



絶対強者の殿堂へ :Linux 領域展開！

2024/10/19 Kazma@SCIST

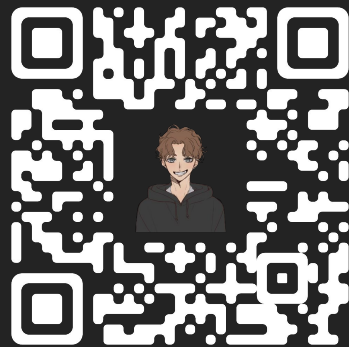


whoami



@kazma.tw

- 本名/ID: 葉東逸/Kazma
- 奧義智慧科技實習生
- 成大資安社 創辦人/社長
- TSC 創辦人 TSCCTF 總召
- 國家資通安全研究院 CTF 種子教練
- AIS3 專題評審/出題者/助教/Junior 助教
- 財團法人電信技術中心資安組前實習生
- HITCON/SITCON/NCKUCTF/SCIST/COSCUP 講者
- Pwner / Reverser @ B33F 50μP



@linktr.ee

Overview

- Linux Intro
- Filesystem Hierarchy
- Read the Manual
- Linux Basic Commands
- The Git
- Searching and Filtering
- File Permissions and Ownership
- I Am Root !
- Advanced Packaging Tool



Overview

- System Information and Monitoring
- Piping and Redirection
- Network and Remote Access
- Vi IMproved
- Shell Scripts
- History
- Let's Attacking !
- RCE Kazma guide
- Save Kazma Mission





Linux Intro

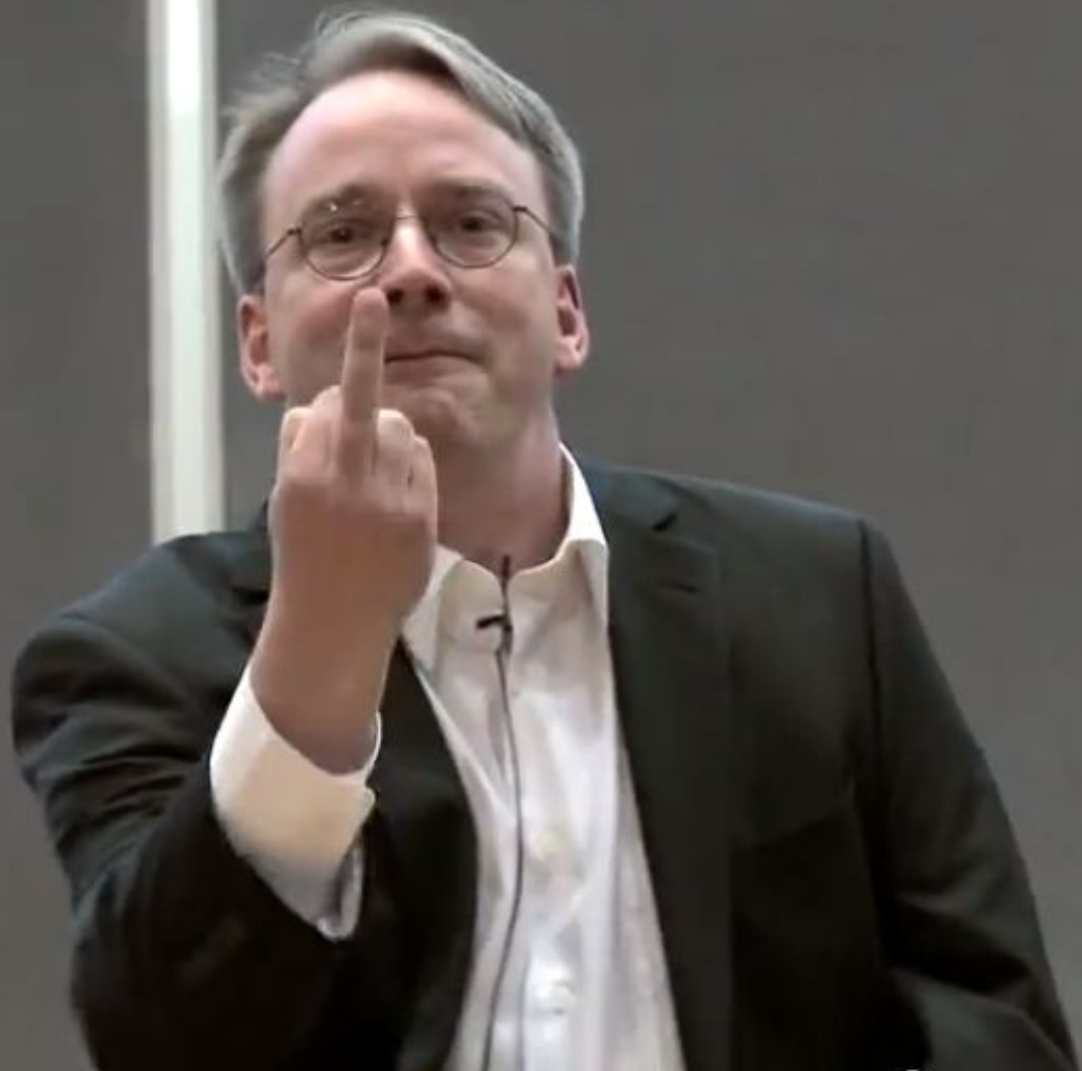
Linux Intro

- Unix & Minix & 386
- 研究所 side project
- Freax -> Linux 與企鵝
- 開源和 Email
- 發行版的出現
- “Talk is cheap. Show me the code.”



