

NASA2022 Homework5

b08902149 資工三 徐晨祐

DNS & DHCP

1. Build DNS and DHCP server

1. Server VM:

(a.)(b.)

我使用的是virtual box，將CentOS安裝好之後，首先我們需要讓該VM新增兩張網卡，一個attach到NAT，一個attach到Internal Network，然後開啟機器。

為了開啟對內的網路，並設定固定IP，將 `/etc/sysconfig/network-scripts/ifcfg-enp0s8` 的內容改成如下：

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=enp0s8
UUID=a75aa5fb-aee2-45d8-be75-cea8057bdc50
DEVICE=enp0s8
ONBOOT=yes
IPADDR=192.168.5.254
GATEWAY=192.168.5.1
NETWORK=192.168.5.0
NETMASK=255.255.255.0
```

再透過 `service network restart` 即可完成。我們可以用 `ip a` 這個指令來檢查：

```
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
```

```

2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
default qlen 1000
    link/ether 08:00:27:c5:3b:6c brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global noprefixroute dynamic enp0s3
        valid_lft 84146sec preferred_lft 84146sec
    inet6 fe80::56f7:c677:abf2:efb5/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
default qlen 1000
    link/ether 08:00:27:7e:26:50 brd ff:ff:ff:ff:ff:ff
    inet 192.168.5.254/24 brd 192.168.5.255 scope global noprefixroute enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe7e:2650/64 scope link
        valid_lft forever preferred_lft forever

```

最後透過 `ifup enp0s3` 開啟對外的網路連線。

Reference:

查詢UUID: <https://www.twblogs.net/a/5b96b6572b717750bda55340>

取得static IP: <https://www.gushiciku.cn/pl/gi8r/zh-tw>

(c.)

我們先用 `yum install bind` 來安裝bind。

接下來執行下列指令，新增一個資料夾來存放zone files：

```

chmod 755 /etc/named
sudo mkdir /etc/named/zones

```

修改 `/etc/named.conf` 成以下內容：

```

options {
    listen-on port 53 { 127.0.0.1; 192.168.5.254; };
    listen-on-v6 port 53 { ::1; };
    directory    "/var/named";
    dump-file    "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    recursing-file  "/var/named/data/named.recurse";
    secroots-file   "/var/named/data/named.secroots";
    allow-query     { localhost; 192.168.5.0/24; };
    allow-recursion   { localhost; 192.168.5.0/24; };
    recursion yes;
    dnssec-enable yes;
    dnssec-validation yes;
    bindkeys-file "/etc/named.root.key";
    managed-keys-directory "/var/named/dynamic";
    pid-file "/run/named/named.pid";
    session-keyfile "/run/named/session.key";
};

```

```

logging {
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
};

zone "." IN {
    type hint;
    file "named.ca";
};

zone "b08902149.com" IN {
    type master;
    file "/etc/named/zones/b08902149.com.zone";
    allow-update { none; };
};

zone "4.3.2.1.in-addr.arpa" IN {
    type master;
    file "/etc/named/zones/1.2.3.4.zone";
    allow-update { none; };
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

```

新增一個 `/etc/named/zones/b08902149.com.zone` 檔案，內容如下：

```

@      IN      SOA      b08902149.com. admin.b08902149.com. (
                  3          ; Serial
                 604800    ; Refresh
                 86400     ; Retry
                2419200   ; Expire
                 604800 )    ; Negative Cache TTL
;
; name servers - NS records
      IN      NS      b08902149.com.
; name servers - A records
b08902149.com.           IN      A      192.168.5.254
www.b08902149.com.       IN      A      1.2.3.4

```

新增一個 `/etc/named/zones/1.2.3.4.zone` 檔案，內容如下：

```
@      IN      SOA      b08902149.com. admin.b08902149.com. (
                      3           ; Serial
                     604800     ; Refresh
                     86400      ; Retry
                    2419200    ; Expire
                   604800 )    ; Negative Cache TTL
; name servers - NS records
IN  NS  b08902149.com.
; PTR records
4.3.2.1.in-addr.arpa.   IN  PTR www.b08902149.com.
254.5.168.192-in.addr.arpa. IN  PTR b08902149.com.
```

可以透過以下指令檢查是否正確，若正確會顯示OK：

