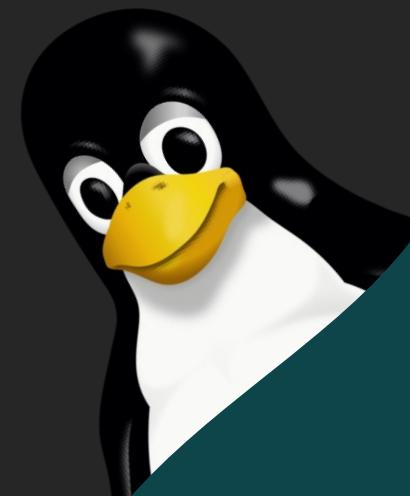




資安基礎

交戰守則 基礎操作手冊

SCIST @ OsGa



\$ whoami

#滲透測試 #安全強化 #網頁安全

OsGa / 黃宥睿

- 國立雲林科技大學
 - 資訊管理系 (人工智慧技優專班)
 - 網管小組系統組組長
 - YunHack 資安社創社社長
- OhYeahSeC 戰隊隊長 (CTF time 台灣第三)
- B33F 50UP 隊員
- 攻防演練攻擊手
- 超過百小時以上的分享經驗 (他校社團、活動)
- 活躍於各社群擔任 規劃、開發、出題
- Btw I use Vim

查看更多 -> <https://osga.dev>



<https://osga.dev>

\$ something u need know..

- 本簡報請配合 SCIST 直播或現場課程食用
- “可能” 會操作到 hackthebox 平台題目
 - 請在空餘時間註冊帳號
- 本日 lab: <https://linux.ctf.scist.org/>
- 請準備一台可以操作的 Linux 系統
- 有任何問題舉手問助教

\$ slido



\$ Outline

- What is CTF
- What is Linux
 - Linux history
- How 2 use / install Linux
- Linux base
- More skills about Linux

CTF、侵入
第壹話

\$ What is CTF

\$ What is 資安

\$ What is 資安

google.com

Google 資安

AI 模式 全部 新聞 圖片 購物 影片 短片 更多 工具

焦點新聞

iThome 【資安日報】10月15日，微軟、SAP發布10月例行更新
34分鐘前

數位時代 如何擋下網攻不破防？華碩資安長曝粗暴解方：強制推行15碼密碼，駭客就會「累到放...
2小時前

CTWANT 公部門資安專才短缺！羅美玲促數發部 強化培訓完善國安防護 | 政治 | CWTWANT
2小時前

三立新聞網SETN.com 攻擊自家資安系統...央廣工程師父親是連鎖電腦公司前董事
12小時前

更多新聞 >

iThome 資安
https://www.ithome.com.tw › security

8小時前 — 在2025年10月第二星期資安新聞中，駭客鎖定Oracle商業應用程式E-Business Suite (EBS)發動零時差漏洞攻擊是主要焦點，還有Red Hat資料外洩恐影響5千家企業的消息引發關注； ...

Microsoft 什麼是資訊安全(資安)？

資訊安全(通常簡稱資安)是一組安全性程序和工具，可廣泛地保護敏感性企業資訊，以免發生使用不當、未經授權的存取、中斷或毀損等狀況。資安涵蓋實體和環境安全性、存取控制 ...

資訊安全

資訊安全，意為保護資訊及資訊系統免受未經授權的進入、使用、披露、破壞、修改、檢視、記錄及銷毀。政府、軍隊、公司、金融機構、醫院、私人企業積累大量與雇員、顧客、產品、研究、金融資料有關的機密資訊，而絕大部分的資訊現在被收集、產生、儲存在電腦內，並透過網路傳送到別的電腦。

資料來源：維基百科

其他人也搜尋了

資料保護 電腦安全 保全 資訊科技

\$ What is 資安

google.com

Google 資安

AI 模式 全部 新聞 圖片 購物 影片 短片 更多 工具

聯合新聞網
治療師在醫院電腦加掛外部程式 輔大醫院今以危害資安解雇他
輔仁大學附設醫院治療師周姓員工，日前遭指控在院內電腦安裝「ngrok」代理伺服器與「RaiDrive」雲端硬碟掛載程式，...
2 天前

iThome
【資安日報】10月15日，微軟、SAP發布10月例行更新
微軟與SAP發布10月份例行更新，其中又以微軟修補175個漏洞，創下今年以來最多的記錄受到關注，值得留意的是，這次有3個漏洞已被用於實際攻擊，...
37 分鐘前

駭客相關新聞

奇摩新聞
攻擊自家資安系統...央廣工程師父親是連鎖電腦公司前董座
12 小時前

ETtoday新聞雲
央廣工程師攻擊自家資安系統！父親是連鎖電腦公司前董座
22 小時前

台視新聞網
1. 侵央廣前工程師竟是白宮

\$ What is 資安



你想像的資安

\$ What is 資安

實際上的資安



\$ What is 資安

目 頁



第三六 章 妨害電腦使用罪

第 358 條 無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。

第 359 條 無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。

第 360 條 無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。

第 361 條 對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。

第 362 條 製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。

第 363 條 第三百五十八條至第三百六十條之罪，須告訴乃論。



\$ What is 資安



\$ What is 資安

About Hacker

- 黑帽：
 - 蓄意利用漏洞做壞事（竊資料、植入勒索或販售漏洞）以謀私利或破壞，通常違法。
- 灰帽：
 - 介於黑與白之間，可能未經授權測試系統或公開弱點，但動機不完全惡意（有時會通知廠商、有時公開披露）。
- 白帽：
 - 受權限與道德規範的安全研究者／滲透測試者，負責找出並修補漏洞以保護系統。

\$ What is 資安

About Hacker

- 黑帽：
 - 蓄意利用漏洞做壞事（竊資料、植入勒索或販售漏洞）以謀私利或破壞，通常違法。
- 灰帽：
 - 介於黑與白之間，可能未經授權測試系統或公開弱點，但動機不完全惡意（有時會通知廠商、有時公開披露）。
- 白帽：
 - 受權限與道德規範的安全研究者／滲透測試者，負責找出並修補漏洞以保護系統。

\$ What is 資安

About Hacker

- 黑帽：
 - 蓄意利用漏洞做壞事（竊資料、植入勒索或販售漏洞）以謀私利或破壞，通常違法。
- 灰帽：
 - 介於黑與白之間，可能未經授權測試系統或公開弱點，但動機不完全惡意（有時會通知廠商、有時公開披露）。
- 白帽：
 - 受權限與道德規範的安全研究者／滲透測試者，負責找出並修補漏洞以保護系統。

\$ What is 資安

About Hacker

- 黑帽：
 - 蓄意利用漏洞做壞事（竊資料、植入勒索或販售漏洞）以謀私利或破壞，通常違法。
- 灰帽：
 - 介於黑與白之間，可能未經授權測試系統或公開弱點，但動機不完全惡意（有時會通知廠商、有時公開披露）。
- 白帽：
 - 受權限與道德規範的安全研究者／滲透測試者，負責找出並修補漏洞以保護系統。

\$ What is 資安

<https://zeroday.hitcon.org>

The screenshot shows the homepage of the ZeroDay platform. At the top, there is a navigation bar with links for '漏洞' (Vulnerabilities), '消息' (Messages), '排行榜' (Ranking), '組織' (Organization), '獎勵計劃' (Reward Plan), '人才媒合' (Talent Matching), '註冊 or 登入' (Register or Log In), and social media icons. The main banner features the 'ZeroDay' logo with a stylized 'D' containing a hat, and the tagline '值得信賴的漏洞通報平台' (A reliable vulnerability reporting platform). Below the banner, there are two sections: '最新消息' (Latest News) and '最新公開' (Latest Public). The '最新消息' section lists four items from 2020 to 2025. The '最新公開' section lists five items from 2020 to 2024.

About Hacker

https://zeroday.hitcon.org

漏洞 消息 排行榜 組織 獎勵計劃 人才媒合 註冊 or 登入

ZeroDay
值得信賴的漏洞通報平台

最新消息

- 2025 春節期間暫時停止服務
- 2022 春節期間暫時停止服務
- 2021 春節期間暫時停止服務
- 2020 春節期間暫時停止服務

最新公開

- 國立高雄科技大學 NI Web-based Monitoring 管理員帳號弱密碼
- 嗨膳海鮮宅配 (Design By 龍心數位科技) 搜尋功能 Reflected XSS
- 富狀元豬腳 id 參數存在 SQL Injection 漏洞
- 億品鍋 成大勝利店 點餐系統RCE

\$ What is CTF

\$ What is Catch The Flag

\$ What is CTF

\$ What is CTF

一種資訊安全的競賽

參賽隊伍依據競賽規則 利用各種駭客技術力

藉由解密或漏洞利用方式取得隱藏的 Flag

模擬實際攻擊時所需要獲得的資訊

\$ What is CTF

Flag

模擬資安攻擊時所需獲取得資訊 / 目標

透過攻擊手法 / 鑑識等資安技術獲取到 Flag

即可到競賽平台繳交獲得相對的分數

FLAG{*.*} / 比賽title{*.*}

分數 -> 排名 -> 競賽

\$ What is CTF

CTF 常見三大競賽模式

- Jeopardy:
 - 像線上解謎闖關遊戲，解出題目、拿到 flag 就能得分。
- Attack & Defense:
 - 同時要守護自己的服務不被攻破，也要找漏洞攻擊別人的伺服器來搶分。
- King of the Hill:
 - 搶下指定主機並盡量維持佔領，守得越久分數越高。

\$ What is CTF

CTF 常見三大競賽模式

- Jeopardy:
 - 像線上解謎闖關遊戲，解出題目、拿到 flag 就能得分。
- Attack & Defense:
 - 同時要守護自己的服務不被攻破，也要找漏洞攻擊別人的伺服器來搶分。
- King of the Hill:
 - 搶下指定主機並盡量維持佔領，守得越久分數越高。

\$ What is CTF

CTF 常見三大競賽模式

- Jeopardy:
 - 像線上解謎闖關遊戲，解出題目、拿到 flag 就能得分。
- Attack & Defense:
 - 同時要守護自己的服務不被攻破，也要找漏洞攻擊別人的伺服器來搶分。
- King of the Hill:
 - 搶下指定主機並盡量維持佔領，守得越久分數越高。

\$ What is CTF

CTF 常見三大競賽模式

- Jeopardy:
 - 像線上解謎闖關遊戲，解出題目、拿到 flag 就能得分。
- Attack & Defense:
 - 同時要守護自己的服務不被攻破，也要找漏洞攻擊別人的伺服器來搶分。
- King of the Hill:
 - 搶下指定主機並盡量維持佔領，守得越久分數越高。

\$ What is CTF

CTF 常見三大競賽模式

- Jeopardy:
 - 像線上解謎闖關遊戲，解出題目、拿到 flag 就能得分。
- Attack & Defense:
 - 同時要守護自己的服務不被攻破，也要找漏洞攻擊別人的伺服器來搶分。
- King of the Hill:
 - 搶下指定主機並盡量維持佔領，守得越久分數越高。

\$ What is CTF

CTF 題日常見分類



Crypto



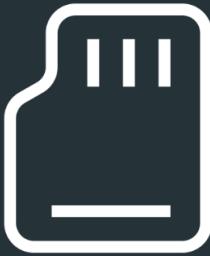
Reverse



Web Security



Forensic



Misc



Pwn

\$ What is CTF

CTF 題日常見分類

Web: 網站安全題，從前端或伺服器漏洞找出藏起來的 flag。

Crypto: 密碼學題，透過加密、解碼或數學運算破解訊息。

Forensics: 鑑識題，分析圖片、封包或記錄檔找線索。

Reverse: 反組譯題，把執行檔拆開，推回原本的邏輯找到 flag。

Pwn: 二進位漏洞利用題，透過程式漏洞取得控制權或 flag。

Misc: 其他類型的題目，像是隱寫、猜謎或開放情報 (OSINT) 等。

\$ What is CTF

CTF 題日常見分類

Web: 網站安全題，從前端或伺服器漏洞找出藏起來的 flag。

Crypto: 密碼學題，透過加密、解碼或數學運算破解訊息。

Forensics: 鑑識題，分析圖片、封包或記錄檔找線索。

Reverse: 反組譯題，把執行檔拆開，推回原本的邏輯找到 flag。

Pwn: 二進位漏洞利用題，透過程式漏洞取得控制權或 flag。

Misc: 其他類型的題目，像是隱寫、猜謎或開放情報 (OSINT) 等。

\$ What is CTF

CTF 題日常見分類

Web: 網站安全題，從前端或伺服器漏洞找出藏起來的 flag。

Crypto: 密碼學題，透過加密、解碼或數學運算破解訊息。

Forensics: 鑑識題，分析圖片、封包或記錄檔找線索。

Reverse: 反組譯題，把執行檔拆開，推回原本的邏輯找到 flag。

Pwn: 二進位漏洞利用題，透過程式漏洞取得控制權或 flag。

Misc: 其他類型的題目，像是隱寫、猜謎或開放情報 (OSINT) 等。

\$ What is CTF

CTF 題日常見分類

Web: 網站安全題，從前端或伺服器漏洞找出藏起來的 flag。

Crypto: 密碼學題，透過加密、解碼或數學運算破解訊息。

Forensics: 鑑識題，分析圖片、封包或記錄檔找線索。

Reverse: 反組譯題，把執行檔拆開，推回原本的邏輯找到 flag。

Pwn: 二進位漏洞利用題，透過程式漏洞取得控制權或 flag。

Misc: 其他類型的題目，像是隱寫、猜謎或開放情報 (OSINT) 等。

\$ What is CTF

CTF 題日常見分類

Web: 網站安全題，從前端或伺服器漏洞找出藏起來的 flag。

Crypto: 密碼學題，透過加密、解碼或數學運算破解訊息。

Forensics: 鑑識題，分析圖片、封包或記錄檔找線索。

Reverse: 反組譯題，把執行檔拆開，推回原本的邏輯找到 flag。

Pwn: 二進位漏洞利用題，透過程式漏洞取得控制權或 flag。

Misc: 其他類型的題目，像是隱寫、猜謎或開放情報 (OSINT) 等。

\$ What is CTF

CTF 題日常見分類

Web: 網站安全題，從前端或伺服器漏洞找出藏起來的 flag。

Crypto: 密碼學題，透過加密、解碼或數學運算破解訊息。

Forensics: 鑑識題，分析圖片、封包或記錄檔找線索。

Reverse: 反組譯題，把執行檔拆開，推回原本的邏輯找到 flag。

Pwn: 二進位漏洞利用題，透過程式漏洞取得控制權或 flag。

Misc: 其他類型的題目，像是隱寫、猜謎或開放情報 (OSINT) 等。

\$ What is CTF

CTF 題日常見分類

Web: 網站安全題，從前端或伺服器漏洞找出藏起來的 flag。

Crypto: 密碼學題，透過加密、解碼或數學運算破解訊息。

Forensics: 鑑識題，分析圖片、封包或記錄檔找線索。

Reverse: 反組譯題，把執行檔拆開，推回原本的邏輯找到 flag。

Pwn: 二進位漏洞利用題，透過程式漏洞取得控制權或 flag。

Misc: 其他類型的題目，像是隱寫、猜謎或開放情報 (OSINT) 等。

\$ What is CTF

電競比賽 ✓



\$ lab time

FLAG{OsGa.dev/Linux.pdf}

Lab: Slides

<https://linux.ctf.scist.org/challenges#Slides-1>

Linux 補完計劃 伺服器 使徒 第貳話

\$ What is Linux

\$ What is Linux

About Linux story

- 因為當時市面上的作業系統不是免費就是封閉，使用限制多。
- 創作者 Linus Torvalds 想在自己的 PC (Intel 80386) 上使用類 UNIX 的系統，但現有選擇不夠理想。
- 他希望建立一個「自由／開源」的系統，讓任何人都能查看、修改源碼。
- 它的出現填補了 GNU 計畫在核心 (kernel) 方面的空缺

\$ What

About L

- 因為當時
- 創作者 Linus Torvalds 在當時的 UNIX 的
- 他希望建立一個可以被他人
- 源碼。
- 它的出現，



formoflife.blog 1d

...