Linux Intro - Linus's Mails

- Mauro, SHUT THE FUCK UP!
- To read things ONE F*CKING BYTE AT A TIME
- Who the f*ck does idiotic things like that
- How did they not die as babies
- Too stupid to find a tit to suck on
- This piece-of-shit commit is more f*cked up than average
- For whatever braindamaged reasons



Linux Intro - Linus Quotes


A decorative graphic consisting of several purple lines of varying lengths and orientations, located in the top-left corner of the slide.

The point about open source has never been that I'm more accessible than anybody else. It's never been that I'm more accessible than anybody else. Anyone reading this column would assume the mounting pressures of my role as chief nerd had turned me into an asshole.


But that's wrong. I always was an asshole.

Linux Intro


install linux on pc



8:38




15:10




Linux Install For Beginners

How to Install Linux in 2024 - A Beginners Guide

觀看次數：11萬次 · 3 個月前

 Michael Horn


Follow me! X ⇌ <https://x.com/@MichaelNROH> Instagram ⇌ <https://www.instagram.com/@MichaelNROH> Mastodon ...

 7 個章節

The power of the Linux Desktop | Choosing a Linux Distribution | How to install Linux [...]


Install Linux instead of Windows 11 - Here's how!

觀看次數：378萬次 · 2 年前

 Linux Tech Tips

Windows 11 is about to make a lot of people feel left behind, but there's one operating system that's recently been gett...


4K 字幕

 10 個章節

Intro | What is Linux and why should I care? | Getting Pop!_OS | Booting & the installer ...

How to Install Linux for Beginners

觀看次數：76萬次 · 5 年前

 Chris Titus Tech

3. Basic configuration Choosing the right version or flavor of Linux -Latest Ubuntu Desktop LTS Installation Process - Download ...



Filesystem Hierarchy

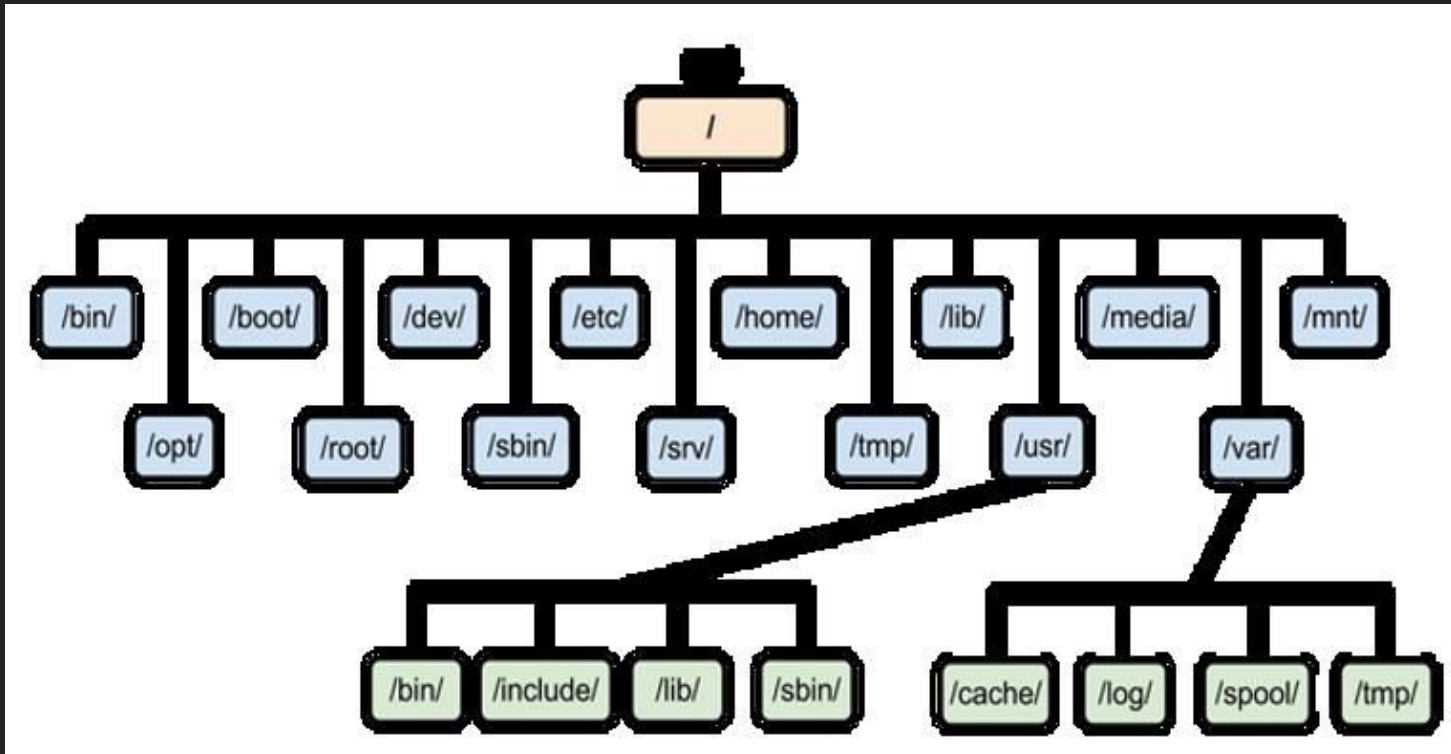


Filesystem Hierarchy - Path

Decorative purple lines consisting of a diagonal line and two horizontal lines.

