x45)				61 (0x3D)			

Img Src: https://en.wikipedia.org/wiki/Base64

base64

- 用途：將檔案 FILE 做 base64 encoding
- -d：進行 decoding
- 注意：若要處理字串，需先寫入檔案，或用 pipe 傳入 stdin

```
┌──(kali㉿kali)-[~]
└─$ echo Hello, World! | base64
SGVsbG8sIFdvcmxkIQo=

┌──(kali㉿kali)-[~]
└─$ echo SGVsbG8sIFdvcmxkIQo= | base64 -d
Hello, World!

┌──(kali㉿kali)-[~]
└─$ echo This is a b64 encodede file. | base64 > encode.b64

┌──(kali㉿kali)-[~]
└─$ cat encode.b64
VGhpcyBpcyBhIGI2NCBlbmNvZGVkZSBmaWxlLgo=

┌──(kali㉿kali)-[~]
└─$ base64 -d encode.b64
This is a b64 encodede file.
```

Number Converversion by Python

- number to string
  - int to bin：hex(number)
  - int to hex：bin(number)
- string to number
  - bin to int：int('number string', 2)
  - hex to int：int('number string', 16)

Base64 in Python

- from base64 import b64encode, b64decode
- b64encode(b’base64 string’)
- b64decode(’base64 string’)

```
1 from base64 import b64encode, b64decode$
2 $
3 s = b'Hello, World!'$
4 $
5 b64_s = b64encode(s)$
6 print(b64_s)$
7 $
8 ori_s = b64decode(b64_s)$
9 print(ori_s)$
```

```
❯ python3 try_b64.py
b'SGVsbG8sIFdvcmxkIQ=='
b'Hello, World!'
```

其他 CTF 常用指令

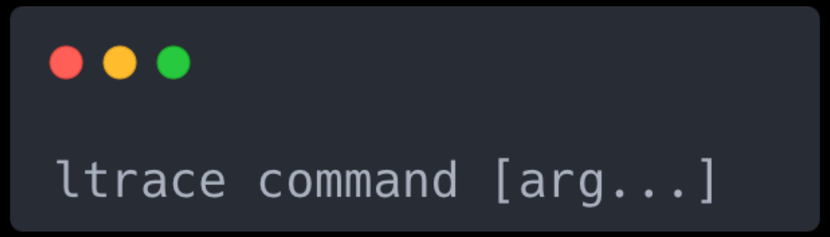
strings

```
strings [-n minlen] FILE...
```

- 用途：印出檔案 FILE 中所有連續數個可視字元組成的字串
- -n：指定字串至少要有連續 minlen 個可視字元，預設為 4
- CTF 應用：查看 binary 檔案中的字串

```
┌──(kali㉿kali)-[~]
└─$ strings hello
/lib64/ld-linux-x86-64.so.2
__isoc99_scanf
puts
printf
__cxa_finalize
__libc_start_main
libc.so.6
GLIBC_2.7
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
[]A\A]A^A_
Hello, World!
Input is %d
;*3$"
GCC: (Debian 11.3.0-5) 11.3.0
Scrt1.o
__abi_tag
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
```

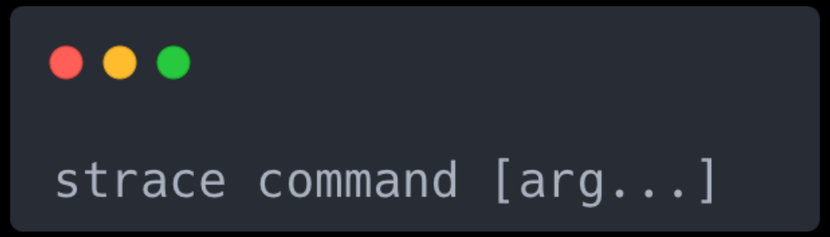
ltrace



- 用途：列出/紀錄 command 執行時所呼叫的 library call
- CTF 應用：查看程式執行時的 library call 和其參數

```
┌──(kali㉿kali)-[~]
└─$ ltrace ./hello
puts("Hello, World!"Hello, World!
)
__isoc99_scanf(0x55b1d5681012, 0x7ffe0a4563ec, 0, 0x7ff5cae4fad0100
)
printf("Input is %d\n", 100Input is 100
)
+++ exited (status 0) +++
```

