NASA 2024 - Homework 0

B11902125 資工二 江融其

## Network Administration

### 1. True/False

1. 線上影音服務會收到VPN伺服器的IP，而非我的IP。答案為是。

1. 只要外面裝置連接的IP(public IP)與我伺服器的IP有被設定於NAT table上，NAT可以將封包的IP轉為我伺服器的IP，它便能主動連接到我伺服器(反之便是將我原本的IP轉為NAT上的public IP)。答案為否。

Ref: <https://hackmd.io/@a000058556/ByuGVhGzs>

1. Gateway可以用於連接LAN和WAN (如residential gateway)，有時也可以透過加密來確保數據傳輸安全。答案為否。

Ref: <https://en.wikipedia.org/wiki/Residential_gateway>

<https://en.wikipedia.org/wiki/Gateway_(telecommunications)>

1. http是用明文來傳輸，因此可以很輕易得知封包內資料。答案為是。

1. private IP並非全域性唯一，因此不能上Internet，只能與在同一個LAN下的其他public IP直接連線。因此答案在通常情況下為否。

Ref: <https://en.wikipedia.org/wiki/Private_network>

1. DDoS是以大量網路流量來消耗目標設備的資源，以造成干擾或破壞，而非通訊雙方中間被攻擊者攔截的資料外洩。因此答案為否。

Ref: [https://zh.wikipedia.org/zh-tw/阻斷服務攻擊](https://zh.wikipedia.org/zh-tw/%E9%98%BB%E6%96%B7%E6%9C%8D%E5%8B%99%E6%94%BB%E6%93%8A)

1. 越長的密鑰代表更多可能性和組合，通常會更難找出正解，但隨機性和與演算法的匹配性等也需考慮。通常正確但不能說一定，答案為否。

### 2. ChatGPT

1. 第一，在網路卡上的出場MAC address的確唯一，但可以透過修改系統中已被讀取出的MAC address來暫時讓其他裝置讀取到更改後的值，並不完全可信。第二，在同一LAN下MAC address需要不同沒錯，但在這之外的網路世界通常用IP address這樣的其他方法來識別。

Ref: [MAC 地址为什么不需要全球唯一](https://blog.csdn.net/weixin_38889300/article/details/107011375?spm=1001.2101.3001.6650.1&utm_medium=distribute.pc_relevant.none-task-blog-2%7Edefault%7ECTRLIST%7ERate-1-107011375-blog-45032111.235%5Ev43%5Epc_blog_bottom_relevance_base4&depth_1-utm_source=distribute.pc_relevant.none-task-blog-2%7Edefault%7ECTRLIST%7ERate-1-107011375-blog-45032111.235%5Ev43%5Epc_blog_bottom_relevance_base4&utm_relevant_index=2)(超連結)

<https://en.wikipedia.org/wiki/MAC_address>

2. 4G不是頻率，是第四代行動通訊技術，而此處談論的行動通訊技術更是與4倍光速無關。簡而言之，這段回應沒什麼邏輯。

Ref: <https://zh.wikipedia.org/zh-tw/4G>

3. 雖然目前IPv4仍然支援大多數應用，新裝置使用IPv4 address也不會有問題，但此處ChatGPT的確按照題目要求去推廣IPv6並嘗試說服學生不要使用舊版的IPv4。因此ChatGPT的描述沒錯。

Ref: <https://hackmd.io/@ki_2CYV1QfCsYx3X8THqiw/pty11111>

### 3. Short Answer

1. 動態主機設定協定，作為網路管理者來自動分配網路連接參數給使用者。用處是透過自動化給予網路連接參數來提高原本手動設定的效率，同時自動設定IP address租期和更新，減少管理員的負擔。

Ref: <https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol>

<https://linux.vbird.org/linux_server/centos6/0340dhcp.php>

1. 虛擬區域網絡，將一個實體LAN分割為多個獨立的VLAN，使不同VLAN之間無法直接互通。主要用處是將Broadcast的範圍從全LAN限制到只有目標的VLAN中，除了讓封包只在目標VLAN內廣播以確保安全性、方便管理、同時也減少不必要的傳輸消耗。

Ref: <https://www.jannet.hk/virtual-lan-vlan-zh-hant/>

1. 交換器，透過每個封包對應的MAC address來將封包傳給已連接的目標裝置。用處是與其連接的裝置可以只將資料發送到目標裝置，而非發給所有裝置，同時支援雙工，提供高效率雙向傳輸。

Ref: <https://en.wikipedia.org/wiki/Network_switch>

1. 廣播風暴，由於大量Broadcast在網絡中傳播而影響傳輸效能，甚至出錯當機的現象。如果網絡中存在迴路，Broadcast可能透過迴路在Switch間不斷散播大量Broadcast，造成壅塞。因此為需要預防的問題，如防止不正確的Switch連線、以VLAN隔開各區域以降低風險、或透過相關協定(如STP，生成樹協定)來避免迴路產生。

Ref: <https://en.wikipedia.org/wiki/Broadcast_storm>

<https://en.wikipedia.org/wiki/Spanning_Tree_Protocol>

1. 0.0.0.0是用來表示一個無效、未知或是無目標廣播的IP，為特殊用途之IP位置。因此算合法。

Ref: <https://dic.vbird.tw/operating_system/2020unit08.php>

[https://ithelp.ithome.com.tw/articles/10311096#:~:text=說明,都能夠訪問該服務。](https://ithelp.ithome.com.tw/articles/10311096%23:~:text=說明,都能夠訪問該服務。)

1. 為IPv6中的localhost address，傳給此IP時會將封包傳給自己。合法。

Ref: <https://www.ibm.com/docs/zh-tw/i/7.2?topic=concepts-ipv6-address-types>

1. 為合法IP位置。

Ref: <https://www.whois365.com/tw/ip/2001:0db8:abcd:0123:4567:890a:bcde:ffff>

|  |  |  |
| --- | --- | --- |
| 名稱 | 功能 | 例子 |
| Physical layer | 以實體設備傳輸數據。 | Hub |
| Data link layer | 建立收發數據時MAC或(和) IP的address，將數據封裝成Data frame。 | Switch |
| Network layer | 處理並選擇封包的傳送路徑。 | Router |
| Transport layer | 將數據標頭加上收發兩端的port，調整與傳送封包，並須保證數據正確送達。 | TCP |
| Application layer | 幫應用程式處理數據以服務使用者。 | DNS |

Ref: <https://medium.com/@z3337059/學習day1-網路架構及基礎知識-1-d6e7744937ec>

<https://dotblogs.azurewebsites.net/Leo_CodeSpace/2019/03/29/203853>

<https://pjchender.dev/internet/internet-tcp-ip-1/>

1. 通訊控制協定。以三次握手與四次揮手保證連接狀態，並且在傳輸數據時使用識別碼與序號，透過接收端發送的確認信號來保證每個封包的完整性與順序，並在出錯時(接收端未發送確認訊息)重傳封包，是可靠的傳輸方式。

