Author : IM B12705014 陳泊華

Network Administration

1-1
是。使用VPN時，真實IP地址會被掩蓋，而在線上影音服務平台接收到的封包的source IP會是VPN伺服器的IP地址，而不是原本的IP。
參考資料：VPN原理 https://nordvpn.com/zh-tw/what-is-a-vpn/ (https://nordvpn.com/zh-tw/what-is-a-vpn/)

1-2
是。在使用NAT的情況下，由於私有伺服器沒有直接暴露在網路上，外部裝置無法通過直接的方式「主動」連接到自身裝置（無法得知內網IP）。（需透過Port Forwarding或設置VPN，但這樣就非對方主動連線了）。
參考資料：NAT https://zh.wikipedia.org/zh-tw/网络地址转换 (https://zh.wikipedia.org/zh-tw/%E7%BD%91%E7%BB%9C%E5%9C%B0%E5%9D%80%E8%BD%AC%E6%8D%A2)

1-3
否。閘道器是指在不同裝置間轉送資料的裝置，可以除了透過硬體實作外，也可以使用軟體的虛擬環境實作。它可以提供路由、NAT等功能來連接LAN和WAN，本身不提供數據安全與完整性保護，但可以透過配置防火牆、使用加密通訊協議（如TLS）等方式來達成。
參考資料：閘道器 https://zh.wikipedia.org/zh-tw/网关 (https://zh.wikipedia.org/zh-tw/%E7%BD%91%E5%85%B3)

1-4
是。由於此資訊網採用http連線，傳輸資料使用明文，只要有權訪問通信路徑取得封包，便能輕易得知其中資訊。
參考資料：https://aws.amazon.com/tw/compare/the-difference-between-https-and-http/ (https://aws.amazon.com/tw/compare/the-difference-between-https-and-http/)

1-5
否。有server端的public IP，client端能夠透過自身的private IP與此IP連線，但缺少了NAT server端回送資料時便無法找到client端IP。
參考資料：https://bravo6608.pixnet.net/blog/post/3536022 (https://bravo6608.pixnet.net/blog/post/3536022)

1-6
否。DDoS是一種針對網路、服務器或應用程序的攻擊，讓合法用戶無法訪問該目標。攻擊者通常通過將大量的流量洪水式發送到目標，使其超過承受能力，導致服務中斷或嚴重降級，且由於攻擊流量來自多個來源，使得防禦變得更加困難。題幹敘述的則較偏向中間人攻擊。
參考資料：DDoS 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)

1-7
不一定。在同一演算法的假設下，雖說密碼長度很大程度上影響了組合數量，增加暴力破解難度，但密碼的多元性（如包含英文字母、大小寫、特殊符號等
）和隨機性（是否是使用有意思的文字）也會影響安全性。

2-1
否。MAC是一個區域網路位址，運作於資料鏈結層上，在設備出廠時便會分配其一個地址，也可透過搜尋器由MAC位址查詢對應廠商，但並不是「獨一無二」的；仍可透過如以下指令或其他軟體服務更改MAC位址（可能為了使用特定服務或提升安全性等）。更改後需視情況重新調整網路設定。

```
sudo ifconfig en0 ether xx:xx:xx:xx:xx:xx
```

參考資料：https://www.alphr.com/change-mac-address-in-macos/ (https://www.alphr.com/change-mac-address-in-macos/)

2-2
有問題。4G並非指傳輸速率或頻率，而是指第四代通信技術，是3G的延伸，在靜態資料傳輸速率上可以達到1Gbps，提供更高的頻譜和傳輸量（透過封包交換系統，將資料切成小封包並標上IP位址）。
參考資料：https://zh.wikipedia.org/zh-tw/4G (https://zh.wikipedia.org/zh-tw/4G) / https://pansci.asia/archives/70062 (https://pansci.asia/archives/70062)

2-3
否。雖然ipv4位址遇到枯竭問題，但透過DHCP、NAT等技術的使用，現在ipv4仍然被廣泛使用。
參考資料：https://zh.wikipedia.org/zh-tw/IPv4位址枯竭 (https://zh.wikipedia.org/zh-tw/IPv4%E4%BD%8D%E5%9D%80%E6%9E%AF%E7%AB%AD)