```
sudo named-checkconf
sudo named-checkzone b08902149.com /etc/named/zones/b08902149.com.zone
sudo named-checkzone 4.3.2.1.in-addr.arpa /etc/named/zones/1.2.3.4.zone
```

將服務開啟：

```
systemctl start named
systemctl enable named
```

設定防火牆：

```
firewall-cmd --permanent --add-port=53/udp
firewall-cmd --reload
```

Reference:

在CentOS上架設DNS server：<https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-private-network-dns-server-on-centos-7>

(d.)

透過以下指令安裝需要的套件：

```
yum install dnf
yum install dhcp
dnf clean all
dnf update
dnf install dhcp-server
```

接著我們修改 `/etc/dhcp/dhcpd.conf` 為以下內容：

```
option domain-name "b08902149.com";
option domain-name-servers 192.168.5.254;
default-lease-time 3600;
max-lease-time 7200;
authoritative;
subnet 192.168.5.0 netmask 255.255.255.0 {
    option routers                 192.168.5.254;
    option subnet-mask             255.255.255.0;
    option domain-name-servers     192.168.5.254;
    range   192.168.5.100         192.168.5.200;
}
```

透過 `sudo systemctl restart dhcpcd` 重啟服務。

設定防火牆：

```
firewall-cmd --permanent --add-port=67/udp
firewall-cmd --reload
```

(Note: 以上操作做完之後如果遇到無法成功運作的狀況，可以 `reboot` 看看)

Reference:

在CentOS上架設DHCP server：<https://linuxapt.com/blog/917-set-up-dhcp-server-centos-8>

2. Client VM:

(a.)

在安裝好ubuntu之後，先安裝一些套件，使用指令：`sudo apt install dhcpcd5`

接著將它的網卡改成一個attach到Internal Network的網卡。

我們可以用`sudo dhcpcd -T`來檢查DHCP server。

接著再透過下列指令取得ip：

```
sudo dhclient -r  
sudo dhclient
```

透過`ip a`檢查ip是否真的在`192.168.5.0/24`底下：

```
willy@willy-laptop:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:81:6b:86 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.5.103/24 brd 192.168.5.255 scope global dynamic enp0s8  
        valid_lft 3485sec preferred_lft 3485sec  
    inet 192.168.5.102/24 brd 192.168.5.255 scope global secondary dynamic enp0s8  
        valid_lft 3490sec preferred_lft 3490sec  
    inet 192.168.5.101/24 brd 192.168.5.255 scope global secondary noprefixroute enp0s8  
        valid_lft forever preferred_lft forever  
    inet6 fe80::4c6f:5e06:9fe4:a135/64 scope link  
        valid_lft forever preferred_lft forever  
willy@willy-laptop:~$ █
```

討論對象：

B09505014 王聖文

(b.)

dig www.b08902149.com 的結果：

```
willy@willy-laptop:~$ dig www.b08902149.com

; <>> DiG 9.16.1-Ubuntu <>> www.b08902149.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53104
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: fad7a627a300dc5c397719f2627e9cafce5c914357cb85a0 (good)
;; QUESTION SECTION:
;www.b08902149.com.           IN      A

;; ANSWER SECTION:
www.b08902149.com.    604800  IN      A      1.2.3.4

;; AUTHORITY SECTION:
b08902149.com.        604800  IN      NS     b08902149.com.

;; ADDITIONAL SECTION:
b08902149.com.        604800  IN      A      192.168.5.254

;; Query time: 8 msec
;; SERVER: 192.168.5.254#53(192.168.5.254)
;; WHEN: 六 五 14 01:52:27 CST 2022
;; MSG SIZE rcvd: 120
```

dig google.com 的結果：

```
willy@willy-laptop:~$ dig google.com

; <>> DiG 9.16.1-Ubuntu <>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21977
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: f6988b20c0177d809f280dec627e9d1c7d71e914a08f003e (good)
;; QUESTION SECTION:
;google.com.           IN      A

;; ANSWER SECTION:
google.com.        300    IN      A      142.251.43.14

;; AUTHORITY SECTION:
google.com.        172800  IN      NS     ns3.google.com.
google.com.        172800  IN      NS     ns1.google.com.
google.com.        172800  IN      NS     ns4.google.com.
google.com.        172800  IN      NS     ns2.google.com.

