install kali linux

1) โหลดใน web kali
2) ใน vm กด add ไฟล์ .vbox

import debian

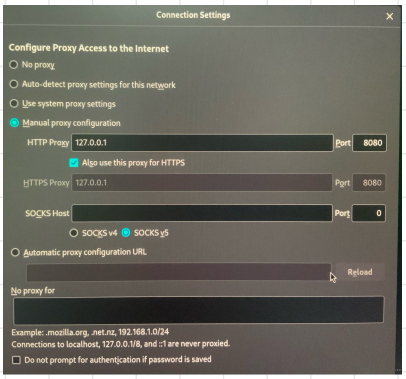
1) file ขยายนน
2) import Appliance
3) เลือกไฟล์ debian.ova
4) finish

การสร้าง NAT

1) Tools → ☰ → Network
2) เลือก NAT network
3) กด create
4) ใส่ name, ip
5) กด apply
6) kali → setting → network → adapter 2
   → ติ๊ก Enable network adapter
   → เลือก NAT network (อัน 3 จากล่าง)
   → เลือก NAT ที่สร้าง
7) debian → ทำเหมือน kali

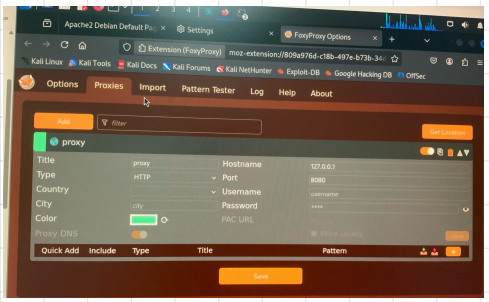
set firefox proxy

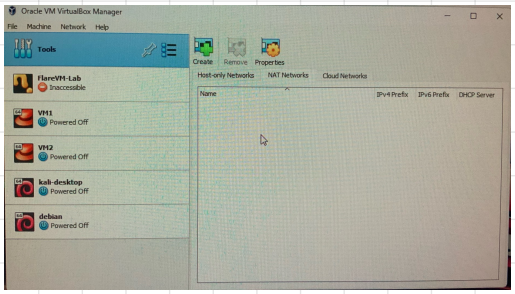
☰ → setting → ล่างสุด → network setting



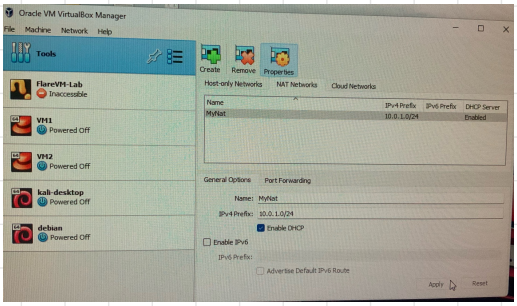
set foxy proxy

download foxy proxy extension
→ option → proxy → ใส่ name, hostname, port
→ save → เลือกลง extension

