tcpdump & iperf

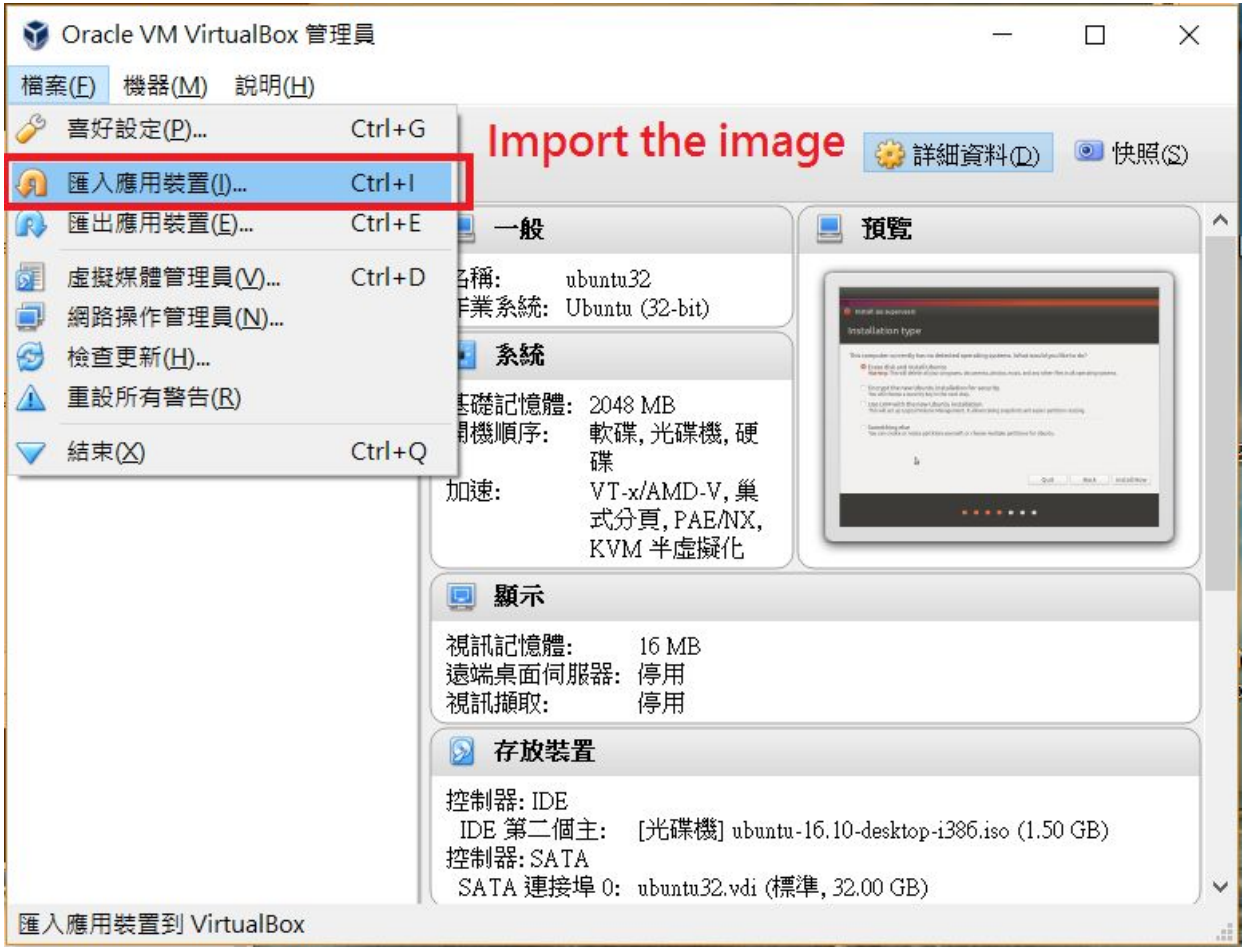
NA 有線組 張庭瑋

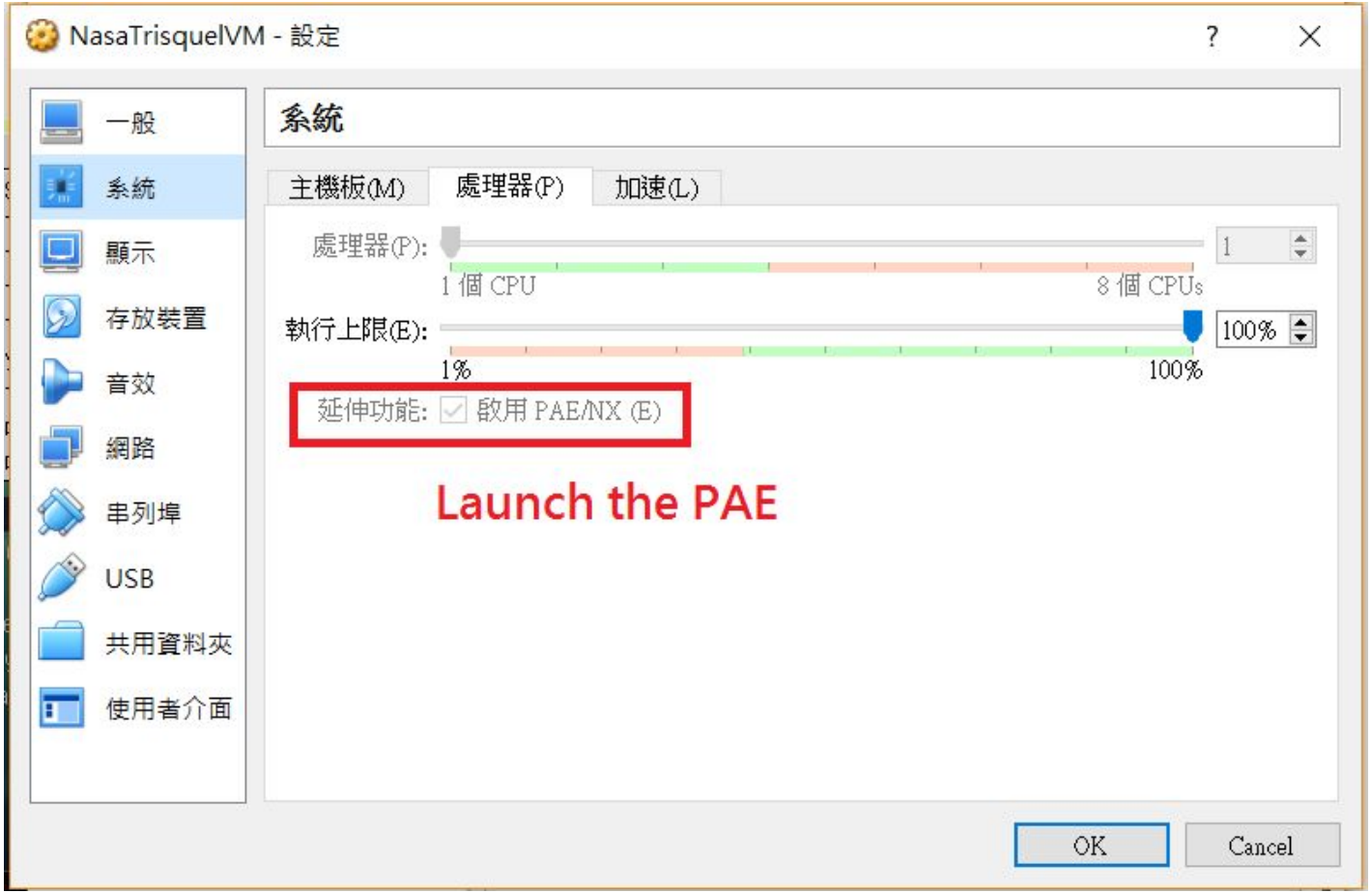
Intro

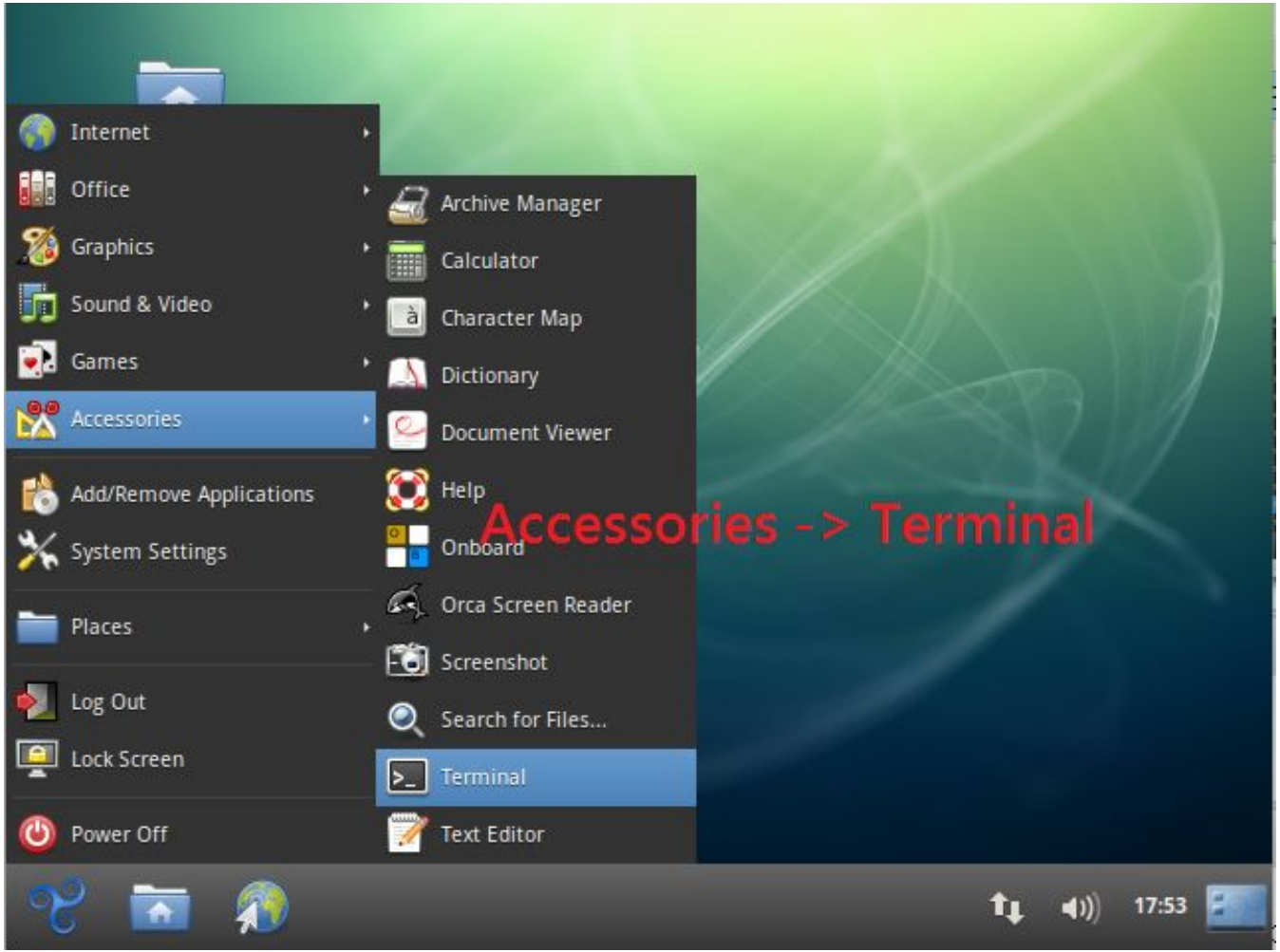
- tcpdump
  - A software tool that sniffs the network traffic transmitted from your own PC.
- iperf
  - A software tool that examines the network bandwidth between 2 hosts.

Get a VM !