;; ADDITIONAL SECTION:
ns2.google.com.    172800  IN      A      216.239.34.10
ns1.google.com.    172800  IN      A      216.239.32.10
ns3.google.com.    172800  IN      A      216.239.36.10
ns4.google.com.    172800  IN      A      216.239.38.10
```

dig -x 1.2.3.4 的結果：

```
willy@willy-laptop:~$ dig -x 1.2.3.4

; <>> DiG 9.16.1-Ubuntu <>> -x 1.2.3.4
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44506
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 5cb64dfcf64fd138448f518f627e9d8250389e8539c1281b (good)
;; QUESTION SECTION:
;4.3.2.1.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
4.3.2.1.in-addr.arpa. 604800 IN PTR www.b08902149.com.

;; AUTHORITY SECTION:
4.3.2.1.in-addr.arpa. 604800 IN NS b08902149.com.

;; ADDITIONAL SECTION:
b08902149.com.        604800 IN A   192.168.5.254

;; Query time: 8 msec
;; SERVER: 192.168.5.254#53(192.168.5.254)
;; WHEN: 六 五 14 01:55:58 CST 2022
;; MSG SIZE rcvd: 138
```

Reference: 無

2. Short Answers

(1.)

DNS-over-HTTPS就是以加密的HTTPS協定進行DNS解析請求，避免原本的DNS query被竊聽或在傳輸過程中被竄改。優點是可以藉此防止中間人攻擊，其中一個缺點是當我們把查詢資料加密之後，就沒有辦法透過黑名單或查詢資料來判斷使用者是否連接到惡意網站。

Reference:

<https://www.ithome.com.tw/news/133499>

(2.)

攻擊者可以透過殭屍電腦群(Botnet)來對未做好安全設定的DNS server發送假冒受害者IP位置的DNS query，這樣受害者就會收到大量的DNS reply導致其無法進行正常服務。由於攻擊者發送的封包大小是小於受害者所收到的封包，在這個攻擊過程中具有流量放大的效果，因此稱作amplification attack。

Reference:

https://www.cc.ntu.edu.tw/chinese/epaper/0028/20140320_2808.html

(3.)

DNS通常都會有cache的功能，讓下次收到一樣的query時可以直接快取。如果DNS server收到假冒的DNS封包，導致將錯誤的IP和domain name對應並且存在cache裏，就會讓之後再query這個domain name的使用者連接到錯誤的IP。防範方法之一是透過DNSEC，這是透過數位簽章的方式來達到驗證目的，其運作方式簡單來說就是透過數位簽章的簽署與驗章的過程，降低DN假冒的風險。

Reference:

https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=5886

(4.)

Kaminsky attack是將流量都redirect到某個惡意的domain，攻擊者首先向目標DNS server發送一個隨機序列與目標域名的組合，例如b08xxx149.ntu.edu，很明顯的這是一個不存在的域名，攻擊者可以在目標DNS server要詢問其他DNS server 這個b08xxx149.ntu.edu所對應之IP時，在目標server收到回覆之前先回覆他說，要查詢ntu.edu請向badserver.ntu.edu查詢，此時該收到回覆的server會將這件事存入cache，之後他要查詢任何有ntu.edu的domain name都會向這個惡意的badserver.ntu.edu查詢。

由於一般的DNS cache poisoning attack都是希望將某個已知存在的域名（也就是使用者真的會去使用到的域名）導向一個錯誤的IP位置，但是如果此時DNS server內的cache已經有儲存這個域名所對應到的IP，那server在一段有效時間(TTL)都不會再向其他server發送解析該域名的請求，攻擊者也將無法得手，尤其現在Cache TTL設置的時間又很長。然而Kaminsky attack克服了這個缺陷，使得攻擊更容易成功也更難防禦。

Reference:

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj2rJGLg973AhXIA4gKH_RN0BUgQFnoECC4QAQ&url=http%3A%2F%2Fwww.securitylab.disi.unitn.it%2Flib%2Fexe%2Ffetch.php%3Fmedia%3Dteaching%253Anetsec%253A2016%253Akaminskyattack_group21_.pdf&usg=AOvVaw2IBpTfZolxKeovNyBiFtDG

<https://wenku.baidu.com/view/04ba655be518964bcf847c6b.html>

NFS & Fix VM

Fix VM

(1.)

首先我們到工作站執行以下指令：