- **Windows**
 - `C:\Users\kazma\Desktop\meow`
- **MacOS**
 - `/Users/kingkazma/Kazma-Linux-Course/lab1`
- **Linux**
 - `/home/kazma/Kazma-CTF-Challenges-Released/ais3_pre_exam/2024`

Filesystem Hierarchy



Filesystem Hierarchy

Decorative purple lines consisting of a diagonal line and two horizontal lines.

- **Root Directory (/)**
 - Top-level directory for all files and folders.
- **/bin**
 - Essential user binaries like bash, ls, cp.
- **/sbin**
 - System administration binaries, typically for system administrators.
- **/etc**
 - Configuration files for the system, e.g., /etc/passwd.

Filesystem Hierarchy

Decorative purple lines consisting of a diagonal line and two horizontal lines.

- **/dev**
 - Device files, representing system hardware like `/dev/sda`.
- **/var**
 - Variable files like logs (`/var/log`), spool files, and temporary files that persist between reboots.
- **/tmp**
 - Temporary files that are cleared on reboot.

Filesystem Hierarchy

- **/usr**
 - Secondary hierarchy for user applications; includes many subdirectories
 - **/usr/bin**: Non-essential user binaries.
 - **/usr/sbin**: Non-essential system binaries.
 - **/usr/local**: Locally installed software.
- **/home**
 - Home directories for individual users.
- **/boot**
 - Boot loader files, kernel images, and configuration files necessary for booting.

The slide features a dark gray background with several horizontal purple lines of varying lengths and thicknesses. These lines are positioned at the top and bottom of the slide, creating a decorative border. The lines are arranged in a way that they appear to be part of a larger, abstract design.

Read the Manual

Read the Manual - man ls

```
LS(1)                                     User Commands                               LS(1)

NAME
    ls - list directory contents

SYNOPSIS
    ls [OPTION]... [FILE]...

DESCRIPTION
    List information about the FILES (the current directory by default). Sort entries alphabetically if none of
    -cftuvSUX nor --sort is specified.

    Mandatory arguments to long options are mandatory for short options too.

    -a, --all
        do not ignore entries starting with .

    -A, --almost-all
        do not list implied . and ..

    --author
        with -l, print the author of each file

    -b, --escape
        print C-style escapes for nongraphic characters

    --block-size=SIZE
        with -l, scale sizes by SIZE when printing them; e.g., '--block-size=M'; see SIZE format below

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

Read the Manual - man ls

NAME

ls - list directory contents

SYNOPSIS

ls [OPTION]... [FILE]...

Read the Manual - man ls

DESCRIPTION

List information about the FILES (the current directory by default). Sort entries alphabetically if none of **-cftuvSUX** nor **--sort** is specified.

Mandatory arguments to long options are mandatory for short options too.

-a, --all

do not ignore entries starting with .

-A, --almost-all

do not list implied . and ..

--author

with **-l**, print the author of each file

Read the Manual - ls --help

```
$ ls --help
```

```
Usage: ls [OPTION]... [FILE]...
```

```
List information about the FILES (the current directory by default).
```

```
Sort entries alphabetically if none of -cftuvSUX nor --sort is specified.
```