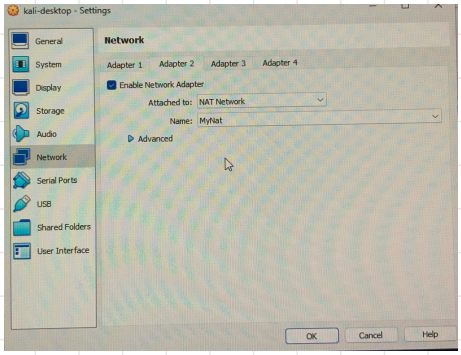




→

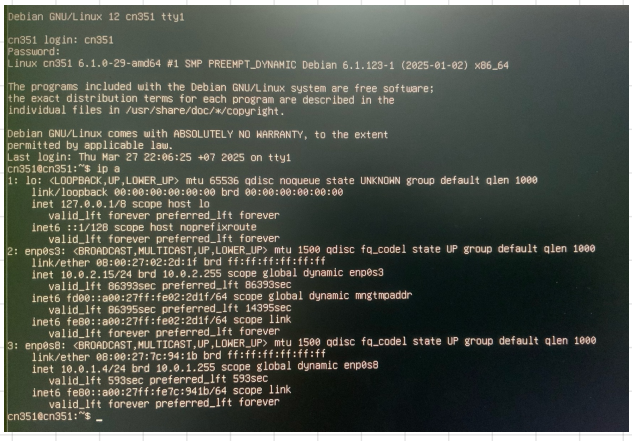


→



8) ใช้ "ip a" command ทั้งคู่จะได้ debian และ kali ดังนี้

debian

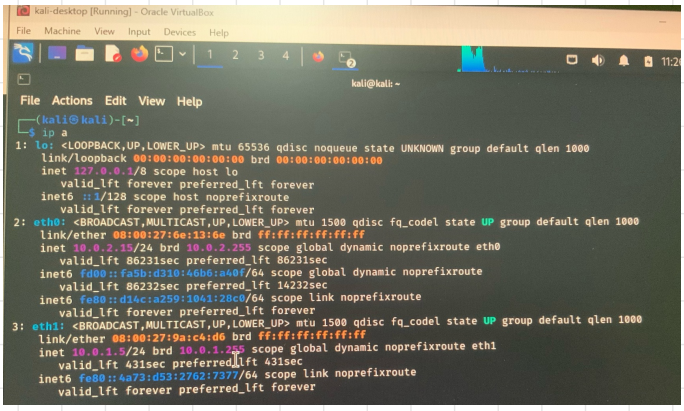


```
Debian GNU/Linux 12 cn351 tty1

cn351 login: cn351
Password:
Linux cn351 6.1.0-29-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.123-1 (2025-01-02) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Mar 27 22:06:25 +07 2025 on tty1
cn351@cn351:~$ 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 noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:02:2d:1f brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 86393sec preferred_lft 86393sec
    inet6 fd00::a00:27ff:fe02:2d1f/64 scope global dynamic mngtmpaddr
       valid_lft 86395sec preferred_lft 14395sec
    inet6 fe80::a00:27ff:fe02:2d1f/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:7c:94:1b brd ff:ff:ff:ff:ff:ff
    inet 10.0.1.4/24 brd 10.0.1.255 scope global dynamic enp0s8
       valid_lft 593sec preferred_lft 593sec
    inet6 fe80::a00:27ff:fe7c:941b/64 scope link
       valid_lft forever preferred_lft forever
cn351@cn351:~$
```