Ref: <https://en.wikipedia.org/wiki/Transmission_Control_Protocol>

1. 用戶資料包協定，發送端會不停發送數據包給接收端，簡單且快速，但不會除錯且不絕對可靠，是注重速度的傳輸方式。

Ref: <https://en.wikipedia.org/wiki/User_Datagram_Protocol>

1. 兩者的優缺點與使用場景如下：

|  |  |  |  |
| --- | --- | --- | --- |
|  | 優點 | 缺點 | 使用場景 |
| TCP | 數據完整性高、傳輸順序正確、流量可控 | 建立連結與發送信號的開銷較多、耗時 | 較要求可靠傳輸(例：電子郵件) |
| UDP | 沒有建立收發兩端連結的開銷、快速 | 數據完整性低、壅塞時會丟包或延遲 | 較要求快速即時  (例：網路電話) |

Ref: <https://nordvpn.com/zh-tw/blog/tcp-udp-bijiao/>

1. 用途簡述：用於管理與讀寫目錄管理服務中資料的協定，如存儲與驗證資訊、訪問與登錄帳號等。其中LDAPS為LDAP加密後的安全版本。預設port： TCP 636。

Ref: <https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol>

<https://support.google.com/cloudidentity/answer/9089736?hl=zh-Hant>

1. 用途簡述：標準化電子郵件從寄件到收件的傳輸流程，讓訪客與伺服器能無視底層硬體與軟體的差異互相傳遞信件。但只支援信件的傳遞，傳遞後仍需其他協定輔助才能閱讀信件。預設port：TCP 25。

Ref: <https://www.cloudflare.com/zh-tw/learning/email-security/what-is-smtp/>

<https://www.cloudflare.com/zh-tw/learning/email-security/smtp-port-25-587/>

1. 用途簡述：用於監視與管理網路設備的協定，為適用TCP/IP的簡單網路管理方式。以樹狀資結的MIB管理數據。由NMS上的SNMP Manager索取與設定數據，然後讓SNMP Agent在MIB收集數據後以SNMP協定和Manager通訊，完成設備管理。預設port：UDP 161。

Ref: <https://www.cc.ntu.edu.tw/chinese/epaper/0047/20181220_4707.html>

<https://www.tsnien.idv.tw/Internet_WebBook/Book_PDF/第十六章%20SNMP%20網路管理協定.pdf>

1. 用途簡述：以文字超連結傳輸網頁文件的方法，統一用戶端向伺服器發送請求與伺服器回應時的標準。其中HTTPS為HTTP加密後的安全版本。預設port：HTTP為TCP 80；HTTPS為TCP 443。

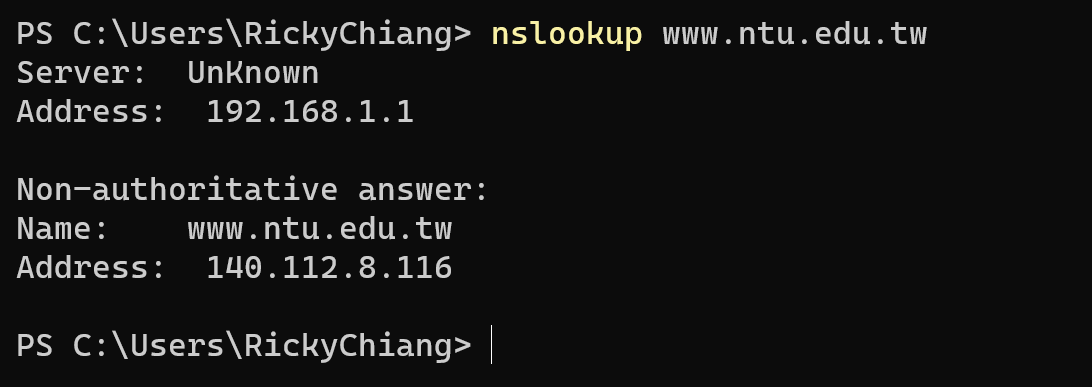
Ref: <https://zh.wikipedia.org/zh-tw/TCP/UDP端口列表>

<https://www.cloudflare.com/zh-tw/learning/ddos/glossary/hypertext-transfer-protocol-http/>

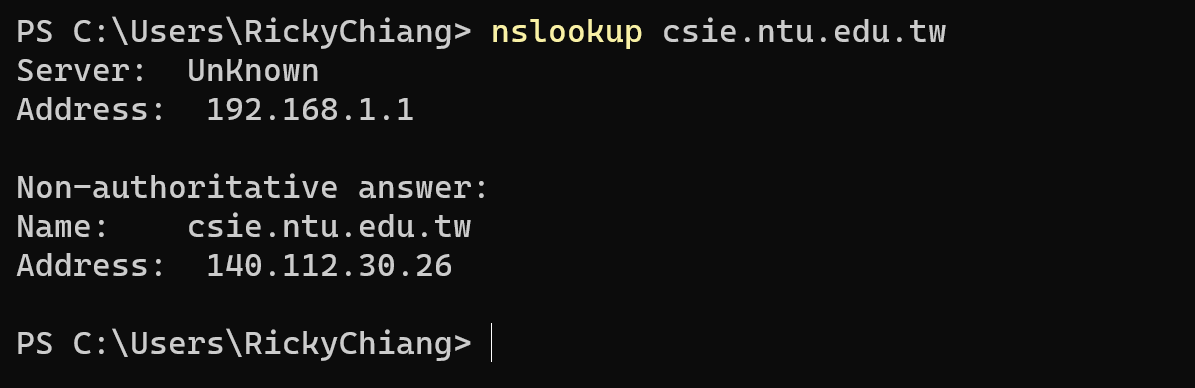
### 4. Command Line Utilities

找出對應的IP address:

1. 使用指令如下圖第一行，IP address為140.112.8.116。



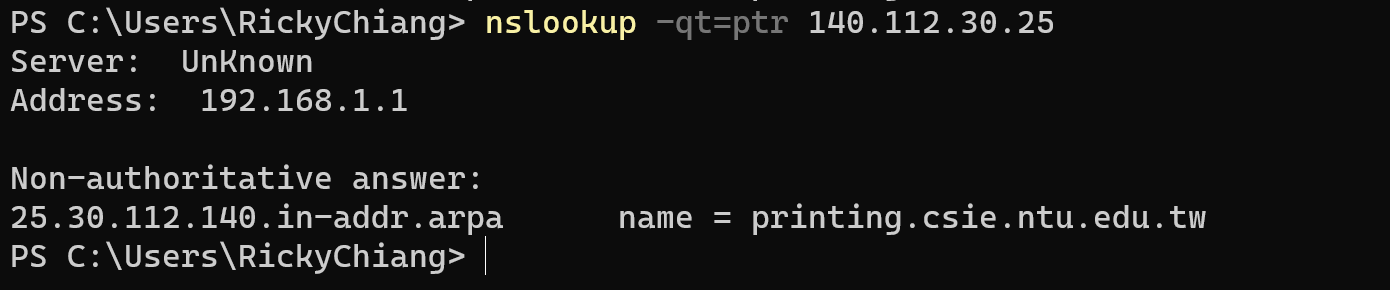
1. 使用指令如下圖第一行，IP address為140.112.30.26。



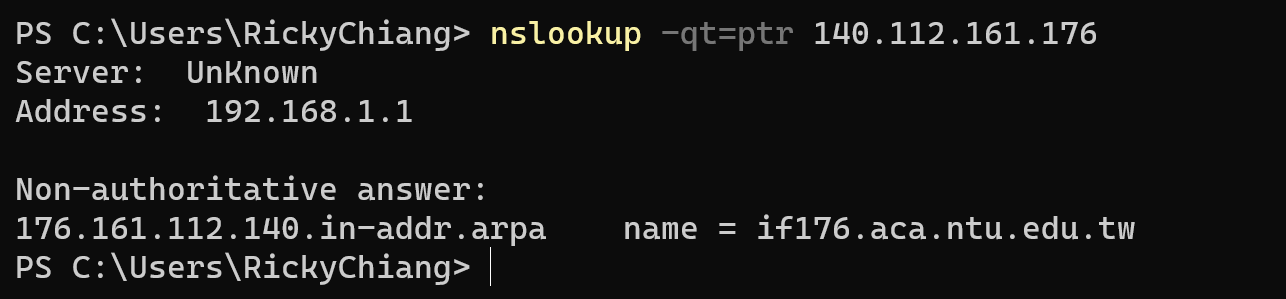
Ref: <https://zhuanlan.zhihu.com/p/382307227>

找出對應的domain name:

1. 使用指令如下圖第一行，domain name為printing.csie.ntu.edu.tw。

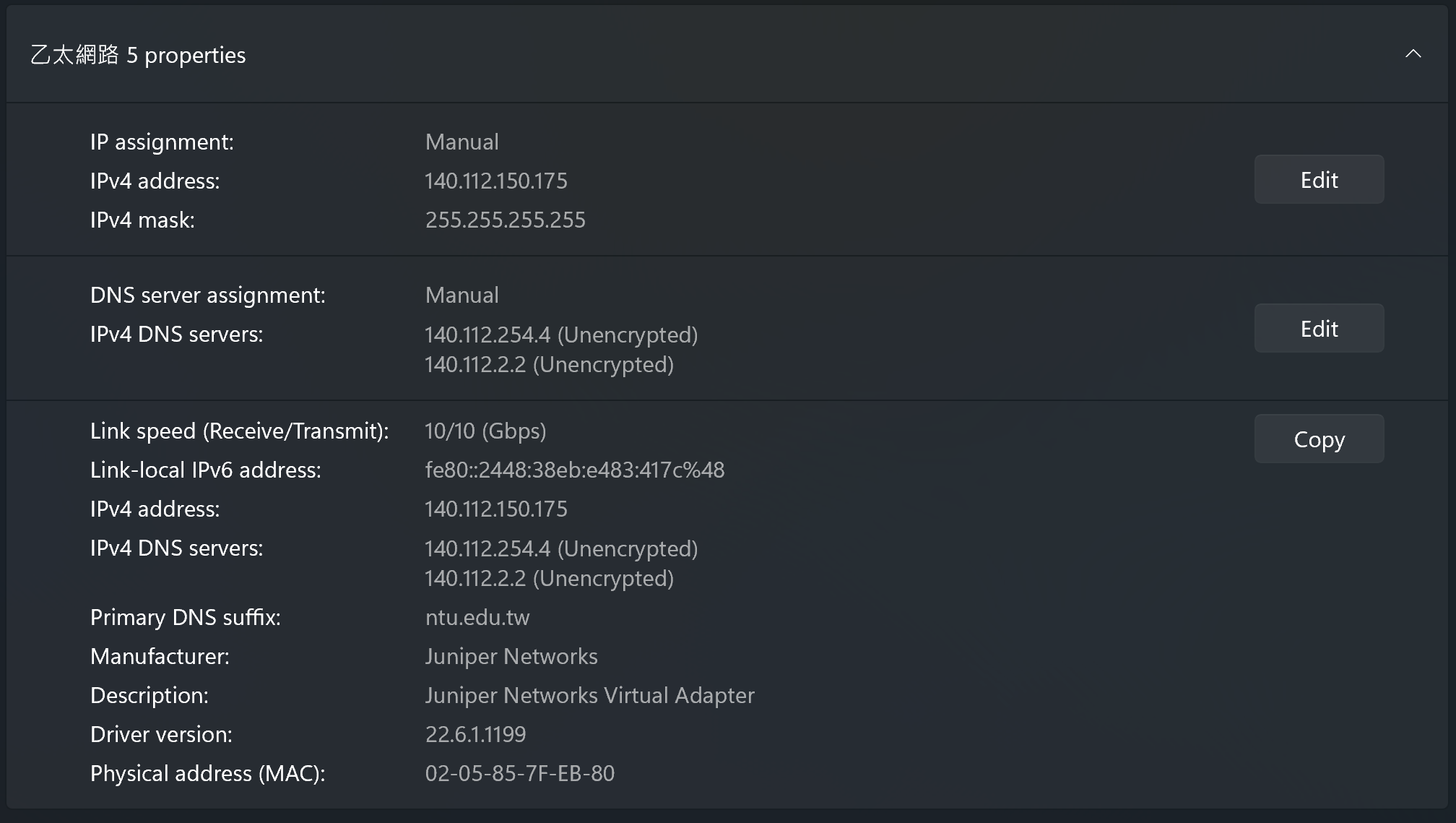


1. 使用指令如下圖第一行，domain name為if176.aca.ntu.edu.tw。

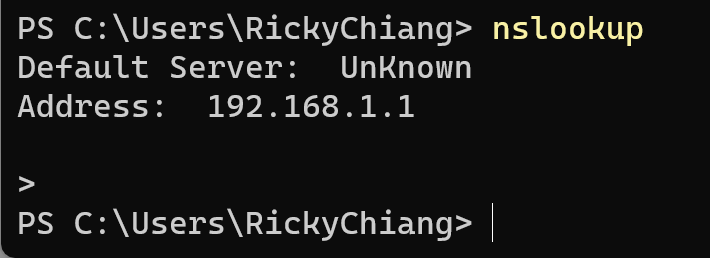
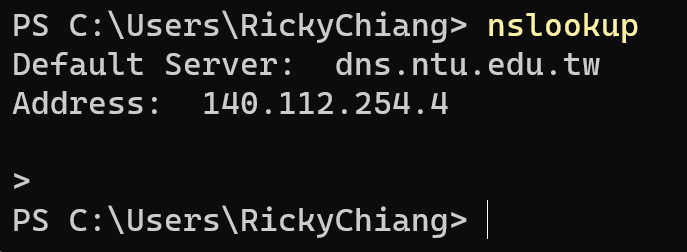