```
Mandatory arguments to long options are mandatory for short options too.
```

-a, --all	do not ignore entries starting with .
-A, --almost-all	do not list implied . and ..
--author	with -l, print the author of each file
-b, --escape	print C-style escapes for nongraphic characters
--block-size=SIZE	with -l, scale sizes by SIZE when printing them; e.g., '--block-size=M'; see SIZE format below

Read the Manual - man find

FIND(1)

General Commands Manual

FIND(1)

NAME

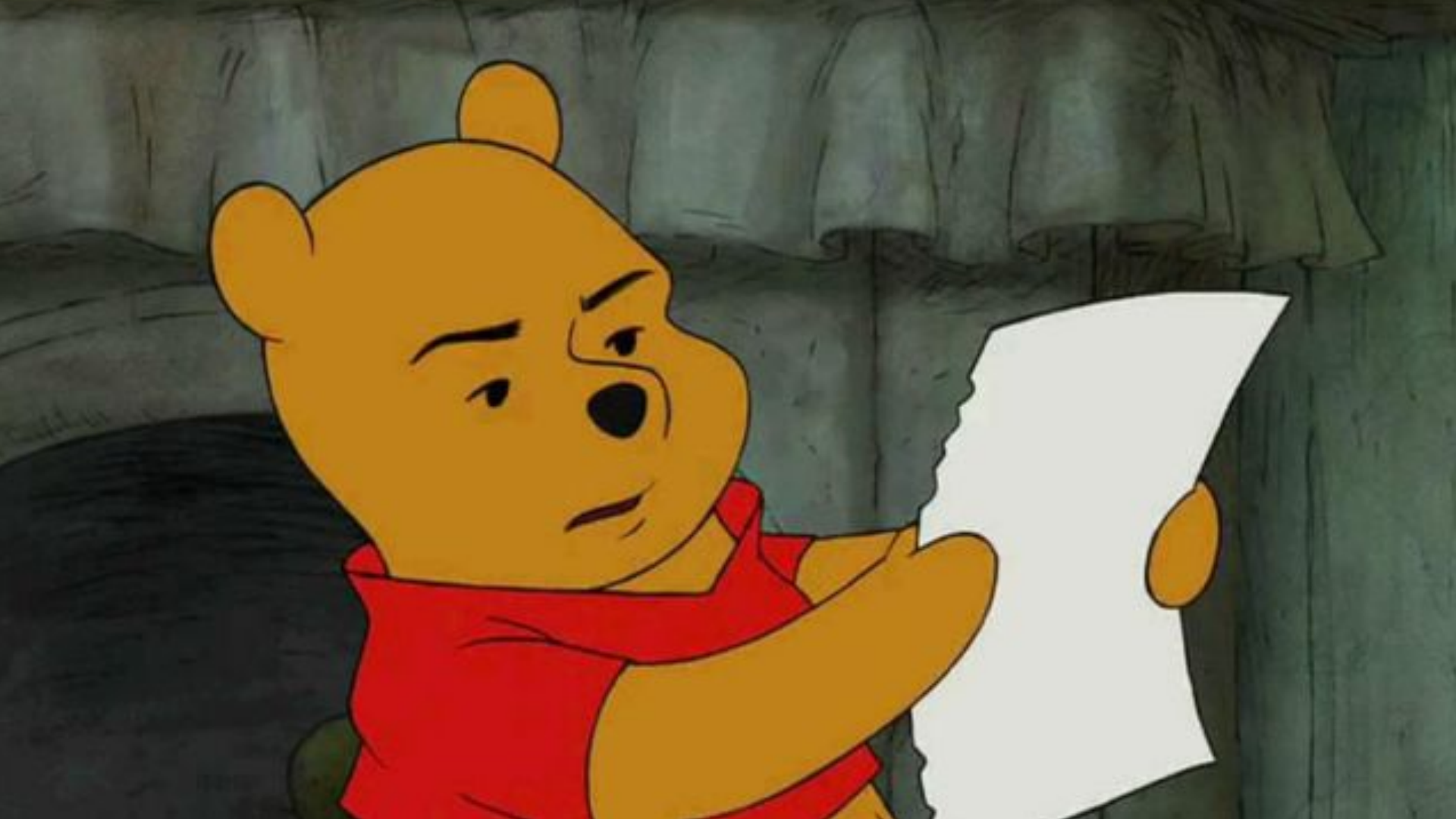
`find` - search for files in a directory hierarchy

SYNOPSIS

`find [-H] [-L] [-P] [-D debugopts] [-Olevel] [starting-point...] [expression]`

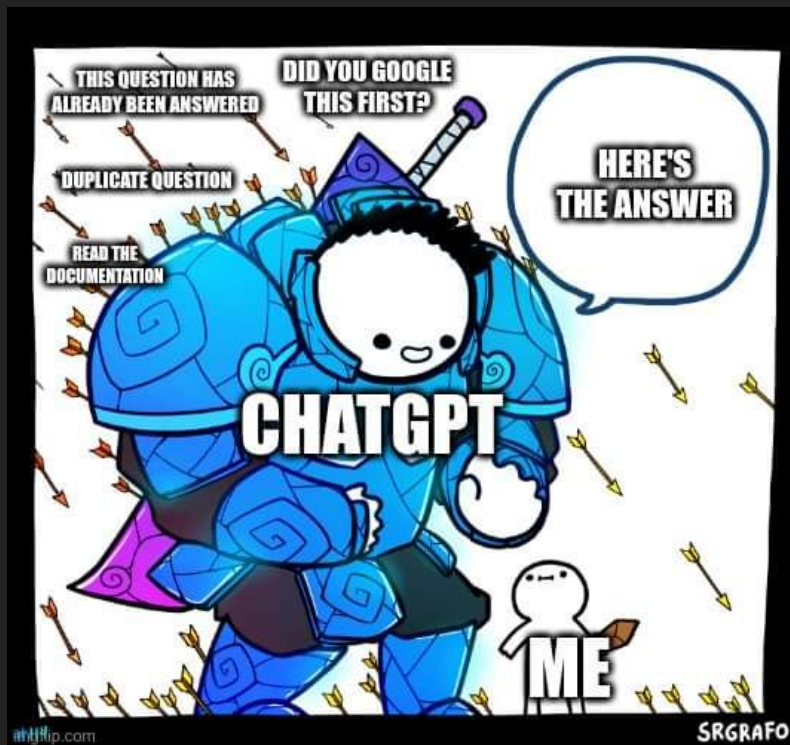
DESCRIPTION

This manual page documents the GNU version of **find**. GNU **find** searches the directory tree rooted at each given starting-point by evaluating the given expression from left to right, according to the rules of precedence (see section OPERATORS), until the outcome is known (the left hand side is false for and operations, true for or), at which point **find** moves on to the next file name. If no starting-point is specified, ``.`` is assumed.



Read the Manual

- Try and Error
- Google
- ChatGPT





Linux Basic Commands



Linux Basic Commands

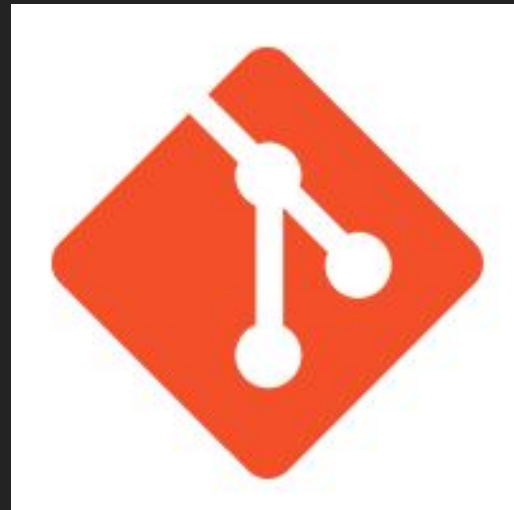
- **pwd (print working directory):** Display the current working directory.
- **ls (list):** List directory contents.
- **cd (change directory):** Change the current directory.