- Why experiment in VM ?
  - tcpdump needs privileged mode to do traffic snffing.
  - Install any package you want !
  - Backup & Recovery
- How ?
  - Import the VM image provided by TAs.
  - Install by yourself.


Oracle VM VirtualBox 管理員
檔案(F)
機器(M)
說明(H)
喜好設定(P)... Ctrl+G
匯入應用裝置(I)... Ctrl+I
匯出應用裝置(E)... Ctrl+E
虛擬媒體管理員(V)... Ctrl+D
網路操作管理員(N)...
檢查更新(H)...
重設所有警告(R)
結束(X) Ctrl+Q
Import the image
詳細資料(D)
快照(S)
一般
名稱: ubuntu32
作業系統: Ubuntu (32-bit)
系統
基礎記憶體: 2048 MB
開機順序: 軟碟, 光碟機, 硬碟
加速: VT-x/AMD-V, 巢式分頁, PAE/NX, KVM 半虛擬化
預覽
顯示
視訊記憶體: 16 MB
遠端桌面伺服器: 停用
視訊擷取: 停用
存放裝置
控制器: IDE
IDE 第二個主: [光碟機] ubuntu-16.10-desktop-i386.iso (1.50 GB)
控制器: SATA
SATA 連接埠 0: ubuntu32.vdi (標準, 32.00 GB)
匯入應用裝置到 VirtualBox

