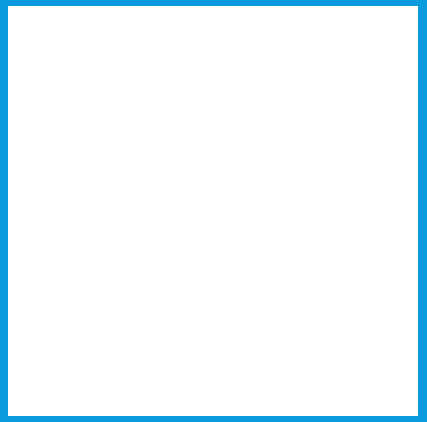
Linux+Forensics

安裝LINUX

- Ubunto
- Debian
- Kali
- 預設工具

虛(VM)擬機

- vmware Workstation Pro
- Oracle VM



CREATE A NEW VIRTUAL MACHINE

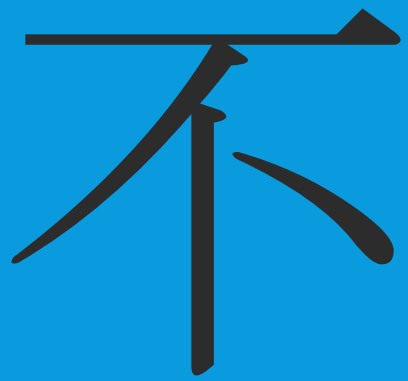
選取光碟映像檔.ISO

LINUX DEBIAN-10

名稱、路徑

設定最大空間

完成?



打開他 CRRL+ALT可以拿回滑鼠

GRAPHICAL INSTALL

設定語言

設定地區

設定鍵盤語言

讓他自己跑

設定装置名稱

設定域名(可以空著)

設定使用者名稱

設定帳號名稱

設定密碼

設定時區

設定硬碟 USE ENTIRE DISK

選磁碟區

系統資料分類方式

完成硬碟設定

確定硬碟變更

繼續跑安裝囉

真的完成了

基本操作

- ls　　列出檔案、資料夾
- cd 路徑　更改工作路徑
- clear　　清除畫面
- pwd　　顯示目前路徑
- user　　顯示目前資料夾
- man 指令 顯示指令所有資料
- apt　　主要的安裝指令
- sudo　指令　以管理員權限執行指令
- vim 檔案 編輯檔案

METADATA

- 拍攝時間、地點等
- ExifTool
- http://metapicz.com/
- 練習題
  - metadata.jpg
  - CTFLearn(Web,Easy) WOW…. So Meta

檔案觀念

- 所有檔案都是由1,0組成，便於觀看以16進制表示
- kali - Bless
- window - HxD
- online - https://hexed.it/
- 安裝　sudo apt install bless

HEX

- 可以看出檔案的秘密
- 練習題
  - hex
  - CTFLearn(Web,Easy) Forensics 101

BINWALK

- 可以看出檔案中的檔案
- 練習題
  - doublefile.jpg
  - CTFLearn(Web,Easy) binwalk
- 沒有linux怎麼辦
- 直接改成.zip有時候有用
- 怎麼做的?
- Window cmd
  - copy /b 檔案1+檔案2 最後檔案

BASE 64

- 以ascii為基礎由8byte一個字改為6byte一個字

- 補位

混合練習

- 練習題
  - CTFLearn(Web,Easy) GandalfTheWise (記得xor嗎)
  - 大亂鬥.jpg

上次補充

- Brute xor
  - https://www.dcode.fr/xor-cipher