- **mkdir (make directory):** Create a new directory.
- **touch:** Create a new, empty file.
- **rm (remove):** Delete files or directories.
- **cp (copy):** Copy files or directories.
- **mv (move):** Move or rename files or directories.
- **cat (concatenate):** Display the contents of a file.

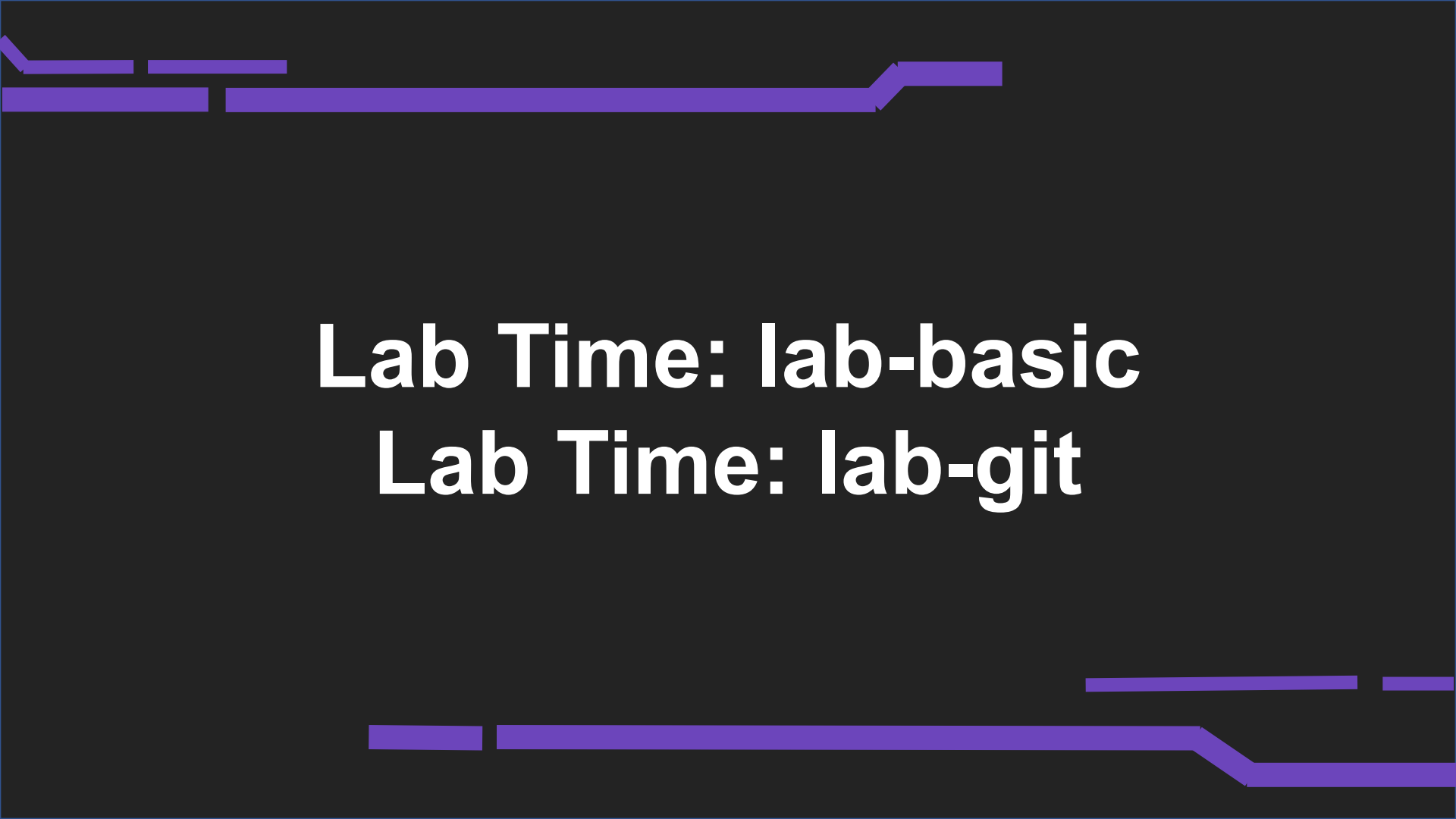


The Git

The Git

- `git clone https://github.com/example/repo.git`
- `git add filename.txt`
- `git commit -m "Add initial project files"`
- `git status`
- `git push origin main`
- `git pull origin main`
- `git branch feature-branch`
- `git checkout feature-branch`
- `git merge feature-branch`






Lab Time: lab-basic
Lab Time: lab-git


Lab Time: lab1

 github.com/kazmatw

 **Kazma-Linux-Course** Public

[Unpin](#) [Unwatch 1](#) [Fork 0](#) [★ Starred 1](#)

[main](#) [1 Branch](#) [0 Tags](#) [Add file](#) [Code](#)

 **kazmatw** Fixed flag_part1 in lab1 095ffe2 · 15 minutes ago 3 Commits

lab1	Fixed flag_part1 in lab1	15 minutes ago
LICENSE	Initial commit	1 hour ago
README.md	Initial commit	1 hour ago

About

This repository is specifically designed for my Linux course. It contains all the necessary lab materials and exercises. Students can complete the assignments and directly submit their flags through the CTFd platform.

[linux](#) [course](#)



Searching and Filtering



Searching and Filtering

- **find**: Search for files in a directory hierarchy.
- **find /path/to/search -name "filename.txt"**
- **grep** (global regular expression print): Search text using patterns.