3-1
(a)
DHCP（Dynamic Host Configuration Protocol）是一種網路協定，用於自動分配IP地址和其他相關的網路配置信息給網路上的設備，主要功能有IP地址分配、子網遮罩分配、。DHCP的優勢在於其簡化了網路管理，特別是對於大型網路而言——它減少了手動配置的需要，確保了有效的IP地址使用，同時提供了易於管理和維護的方式。 DHCP是TCP/IP網路中廣泛使用的協定，在家庭、企業和其他組織環境中尤其常見。
參考資料：https://zh.wikipedia.org/zh-tw/动态主机设置协议 (https://zh.wikipedia.org/zh-tw/%E5%8A%A8%E6%80%81%E4%B8%BB%E6%9C%BA%E8%AE%BE%E7%BD%AE%E5%8D%8F%E8%AE%AE)

(b)
VLAN（Virtual Local Area Network）是一種在物理網路上建立邏輯上獨立的虛擬網路的技術。VLAN的目的是將一個物理網路分割成多個虛擬區域進行管理，這些區域可以跨越

多個交換機，降低區域網路廣播時造成擁塞的可能性。
參考資料：https://www.cs.nthu.edu.tw/~nfhuang/chap16.htm (https://www.cs.nthu.edu.tw/~nfhuang/chap16.htm) （b12705064趙子佾提供）

©
Switch是屬於資料連結層的一種多埠設備，作用於區域網路（LAN），在裝置間透過MAC address轉送封包。
參考資料：https://www.tp-link.com/tw/blog/119/交換器是什麼-3種常見的交換器接法-應用場景及功能介紹/ (https://www.tp-link.com/tw/blog/119/%E4%BA%A4%E6%8F%9B%E5%99%A8%E6%98%AF%E4%BB%80%E9%BA%BC-3%E7%A8%AE%E5%B8%B8%E8%A6%8B%E7%9A%84%E4%BA%A4%E6%8F%9B%E5%99%A8%E6%8E%A5%E6%B3%95-%E6%87%89%E7%94%A8%E5%A0%B4%E6%99%AF%E5%8F%8A%E5%8A%9F%E8%83%BD%E4%BB%8B%E7%B4%B9/)

(d)
Broadcast Storm 是指在計算機網路中，當有大量的廣播消息不斷地在網路上傳播，導致網路飽和，性能下降的「現象」。這種情況可能會對整個網路造成效能問題，因為大量的廣播流量會消耗帶寬並引起網路擁塞。可能造成原因有循環性廣播、不斷產生新的廣播消息等，發生時除了透過找出廣播來源加以阻止外，也可利用VLAN處理。
參考資料：https://zh.wikipedia.org/zh-tw/廣播風暴 (https://zh.wikipedia.org/zh-tw/%E5%BB%A3%E6%92%AD%E9%A2%A8%E6%9A%B4)

3-2
(a)
合法，但僅在特定情況下可使用。0.0.0.0是一個保留的IPv4地址，通常用於表示未知或無效的地址；代表本機上的所有IPV4地址，如果一個主機有兩個或以上的IP地址，並且該主機上的一個服務監聽的地址是0.0.0.0，那麼通過任一ip地址都能夠訪問該服務。另外其也可作為默認路由，即當路由表中沒有找到完全匹配的路由的時候所對應的路由。
參考資料：https://ithelp.ithome.com.tw/articles/10311096 (https://ithelp.ithome.com.tw/articles/10311096)

(b)
合法。::1是IPv6中的loopback地址，也可寫成0:0:0:0:0:0:0:1，等效於IPv4中的127.0.0.1，用於本地主機上的自我測試和迴圈測試——節點會使用迴圈位址傳送封包給自己。
參考資料：https://ithelp.ithome.com.tw/articles/10311096 (https://ithelp.ithome.com.tw/articles/10311096)

(c)
合法，但僅在特定情況下可使用。其包含128位元長度，以16位元為一組，每組以冒號隔開，分為8組，且每組以4位十六進制方式表示，但是被預留作為文件或範例位址，因此不適合作為public IP。
參考資料：https://zh.wikipedia.org/zh-tw/IP地址 (https://zh.wikipedia.org/zh-tw/IP%E5%9C%B0%E5%9D%80)

3-3

(1) 實體層 physical layer: 利用實體設備進行資料傳輸，如數據機、光纖。
(2) 資料連結層 data link layer: 將實體層訊號封裝成訊框在區域網路中進行傳輸，如乙太網路。
(3) 網路層 network layer: 把資料和IP打包成封包進行區域網路間的傳輸。
(4) 傳輸層 transport layer: 在封包傳輸的過程中確保通訊順利進行（如阻塞、錯誤偵測）。常見如TCP、UDP。
(5) 應用層 application layer: 將收到的資料結合應用程式介面呈現，以及提供常見如http、DNS、FTP等網路服務。