當你感到焦慮落後的時候，請你記得這個人直到 21 歲才把 Linux 開發出來 Translate



別多。
使用類
查看、修改

2.3K

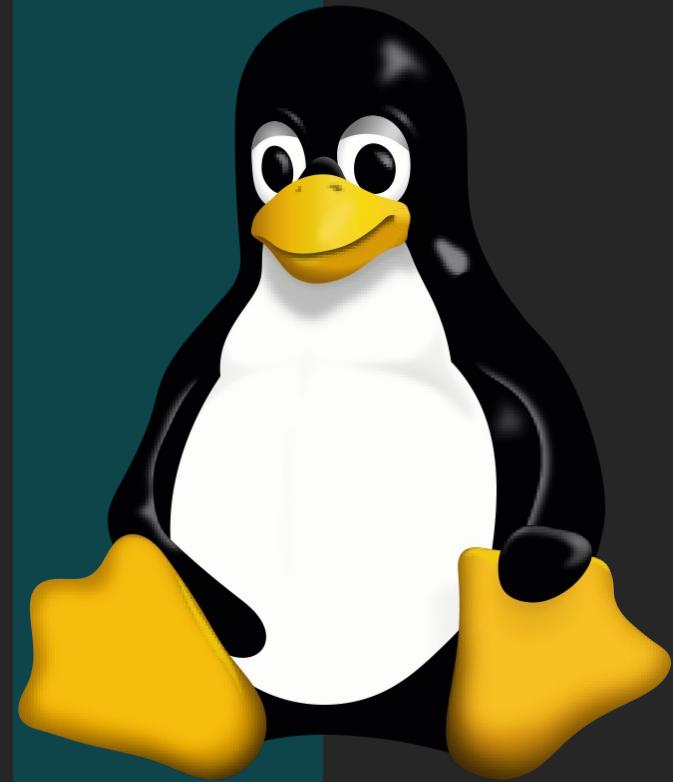
213

193

676

\$ What is Linux

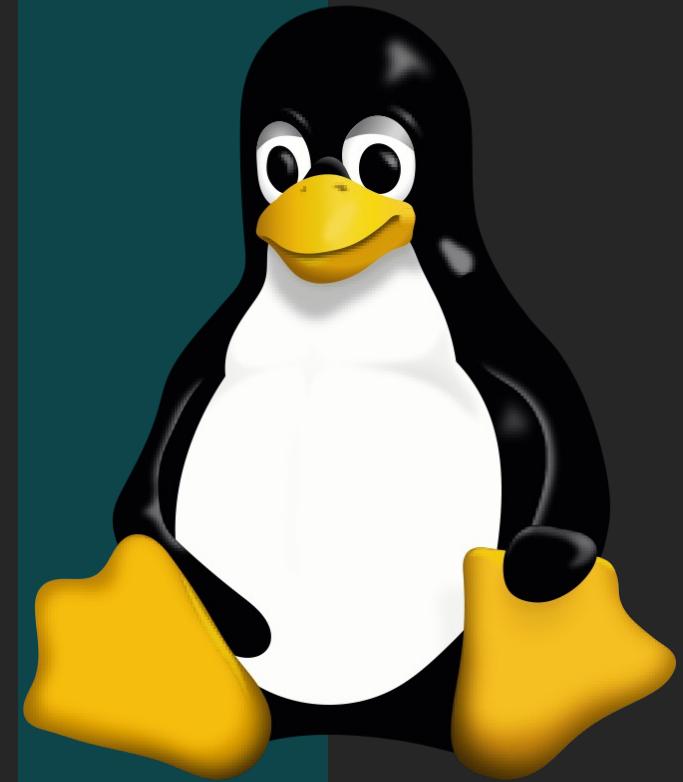
Basic concept



\$ What is Linux

Basic concept

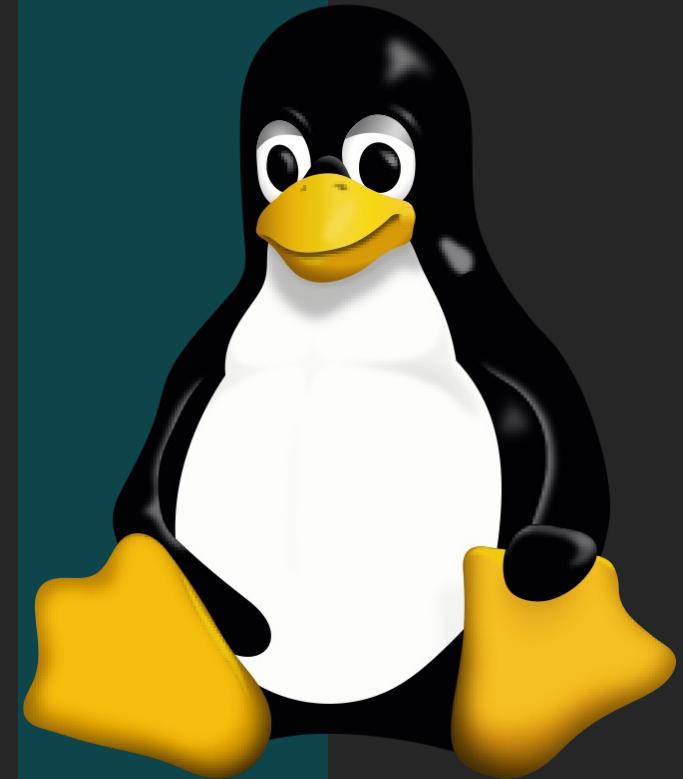
- Linux is an Operating System
- Open Source
- Based on the UNIX design
- Highly Customizable
- Stable and Secure
- Runs on servers, desktops, and embedded systems
- ~~F**k Microsoft~~



\$ What is Linux

Basic concept

- Linux is an Operating System
- Open Source
- Based on the UNIX design
- Highly Customizable
- Stable and Secure
- Runs on servers, desktops, and embedded systems
- ~~F**k Microsoft~~



\$ What is Linux

Operating System



Windows 11



\$ What is Linux

Operating System



Windows 11



\$ What is Linux

Operating System



\$ What is Linux

A screenshot of a GitHub repository page for the Linux kernel. The URL in the address bar is `github.com/torvalds/linux`. The repository is public and has 1,396,997 commits. It features 1 branch and 903 tags. The repository is maintained by Linus Torvalds, with the latest commit being a merge tag from the rust-rustfmt project. The repository has 205k stars, 7.7k watchers, and 57.9k forks.

The repository page includes sections for About, Releases, Packages, and Contributors. The About section provides details about the Linux kernel source tree, including links to Readme, View license, Activity, and Report repository. The Releases section lists 903 tags. The Packages section indicates no packages have been published. The Contributors section shows over 5,000 contributors, with small profile pictures for many of them.

About

Linux kernel source tree

- Readme
- View license
- Activity
- 205k stars
- 7.7k watching
- 57.9k forks

Report repository

Releases

903 tags

Packages

No packages published

Contributors 5,000+

\$ What is Linux

github.com

torvalds / linux

Type / to search

Code Pull requests Actions Projects Security Insights

linux Public

Watch 7736 Fork 57.9k

master 1 Branch 903 Tags

Go to file Add file Code

torvalds Merge tag 'rust-rustfmt' of git://git.kernel.org/pub/scm/linux/kernel... 1c64efc · 11 hours ago 1,396,997 Commits

Documentation Merge tag 'rust-rustfmt' of git://git.kernel.org/pub/scm/linux/kernel... 11 hours ago

LICENSES LICENSES: Replace the obsolete address of the FSF in th... 3 months ago

arch Merge tag 'for-linus' of git://git.kernel.org/pub/scm/virt/kv... 14 hours ago

block Merge tag 'block-6.18-20251016' of git://git.kernel.org/pu... 2 days ago

certs sign-file,extract-cert: use pkcs11 provider for OPENSSL M... last year

crypto Merge tag 'v6.18-p3' of git://git.kernel.org/pub/scm/linux/... last week

drivers Merge tag 'tpmdd-next-v6.18-rc2' of git://git.kernel.org/p... 12 hours ago

fs Merge tag 'exfat-for-6.18-rc2' of git://git.kernel.org/pub/s... 13 hours ago

include Merge tag 'hid-for-linus-2025101701' of git://git.kernel.or... 12 hours ago

init Merge tag 'printk-for-6.18' of git://git.kernel.org/pub/scm/... 2 weeks ago

io_uring Merge tag 'io_uring/rw: check for NULL io_br_sel when putting a buff... 3 days ago

ipc Merge tag 'namespace-6.18-rc1' of git://git.kernel.org/pu... 3 weeks ago

About

Linux kernel source tree

Readme View license Activity 205k stars 7.7k watching 57.9k forks

Report repository

Releases 903 tags

Packages No packages published

Contributors 5,000+

KALI

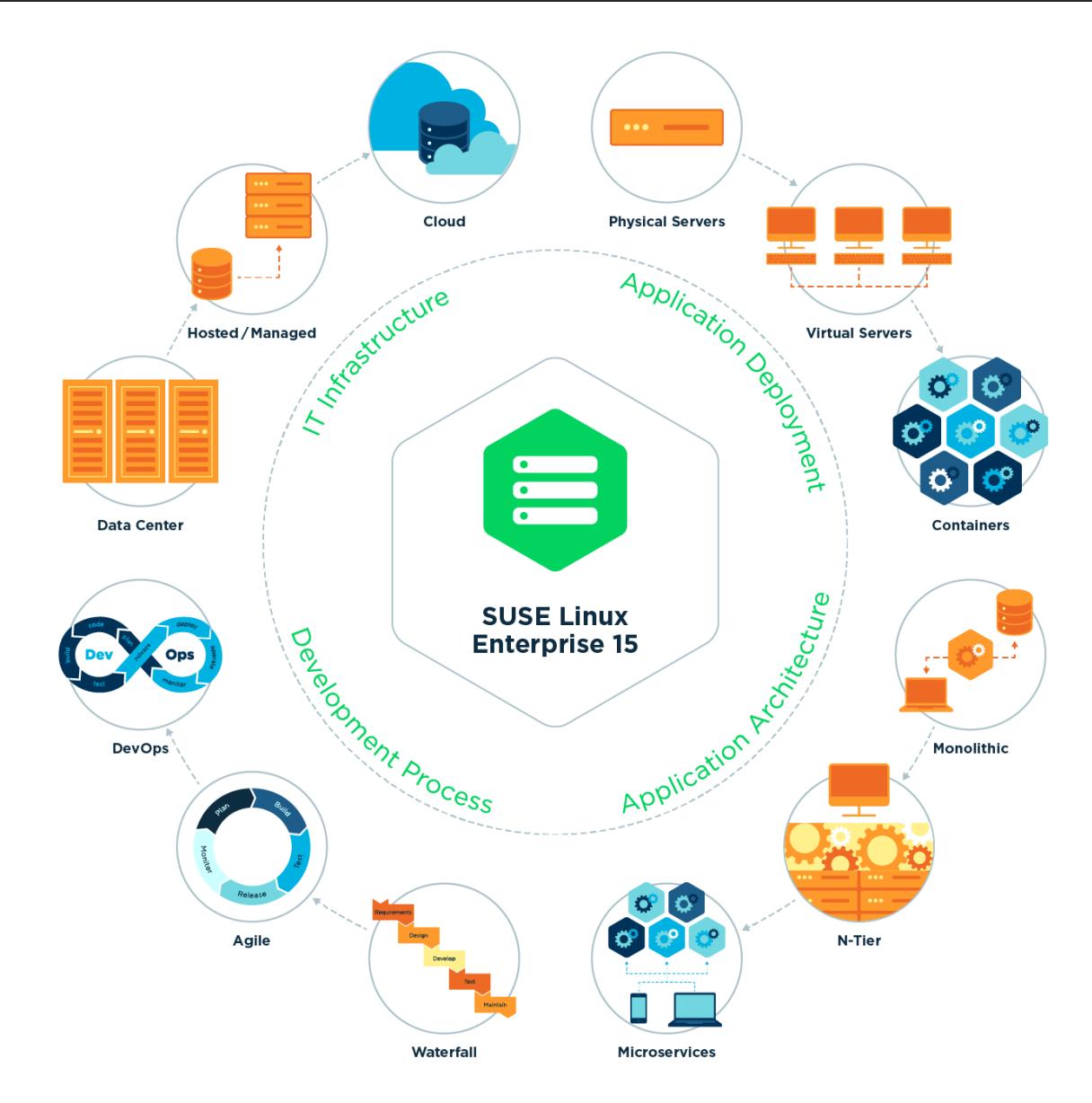
\$ What is Linux

Runs on servers, desktops, and embedded systems

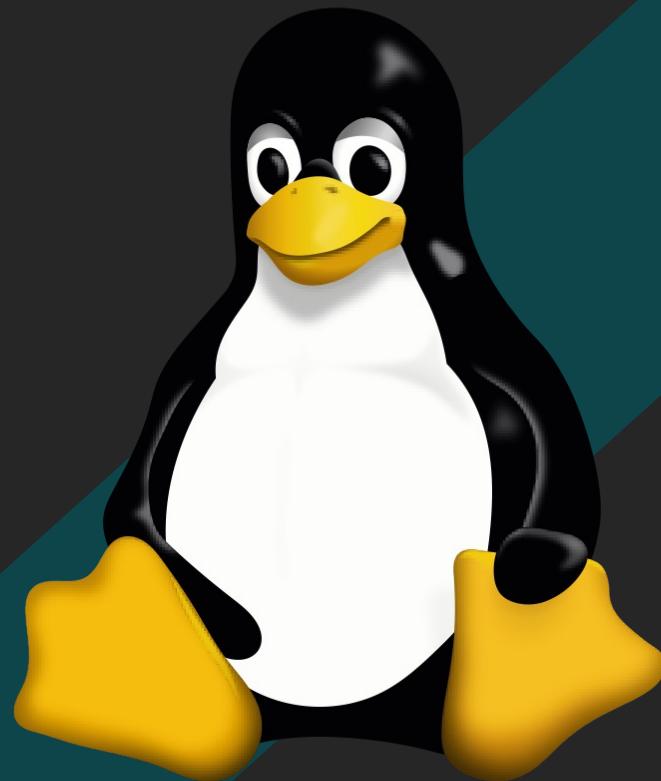
\$ What is Linux

Runs on

systems



\$ What is Linux



健
康
安
樂

第參話

\$ How 2 install Linux

\$ How 2 install Linux

- VM (虛擬機)
- Sub System
- 雙系統 (一台電腦同時安裝不同系統)
- ALL IN Linux

\$ How 2 install Linux

- VM (虛擬機)
- Sub System
- 雙系統 (一台電腦同時安裝不同系統)
- ALL IN Linux

\$ How 2 install Linux

- **VM (虛擬機)**

- VMware
- Virtual Box

- **Sub System**

- WSL
- Orb (類 docker)