```
(kazmatw@kasma-kali) - [~/yzuimsc]  
$ grep -r "YZUIMSC{*"  
flag: YZUIMSC{grep_is_powerful}
```




Lab Time: lab-grep



Lab Time: lab2

Kazma-Linux-Course / lab2 / 



kazmatw First push lab2

Name	Last commit message
 ..	
 maybe_here	First push lab2
 wtf.sh	First push lab2





File Permissions and Ownership



File Permissions and Ownership

- **chmod (change mode):** Change file permissions.

- **drwxrwxrwx**

- **+ / -**

- **0~7**

Linux File Permissions

 blog.bytebytego.com

Binary	Octal	String Representation	Permissions
000	0 (0+0+0)	---	No Permission
001	1 (0+0+1)	--x	Execute
010	2 (0+2+0)	-w-	Write
011	3 (0+2+1)	-wx	Write + Execute
100	4 (4+0+0)	r--	Read
101	5 (4+0+1)	r-x	Read + Execute
110	6 (4+2+0)	rw-	Read + Write
111	7 (4+2+1)	rwx	Read + Write + Execute

Owner			Group			Other		
r w x			r w -			r - x		
r	Read	4	r	Read	4	r	Read	4
w	Write or Edit	2	w	Write or Edit	2	-	No Permission	0
x	Execute	1	-	No Permission	0	x	Execute	1
7			6			5		

File Permissions and Ownership - setuid

- `chmod u+s filename`
- ex: `-rwsr-xr-x`
- 可以獲得擁有者的執行權限





Lab Time: lab-setuid



The image features a dark gray background with several horizontal purple lines of varying lengths and orientations at the top and bottom, creating a stylized border. The text "I Am Root !" is centered in a bold, white, sans-serif font.

I Am Root !

I Am Root !

