install kali linux

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

import debian

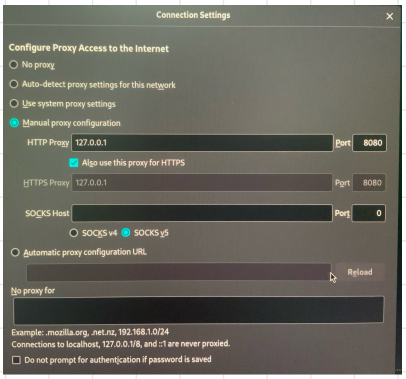
1) file ขยายนน
2) import Appliance
3) เลือกไฟล์ debian.ova
4) finish

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

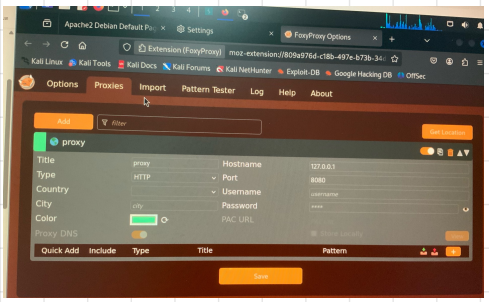
set firefox proxy

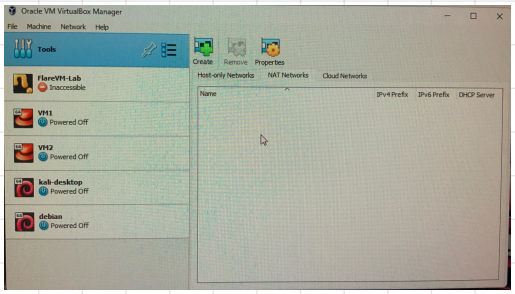
☰ → setting → ล่างสุด → network setting



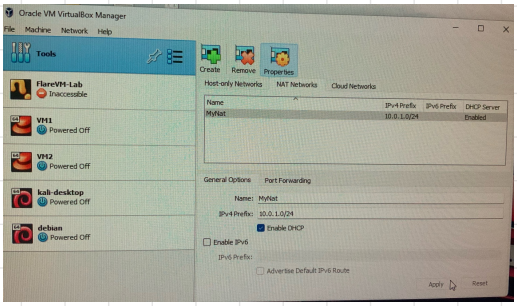
set foxy proxy

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

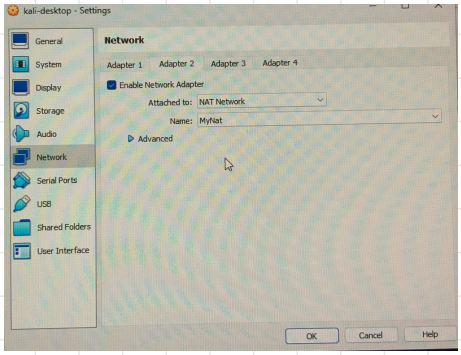




→

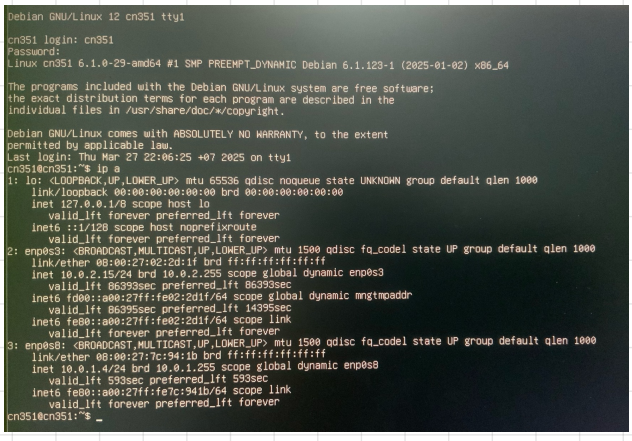


→



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

debian

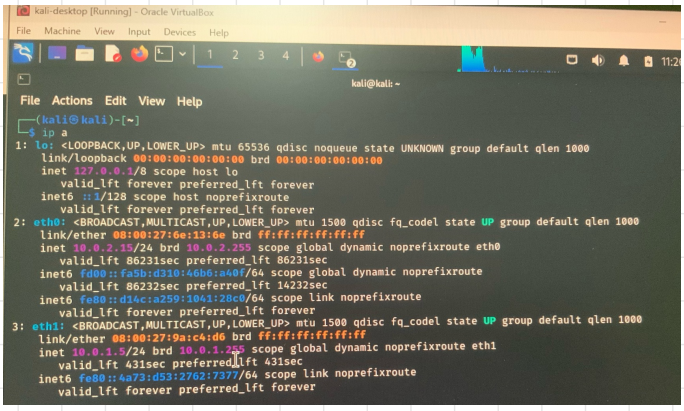


```
Debian GNU/Linux 12 cn351 tty1

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