Ref: <https://zhuanlan.zhihu.com/p/382307227>

1. 下圖為連上VPN後，電腦網路設定的其中一項properties的截圖。可以看到乙太網路5的Primary DNS suffix(倒數第二行)為ntu.edu.tw，表示這是台大VPN給的properties。則可以得知IP address(第二行)為140.112.150.175。



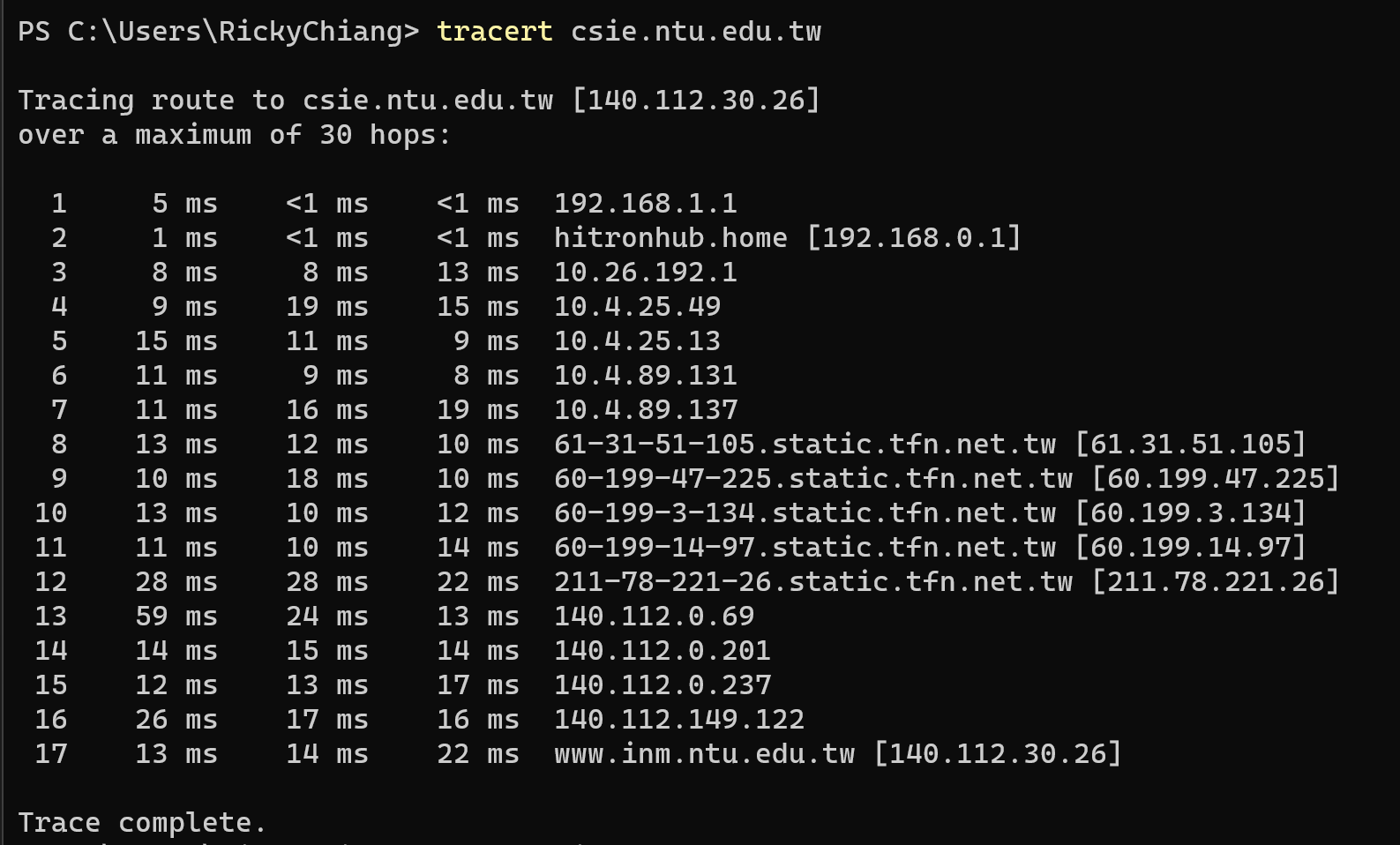
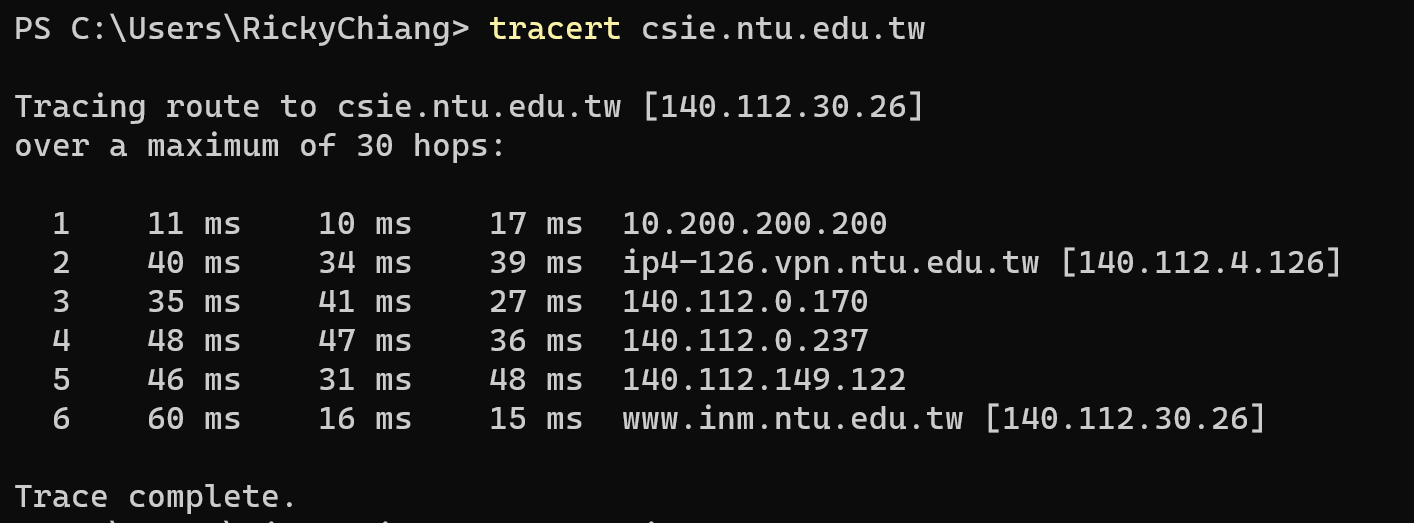
1. 下兩圖為使用VPN前後，以指令 **nslookup**追蹤routing path的截圖。可以知道DNS server IP在使用前後分別為192.168.1.1和140.112.254.4。