參考資料：https://zh.wikipedia.org/zh-tw/TCP/IP协议族 (https://zh.wikipedia.org/zh-tw/TCP/IP%E5%8D%8F%E8%AE%AE%E6%97%8F)

3-4
(a)
TCP（Transmission control protocol）是在資料傳輸層的一種協定，連線時採用三次握手，封包標識符欄位提供擁塞、流量等資訊，確保資料傳輸正確性。
參考資料：https://zh.wikipedia.org/wiki/传输控制协议 (https://zh.wikipedia.org/wiki/%E4%BC%A0%E8%BE%93%E6%8E%A7%E5%88%B6%E5%8D%8F%E8%AE%AE)

(b)
UDP（User Datagram Protocol）是在資料傳輸層的一種協定，提供不可靠傳輸，在IP封包頭部僅加入復用和資料校驗欄位，然傳輸效率高。協定如DNS、DCHP均使用UDP傳輸。
參考資料：https://zh.wikipedia.org/wiki/用户数据报协议 (https://zh.wikipedia.org/wiki/%E7%94%A8%E6%88%B7%E6%95%B0%E6%8D%AE%E6%8A%A5%E5%8D%8F%E8%AE%AE)

(c)
TCP的優點在於傳輸過程較嚴謹、穩定，透過三次握手、校驗和演算法等機制確保數據傳輸的正確性，常用於如http（確保頁面元素按照正確順序顯示）、ftp等協定。
UDP則有直接傳輸數據、效能高的優點，常用於視訊、語音通話等即時通訊服務，講求速率而可犧牲部分準確性。
參考資料：https://ithelp.ithome.com.tw/articles/10294859 (https://ithelp.ithome.com.tw/articles/10294859)

3-5
(a)
LDAP（Lightweight Directory Access Protocol）是一種用於訪問和維護分散式目錄信息的協定。它通常用於管理和檢索組織中的用戶帳戶、密碼、郵件、協作和其他資訊。
LDAP是一種客戶端-伺服器協定，基於TCP/IP通訊；預設使用TCP埠389。常見操作包括搜索（查詢）、添加（新增）、刪除、修改等。
LDAPS則是LDAP的加密版本，它使用SSL（Secure Sockets Layer）或TLS（Transport Layer Security）來加密LDAP通信，以提高安全性；預設使用TCP埠636。透過提高身份

驗證授權、電子郵件傳輸、登陸、組織管理等行為的安全性。
參考資料：https://docs.vmware.com/tw/VMware-vSphere/6.7/com.vmware.psc.doc/GUID-98B36135-CDC1-435C-8F27-5E0D0187FF7E.html (https://docs.vmware.com/tw/VMware-vSphere/6.7/com.vmware.psc.doc/GUID-98B36135-CDC1-435C-8F27-5E0D0187FF7E.html)

(b)
SMTP（Simple Mail Transfer Protocol）是用於電子郵件的一種應用層協定，它定義了電子郵件的發送和傳遞方式。SMTP通常用於發送郵件，而不是接收郵件，因此在電子郵件系統中，SMTP被用於將郵件從發件人的郵件伺服器發送到收件人的郵件伺服器；預設使用TCP埠587。另外，SMTP的安全性主要是通過加密通信（SSL, TLS）以保護郵件內容和身份驗證信息。
參考資料：https://www.cloudflare.com/zh-tw/learning/email-security/what-is-smtp/ (https://www.cloudflare.com/zh-tw/learning/email-security/what-is-smtp/)

(c)
SNMP（Simple Network Management Protocol）是一個用於管理和監控網路設備的協定。它是一種應用層協定，允許管理員通過網路監控和設置連接到網路上的各種設備；預設使用UDP埠161。常使用MIB層次化的樹狀結構作為資料信息庫使用，可用於監控和收集性能信息、配置管理、故障排除等設備管理功能。
參考資料：https://www.cc.ntu.edu.tw/chinese/epaper/0047/20181220_4707.html (https://www.cc.ntu.edu.tw/chinese/epaper/0047/20181220_4707.html)