\$ How 2 install Linux

- **VM (虛擬機)**

- 不會影響主系統，可安全測試與練習。
- 可同時運行多個系統（例如 Windows 與 Linux 共存）。
- 方便重置、快照、備份與還原。
- 節省硬體資源，不需額外安裝實體電腦。
- 方便練習指令、伺服器設定或網路實驗。
- 可隨時刪除或更換不同 Linux 發行版。

\$ How 2 install Linux

• 使用 VM 的優點

- 不會影響主系統，可安全測試與練習。
- 可同時運行多個系統（例如 Windows 與 Linux 共存）。
- 方便重置、快照、備份與還原。
- 節省硬體資源，不需額外安裝實體電腦。
- 方便練習指令、伺服器設定或網路實驗。
- 可隨時刪除或更換不同 Linux 發行版。

\$ How 2 install Linux

- **使用 VM 的缺點**

- 效能較低：虛擬機需要同時運行主系統與虛擬系統，佔用記憶體與 CPU。
- 硬體加速受限：無法完整使用顯示卡、USB 裝置或特殊硬體功能。
- 儲存空間占用大：虛擬磁碟檔案 (.vdi、.vmdk) 可能佔用數十 GB。
- 無法完全模擬真實環境：與實體安裝相比，有些驅動或網路設定行為不同。

\$ How 2 install Linux

- **使用 Sub System 的優點**

- 無需安裝虛擬機或重開機即可在 Windows 中使用 Linux
- 效能接近原生，啟動速度快
- 可直接使用 Linux 指令與套件管理（如 apt、bash）
- 能與 Windows 系統共用檔案與路徑
- 方便開發者進行程式開發、伺服器模擬與測試

\$ How 2 install Linux

- **使用 Sub System 的缺點**

- 硬體整合有限 (如 USB、藍牙裝置支援不完全) 。
- 效能仍略低於原生安裝或完整虛擬機。
- 某些低階系統功能或模組 (例如 kernel module、systemd 服務)
在舊版 WSL 不支援。

\$ How 2 install Linux

• 一些注意事項

- 注意自己電腦是否有足夠的儲存空間
- Windows 用戶要先於 bios 設定開啟虛擬化
 - 相關文件
- 注意電腦的系統架構
 - Mac M 系列晶片 (ARM)
 - Intel、AMD 相關 (x86)
- VM 安裝教學 by SCIST fearnnot