```
curl http://linux7.csie.ntu.edu.tw:17718/init.sh | bash  
screen  
bash /tmp2/b08902149/NASAHW5/run.sh 1234 32
```

之後我們就可以在自己的本機開啟vnc viewer來使用，由於我上述指令是用 `linux7.csie.ntu.edu.tw` 開的，所以我在我的vnc viewer打上 `linux7.csie.ntu.edu.tw:5932` 來連線。

連線成功之後，因為我知道vim的swap file的檔名通常是以 `.swp` 結尾，因此我透過 `find \ -name *.swp` 來掃看看有沒有這樣的檔案，結果就看到了一個 `/.hidden_file/1/4/7/11/12/.shadow.swp`，於是將它複製到工作站，透過下列指令：

```
scp /.hidden_file/1/4/7/11/12/.shadow.swp b08902149@linux7.csie.ntu.tw:/tmp2/b08902149
```

接下來，我將該檔案 `cat` 出來，發現其內容可以透過 `hashcat` 去破解，於是將root的部分複製下來，在我的本機使用以下指令破解：

```
hashcat -a 0 -m 1800 /Users/chriscyhxx/Desktop/hw5_shadow.txt  
/Users/chriscyhxx/Desktop/wordlist
```

就得到了root密碼為 kamisama 。

其中，wordlist是從<https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credential-Lists/10-million-password-list-top-1000000.txt>下載的。

在此紀錄一下 hashcat 在mac上可能遇到的一些問題，

第一個是安裝的指令

```
git clone https://github.com/hashcat/hashcat.git
cd hashcat
make
sudo make install
```

接下來如果我們安裝好後直接透過 hashcat 指令去解密，可能會跳出以下的error：

```
fatal error: 'inc_vendor.h' file not found
```

此時的解決方法是，進入 /usr/local/share/hashcat/OpenCL/ 這個資料夾在進行 hashcat 這個指令

接著解釋一下上述的 hashcat 指令，-a 是去說明要用什麼方式破解，0 是代表用字典破解；-m 是說明加密的方法，由於從 .shadow.swp 這個檔案可以看到root加密是用 \$6\$ 也就是 sha512，所以我們選擇用 -m 1800 。

Reference:

hashcat用法：<https://xz.aliyun.com/t/4008>

vim swap file：<https://www.quora.com/What-are-swap-files-in-vim-and-how-to-deal-with-them>

(2.)

透過 journalctl -u sshd 去查看ssh失敗的原因。

發現pam在認證的過程中會使用google_authenticator，於是透過下列指令去找尋在哪個configuration file裡有設定到要使用該套件：

```
grep google /etc/pam.d/*
```

會發現到在 /etc/pam.d/system-remote-login 裡有以下的設定：

```
auth required pam_google_authenticator.so
```

將其註解掉，再透過 systemctl restart sshd 即可正常連線。

Reference:

journalctl 用法：<https://www.gushiciku.cn/pl/peum/zh-tw>

ssh修正：<https://linuxhint.com/fix-ssh-permission-denied-public-key/>

討論對象：B09505014 王聖文

PXE boot using NFS

(1.)

PXE(Preboot eXecution Environment)提供客戶端以介面卡下載映像檔來開機，而不需依靠本地端的儲存裝置，客戶端會先以DHCP協定搜尋是否有可用的DHCP server，若有即向其詢問網路啟動程式的路徑，且透過TFTP來傳輸。PXE boot主要的使用情境是在一個或多個全新或是故障的電腦上安裝作業系統，例如學校的電腦教室可以透過PXE boot來安裝linux，省去分割磁碟機的困擾。其有幾項優點：

- 客戶端機器無需storage device或os
- 由於PXE獨立於供應商，因此要做Network extension很方便
- 大多數的任務都是遠程執行即可，簡化了維護的過程

Reference:

優點：<https://www.techopedia.com/definition/26200/preboot-execution-environment-pxe>

使用情境：<https://www.techtarget.com/searchnetworking/definition/Preboot-Execution-Environment>

(2.)

首先，我在工作站上透過下列指令下載 qcow2：