```
user$ rm somefile  
rm: somefile: Permission denied  
user$ sudo rm somefile
```





Advanced Packaging Tool



Advanced Packaging Tool

- Store of Debian GNU/Linux
- `sudo apt update`
- `sudo apt install packagename`
- `sudo apt upgrade`
- `sudo apt remove packagename`
- `apt search keyword`
- `apt show packagename`





System Information and Monitoring

System Information and Monitoring

- `whoami`
- `id`
- `top`
- `htop`
- `vmstat 1`
- `free -h`
- `uname -a`

whoami



@kazma.tw



@linktr.ee

- 本名/ID：葉東逸/Kazma
- 奧義智慧科技實習生
- 成大資安社 創辦人/社長
- TSC 創辦人 TSCCTF 總召
- 國家資通安全研究院 CTF 種子教練
- AIS3 專題評審/出題者/助教/Junior 助教
- 財團法人電信技術中心資安組前實習生
- HITCON/SITCON/NCKUCTF/SCIST/COSCUP 講者
- Pwner / Reverser @ B33F 50μP

System Information and Monitoring - top

- **h or ?**: Display help screen listing all commands and their functions.
- **q**: Quit top.
- **k**: Kill a process. You will need to specify the process ID and signal to send (usually 9 for SIGKILL).
- **r**: Renice a process to change its priority.
- **f or F**: Add or remove columns from the display, customizing the process information presented.
- **o or O**: Change the sort order of the process list.
- **u**: Filter the processes by username or user ID.
- **M**: Sort by memory usage.
- **P**: Sort by CPU usage.
- **T**: Sort by time/cumulative time.
- **z**: Toggle color mode.
- **t**: Toggle the display of the top CPU and memory status bars.
- **B**: Toggle bold display; turning off bold can disable highlighting.

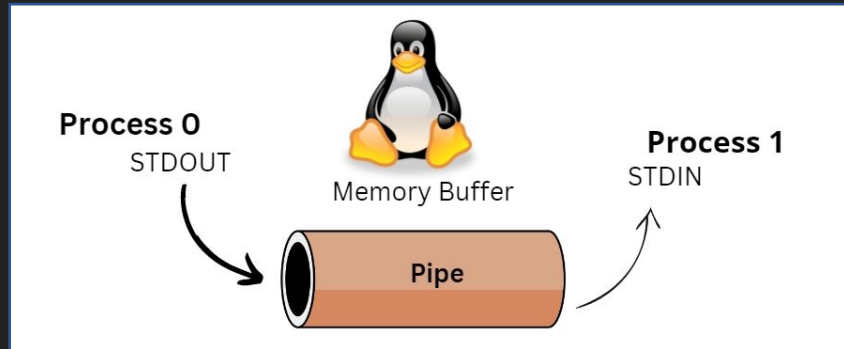


Piping and Redirection



Piping and Redirection

- **more:** View the contents of a file one screen at a time.
- **less:** View the contents of a file with backward and forward navigation.
- **head:** Display the first few lines of a file.
- **tail:** Display the last few lines of a file.



Piping and Redirection - less

- Space bar: Scroll down one screen.
- b: Scroll back one screen.
- Up Arrow and Down Arrow: Move up or down one line at a time.
- Right Arrow and Left Arrow: Scroll horizontally right or left (if line wrapping is off).
- G: Go to the end of the file.
- g or < or 1G: Go to the beginning of the file.
- /pattern: Search forward for a pattern. After typing the pattern, press Enter to perform the search.
- ?pattern: Search backward for a pattern.
- n: Repeat the previous search in the same direction.
- N: Repeat the previous search in the opposite direction.
- q: Quit less.



Network and Remote Access



Network and Remote Access

Decorative purple lines consisting of a diagonal line and two horizontal lines.

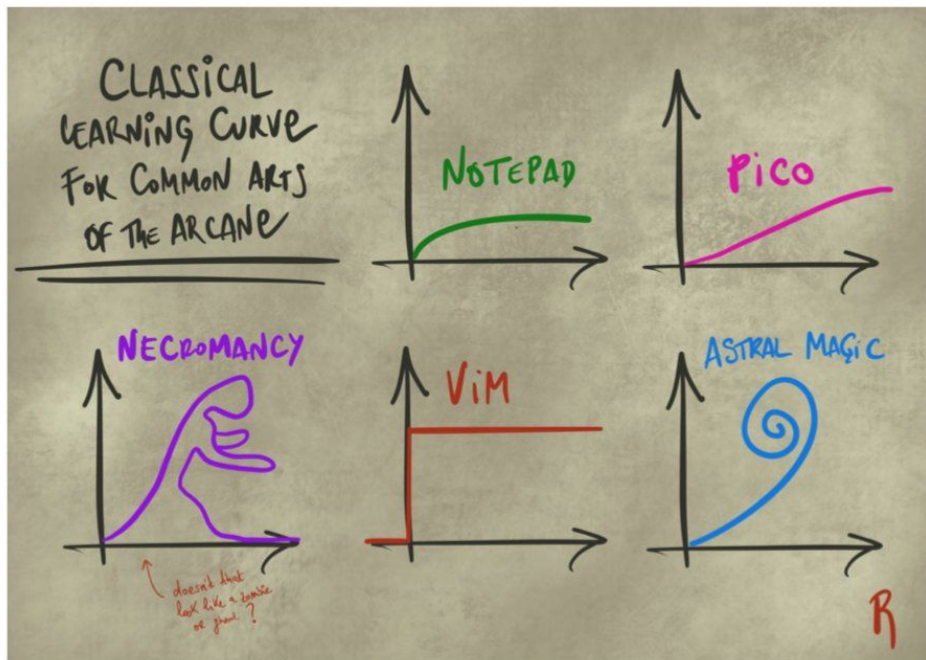
- **ping**: Send ICMP ECHO_REQUEST to network hosts.
- **wget** (web get): Non-interactive network downloader.
- **curl** (client URL): Transfer data from or to a server.
- **ssh** (secure shell): OpenSSH remote login client.
- **scp** (secure copy): Securely copy files between hosts.
- **ifconfig** (interface configuration): Configure network interfaces.



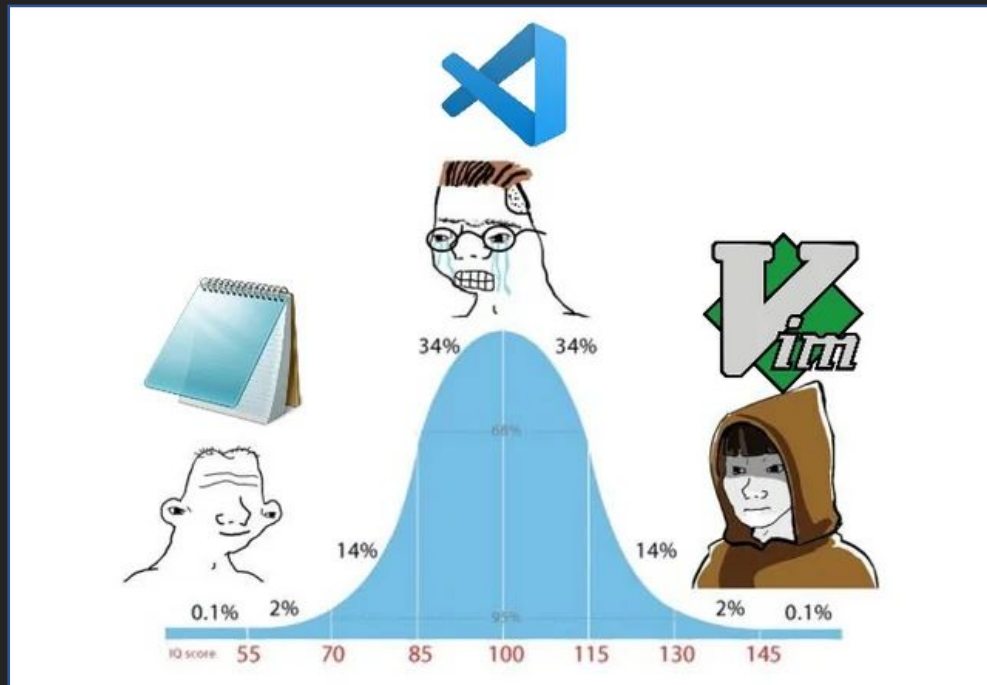
Vi IMproved



Vi IMproved - why vim



Vi IMproved - why vim



圖片來源: https://www.reddit.com/r/ProgrammerHumor/comments/odsyhl/change_my_mind/

Vi IMproved - how to exit vim

WHEN YOU TRY TO EXIT VIM



« We don't do that here. »



Tiny Lab Time: Open Vim

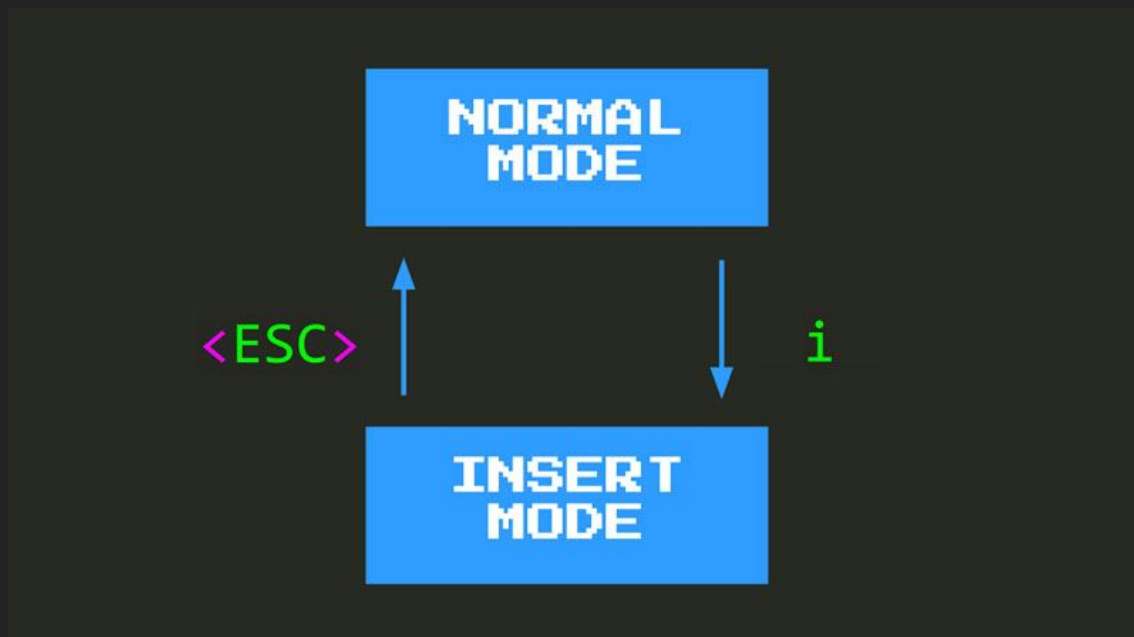




Tiny Lab Time: Exit Vim



Vi IMproved





Shell Scripts



Shell Scripts

- `#!/bin/bash`
- `# This is a comment`