第肆話

始、用

\$ Linux base

\$ Linux base

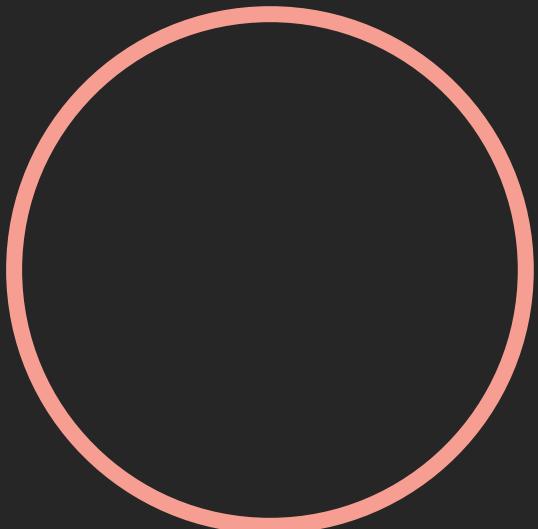
使用者群組

\$ Linux base

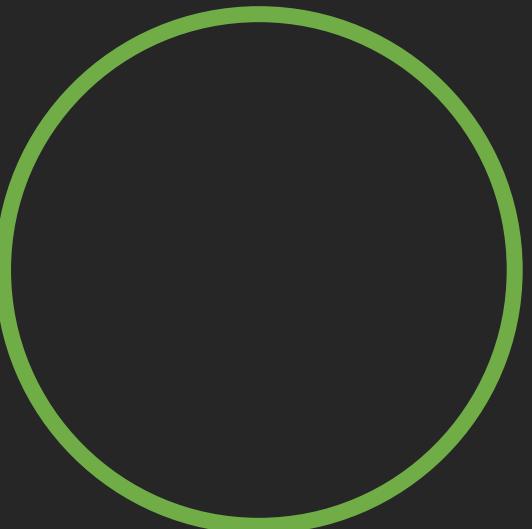
User

\$ Linux base

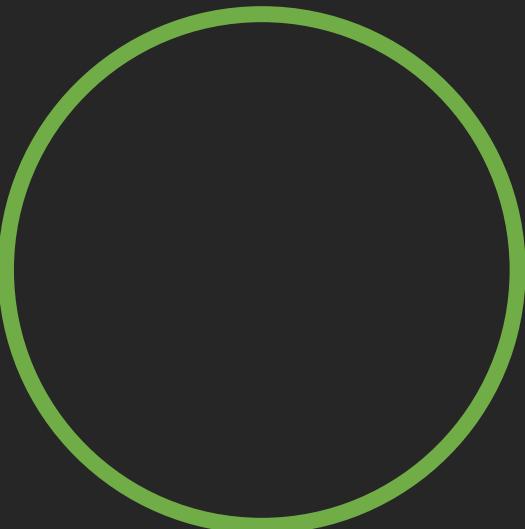
User Group



root



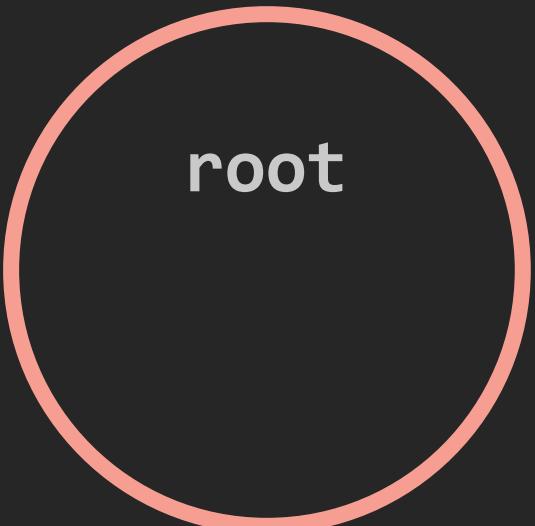
sudo



user

\$ Linux base

User Group



root



sudo

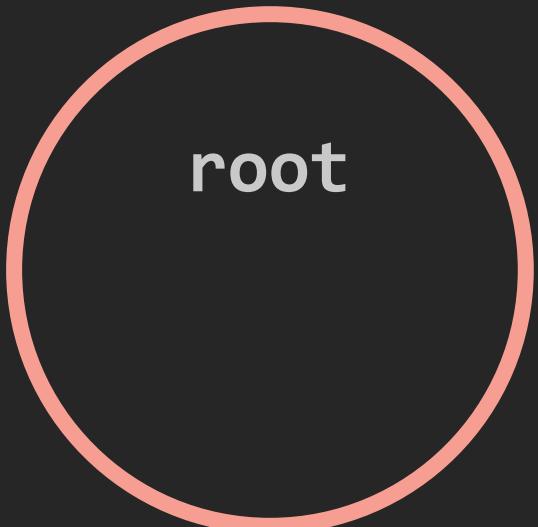


OsGa

\$ Linux base

User Group

如果 OsGa 是第一個使用者



root



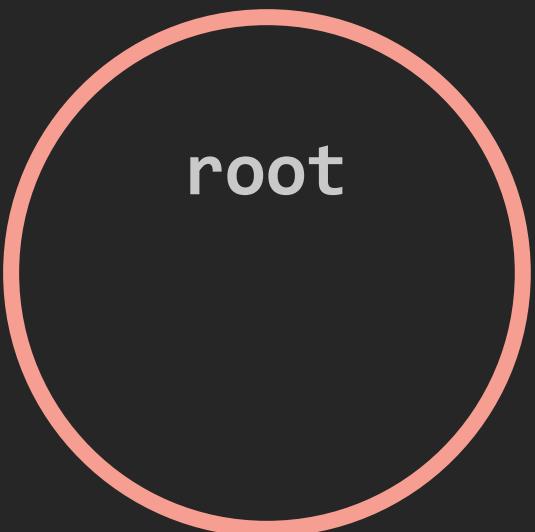
sudo



OsGa

\$ Linux base

User Group



root



sudo



OsGa

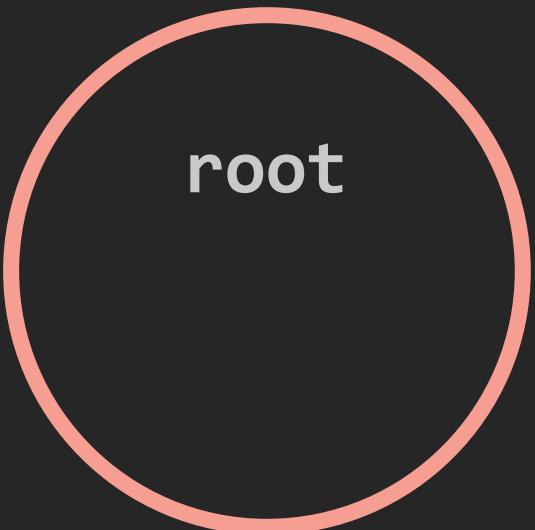
新使用者 - Tony



Tony

\$ Linux base

User Group



root



sudo

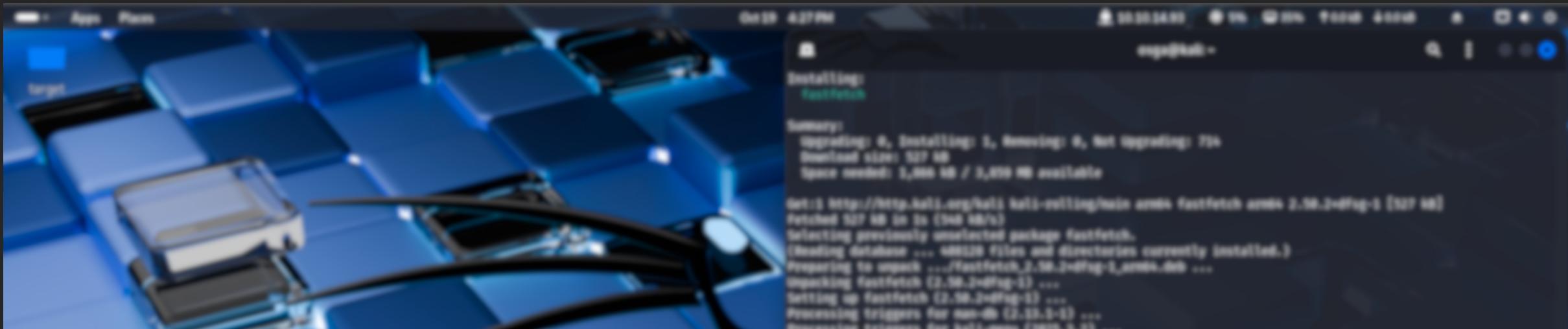


OsGa

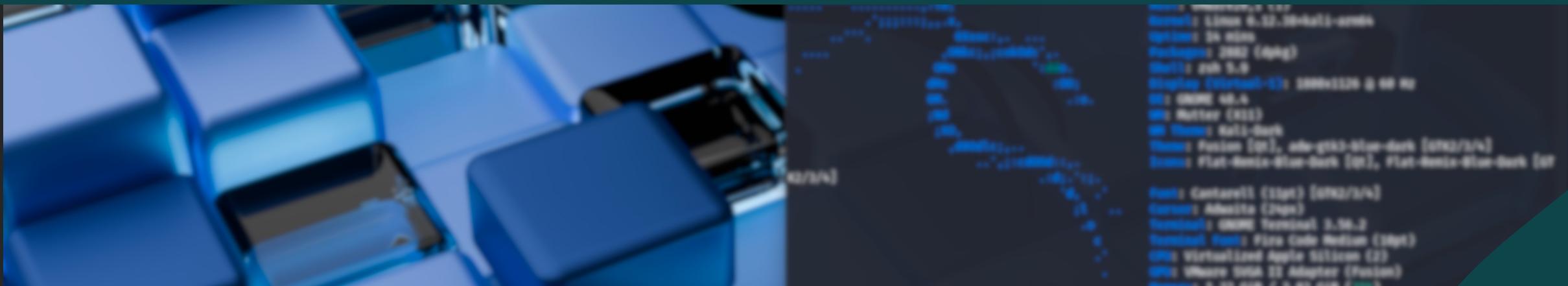


Tony

\$ Linux base

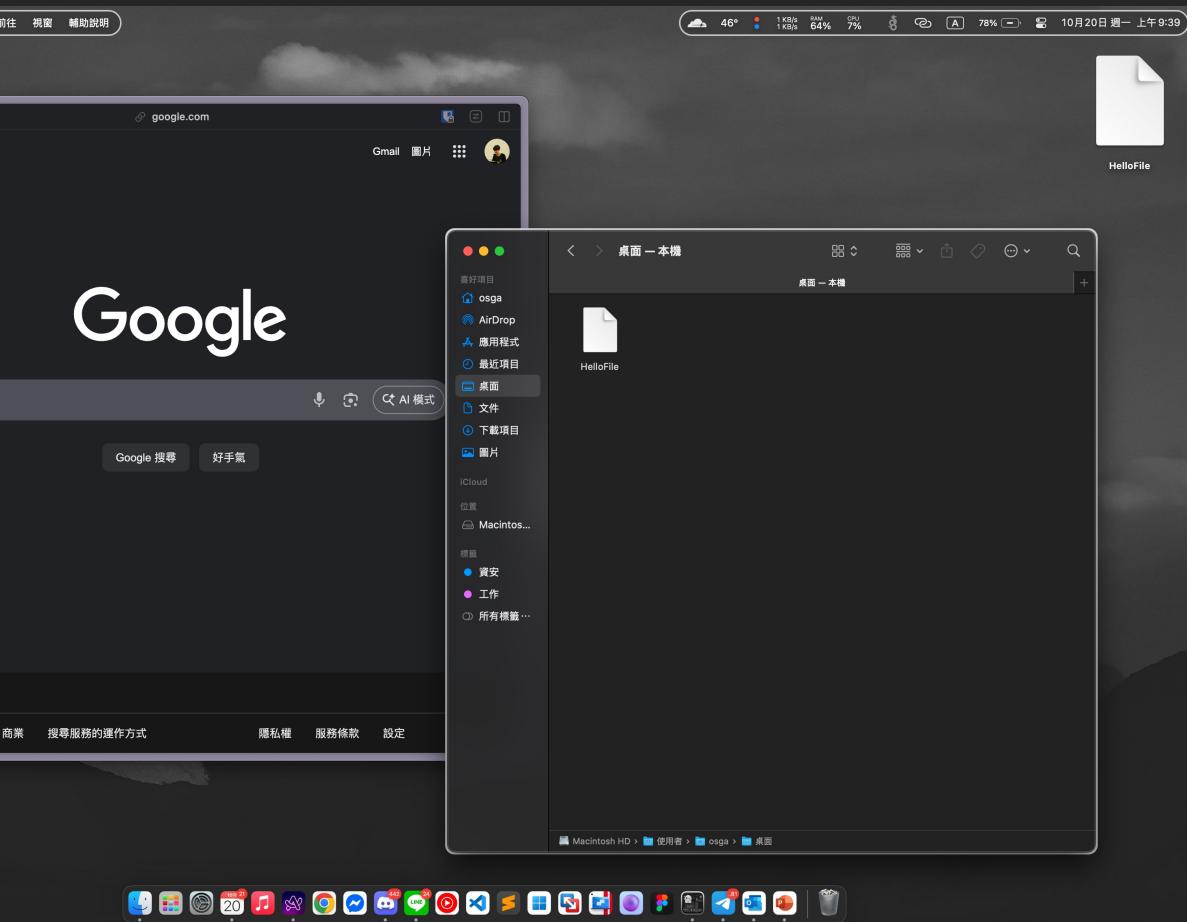


GUI vs CLI



\$ Linux base

GUI vs CLI

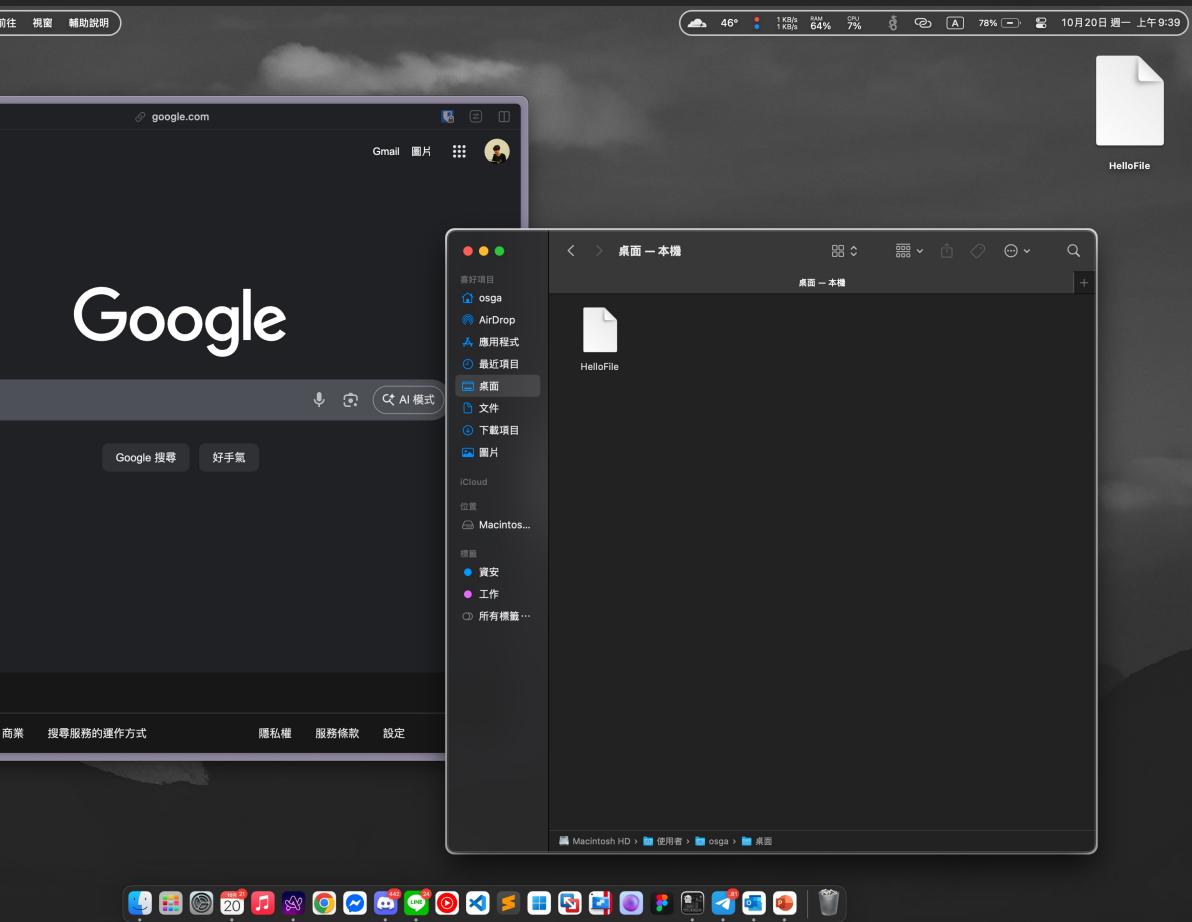


```
osga@OsGa-mbp ~ % cd ~/Desktop
osga@OsGa-mbp ~ % ls
osga@OsGa-mbp ~ % touch HelloFile
osga@OsGa-mbp ~ %
```

\$ Linux base

GUI vs CLI

那麼麻煩為什麼要使用 CLI ?



```
osga@0sGa-mbp ~ % cd ~/Desktop  
osga@0sGa-mbp ~ % ls  
HelloFile  
osga@0sGa-mbp ~ %
```

A screenshot of a terminal window titled "zsh*". The window shows a command-line session where the user has navigated to the ~/Desktop directory and listed files. A file named "HelloFile" is visible in the list. The terminal window has a dark theme with blue text for output and red text for errors.

\$ Linux base

GUI vs CLI

那麼麻煩為什麼要使用 CLI ?

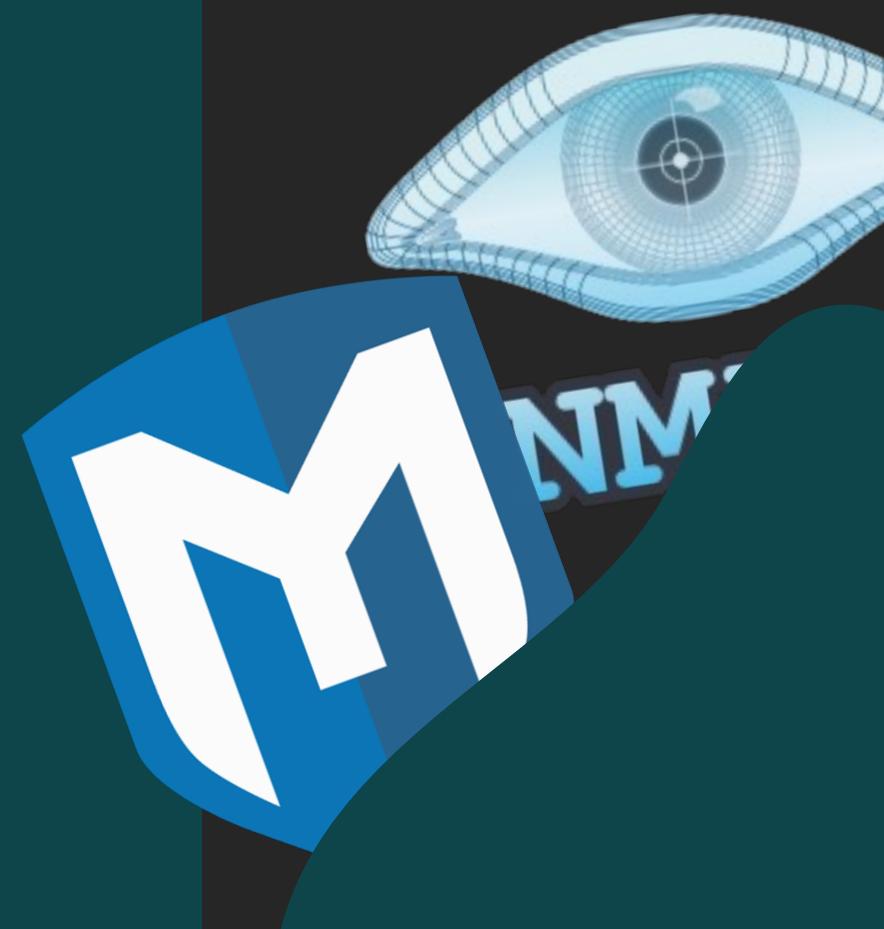
- 操作速度快，不需等待圖形介面載入
- 手只要維持在鍵盤，不需要透過滑鼠操作
- 佔用資源少，適合遠端或低效能環境
- 許多好用工具都透過指令操作
- 可自動化操作（透過指令串接或 Shell Script）
- 精準控制系統與程式行為
- 記錄與重現性高，方便除錯與教學
- 幾乎所有 Linux 系統都內建，通用性強
- 看起來比較像電影裡的駭客

\$ Linux base

GUI vs CLI

那麼麻煩為什麼要使用 CLI ?

- 操作速度快，不需等待圖形介面載入
- 手只要維持在鍵盤，不需要透過滑鼠操作
- 佔用資源少，適合遠端或低效能環境
- 許多好用工具都透過指令操作
- 可自動化操作（透過指令串接或 Shell Script）
- 精準控制系統與程式行為
- 記錄與重現性高，方便除錯與教學
- 幾乎所有 Linux 系統都內建，通用性強
- 看起來比較像電影裡的駭客

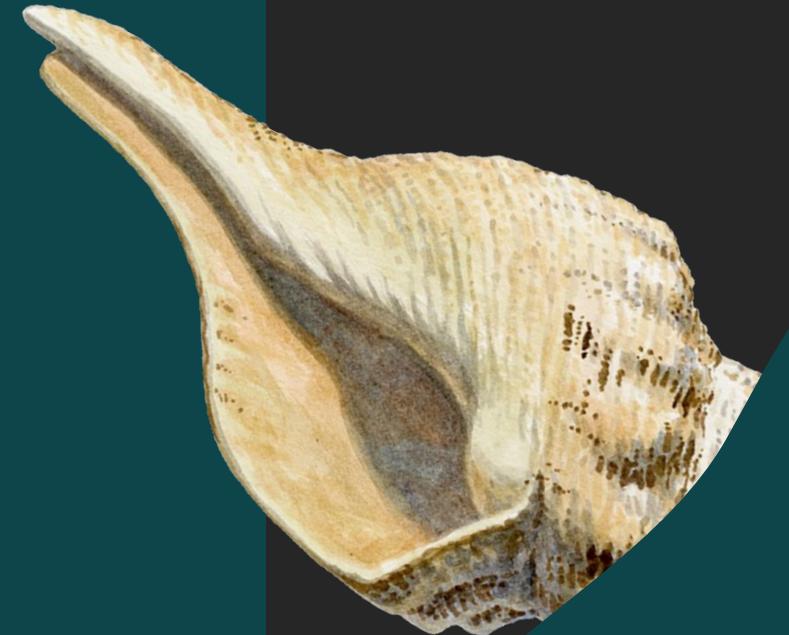


\$ Linux base
CLI - \$shell



\$ Linux base CLI - \$shell

- Shell 是使用者與作業系統之間的介面
- 可透過命令列 (CLI) 輸入指令來操作系統
- 負責接收指令、執行並回傳結果
- 常見的 Shell 有 Bash、Zsh、Fish 等
- 可撰寫 Shell Script 自動化多步驟任務
- 在 Linux、macOS、WSL 等系統中皆可使用
- 是系統管理與開發中最核心的工具之一



```
$ Linux base  
CLI - $shell
```

- Shell 是使用者與作業系統之間的介面
- 可透過命令列 (CLI) 輸入指令來操作系統
- 負責接收指令、執行並回傳結果
- 常見的 Shell 有 Bash、Zsh、Fish 等
- 可撰寫 Shell Script 自動化多步驟任務
- 在 Linux、macOS、WSL 等系統中皆可使用
- 是系統管理與開發中最核心的工具之一

```
echo $SHELL
```