(使用前) (使用後)

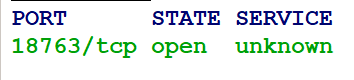
Ref: <https://www.atcnet.com.hk/eduInfoContent_221.html>

1. 下兩圖為使用VPN前後，執行 **tracert csie.ntu.edu.tw**追蹤routing path的截圖。可以知道使用VPN時會先連到VPN server，而未使用時不會。

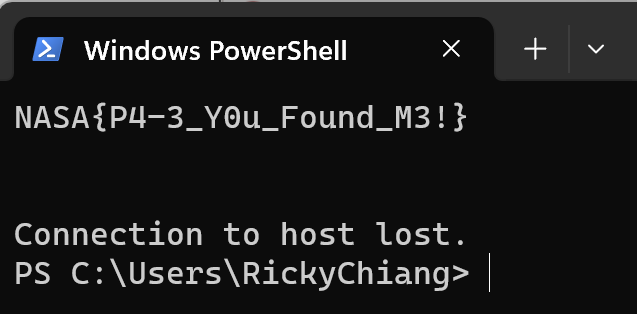
(使用前) (使用後)

1. 流程如下：
2. 下圖為Zenmap執行 **nmap -p 1-65535 -v 140.112.30.158** 得出的open Port結果。



可以得知，Port 18763便是目標伺服器。

1. 在終端機執行**telnet 140.112.30.158 18763** ，就可以收到訊息(如下圖)。



Ref: <https://help.aliyun.com/zh/ecs/enable-the-telnet-command-in-windows>

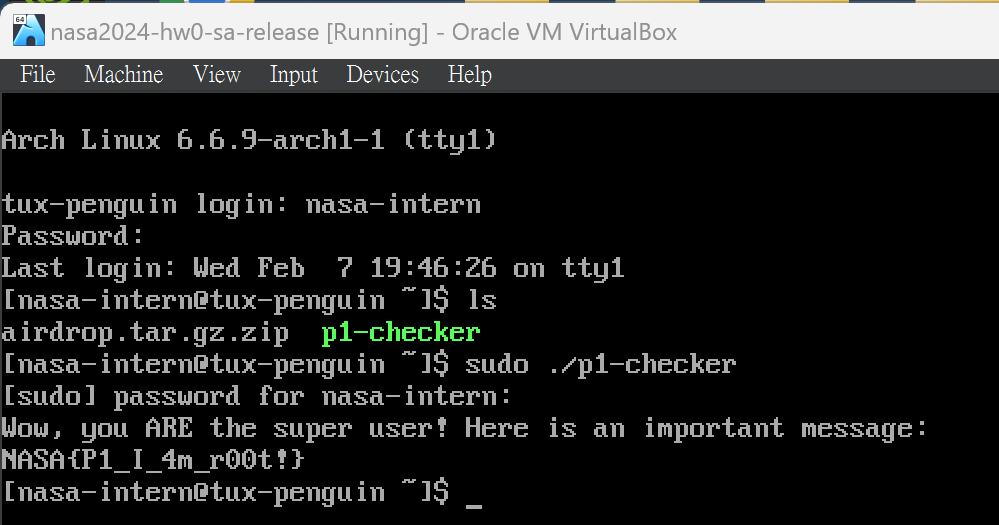
<https://hackmd.io/@Not/nmapparameter>

<https://www.ifmicro.com/记录/2017/12/12/netcat-usage/>

## System Administration

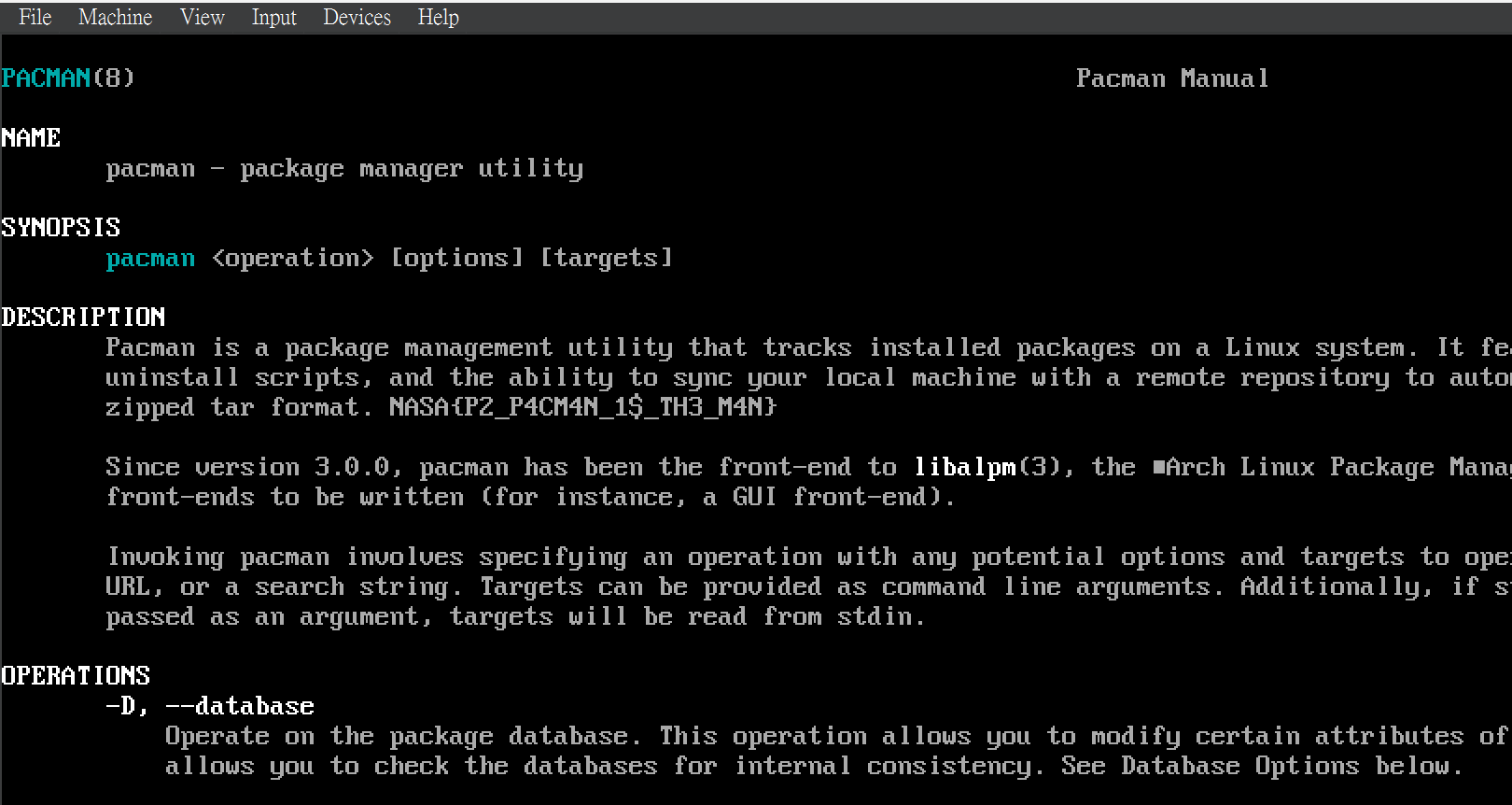
1. 下圖為使用Virtual box匯入VM後，登入並執行 **sudo ./p1-checker** 的結果。