```
qemu-img convert -O vdi host.qcow2 host.vdi
```

將其下載到本機之後，使用virtual box新增一個arch linux，在setting > storage透過Adds new storage attachment將host.vdi加上去。接著到setting > system將Enable EFI打勾，並開啟vm。

開啟之後，先打exit離開Shell，進到Boot Maintenance Manager > Boot Options > Add Boot Option > EFI > grub，在description的欄位隨便打，我打了hellohello。

回到首頁，點選Boot Maintenance Manager > Boot Options > Change Root Order，將hellohello移到最高位，再回到首頁，點選reset，就完成安裝vm了。

登入後，我們先更新一下，並且給他一個固定IP：

```
pacman -Syu  
ip addr add 192.168.0.1/24 dev enp0s8
```

因為我們需要DHCP+TFTP，因此我們安裝dnsmasq：

```
pacman -Sy dnsmasq  
systemctl start dnsmasq  
systemctl enable dnsmasq
```

透過下列指令安裝iso：

```
curl -O http://mirror.archlinux.tw/ArchLinux/iso/2022.05.01/archlinux-2022.05.01-x86_64.iso
```

然後我們必須先reboot，開機後重新要一次IP：`ip addr add 192.168.0.1/24 dev enp0s8`，之後透過以下方式來mount iso：

```
mkdir -p /mnt/archiso
mount -o loop,ro archlinux-2022.05.01-x86_64.iso /mnt/archiso
```

接著我們修改 `/etc/dnsmasq.conf` 為以下內容：

```
port=0
interface=enp0s8
bind-interfaces

dhcp-range=192.168.0.50,192.168.0.150,12h
dhcp-boot=syslinux/lpxelinux.0,192.168.0.1
dhcp-option=3,192.168.0.1
dhcp-option=6,8.8.8.8