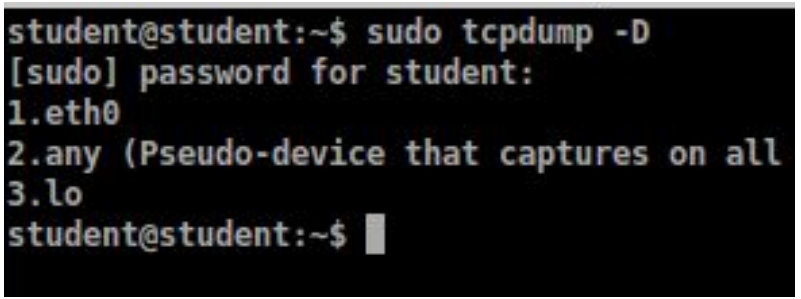

NasaTrisquelVM - 設定
一般
系統
顯示
存放裝置
音效
網路
串列埠
USB
共用資料夾
使用者介面
系統
主機板(M)
處理器(P)
加速(L)
處理器(P):
1
1 個 CPU
8 個 CPUs
執行上限(E):
100%
1%
100%
延伸功能:
啟用 PAE/NX (E)
Launch the PAE
OK
Cancel


Internet
Office
Graphics
Sound & Video
Games
Accessories
Add/Remove Applications
System Settings
Places
Log Out
Lock Screen
Power Off
Archive Manager
Calculator
Character Map
Dictionary
Document Viewer
Help
Onboard
Orca Screen Reader
Screenshot
Search for Files...
Terminal
Text Editor
Accessories -> Terminal
17:53

Out VM Enviroment

- OS: Trisquel 7.0 (A branch from Ubuntu, light-weight OS)
- Account/Password: student/student
- Shortcut for Terminal: Ctrl + Alt + T
- Install tcpdump:
  - **sudo apt-get install tcpdump**
- Install iperf:
  - **sudo apt-get install iperf**

TCP Dump



- Command line uility
- Pre-installed in some Unix-based OS.
- Need the privileged mode (sudo)
- Can see the most original content of packets.
- command example:

sudo tcpdump -D

sudo tcpdump -i any -A -s 1024 “dst port 80”

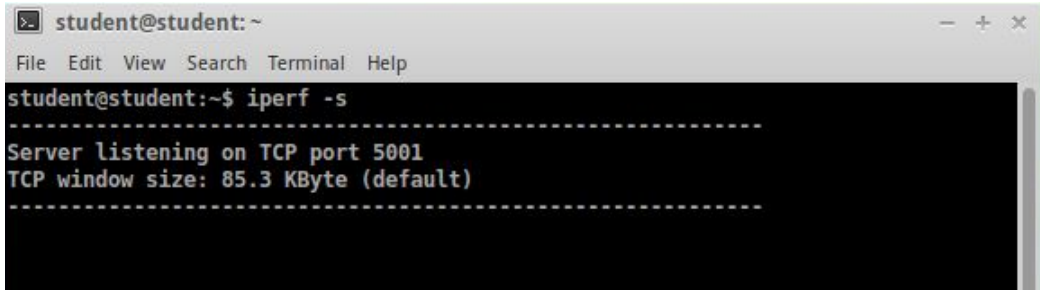
Iperf

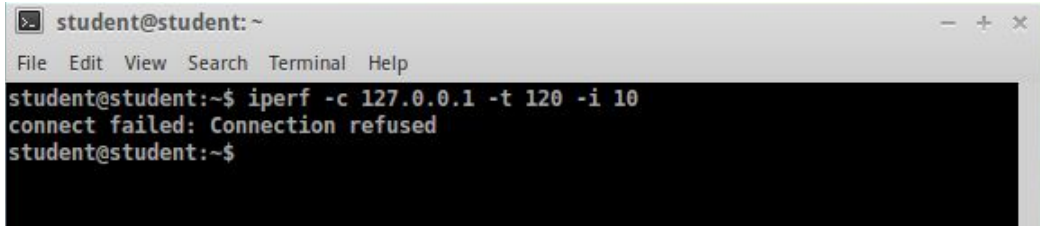
- Command Line utility
- Server-side command:

  iperf -s

- Client-side command:

  iperf -c <Server's IP>





Exercise 1

- Start sniffing the network traffic with **tcpdump**
- Try to login the following page with any string for Username/Password. e.g. your student ID
- Stop sniffing and find the transmitted packet.
- Find the Username/Password string you typed previously.

Exercise 1

- In our VM environment, is tcpdump available for SSL packets ?

  Hint: change the website url http to https
  Hint: *ssldump*

Exercise 2

- Find a partner, and test the bandwidth between your VMs using iperf.
- In our VM environment, is server-side IP accessible from the client-side?

  Hint: Adjust your VM’s network interface to “Bridged” not “NAT”.