(d)
HTTP是一種應用層協定，用於在網際網路上傳輸超文本（hypertext）文檔，通常是HTML文檔。它是Web的基礎協定，用於瀏覽器和Web伺服器之間的通信；預設使用TCP/UDP埠80。HTTPS則是HTTP的安全版本，在HTTP的基礎上添加了加密和身份驗證機制（TLS）。這使得數據在傳輸過程中更加安全，並確保通信雙方的身份；預設使用TCP埠443。

4-1
-IP Address
(a)

```
$ dig www.ntu.edu.tw
```

IP: 140.112.8.116 (ipv4)

```
❯ dig www.ntu.edu.tw

; <<>> DiG 9.10.6 <<>> www.ntu.edu.tw
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35241
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.ntu.edu.tw.                        IN      A

;; ANSWER SECTION:
www.ntu.edu.tw.         301     IN      A       140.112.8.116

;; Query time: 29 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Thu Feb 08 16:00:00 CST 2024
;; MSG SIZE  rcvd: 59
```

(b)

```
$ dig csie.ntu.edu.tw
```

IP: 140.112.30.26 (ipv4)

```
32 packets transmitted, 0 packets received, 100.0% packet loss
❯ dig csie.ntu.edu.tw

; <<>> DiG 9.10.6 <<>> csie.ntu.edu.tw
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9240
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;csie.ntu.edu.tw.               IN      A

;; ANSWER SECTION:
csie.ntu.edu.tw.        577     IN      A       140.112.30.26

;; Query time: 5 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Thu Feb 08 15:46:57 CST 2024
;; MSG SIZE  rcvd: 60
```

-Domain Name

(a)

```
$ nslookup 140.112.30.25
```

Domain name: printing.csie.ntu.edu.tw (http://printing.csie.ntu.edu.tw).

```
❯ nslookup 140.112.30.25
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
25.30.112.140.in-addr.arpa      name = printing.csie.ntu.edu.tw.
```

(b)

```
$ nslookup 140.112.161.176
```

Domain name: if176.aca.ntu.edu.tw (http://if176.aca.ntu.edu.tw).

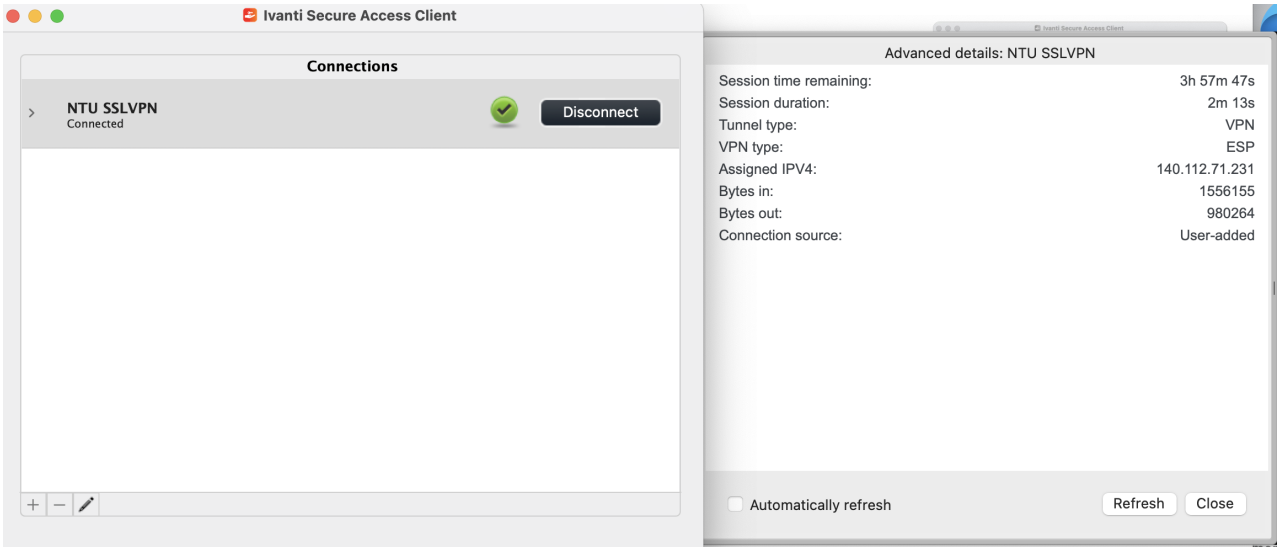
```
❯ nslookup 140.112.161.176
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
176.161.112.140.in-addr.arpa    name = if176.aca.ntu.edu.tw.
```