```
bash
```

```
name="John"  
echo "Hello, $name"
```

```
bash
```

```
if [ $number -gt 10 ]; then  
    echo "The number is greater than 10."  
elif [ $number -eq 10 ]; then  
    echo "The number is equal to 10."  
else  
    echo "The number is less than 10."  
fi
```

```
bash
```

```
for i in {1..5}  
do  
    echo "Looping ... number $i"  
done
```



Lab Time: lab-scripts



History

History

```
history | grep hexo | tail
9782 sudo hexo new draft "Flipper Zero 宇宙最強攻略：30 天帶你從入門到入坑 Day25"
9804 history | grep hexo
9805 sudo hexo new draft "Flipper Zero 宇宙最強攻略：30 天帶你從入門到入坑 Day26"
9824 sudo hexo new draft "Flipper Zero 宇宙最強攻略：30 天帶你從入門到入坑 Day27"
9838 sudo hexo new draft "Flipper Zero 宇宙最強攻略：30 天帶你從入門到入坑 Day28"
9839 sudo hexo new draft "Flipper Zero 宇宙最強攻略：30 天帶你從入門到入坑 Day29"
9870 sudo hexo new draft "Flipper Zero 宇宙最強攻略：30 天帶你從入門到入坑 Day30"
9898 history | grep hexo
10352 history | grep hexo
10353 history | grep hexo | head
```

```
!9782
```



Let's Attacking !



Let's Attacking ! - hashcat

- `hashcat [options] <hashfile> <wordlist>`
- `hashcat -m 0 -a 0 -o cracked.txt hashes.txt wordlist.txt`



Let's Attacking ! - hydra

- `hydra [options] server service [module-options]`
- `hydra -L /path/to/user/list.txt -P /path/to/password/list.txt ssh://192.168.0.1`





Lab time: lab-hashcat





RCE Kazma guide





Save Kazma Mission

Save Kazma Mission

```
*** System restart required ***
Last login: Sat Jul 27 16:46:10 2024 from 10.129.0.58
kazmatw@kazma-lab:~$ sudo vim /etc/ssh/sshd_config
kazmatw@kazma-lab:~$ sudo systemctl restart ssh
kazmatw@kazma-lab:~$ exit
logout
Connection to 10.129.0.57 closed.

(kazmatw@kazma-kali) - [~/Kazma-CTF-Challenges/linux]
$ ssh kazmatw@10.129.0.57
kazmatw@10.129.0.57: Permission denied (publickey).
```



Any Questions?



Thank You