flag為 **NASA{P1\_I\_4m\_r00t!}**

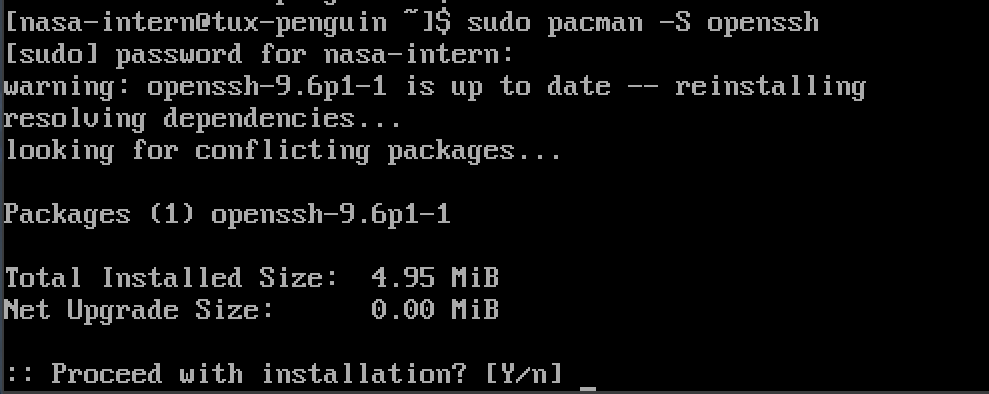


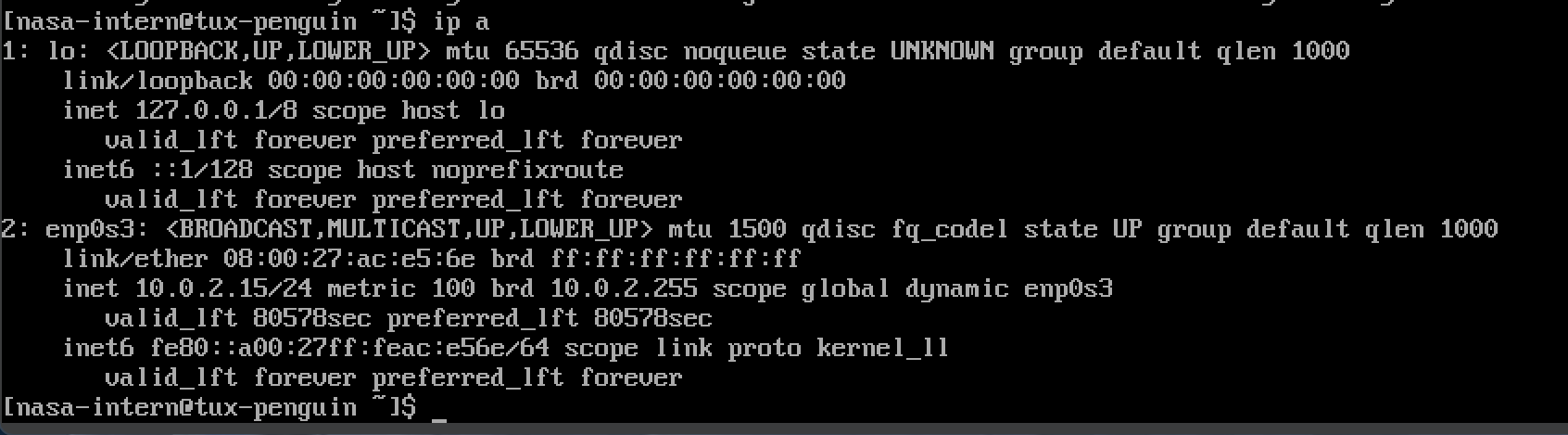
1. 下圖為執行 **man pacman** 指令後終端機的顯示頁面，可以發現flag就藏在黃色框框的位置。

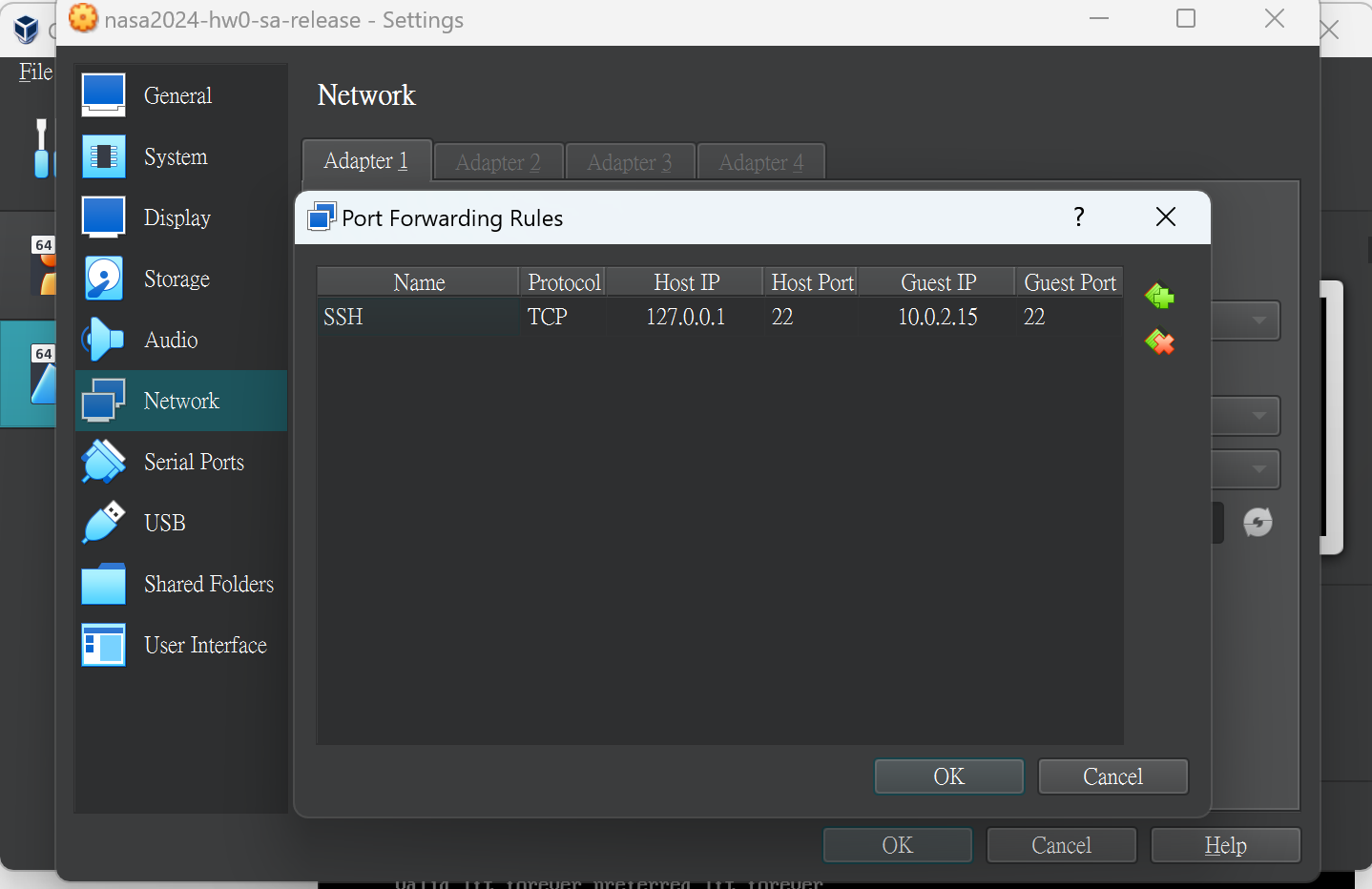
flag為 **NASA{P2\_P4CM4N\_1$\_TH3\_M4N}**