4-2

(a)

IP: 140.112.71.231

得知方法: 利用Ivanti Secure Access Client連到NTU SSL VPN，從Connections下查看Advanced details。



(b)

```
$ ifconfig #取得當前主機ip（連手機熱點）
```

```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=6463<RXCSUM,TXCSUM,TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        ether b0:be:83:02:19:f8
        inet6 fe80::c86:a98d:75be:d825%en0 prefixlen 64 secured scopeid 0xb
        inet 172.20.10.2 netmask 0xfffffff0 broadcast 172.20.10.15
        inet6 2404:0:823e:bc1e:182d:850e:d1fb:d464 prefixlen 64 autoconf secured
        inet6 2404:0:823e:bc1e:b09e:1958:6a7:d3d4 prefixlen 64 autoconf temporary
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
```

1. DNS server IP

```
$dig 8.8.8.8
```

Before VPN: fe80::14d1:9eff:fe2d:9e64%11

```
❯ dig 8.8.8.8

; <<>> DiG 9.10.6 <<>> 8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 31389
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;8.8.8.8.                       IN      A

;; AUTHORITY SECTION:
.                       300     IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2024022102 1800 900 604800 86400

;; Query time: 504 msec
;; SERVER: fe80::14d1:9eff:fe2d:9e64%11#53(fe80::14d1:9eff:fe2d:9e64%11)
;; WHEN: Thu Feb 22 11:06:22 CST 2024
;; MSG SIZE  rcvd: 111
```

After VPN: 140.112.254.4

```
❯ dig 8.8.8.8

; <<>> DiG 9.10.6 <<>> 8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 57246
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;8.8.8.8.                       IN      A

;; AUTHORITY SECTION:
.                       9667    IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2024022102 1800 900 604800 86400

;; Query time: 74 msec
;; SERVER: 140.112.254.4#53(140.112.254.4)
;; WHEN: Thu Feb 22 11:08:23 CST 2024
;; MSG SIZE  rcvd: 111
```

2. Routing path
   Before VPN

```
$ traceroute6 fe80::14d1:9eff:fe2d:9e64%11
$ dig +trace csie.ntu.edu.tw
```

After VPN:

```
$ traceroute 140.112.254.4
$ dig +trace csie.ntu.edu.tw #
```

參考資料：https://www.cisco.com/c/zh_tw/support/docs/ios-nx-os-software/ios-software-releases-121-mainline/12778-ping-traceroute.html (https://www.cisco.com/c/zh_tw/support/docs/ios-nx-os-software/ios-software-releases-121-mainline/12778-ping-traceroute.html) / https://blog.csdn.net/u013617791/article/details/115035664 (https://blog.csdn.net/u013617791/article/details/115035664)

4-3

```
$ sudo nmap -Pn -sS -p 0-65535 140.112.30.158 #掃描指定範圍的port，並使用-Pn省
$ nc 140.112.30.158 18763
```

開啟的port: 18763/tcp
訊息: NASA{P4-3_Y0u_Found_M3!}

```
❯ sudo nmap -Pn -sS -p 0-65535 140.112.30.158
Password:
Sorry, try again.
Password:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-08 21:16 CST
Nmap scan report for 140.112.30.158
Host is up (0.034s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE    SERVICE
0/tcp     filtered unknown
137/tcp   filtered netbios-ns
138/tcp   filtered netbios-dgm
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
18763/tcp open     unknown
65535/tcp filtered unknown
```

參考資料：https://phoenixnap.com/kb/nc-command (https://phoenixnap.com/kb/nc-command)

System Administration

(1) flag: NASA{P1_I_4m_r00t!}

```
$ sudo -i #取得super user
$ /home/nasa-intern/p1-checker #執行檔案
```

```
[nasa-intern@tux-penguin ~]$ sudo -i
[sudo] password for nasa-intern:
[root@tux-penguin ~]# pwd
/root
[root@tux-penguin ~]# /home
-bash: /home: Is a directory
[root@tux-penguin ~]# /home/nasa-intern/p1-checker
Wow, you ARE the super user! Here is an important message:
NASA{P1_I_4m_r00t!}
```

參考資料：終端機基本指令 https://dylan237.github.io/post_wasted/command-line.html (https://dylan237.github.io/post_wasted/command-line.html)