strace

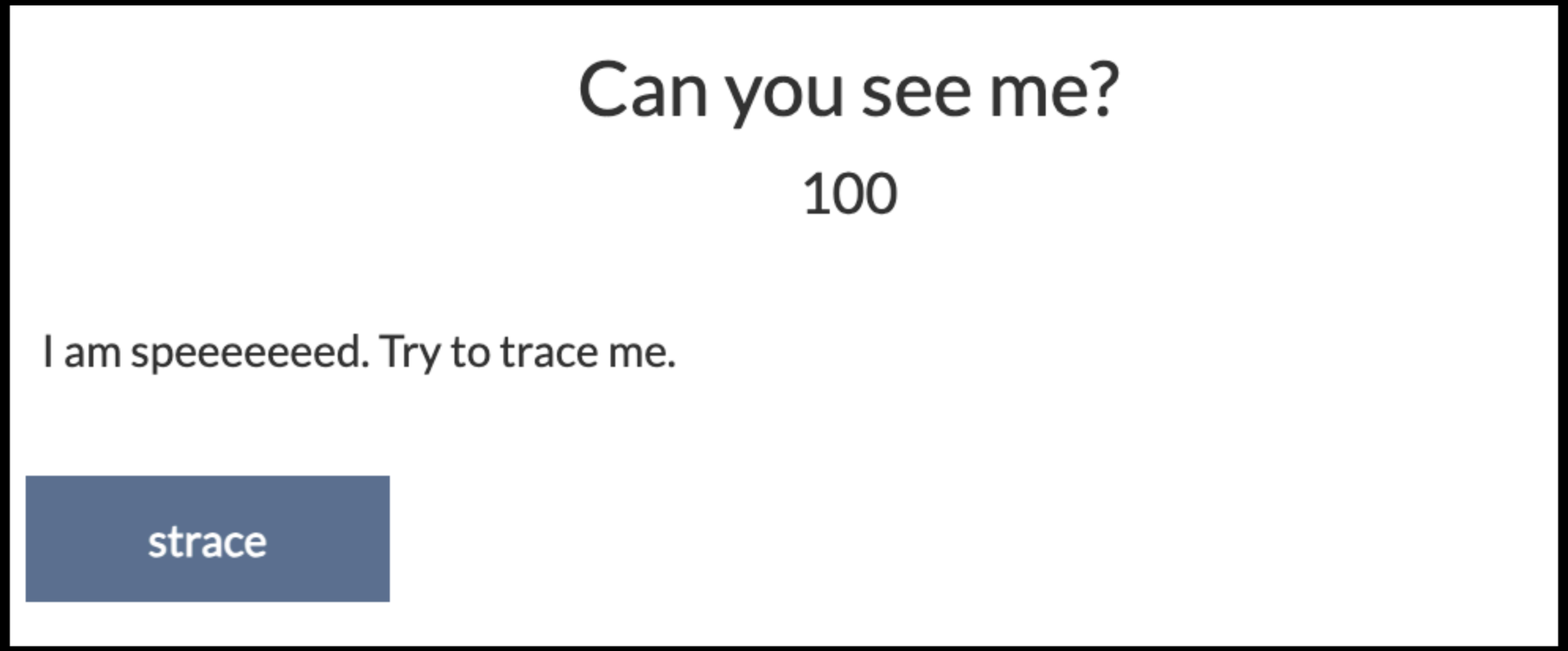


- 用途：列出/紀錄 command 執行時所呼叫的 system call 和接收的 signals
- CTF 應用：查看程式執行時的 system call 和其參數