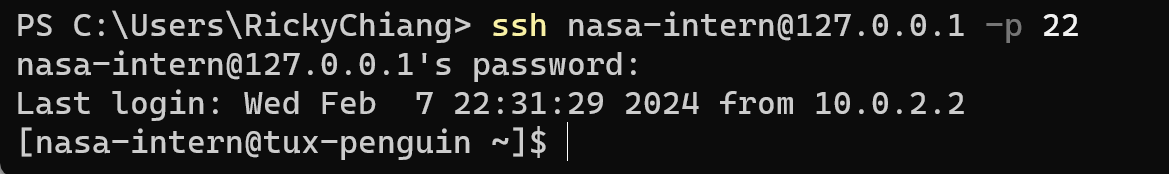
1. 流程如下：
2. 開啟並以前面的帳密登入VM，執行 **sudo pacman -S openssh** ，結果如下圖。因為已更新到最新版，因此跳過openssh的更新。



1. 執行**sudo systemctl start sshd，開啟**OpenSSH的sshd服務。
2. 執行**ip a**(如下圖)。可以得知此時VM的ip address為10.0.2.15。
3. 在Virtual Box的VM設定中增加新的Port Forwarding項目(如下圖)，其中Guest IP為步驟(3)中得到之10.0.2.15，port 為SSH預設值TCP 22。



1. 保存設定後執行 **sudo systemctl status sshd ，**確保連線成功。
2. 在電腦本機終端執行**ssh** [**nasa-intern@127.0.0.1**](mailto:nasa-intern@127.0.0.1) **-p 22** ，即可連上VM (第一次會需要確認連線，打yes)。下圖為連上VM後打密碼nasa2024以確認連線成功的截圖。



Ref: <https://cn.linux-console.net/?p=16559>

<https://www.kjnotes.com/devtools/77>

1. 流程如下：
2. 執行**unzip airdrop.tar.gz.zip**，得到解壓縮的airdrop.tar.gz。
3. 執行**tar -zx -f airdrop.tar.gz**
4. **cd**至p4的資料夾中並執行**cat flag**

flag為**NASA{P4\_Matryoshka\_Files}**

Ref: [https://linux.vbird.org/linux\_basic/centos7/0240tarcompress.php#compress\_name](https://linux.vbird.org/linux_basic/centos7/0240tarcompress.php%23compress_name)

1. 流程如下：
2. 執行更新指令**sudo pacman -Syu**
3. 執行更新指令**sudo pacman -S inetutils**
4. 執行**sudo hostname totally-not-tux**並重新開機以確保正常
5. 執行**sudo usermod -c ‘Definitely Legit Guy’ nasa-intern**更改全名
6. **cd**至p5的資料夾中並執行**./security**

flag為 **NASA{P5\_Th3\_5PY\_1s\_Am0nG\_U5}**

Ref: <https://linuxtect.com/how-to-change-user-full-name-in-linux/>

<https://linux.vbird.org/linux_basic/centos7/0410accountmanager.php>

1. 流程如下：
2. 執行**sudo useradd coolguy**
3. 執行**sudo groupadd friends**
4. 執行**sudo usermod –gid friends nasa-intern**
5. 執行**sudo usermod –gid friends coolguy**
6. **cd**至p5的資料夾中並執行**./friendship-test**

flag為 **NASA{P6\_W3\_4r3\_fri3nd5\_n0t\_f00d}**

Ref: <https://officeguide.cc/linux-add-user-to-group-tutorial/>

1. **cd**至airdrop資料下執行 **chmod 710 p7**，再重新進入p7資料夾執行**./pentester**便得到flag。

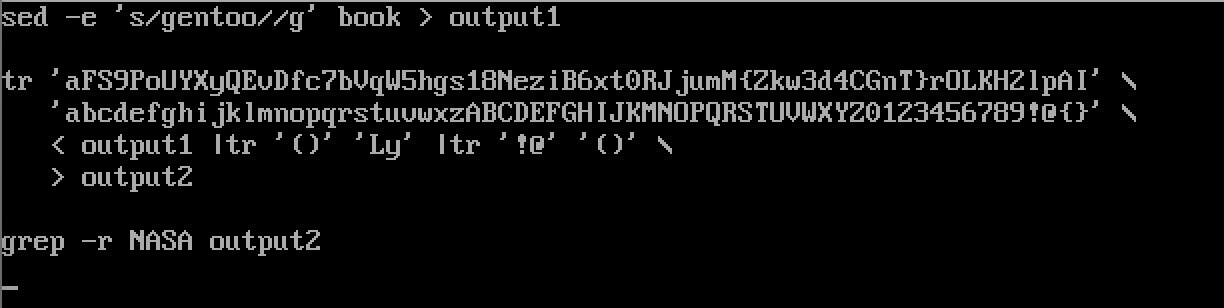
flag為**NASA{P7\_I5\_th1s\_TH3\_h0m3w0rk\_f0ld3er?}**