dhcp-option-force=209,archiso_pxe.cfg
pxe-prompt="Press F8 for PXE Network boot",5
enable-tftp
tftp-root=/mnt/archiso
```

用下列指令開啟 `dnsmasq` 服務：

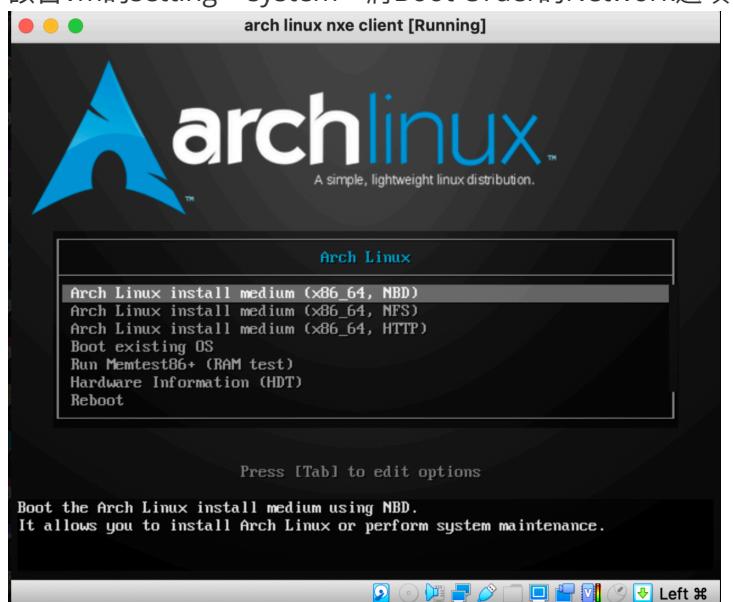
```
systemctl start dnsmasq
systemctl enable dnsmasq
```

接下來要配置nfs server，首先安裝：`pacman -Sya nfs-utils`，接下來執行以下指令：

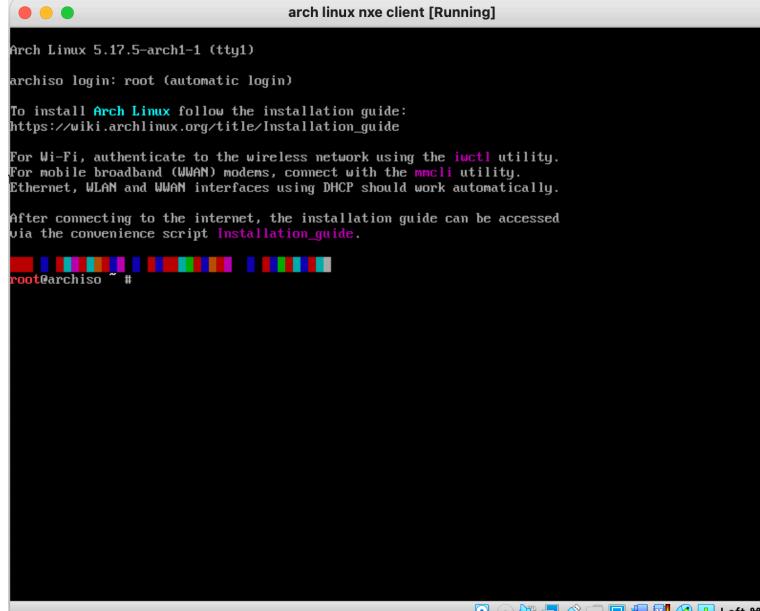
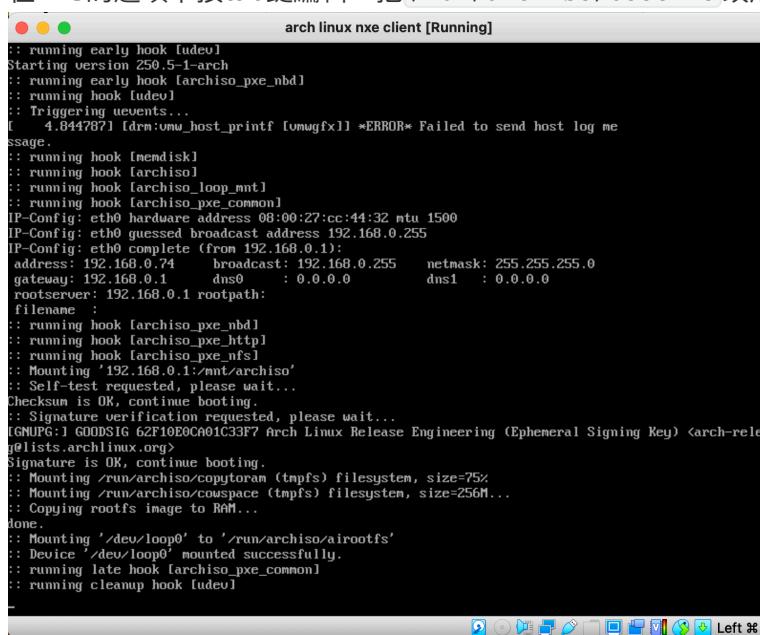
```
cat >> /etc/exports << EOF
> /mnt/archiso 192.168.0.0/24(ro,no_subtree_check)
> EOF
```

```
exportfs -arv
systemctl enable --now nfs-server
```

接著我們就可以使用virtual box新增一台vm，記得要把memory設大一點，否則安裝時會out of memory。之後在該台vm的setting > system，將Boot Order的Network選項勾選並移到最頂，之後開啟該vm，進到此畫面：



在NFS的選項下按tab鍵編輯，把 /run/archiso/bootmnt 改成 /mnt/archiso 並enter。



Reference:

https://wiki.archlinux.org/title/Preboot_Execution_Environment#Server_setup

討論對象：B09505014 王聖文

(3.)

Step1: 我們先用 `ping google.com` 確定有網路連接。

Step2: 透過 `timedatectl set-ntp true` 讓系統可以由網路來更新時間。

Step3: 接著切割drive，輸入 `fdisk /dev/sda`，並選擇dos > New，輸入要切割的大小，在此我選了6G，enter 後選擇primary > Bootable，並且重複一樣的過程來把剩下的空間都拿來新增一個partition。接著選擇 `/dev/sda2` > type > Linux swap / Solaris。然後選擇write，輸入yes，就可以退出 `fdisk` 了。

Step4: 以 `mkfs.ext4 /dev/sda1` 來create一個ext4的file system。並且用 `mkswap /dev/sda2` 開一個swap space。

Step5: 用 `mount /dev/sda1 /mnt` 和 `swapon /dev/sda2` 來mount file system。

Step6: 執行以下指令：