(2) flag: NASA{P2_P4CM4N_1$_TH3_M4N}

```
S man pacman #查看pacman檔案尋找flag
```

參考資料：https://wiki.archlinux.org/title/pacman (https://wiki.archlinux.org/title/pacman)

(3) no flag

1. Virtualbox操作-啟用sshd

```
$ pacman -S openssh
$ systemctl enable sshd
$ systemctl start sshd #讓virtualbox變成ssh server
$ ifconfig #取得virtualbox IP以利port forwarding設定（客體IP，須先pacman -S ne
```

2. 接著進行port forwarding設定：
   機器 -> 設定 -> 網路 -> 進階 -> 更改設定

名稱	協定	主機 IP	主機連接埠	客體 IP	客體連接埠
test	TCP	192.168.3.109	2222	10.0.2.15	22

Remote Desktop操作

```
$ ifconfig #取得remote desktop IP 以利port forwarding設定（主體IP，須先pacman
$ ssh nasa-intern@192.168.3.109 -p 2222
```

```
nasa-student@nasa-student-09:~$ ssh nasa-intern@192.168.3.109 -p 2222
nasa-intern@192.168.3.109's password:
Last login: Sat Feb 10 10:03:43 2024
[nasa-intern@totally-not-tux ~]$
```

#遠端桌面已經用本機nmap掃過沒開

參考資料：
https://yenslife.top/2023/01/27/Ubuntu-remote-ssh-macbook/
(https://yenslife.top/2023/01/27/Ubuntu-remote-ssh-macbook/)
https://snoopy30485.github.io/2018/06/30/VirtualBox使用SSH連線/
(https://snoopy30485.github.io/2018/06/30/VirtualBox%E4%BD%BF%E7%94%A8SSH%E9%80%A3%E7%B7%9A/)

(4) flag: NASA{P4_Matryoshka_Files}

```
unzip airdrop.tar.gz.zip #解開zip檔
tar -zxvf airdrop.tar.gz #解開tar.gz檔；-z表用gzip解壓縮，-x表解包，-v表詳細模式
```

參考資料：Linux更改檔案權限
https://linux.vbird.org/linux_basic/centos7/0210filepermission.php
(https://linux.vbird.org/linux_basic/centos7/0210filepermission.php)

(5) flag: NASA{P5_Th3_5PY_1s_Am0nG_U5}

```
$ cd /etc
$ sudo nano hostname #更改hostname
$ sudo chfn nasa-intern #change finger information for nasa-intern
```

參考資料：Linux更改hostname https://aiops.com/news/post/6870.html
(https://aiops.com/news/post/6870.html)

(6) flag: NASA{P6_W3_4r3_fri3nd5_n0t_f00d}

```
$ sudo useradd coolguy
$ cat /etc/passwd #確認user創建成功
$ sudo groupadd friends
$ cat /etc/group #確認group創建成功
$ sudo usermod -aG friends coolguy
$ sudo usermod -aG friends nasa-intern
$ getent group friends #查看friends群組成員
```

```
[nasa-intern@totally-not-tux p6]$ getent group friends
friends:x:1001:nasa-intern,coolguy
```

參考資料：帳號與身份管理
https://linux.vbird.org/linux_basic/mandrake9/0410accountmanager.php#groups
(https://linux.vbird.org/linux_basic/mandrake9/0410accountmanager.php#groups)

(7) flag: NASA{P7_l5_th1s_TH3_h0m3w0rk_f0ld3er?}

```
$ cd airdrop
$ chmod 710 p7 #群組成員可以進資料夾但不能讀寫
```

參考資料：
https://linux.vbird.org/linux_basic/mandrake9/0210filepermission.php#chmod
(https://linux.vbird.org/linux_basic/mandrake9/0210filepermission.php#chmod)

(8)
lolcat
P8_cowsay -f dragon-and-cow Hello there!}
flag1: NASAflag2: NASA{P8_cowsay -f dragon-and-cow My name is MSI RTX 4090

```
$ pacman -S cowsay
$ cowsay -f dragon-and-cow Hello there!
$ cowsay -f dragon-and-cow My name is MSI RTX 4090 | lolcat
```

參考資料：cowsay https://hackmd.io/@brlin/SkJi-KlWV/https%3A%2F%2Fhackmd.io%2FS91yaPSqSI6K3xhg1JfB8w?type=book
(https://hackmd.io/@brlin/SkJi-KlWV/https%3A%2F%2Fhackmd.io%2FS91yaPSqSI6K3xhg1JfB8w?type=book)