1. 黑白版：**NASA{P8\_cowsay -f dragon-and-cow “Hello there!”}**

彩色版：**NASA{P8\_ cowsay -f dragon-and-cow “My name is MSI RTX 4090” | lolcat}**

Ref: <https://opensource.com/article/18/12/linux-toy-cowsay>

<https://cloud.tencent.com/developer/article/1619538>

1. 流程如下：
2. 在p9資料夾下執行**touch test.sh** 新建shell script檔案
3. 在檔案中依序使用sed、tr、grep的指令如下：
4. 執行**sh test.sh**，即可得到包含flag的段落

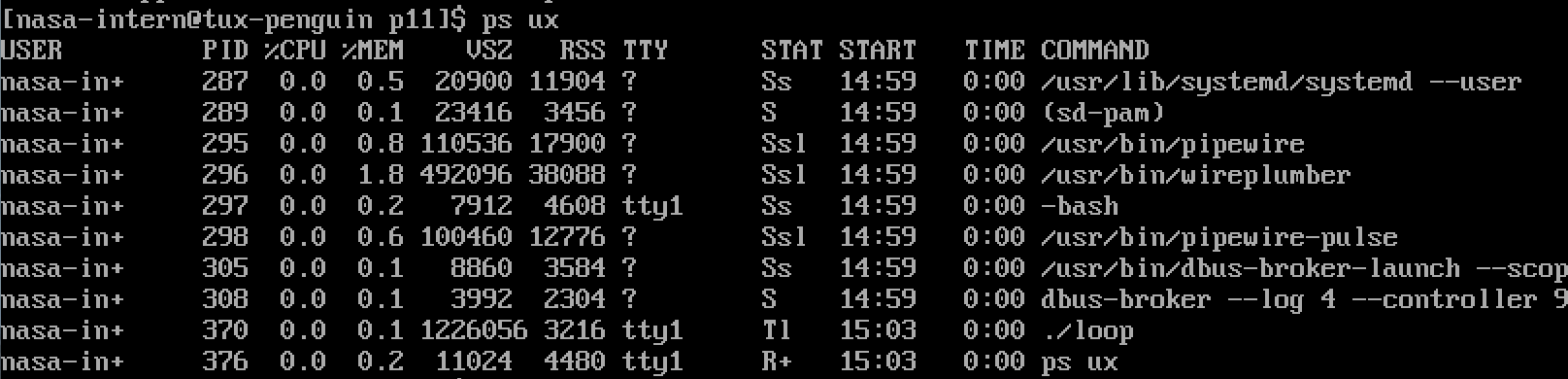
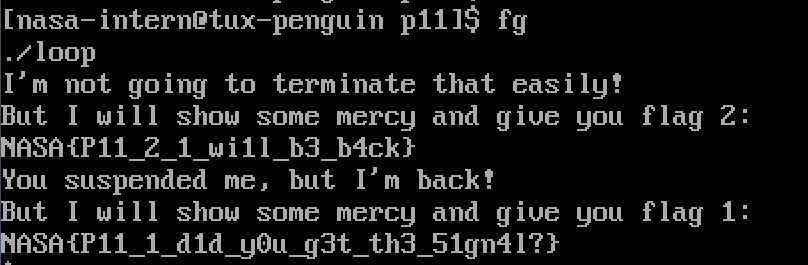
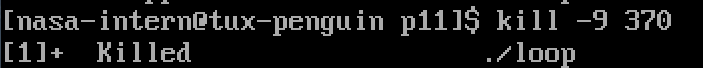
flag為**NASA{P9\_I\_Prefer\_Arch}**

Ref: <https://www.runoob.com/linux/linux-comm-sed.html>

<https://www.ibm.com/docs/zh-tw/aix/7.3?topic=t-tr-command>

1. 執行**find -name “NASA\*”**，即可得到flag檔案

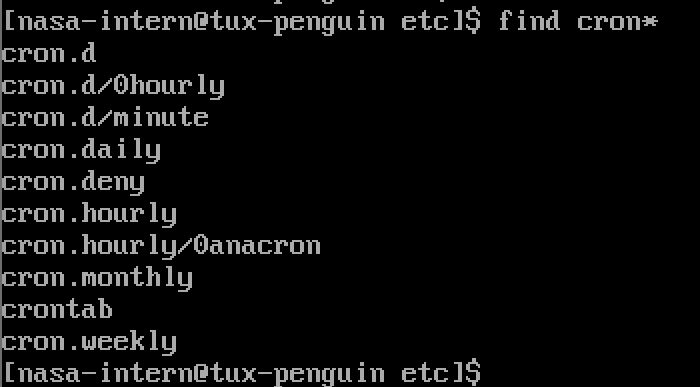
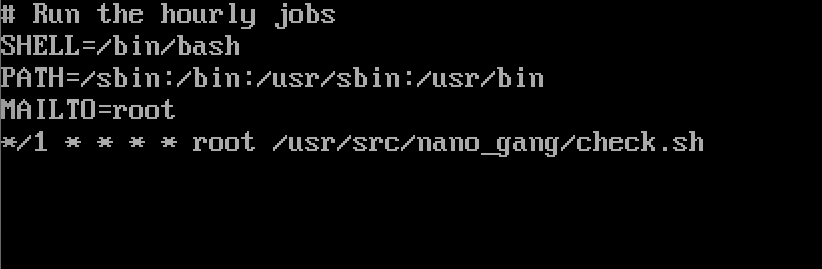
flag為**NASA{P10\_D0\_Y0U\_F1ND\_DA\_W43}**

1. 流程如下：
2. 執行**./loop**，然後按Ctrl+Z暫停程式
3. 執行 **ps ux**，找到目標process的PID (此截圖的PID為370)
4. 執行 **kill 370**
5. 執行 **fg**，回到loop中並得到兩個flag 
6. 按Ctrl+Z暫停程式，執行 **kill -9 370**，並得到與題目相符的結果

三個flag為 **NASA{P11\_1\_did\_y0u\_g3t\_th3\_51gn4l?}**

**NASA{P11\_2\_1\_wi1l\_b3\_b4ck}**

**NASA{P11\_kill -9 370}**

1. 流程如下：
2. 因為每分鐘都會有循環性工作排程來更新檔案，所以需要到 /etc 找cron相關設定。執行**find cron\***結果如下圖。
3. 因為檢查是每分鐘為單位進行的，因此查看cron.d/minute檔案(如下)，即可發現他每分鐘都會執行一次check.sh。
4. 以**sudo nano cron.d/minute**將它的最後一行註解存檔。
5. 以cd回到原目錄，將 .bashrc中的vim、vi、emacs的三行alias設定註解，並存檔重開機。
6. 重新登入與等待後都可正常使用vim及emacs

Ref: <https://linux.vbird.org/linux_basic/centos7/0430cron.php#crontab_user>