\$ Linux base
CLI

\$ Linux base CLI

- Who am I
- Where am I
- What should I do

\$ Linux base CLI

- Who am I
- Where am I
- What should I do

osga@kali:~\$ ls

\$ Linux base CLI

- Who am I
- Where am I
- What should I do

osga@kali:~\$ ls

\$ Linux base CLI

- Who am I
- Where am I
- What should I do

osga@kali:~\$ ls

\$ Linux base CLI

- Who am I
- Where am I
- What should I do

osga@kali:/tmp\$ ls

\$ Linux base CLI

- Who am I
- Where am I
- What should I do

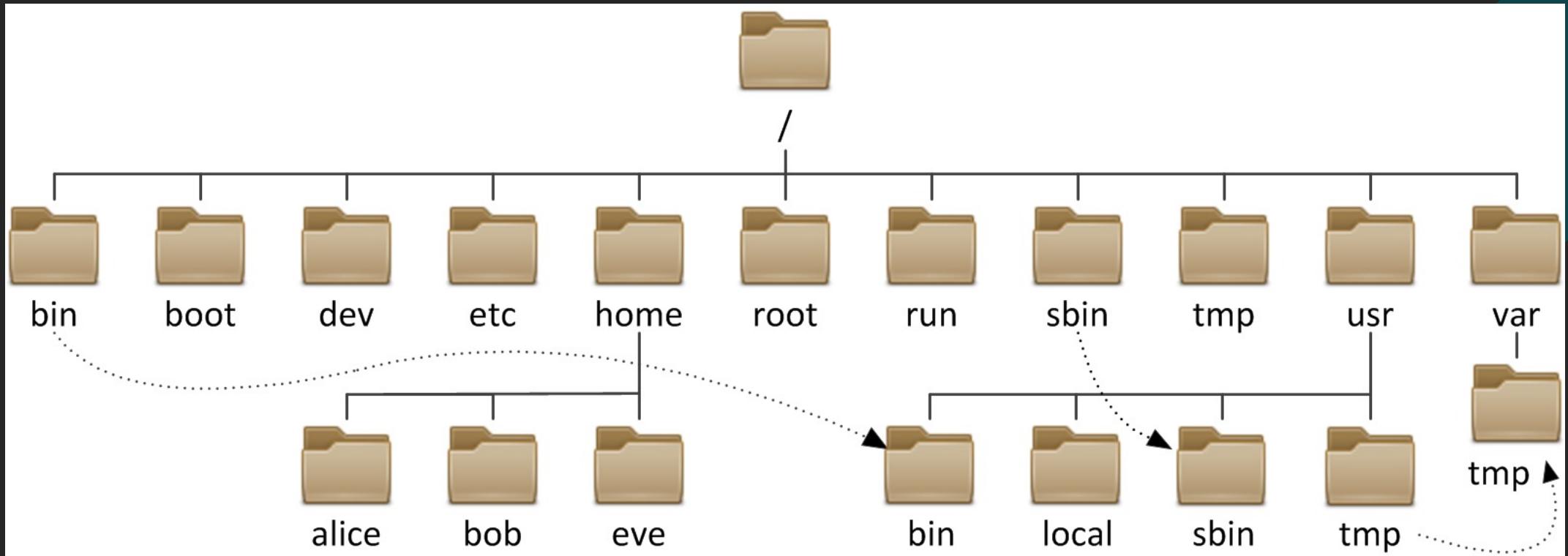
osga@kali:~\$ ls

\$ Linux base CLI

- Where am I

\$ Linux base CLI - Directory Structure

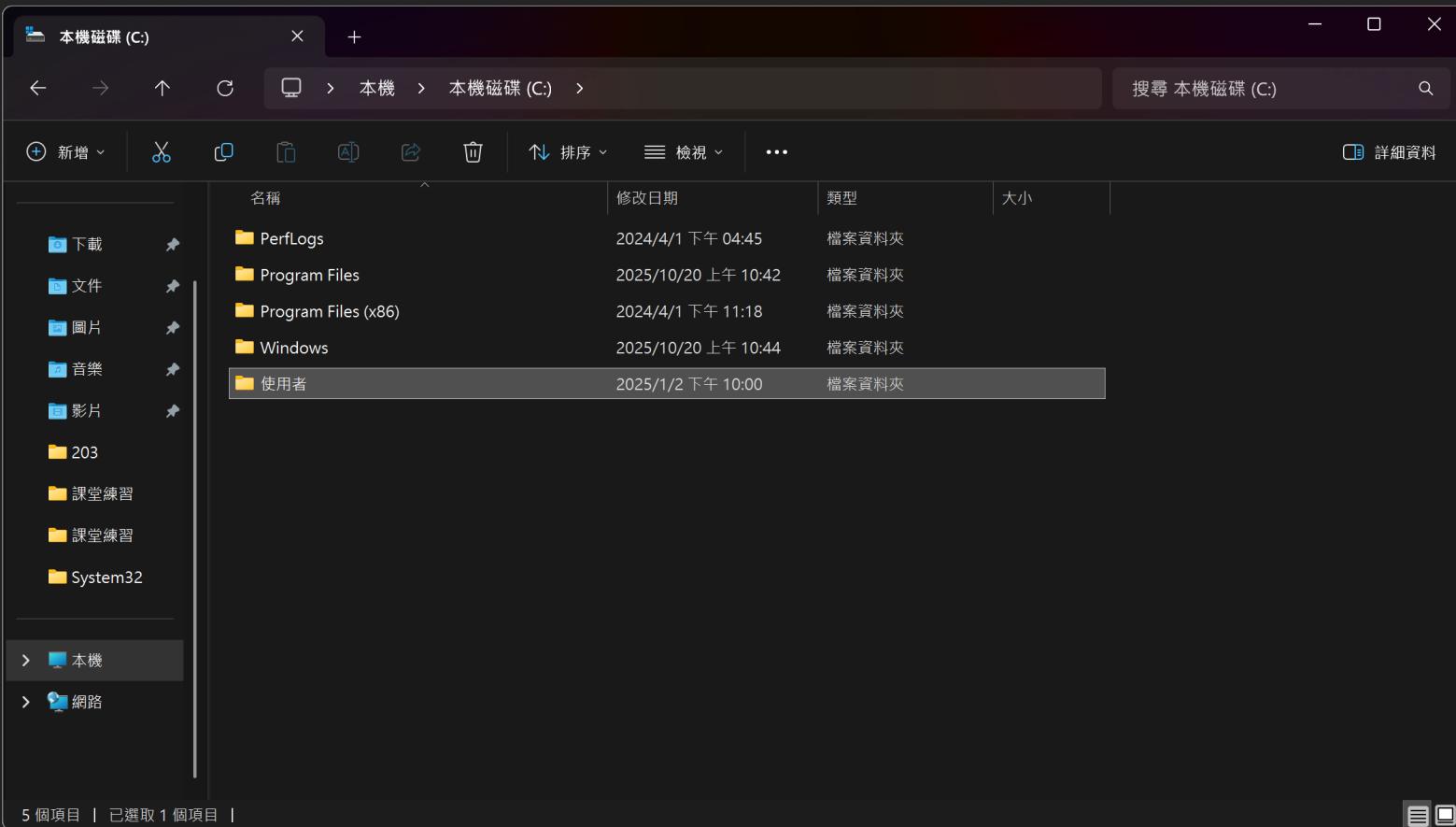
\$ Linux base CLI - Directory Structure



\$ Linux base

CLI - Directory Structure

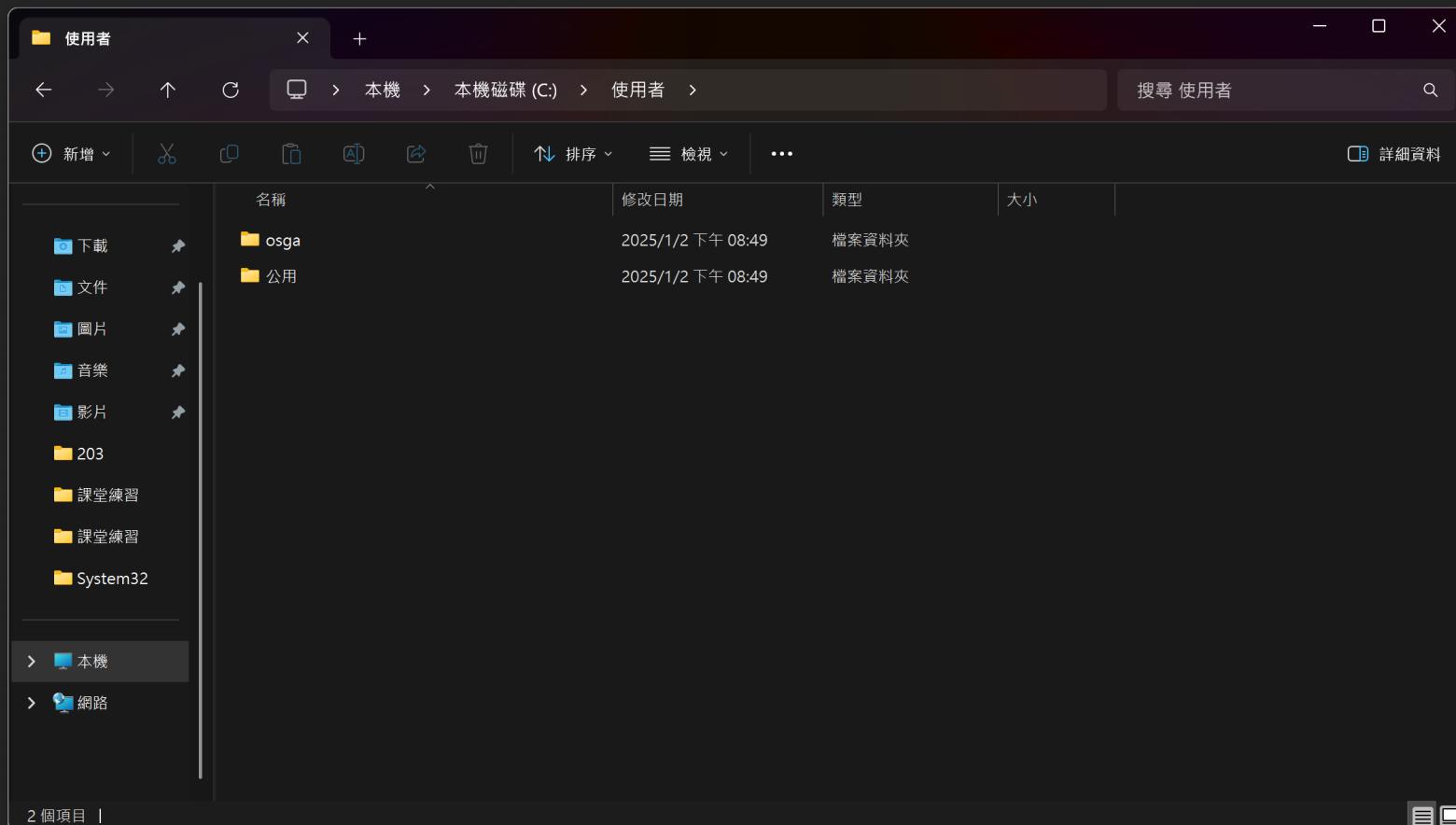
C:\



\$ Linux base

CLI - Directory Structure

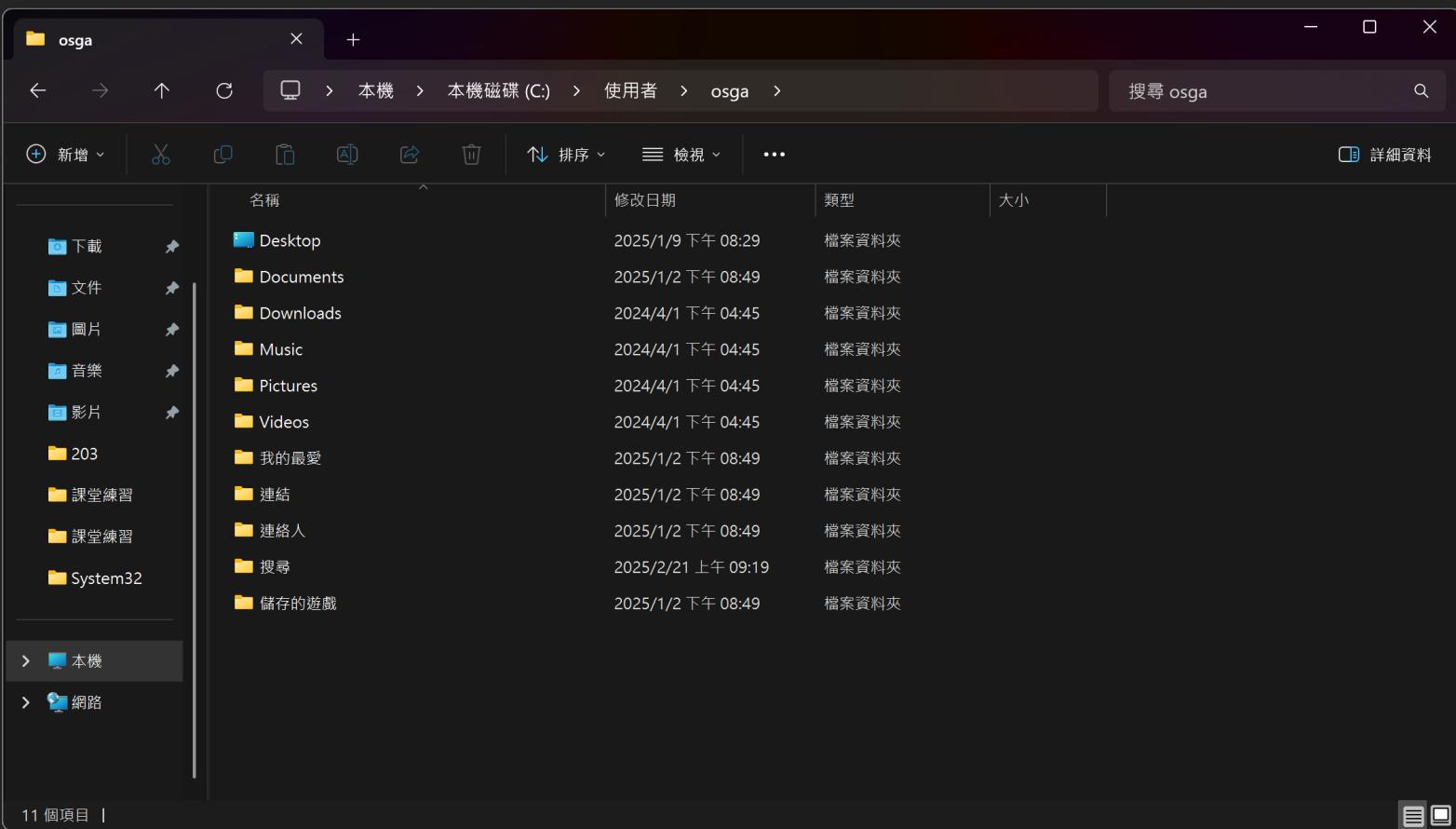
C:\Users