(9) flag: NASA{P9_I_Prefer_Arch}

```
$ sed 's/gentoo//g' book > output #過濾原文中的gentoo
$ cat output | tr 'aFS9PoUYXyQEvDfc7bVqW5hg)s18NeziB6xt0(RJjumM{Zkw3d4CGn
$ cat output2 |grep NASA #快速找出flag位置
```

參考資料：Linux正則表達式 https://ithelp.ithome.com.tw/articles/10210434?sc=iThelpR (https://ithelp.ithome.com.tw/articles/10210434?sc=iThelpR)

(10) flag: NASA{P10_D0_Y0U_F1ND_DA_W43}

```
$ find ./ |grep NASA #以flag的型態來篩選
```

(11)
flag1: NASA{P11_1_d1d_y0u_g3t_th3_51gn4l?}

```
$ Ctrl + Z #暫停程式並移至後景執行
$ bg #將程式移景繼續執行
```

flag2: NASA{P11_2_1_wi1l_b3_b4ck}

```
$ ./loop
$ ps aux |grep loop #找出./loop的PID
$ kill -15 <PID>
```

flag3: NASA{P11_kill -9 <PID>}

```
$ ./loop
$ ps aux |grep loop #找出./loop的PID
$ kill -9 <PID>
```

參考資料：查看PID https://www.itcool.net/909.html (https://www.itcool.net/909.html)

(12)

1. 暫時解法：直接修改alias或修改bash.bashrc中的alias

```
$ alias vim='vim'
$ alias emacs='emacs'
```

```
$ cd /etc
$ sudo nano bash.bashrc
$ alias vim='vim' #在.bashrc檔案中更改設定
$ alias emacs='emacs'
```

```
[nasa-intern@totally-not-tux cron.d]$ cat /usr/src/nano_gang/check.sh
#!/usr/bin/env bash

username='nasa-intern'
bashrcToCheck="/home/${username}/.bashrc"
bashrcBackup='/root/.docker.service'
msgFile='/root/.docker.service.log'

rollback() {
    cat ${msgFile} | wall 2>/dev/null
    cp "${bashrcBackup}" "${bashrcToCheck}"
    chown "${username}:${username}" "${bashrcToCheck}"
}

if [ ! -f "${bashrcToCheck}" ]; then
    rollback
fi

diff "${bashrcToCheck}" "${bashrcBackup}" > /dev/null
if [ $? -ne 0 ]; then
    rollback
fi
```

#發現跳出nano gang

2. 永久解法：

```
$ cd /etc/cron.d
```

發現hour、minute檔案，打開minute檔案

```
[nasa-intern@totally-not-tux cron.d]$ ls
0hourly  minute
[nasa-intern@totally-not-tux cron.d]$ cat minute
```

找到nano gang的位置，以及裡面的check.sh (http://xn--check-ok2hl60a9p6e2s8a4k4a.sh)

```
$ cat /usr/src/nano_gang/check.sh
```

```
[nasa-intern@totally-not-tux cron.d]$ cat /usr/src/nano_gang/check.sh
#!/usr/bin/env bash

username='nasa-intern'
bashrcToCheck="/home/${username}/.bashrc"
bashrcBackup='/root/.docker.service'
msgFile='/root/.docker.service.log'

rollback() {
    cat ${msgFile} | wall 2>/dev/null
    cp "${bashrcBackup}" "${bashrcToCheck}"
    chown "${username}:${username}" "${bashrcToCheck}"
}

if [ ! -f "${bashrcToCheck}" ]; then
    rollback
fi

diff "${bashrcToCheck}" "${bashrcBackup}" > /dev/null
if [ $? -ne 0 ]; then
    rollback
fi
```

發現「cp "*bashrcBackup*"{bashrcToCheck}"」會檢查

```
$ sudo nano /root/.docker.service
```

打開.docker.service，刪除nano gang部分

重新登入後發現可使用vim

#<另>也可觀察check.sh發現沒有追蹤profile，但shell啟動時也會讀取進而修改

參考資料：https://www.ibm.com/docs/zh-tw/aix/7.1?topic=commands-creating-command-alias-alias-shell-command (https://www.ibm.com/docs/zh-tw/aix/7.1?topic=commands-creating-command-alias-alias-shell-command)