* debian : status → sudo systemctl status networking

restart → sudo systemctl restart networking

kali

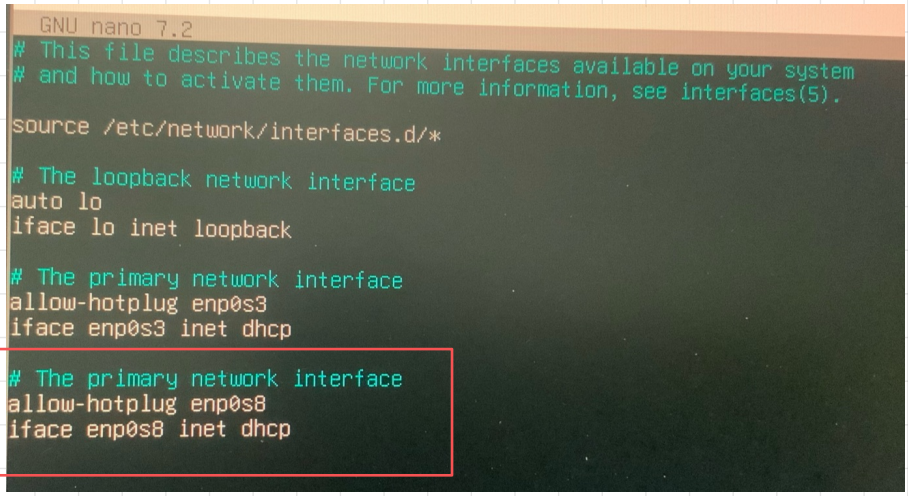


```
kali-desktop [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:6e:13:6e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 86231sec preferred_lft 86231sec
    inet6 fd00::fa5b:d310:46b6:a40f/64 scope global dynamic noprefixroute
       valid_lft 86232sec preferred_lft 14232sec
    inet6 fe80::d14c:a259:1041:28c0/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:9a:c4:d6 brd ff:ff:ff:ff:ff:ff
    inet 10.0.1.5/24 brd 10.0.1.255 scope global dynamic noprefixroute eth1
       valid_lft 431sec preferred_lft 431sec
    inet6 fe80::4a73:d53:2762:7377/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

* kali : status → sudo systemctl status NetworkManager
  → service networking status

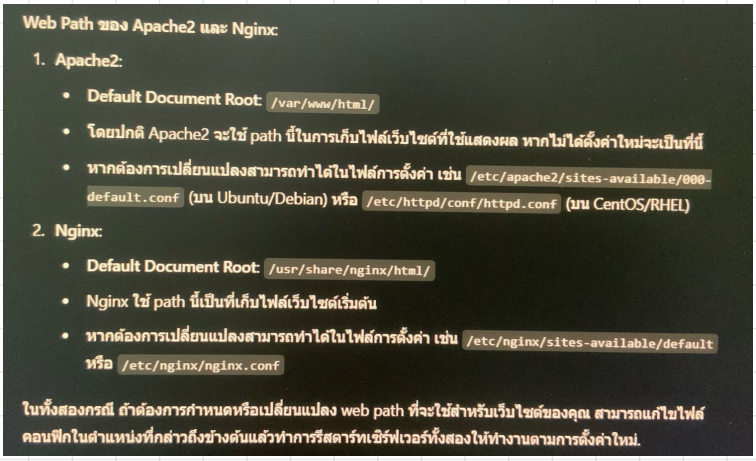
restart → sudo systemctl restart NetworkManager
  → service networking restart

9) add interfaces ใน debian



web path

1) sudo apt install apache2
2) sudo systemctl start apache2 or sudo service apache2 start
3) systemctl status apache2 or service apache2 status



วิธีดู target ip

① sudo nmap " Nat network" (10.0.1.0/24)

② sudo arp-scan -l --interface=eth1 (อันนี้ง่ายสุด)

หา port ของ target (check for http by url = http://target-ip:port

① ใช้ sudo nmap "target ip" -p 0-65535 | can nmap their self using 127.0.0.1

ดู default web page ของ target (ดู port จาก nmap ที่ scan ได้)

<u>lowest port</u>
http://<target_ip>:<lowest_port>
<u>highest port</u>
http://<target_ip>:<highest_port>

brute fore เพื่อหา password เนื่องจาก password อ่อนแอ
การดู cookie สำคัญข้อมูล user อะไรที่ใช้ในการ login ได้ไหม

แก้ ติ่งรหัสผ่านให้ยาก ข้อกำหนดพิเศษ การไม่เก็บข้อมูลสำคัญไว้ใน cookie

เข้าเว็บ

3 request: /favicon.ico; style.css; /

ssh

1. Open Port 22 on the Debian VM's Firewall

Using `ufw` (Uncomplicated Firewall):

1. **Check if `ufw` is installed:** If `ufw` is not installed, you can install it by running:

```bash
sudo apt update
sudo apt install ufw
```

2. **Allow port 22:** Run the following command to allow inbound SSH connections on port 22:

```bash
sudo ufw allow 22/tcp
```

3. **Enable the firewall** (if not already enabled):

```bash
sudo ufw enable
```

4. **Check the status** of the firewall to verify the rule:

```bash
sudo ufw status
```

It should show something like:

```vbnet
Status: active
To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
```

Using `iptables` (if you're not using `ufw`):

If you want to use `iptables` instead of `ufw`, you can run the following command to open port 22 for SSH:

```bash
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

To make the `iptables` rule persistent across reboots, save the configuration:

```bash
sudo apt install iptables-persistent
sudo netfilter-persistent save
```

2. Ensure SSH Server is Installed and Running

Debian does not always come with an SSH server installed by default. To make sure the **OpenSSH server** is installed and running:

1. **Install OpenSSH server:** If it's not installed, you can install it with:

```bash
sudo apt update
sudo apt install openssh-server
```

2. **Start and enable SSH:** To start the SSH service and ensure it starts on boot:

```bash
sudo systemctl start ssh
sudo systemctl enable ssh
```

3. **Verify SSH service status:** To check if the SSH service is running:

```bash
sudo systemctl status ssh
```

The output should indicate that the SSH service is active and running.

3. Check NAT Configuration

If your Debian VM is running in a **local network** (on the same NAT), it should be able to access SSH using the **local IP address** (e.g., `192.168.x.x`).

You can check your local IP address by running:

```bash
ip a
```

Look for the IP address under the network interface, usually something like `inet 192.168.x.x`.

4. Test SSH Connection

From another device in the same network, use the following SSH command to connect to your Debian VM:

```bash
ssh username@your_debian_vm_ip
```

For example:

```bash
ssh user@192.168.1.100
```