```
pacman -Syy  
pacman -S reflector  
cp /etc/pacman.d/mirrorlist /etc/pacman.d/mirrorlist.bak  
reflector -c "TW" -f 12 -l 10 -n 12 --save /etc/pacman.d/mirrorlist
```

Step7: 透過 `pacstrap /mnt base linux linux-firmware` 來安裝Arch Linux。

Step8: 透過 `arch-chroot /mnt`，以root的身份進到mounted disk，將root設在新安裝好的這個Arch Linux system。

Step9: 可以用 `timedatectl list-timezones` 查看有哪些time zone，我用 `timedatectl set-timezone Asia/Taipei` 將time zone設成台北。

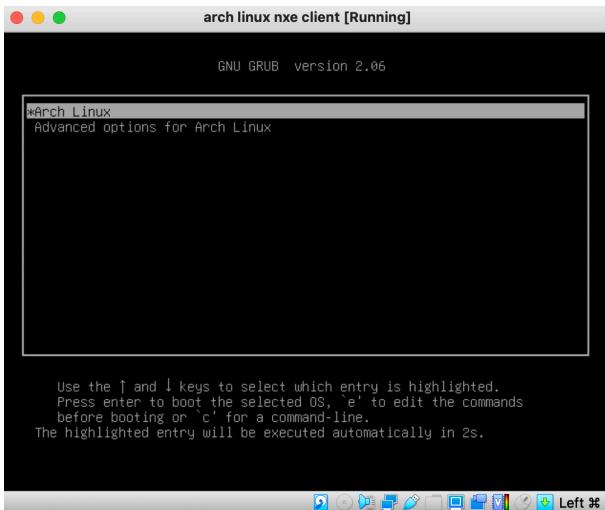
Step10: 以下列指令安裝grub bootloader：

```
pacman -S grub os-prober  
grub-install /dev/sda  
grub-mkconfig -o /boot/grub/grub.cfg
```

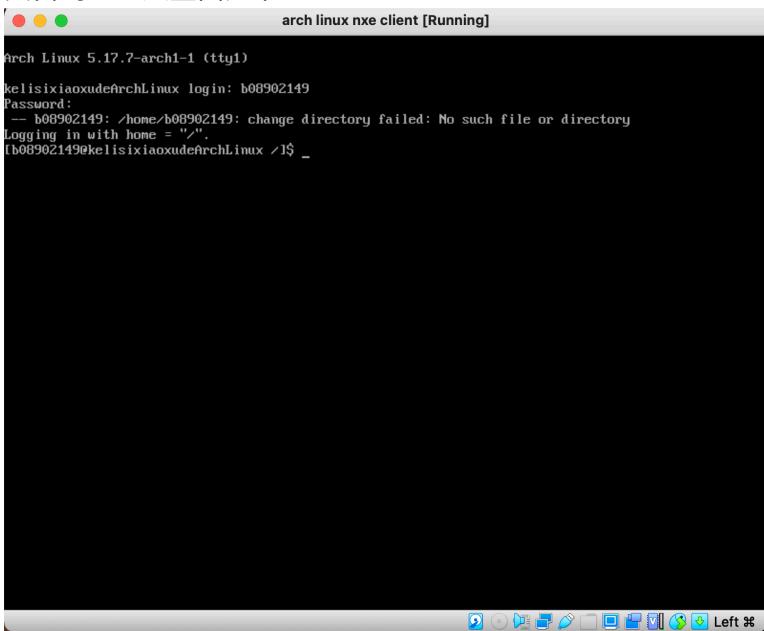
Step11: 可以新增 `/etc/hostname`，並在該檔案中輸入想要的命名，就可以修改hostname。

Step12: 用 `passwd` 改root密碼，並且輸入 `exit` 離開。

Step13: 將vm關機，在virtual box設定該台vm，進到setting > system，將Boot order中的Network選項取消，並且重新開機，可以看到以下畫面。



Step14: 登入root之後，用 `useradd b08902149` 新增一個user叫b08902149，並且用 `passwd b08902149` 設定其密碼，登入畫面如下：



Reference:

hostname設定：https://wiki.archlinux.org/title/installation_guide

Arch Linux 安裝：<https://phoenixnap.com/kb/arch-linux-install>