\$ Linux base

CLI - Directory Structure

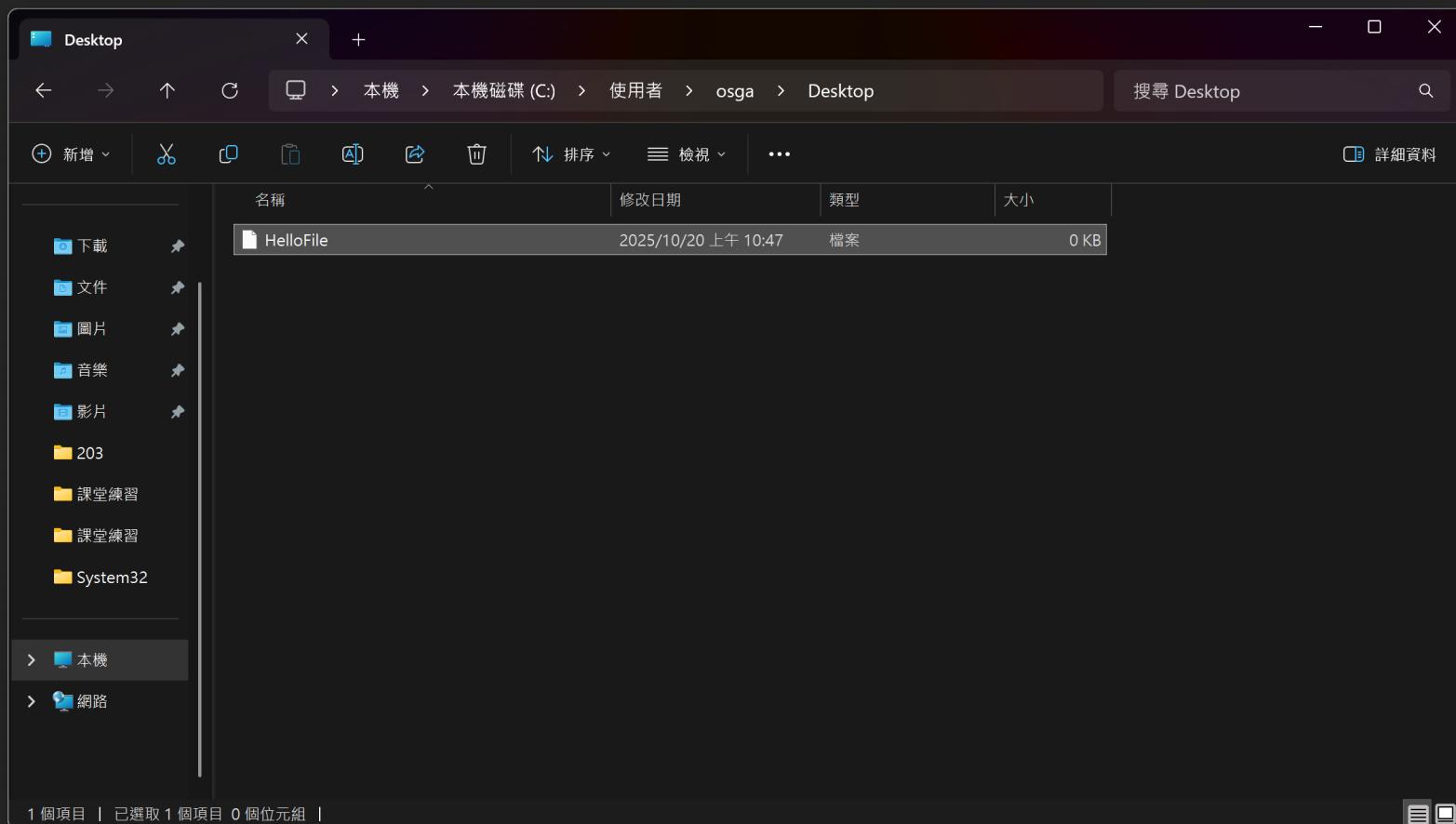
C:\Users\osga



\$ Linux base

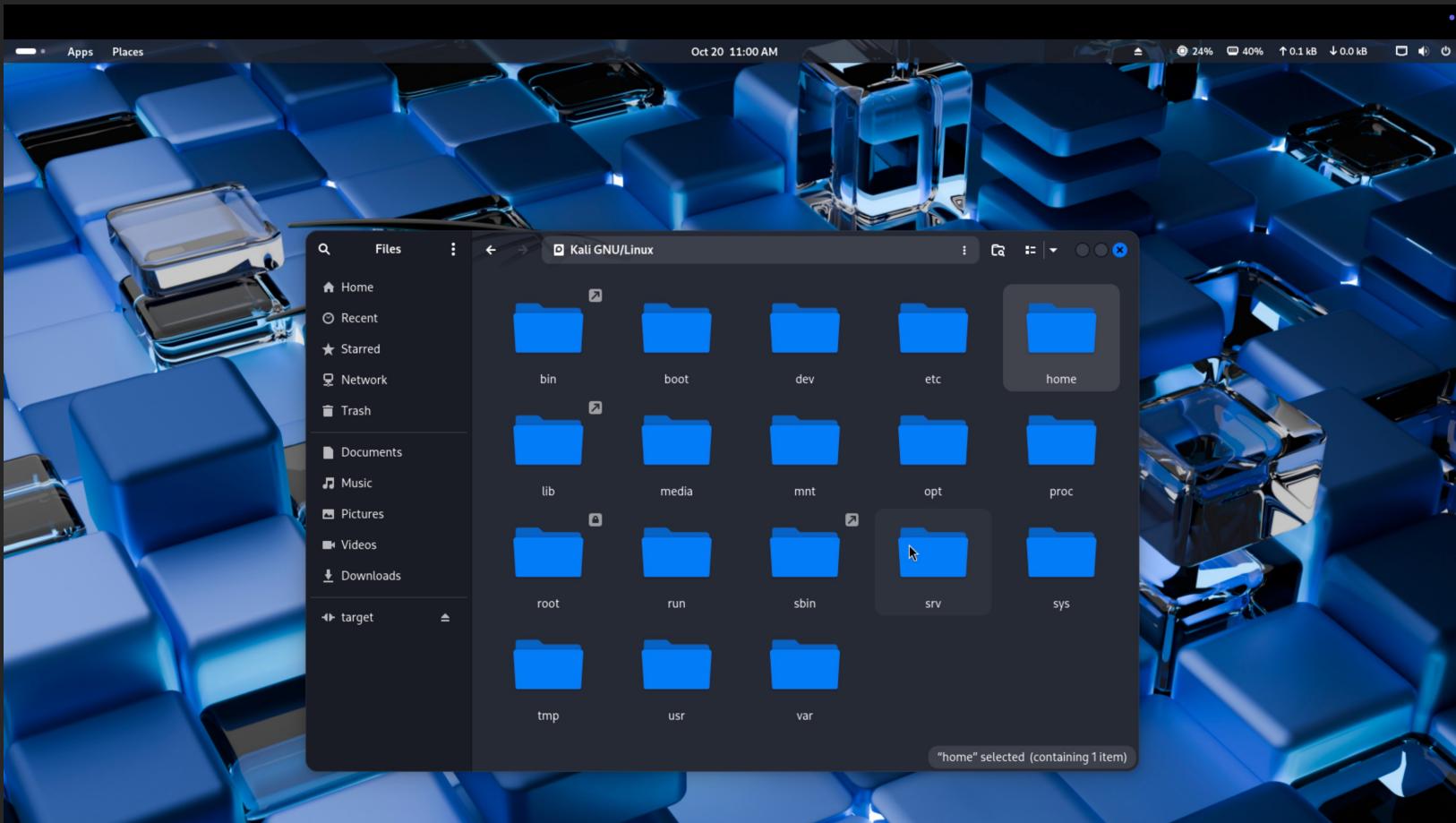
CLI - Directory Structure

C:\Users\osga\Desktop



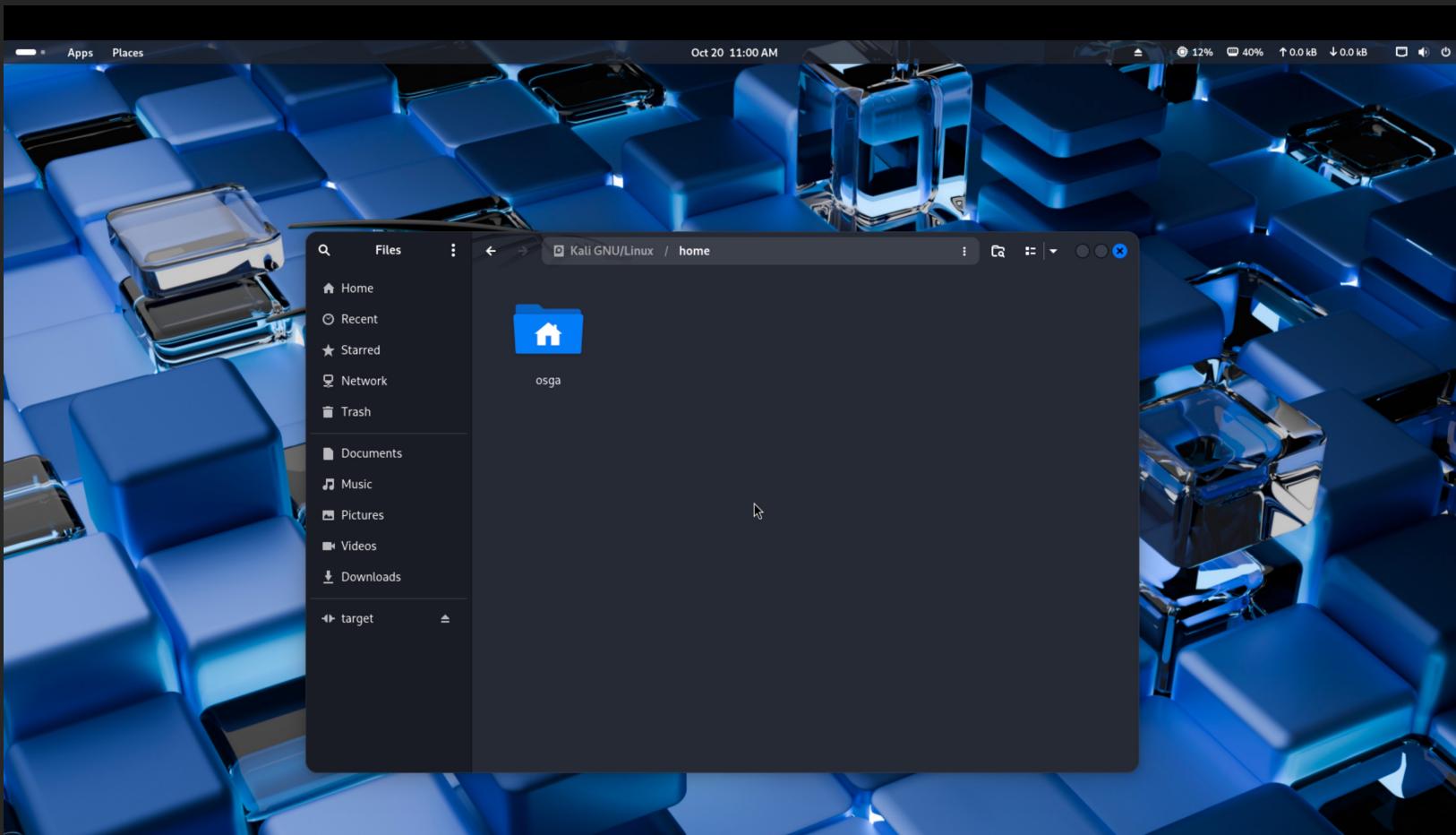
\$ Linux base CLI - Directory Structure

/



\$ Linux base CLI - Directory Structure

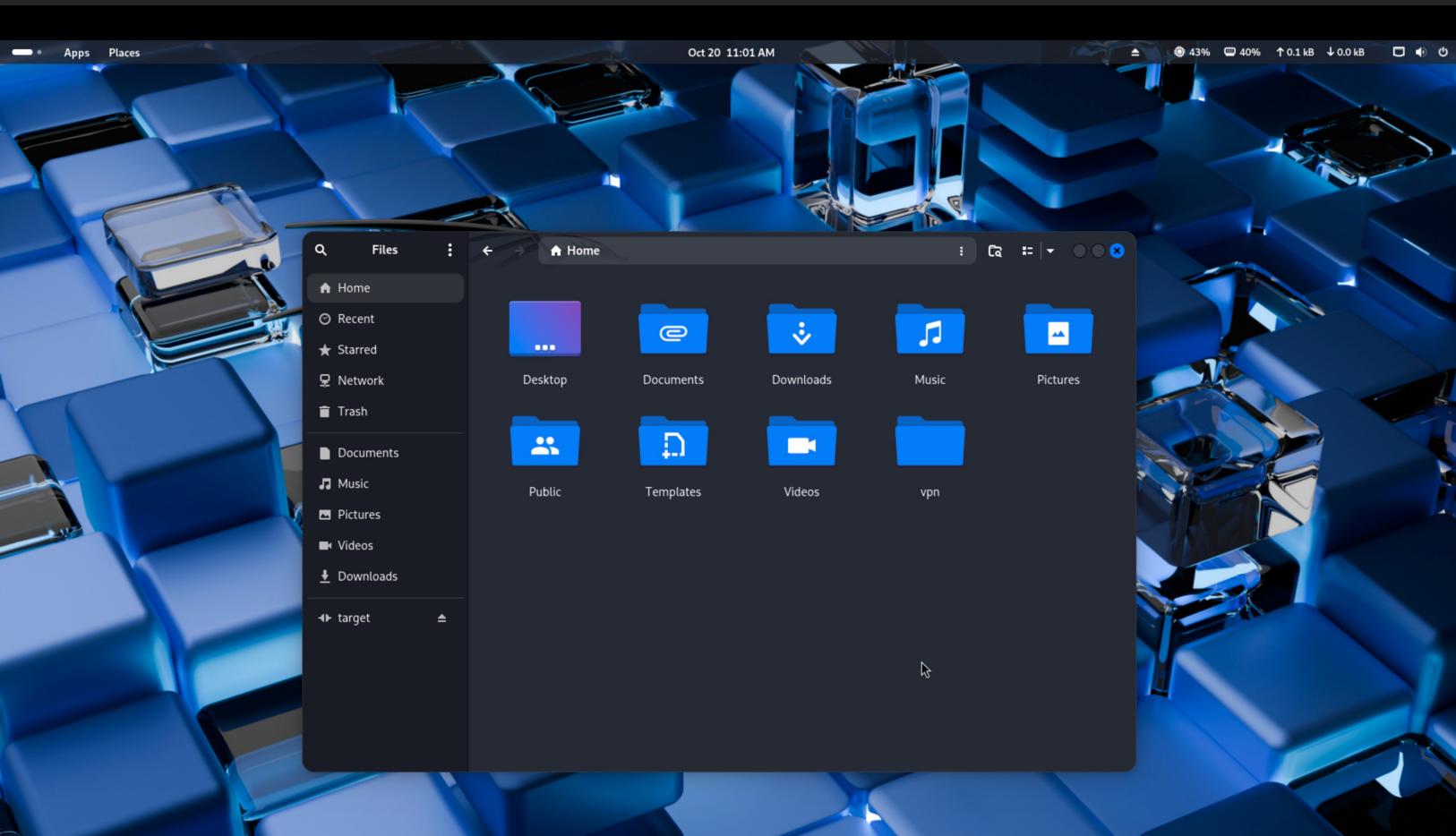
/home



\$ Linux base

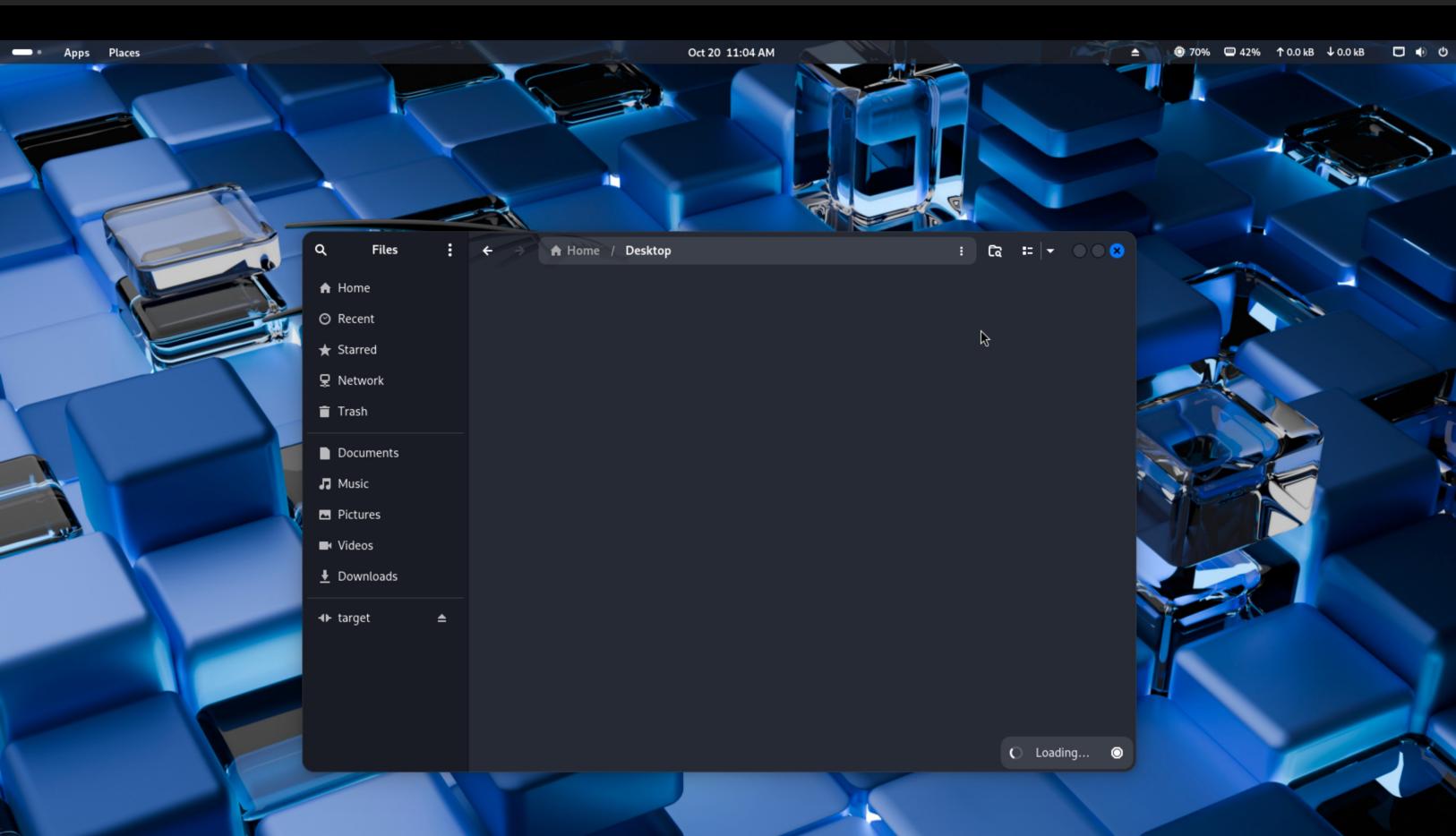
CLI - Directory Structure

/home/osga



\$ Linux base CLI - Directory Structure

/home/osga/Desktop



\$ Linux base

CLI - Directory Structure

- 所有目錄都建立於 / (根目錄)
- 副檔名並不重要
 - 檔案 test 在 osga 的桌面
 - /home/osga/Desktop/test
- 結尾加上 / 為目錄，但不加也行
 - 架設 testFolder 是一個在 osga 桌面的資料夾
 - /home/osga/Desktop/testFolder/
 - /home/osga/Desktop/testFolder

\$ Linux base CLI - Directory Structure

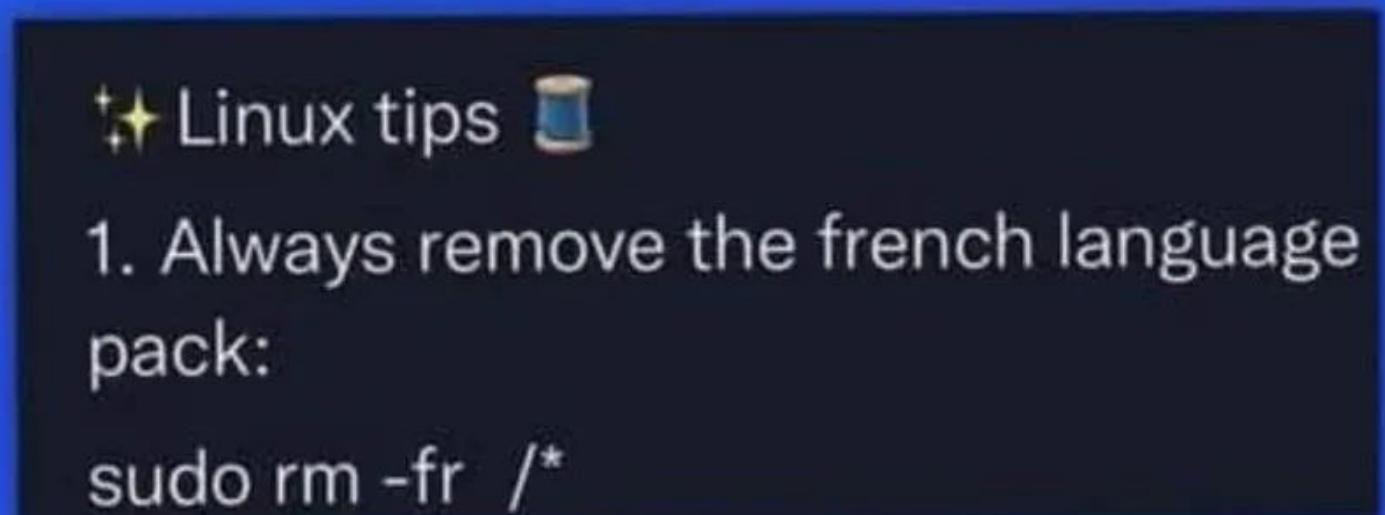
- /
- ~
- ..
- ...