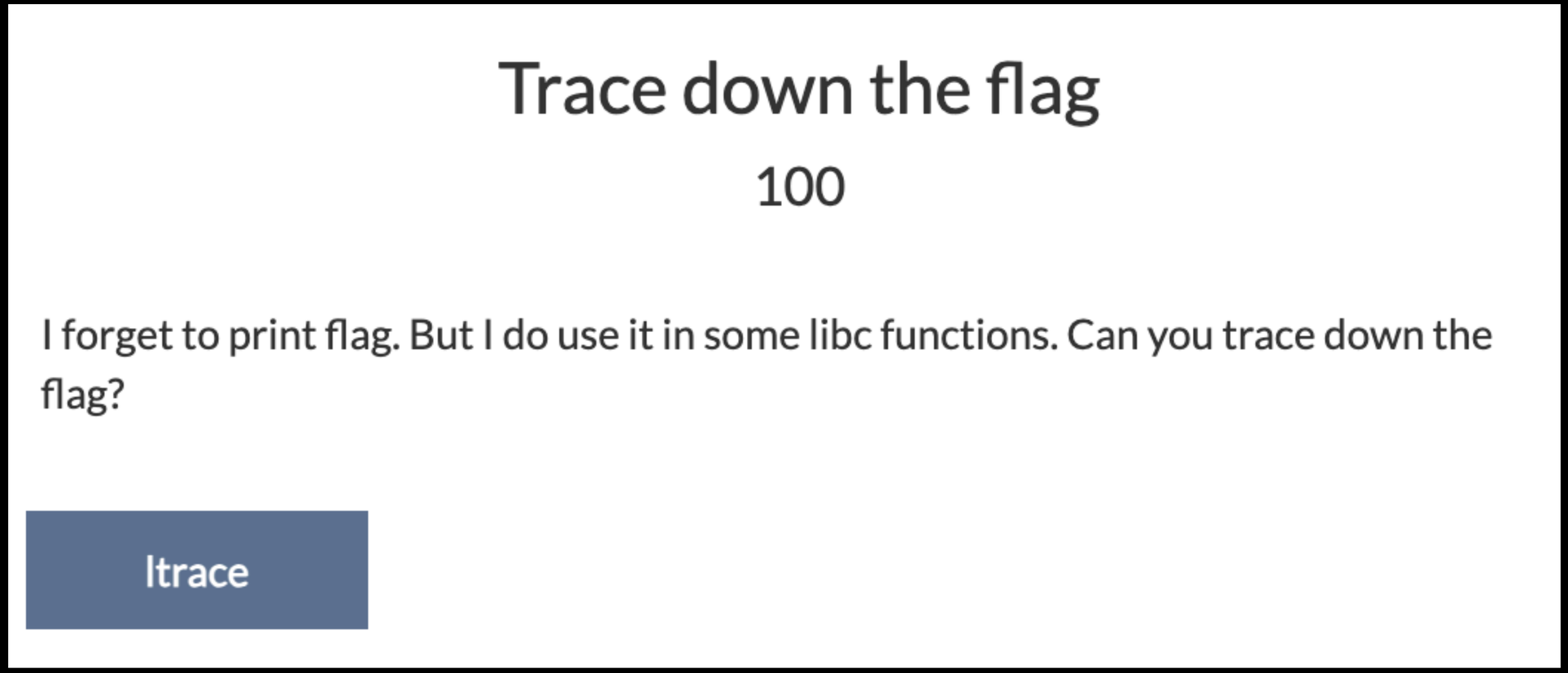
```
┌──(kali㉿kali)-[~]
└─$ strace ./hello
execve("./hello", ["./hello"], 0x7ffd70c90e60 /* 35 vars */) = 0
brk(NULL)                               = 0x5599f9a9d000
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
newfstatat(3, "", {st_mode=S_IFREG|0644, st_size=73494, ...}, AT_EMPTY_PATH) = 0
mmap(NULL, 73494, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f54061ff000
close(3)                                = 0
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f54061fd000
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\220x\2\0\0\0\0\0"..., 832) = 832
pread64(3, "\6\0\0\0\4\0\0\0@\0\0\0\0\0\0\0@\0\0\0\0\0\0\0@\0\0\0\0\0\0\0"..., 784, 64) = 784
newfstatat(3, "", {st_mode=S_IFREG|0755, st_size=1926256, ...}, AT_EMPTY_PATH) = 0
pread64(3, "\6\0\0\0\4\0\0\0@\0\0\0\0\0\0\0@\0\0\0\0\0\0\0@\0\0\0\0\0\0\0"..., 784, 64) = 784
mmap(NULL, 1974096, PROT_READ, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7f540601b000
mmap(0x7f5406041000, 1396736, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0x26000) = 0x7f5406041000
```

```
write(1, "Hello, World!\n", 14Hello, World!
)          = 14
newfstatat(0, "", {st_mode=S_IFCHR|0620, st_rdev=makedev(0x88, 0x1), ...}, AT_EMPTY_PATH) = 0
read(0, 100
"100\n", 1024)                  = 4
write(1, "Input is 100\n", 13Input is 100
)          = 13
lseek(0, -1, SEEK_CUR)                  = -1 ESPIPE (Illegal seek)
exit_group(0)                           = ?
+++ exited with 0 +++
```

Lab — Can you see me?



Lab — Trace down the flag



Q & A