\$ Linux base CLI - Directory Structure

- /
 - 根目錄 所以有目錄的最頂層
- ~
 - 家目錄 假設使用者為 osga
 - /home/osga
- .
 - 當前目錄
- ..
 - 上層目錄

\$ Linux & CLI - Directo

- /
- 根目錄 所以
- ~
- 家目錄 假設
- /home/osgoe
- ..
- 當前目錄
- ..
- 上層目錄



\$ Linux base

Basic command

\$ Linux base

Basic command

- Every thing is the \$FILE
- Tab 是你的好朋友
- 如果指令卡住 可以 Crtl + C
- 所有指令都是相同格式
 - Command [-options [value]] [arguments]

\$ Linux base

Basic command

- 所有指令都是相同格式
 - Command [-options [value]] [arguments]
 - Ex. ls

\$ Linux base

Basic command

- 所有指令都是相同格式
 - Command [-options [value]] [arguments]
 - Ex. ls /home/osga/Desktop

\$ Linux base

Basic command

- 所有指令都是相同格式
 - Command [-options [value]] [arguments]
 - Ex. ls -a /home/osga/Desktop

\$ Linux base

Basic command

- 所有指令都是相同格式
 - Command [-options [value]] [arguments]
 - Ex. cp -r /home/osga/Desktop /home/osga/Download

\$ Linux base

Basic command - about file & dir

\$ Linux base

Basic command - about file & dir

- ls — 列出目前目錄的內容
 - -a — 顯示所有檔案
 - -l — 顯示詳細資料
- cd [directory] — 切換目錄
- pwd — 顯示目前所在路徑
- mkdir [directory] — 建立新目錄
- cp [source] [destination] — 複製檔案或資料夾
 - 資料夾（目錄）要配合 -rf

\$ Linux base

Basic command - about file & dir

- mv [source] [destination] — 移動或重新命名檔案
- rm [file] — 刪除檔案
 - rm -rf [directory] — 刪除目錄
 - rmdir [directory] — 刪除目錄
- cat [file] — 顯示檔案內容
- touch [file] — 建立空白檔案或更新檔案時間
- file [file] — 查看檔案資訊

\$ Linux base

Basic command - about user

\$ Linux base

Basic command - about user

- whoami — 顯示目前登入的使用者名稱
- id — 顯示目前使用者的 UID、GID、所屬群組
- users — 列出目前登入的所有使用者帳號
- adduser [username] — 新增使用者
- passwd [username] — 設定或修改使用者密碼
- deluser [username] — 刪除使用者
- su [username] — 切換到其他使用者帳號
- sudo [command] — 以系統管理員 (root) 身份執行指令

\$ Linux base

Basic command - about groups

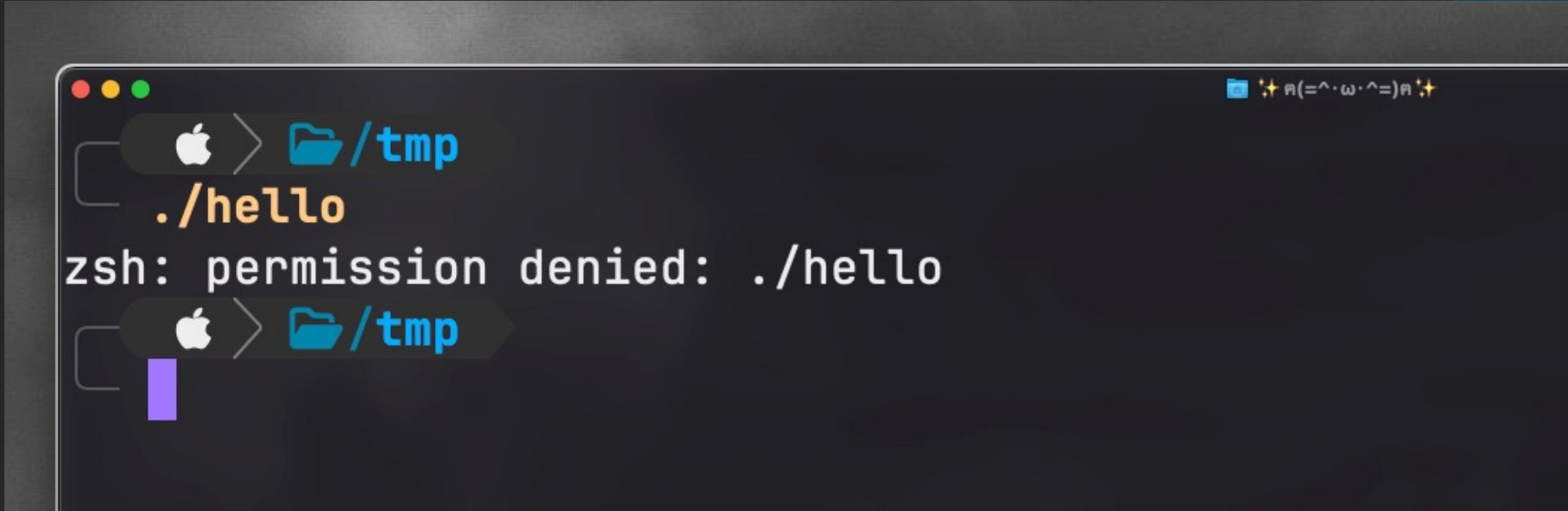
- groupadd [groupname] — 新增群組
- groupdel [groupname] — 刪除群組
- usermod -aG [groupname] [username] — 將使用者加入群組
- groups [username] — 顯示使用者所屬群組

\$ Linux base

Basic command - about permissions

\$ Linux base

Basic command - about permissions



A screenshot of a macOS terminal window. The window title bar shows the Apple logo and the path '/tmp'. The main pane of the terminal displays the following text:

```
./hello
zsh: permission denied: ./hello
```

The terminal has a dark mode theme with light-colored text. A purple cursor bar is visible at the bottom left of the terminal window.

\$ Linux base

Basic command - about permissions

- 權限問題
 - 保護系統安全，防止未授權使用者修改或刪除重要檔案
 - 確保多使用者環境下，每個人只能操作自己有權限的資料
 - 降低錯誤操作導致系統崩潰或資料遺失的風險
 - 控制執行權限，避免惡意程式被隨意執行
 - 支援協作時的安全共享（可設定群組可讀或可寫）

\$ Linux base

Basic command - about permissions

- 查看與修改
 - ls -l — 查看檔案或目錄的權限、擁有者與群組。
 - chmod [mode] [file] — 修改檔案的存取權限
 - Ex. chmod 755 file.txt
 - chown [user]:[group] [file] — 改變檔案擁有者與所屬群組。
 - Ex. chown user:staff file.txt
 - chgrp [group] [file] — 改變檔案的群組。
 - Ex. chgrp admin file.txt

\$ Linux base

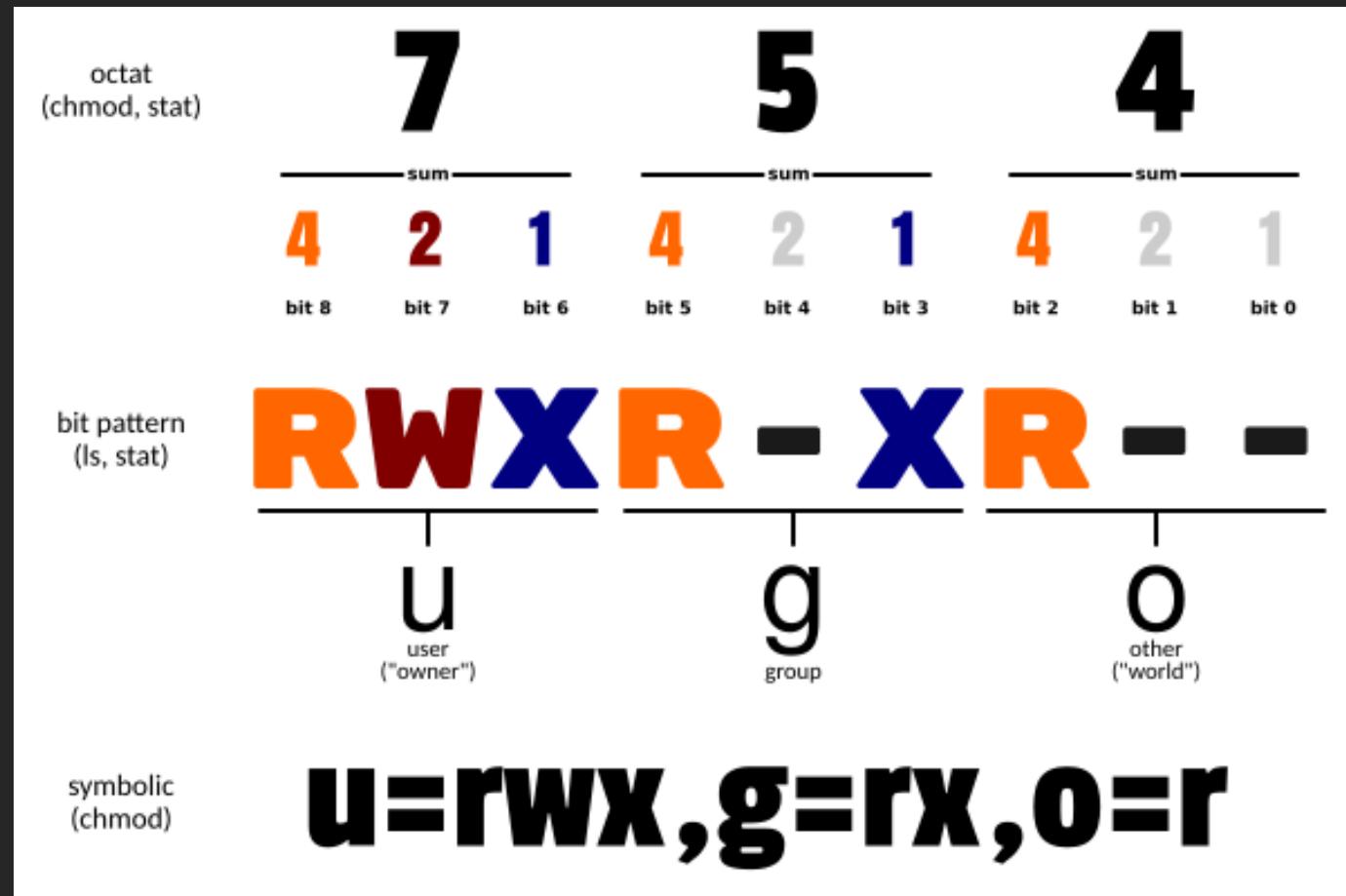
Basic command - about permissions

- 查看與修改
 - ls -l — 查看檔案或目錄的權限、擁有者與群組。
 - chmod [mode] [file] — 修改檔案的存取權限
 - Ex. chmod 755 file.txt
 - chown [user]:[group] [file] — 改變檔案擁有者與所屬群組。
 - Ex. chown user:staff file.txt
 - chgrp [group] [file] — 改變檔案的群組。
 - Ex. chgrp admin file.txt

\$ Linux base

Basic command - about permissions

- chmod [mode] [file] — 修改檔案的存取權限



\$ Linux base

Basic command - help me!!!

- [command] -help
- man [command]

\$ Linux base

Basic command - help me!!!

- [command] -help
- man [command]



\$ Linux base

Basic command - help me!!!

- [command] -help
- man [command]



\$ Linux base

Basic command - ()@!*\${#^*(%&#

\$ Linux base

Basic command - ()@!*\$(#^*%&#

- ; — 依序執行多個指令 (不論前一個是否成功)
 - 例: ls; pwd; whoami
- && — 前一個指令成功時才執行下一個
 - 例: mkdir test && cd test
- || — 前一個指令失敗時才執行下一個
 - 例: make || echo "Build failed"

\$ Linux base

Basic command - ()@!*\$(#^*(%&#

- > — 將輸出覆蓋寫入檔案
 - 例: echo "hi" > out.txt
- >> — 將輸出附加到檔案末尾
 - 例: echo "hi" >> log.txt
- < — 從檔案讀取作為輸入
 - 例: sort < data.txt
- | — 將前一個指令的輸出傳給下一個指令 (管線)
 - 例: cat file | grep "keyword"

\$ Linux base

Basic command - ()@!*\$(#^*(%&#

- * — 匹配任意多個字元 (萬用字元)
- ? — 匹配單一字元
- ~ — 使用者家目錄 (home directory)
- \$ — 變數標示，例如 \$USER, \$PATH
- # — 註解符號 (在指令或腳本中忽略該行內容)
- \ — 轉義字元，用來避免符號被解讀
- & — 將指令放到背景執行
- 例: python app.py &

\$ Linux base

Basic command - scratch file / content

\$ Linux base

Basic command - scratch file / content

- find
 - find 查詢目錄位置 -name <檔案名稱>
 - Ex. find -name fla* /tmp
- grep
 - 需要配合前面的 | 進行輸出
 - Ex. cat system.log | grep “Flag{“

\$ Linux base

Basic command - install new tools

\$ Linux base

Basic command - install new tools



\$ Linux base

Basic command - install new tools

- APT 是 Debian 系列 (如 Ubuntu) 的套件管理工具。
- 用來安裝、更新、移除軟體套件。
- 能自動處理相依性 (dependencies) 。
- 使用網路上的 repository (套件庫) 下載軟體。



\$ Linux base

Basic command - install new tools

apt update — 更新套件清單

apt upgrade — 升級已安裝的所有套件

apt install [package] — 安裝新套件

apt remove [package] — 移除已安裝的套件

apt autoremove — 自動移除不再需要的套件

apt search [keyword] — 搜尋套件

apt show [package] — 顯示套件資訊

需要用 sudo 或 root 安裝



\$ Linux base

Basic command - install new tools

Try it!

- cowsay
- sl
- cmatrix
- nyancat



\$ Linux base

Basic command - ssh

\$ Linux base

Basic command - ssh

- SSH 是一種安全的遠端連線協定 (Secure Shell Protocol)
- 用於加密連線到遠端主機 (例如伺服器、樹莓派、雲端主機)
- 取代舊的 Telnet，提供加密與身份驗證機制

\$ Linux base

Basic command - ssh

- 遠端登入系統: ssh <hostname or ip>
- 端執行指令: ssh <hostname or ip> 'command'
- 檔案傳輸:
 - scp file user@<hostname or ip>:/path
 - sftp user@hostname

\$ Linux base

Basic command - network

\$ Linux base

Basic command - network

- ping [host]
 - 測試是否與目標主機連線正常
 - Ex. ping 8.8.8.8 / ping google.com
- ip a
 - be like ipconfig
 - 顯示網路資訊

\$ Linux base

Basic command - network

- wget [URL]
 - 從網路上下載檔案
- curl [URL]
 - Cat URL
 - 傳送或接收網路請求，可檢查 API、下載內容
- nc
 - 可用於建立 TCP 或 UDP 連線、傳輸資料、測試連線、除錯等
 - Ex. Reverse Shell

\$ Linux base

Basic command - editor on CLI

\$ Linux base

Basic command - editor on CLI

- VIM
- nano

\$ Linux base

Basic command - editor on CLI

- VIM
 -  操作快速，功能強大，可高度客製化
 -  學習曲線陡峭，不直覺
- Nano
 -  操作方便，明顯直覺
 -  功能較少，不適合編輯大型檔案

\$ Linux base

Basic command - editor on CLI

- VIM
 -  操作快速，功能強大，可高度客製化
 -  學習曲線陡峭，不直覺
- Nano
 -  操作方便，明顯直覺
 -  功能較少，不適合編輯大型檔案

\$ Linux b Basic command

- VIM
 - ✓ 操作快
 - ✗ 學習曲
- Nano
 - ✓ 操作方
 - ✗ 功能較



\$ Linu Basic co

- VIM

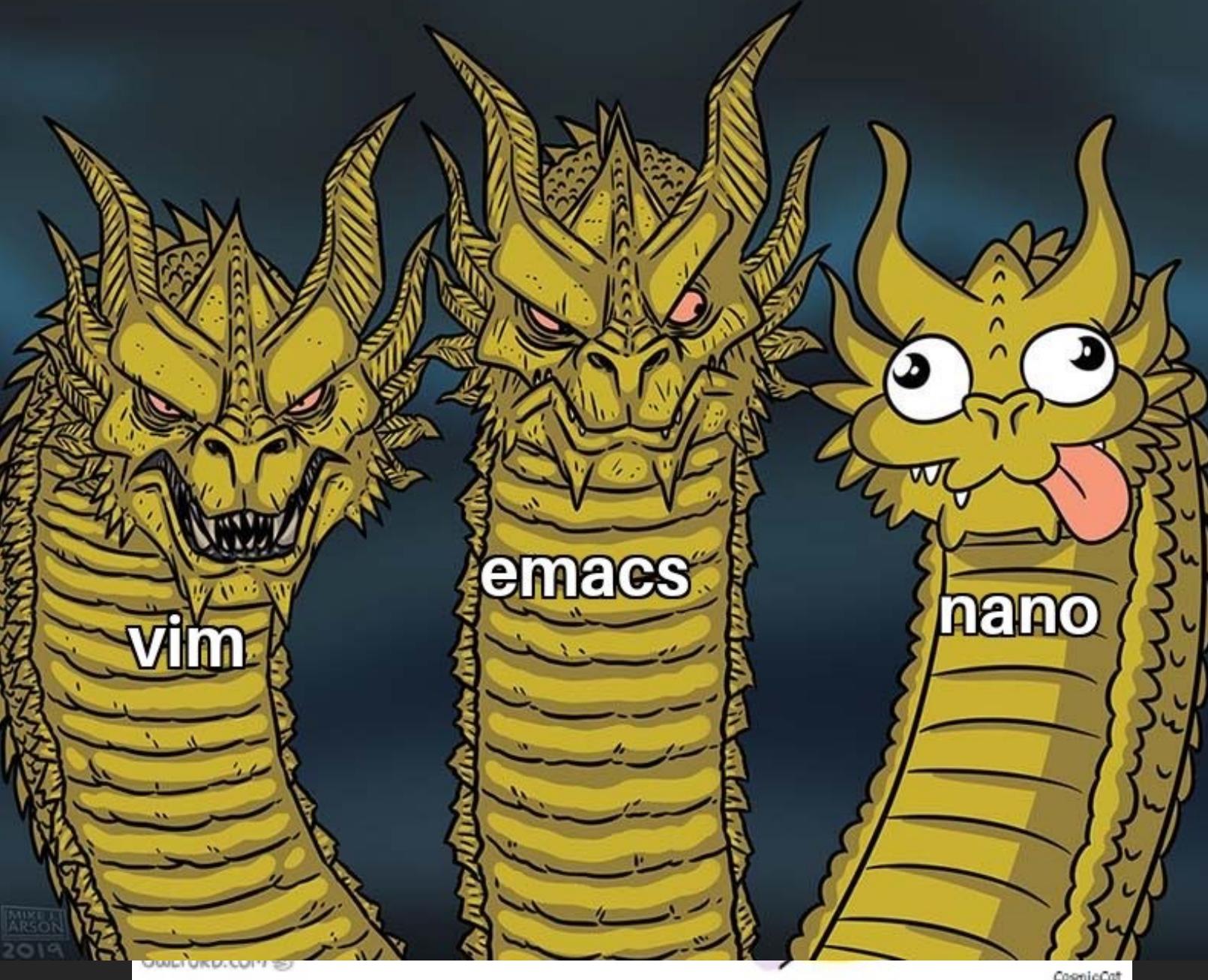
- ✓ 操

- ✗ 學

- Nano

- ✓ 操

- ✗ 功



\$ Linux base

Basic command - editor on CLI

- VIM
 - Ex. vim / vi <file>
- Nano
 - Ex. nano <file>

\$ Linux base

Basic command - editor on CLI

- VIM

\$ Linux base

Basic command - editor on CLI

- VIM
 - Normal 模式：預設模式，用來移動、刪除、複製等
 - Insert 模式：輸入文字（按 i 進入，Esc 返回 Normal）
 - Command 模式：輸入冒號：進行指令操作

\$ Linux base

Basic command - editor on CLI

- VIM
 - i — 進入插入模式 (Insert)
 - Esc — 返回普通模式 (Normal)

\$ Linux base

Basic command - editor on CLI

- VIM
 - :w — 儲存檔案 (write)
 - :q — 離開 Vim (quit)
 - :wq — 儲存並離開
 - :q! — 不儲存強制離開



\$ Linux base

Basic command - editor on CLI

- VIM
 - x — 刪除游標所在字元
 - dd — 刪除一整行
 - yy — 複製一行
 - p — 貼上複製的內容
 - /文字 — 搜尋文字
 - u — 復原 (undo)
 - Ctrl + r — 重做 (redo)

\$ Linux base

More Resources

\$ Linux base

More Resources

- <https://labex.io/linuxjourney>
- <https://labex.io/courses/labex-playground>
- <https://overthewire.org/wargames/>



\$ lab time

FLAG{OsGa.dev/Linux.pdf}

Lab: RPG

<https://linux.ctf.scist.org/challenge>

第伍話

滲透、誠

測試

\$ More skills

\$ More skills

滲透測試？

\$ More skills

滲透測試？

- 模擬攻擊者對系統/網路/應用做攻擊性測試，找出弱點並評估風險
- 黑箱 / 灰箱 / 白箱 / 上香 (我)
- 偵察 → 掃描 → 評估/驗證 → 分析 → 報告與修補建議
- 預先找出弱點進行修補
- Ex.
 - 請白帽小偷來你家試門窗
 - 並把所有能進來的方式列出來與如何加鎖的建議寫成報告

\$ More skills

滲透測試？不就跟紅隊演練很像？

- 模擬攻擊者對系統/網路/應用做攻擊性測試，找出弱點並評估風險
- 黑箱 / 灰箱 / 白箱 / 上香 (我)
- 偵察 → 掃描 → 評估/驗證 → 分析 → 報告與修補建議
- 預先找出弱點進行修補
- Ex.
 - 請白帽小偷來你家試門窗
 - 並把所有能進來的方式列出來與如何加鎖的建議寫成報告

\$ More skills

滲透測試？ 不都跟紅隊演練很像？

- 模擬攻擊者對系
- 黑箱 / 灰箱 / 白
- 偵察 → 掃描 →
- 預先找出弱點進
- Ex.
 - 請白帽小偷來
 - 並把所有能進



弱點並評估風險

議

寫成報告

\$ More skills

滲透測試？不就跟紅隊演練很像？

- 紅隊演練
 - 模擬真實攻擊者的全面攻擊，測試檢測與應變
 - 想評估企業整體防禦、跨部門協作與人為因子的實戰能力時
- 滲透測試
 - 找出並驗證具體漏洞，重點在「可複現的弱點/修補建議」
 - 通常不刻意規避偵測，目的是確認漏洞存在與可利用性

\$ More skills

Pen Test

\$ More skills

Pen Test

- SUID / SGID 檔案
- sudo 配置錯誤
- World-writable 檔案/目錄
- 弱或洩漏的憑證
- 不安全的 NFS / 共享掛載
- ...

\$ More skills

Pen Test

- SUID / SGID 檔案
- sudo 配置錯誤
- World-writable 檔案/目錄
- 弱或洩漏的憑證
- 不安全的 NFS / 共享掛載
- • •

已思考 16s

下面是簡短條列版、針對滲透測試常會關注的 Linux 技術項目（像 SUID 類型），每項都附一行說明與一個僅作檢查/稽核用的指令範例。僅在你有授權的環境或靶機上執行。

- SUID / SGID 檔案 — 程式以檔案擁有者權限執行，錯誤設定會有提權風險。
 - 檢查：`find / -perm -4000 -type f 2>/dev/null`
- World-writable 檔案/目錄 — 任何人可寫入，可能被用來植入或替換程式。
 - 檢查：`find / -xdev -type d -perm -0002 2>/dev/null`
- 可寫的 root 擁有檔案/目錄 — root 擁有但他人可寫入尤其危險。
 - 檢查：`find / -user root -writable 2>/dev/null`
- sudo 配置錯誤 (`sudoers`) — 不當授權可讓低權限帳號執行高權限指令。
 - 檢查（在已登入帳號下）：`sudo -l`
- Cron / scheduled tasks — 定時任務若以高權限執行或讀取不安全檔案，可能被濫用。
 - 檢查：`ls -la /etc/cron* /var/spool/cron* 2>/dev/null`
- 可寫的服務目錄或配置檔 — 服務（如 web、daemon）配置或執行檔可被替換導致提權或持久化。
 - 檢查範例：`ss -tulpn`（看在跑哪些服務）+ 檢查該服務的執行檔與配置權限
- 弱或洩漏的憑證（SSH keys / 密碼） — 未受保護的私鑰或弱密碼會直接導致横向移動。
 - 檢查（稽核）：查看 `~/.ssh/authorized_keys` 與 `.ssh` 權限
- 不安全的 NFS / 共享掛載 — NFS 等若設為可寫或 root squash 配置不當會衍生風險。
 - 檢查（網路 / 主機視角）：`showmount -e <target>` 或 `mount`（本機）
- setcap / capabilities — 透過 file capabilities 賦予二進位檔特權，配置錯誤亦有風險。
 - 檢查：`getcap -r / 2>/dev/null`（需要有 `getcap`）
- 可疑 suid 程式庫或 kernel module — 非標準或可寫的模組/庫可能被濫用。
 - 檢查：檢視 `/lib/modules/` 與已載入模組 `lsmod`
- 過時的 Kernel / 套件 — 已知漏洞的版本會被連鎖利用。
 - 檢查：`uname -a` 與發行版套件版本查詢（如 `dpkg -l | grep <pkg>`）
- 容器 / Docker 誤配置 — Docker 套件與容器若以 root 或不當權限運行，主機可能被控。
 - 檢查（在有 docker 權限下）：`docker ps -a`、檢查是否有 `--privileged` 或 host volume 掛載

\$ More skills

Pen Test

- SUID / SGID 檔案
 - SUID (Set-User-ID)
 - 執行該執行檔時會以檔案擁有者的 UID (通常是 root) 執行
 - SGID (Set-Group-ID)
 - 執行檔以檔案所屬群組的 GID 執行；資料夾上的 SGID 會讓新建立檔案繼承該群組

\$ More skills

Pen Test

- SUID / SGID 檔案
 - 被錯誤設定或存在漏洞的 SUID/Sgid 程式，可能讓一般使用者取得比自己更高的權限（提權風險）
 - SUID/Sgid 程式若可被修改或其輸入可被操控，將成為攻擊向量

SUID

```
find / -perm -4000 -type f 2>/dev/null
```

SGID

```
find / -perm -2000 -type f 2>/dev/null
```

\$ More skills

Pen Test

- sudo 配置錯誤
 - sudo 允許被授權的使用者以其他身份執行特定指令
 - sudo 的行為由 /etc/sudoers 與 /etc/sudoers.d/ 控制

\$ More skills

Pen Test

- sudo 配置錯誤
 - sudo 允許被授權的使用者以其他身份執行特定指令
 - sudo 的行為由 /etc/sudoers 與 /etc/sudoers.d/ 控制

sudo -l

\$ More skills

Pen Test

- sudo 配置錯誤
 - sudo 允許被授權的使用者以其他身份執行特定指令
 - sudo 的行為由 /etc/sudoers 與 /etc/sudoers.d/ 控制

sudo -l

\$ More skills

Pen Test - tools

- **nmap** — 網路掃描與指紋識別
- **netcat** — TCP/UDP 連線、簡易伺服器/傳檔
- **dirb / dirsearch / gobuster / ffuf** — 目錄與檔名爆破、模糊測試
- **sqlmap** — 自動化 SQL 注入測試與資料庫指紋
- **metasploit (msfconsole)** — 漏洞利用與後續測試的框架
- **nikto** — Web 伺服器掃描器
- 好多好多好多

\$ More skills

Pen Test - tools

- **nmap** — 網路掃描與指紋識別
- **netcat** — TCP/UDP 連線、簡易伺服器/傳檔
- **dirb / dirsearch / gobuster / ffuf** — 目錄與檔名爆破、模糊測試
- **sqlmap** — 自動化 SQL 注入測試與資料庫指紋

• m
• n
• h



Meow
VERY EASY



Machine Pwned

<https://app.hackthebox.com/startng-point>

\$ More skills



\$ 參考連結

- 【成大資安社社課】 Linux 基礎教學: <https://youtube.com/live/W9HdkgfpJCU>
- 【成大資安社社課】 Linux 基礎指令與使用者管理: <https://youtu.be/8WVrUqjBsRE>
- 【資訊安全 Week 1 – Linux 】 SCIST S5 培訓課程 – 113 學年度:
 - <https://github.com/kazmatw/Kazma-Linux-Course>
- 【Linux】 SCIST S4 資訊安全 week 1: <https://youtu.be/80SMzZS-DAs>
- Linux: From Zero to Hero : https://docs.google.com/presentation/d/1n-muc56hprxmFlva5ldowBihMOfzVmnh/edit?slide=id.g377ae7585ad_0_61#slide=id.g377ae7585ad_0_61
- <https://zh.wikipedia.org/zh-tw/資訊安全>
- https://en.wikipedia.org/wiki/Linux_distribution
- <https://note.drx.tw/2008/04/command.html>
- SCINT 基礎實務教學：他們影片回播還沒出來 QQ

thank for listen



Content me