```
  GNU nano 7.2
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet dhcp

# The primary network interface
allow-hotplug enp0s8
iface enp0s8 inet dhcp
```

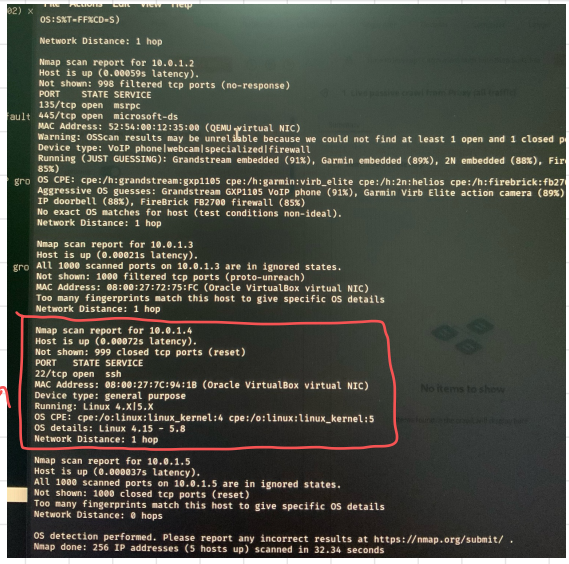
web path

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

Web Path ของ Apache2 และ Nginx:

1. **Apache2:**
   - **Default Document Root:** `/var/www/html/`
   - โดยปกติ Apache2 จะใช้ path นี้ในการเก็บไฟล์เว็บไซต์ที่ใช้แสดงผล หากไม่ได้ตั้งค่าใหม่จะเป็นที่นี้
   - หากต้องการเปลี่ยนแปลงสามารถทำได้ในไฟล์การตั้งค่า เช่น `/etc/apache2/sites-available/000-default.conf` (บน Ubuntu/Debian) หรือ `/etc/httpd/conf/httpd.conf` (บน CentOS/RHEL)
2. **Nginx:**
   - **Default Document Root:** `/usr/share/nginx/html/`
   - Nginx ใช้ path นี้เป็นที่เก็บไฟล์เว็บไซต์เริ่มต้น
   - หากต้องการเปลี่ยนแปลงสามารถทำได้ในไฟล์การตั้งค่า เช่น `/etc/nginx/sites-available/default` หรือ `/etc/nginx/nginx.conf`

ในทั้งสองกรณี ถ้าต้องการกำหนดหรือเปลี่ยนแปลง web path ที่จะใช้สำหรับเว็บไซต์ของคุณ สามารถแก้ไขไฟล์คอนฟิกในตำแหน่งที่กล่าวถึงข้างต้นแล้วทำการรีสตาร์ทเซิร์ฟเวอร์ทั้งสองให้ทำงานตามการตั้งค่าใหม่



วิธีดู target ip

① sudo nmap "Nat network" (10.0.1.0/24) ✓ | sudo nmap -O "Nat network" ดู OS debian

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

หา port ของ target (check for http by url = http://target-ip:port ดูจาก nmap http service)

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)

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

เข้าเว็ป

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

brute fore เพื่อหา password เพื่องจาก password อ่อนเกิน
การดู cookie สำคัญข้องมูล user อะไรที่ใช้ตอนที่ login ได้ไหม

แก้ ถึงรหัสผ่านให้ยาก ซับซ้อนมีเครื่องหมาย การไม่เก็บข้อมูลสำคัญไว้ใน cookie

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
```

Brute fore (burpsuite intruder)

Here's a detailed, step-by-step guide to using **Burp Suite Intruder** for brute-forcing:

Step 1: Set Up Burp Suite

1. **Open Burp Suite.**
2. **Configure your browser to use Burp Suite as a proxy:**
   - By default, Burp listens on `127.0.0.1:8080`.
   - Set your browser's proxy settings to `127.0.0.1:8080` for HTTP and HTTPS traffic.

Step 2: Capture the Request

1. Open **Burp Suite** and go to the **Proxy** tab.
2. Make sure **Intercept** is on. If you are testing a website, go to the login page or the page you want to brute-force.
3. Fill out the form with dummy data and submit it (for example, entering a username and password if you're testing a login form).
4. Burp will intercept this request. Click **Forward** to pass the request to the server, or you can **Send to Intruder** directly from here.

Step 3: Send the Request to Intruder

1. Once the request is intercepted, right-click on it and choose **Send to Intruder**. This will open the **Intruder** tab.
2. In the **Intruder** tab, you'll see the request in the main window.

Step 4: Configure Intruder Positions

1. In the **Intruder** tab, go to the **Positions** sub-tab.
2. You'll see the request's parameters highlighted in the URL or the body of the request.
3. Burp will automatically try to mark the parameters for injection. In the case of a login form, it may highlight the username and password parameters.
4. **Highlight the part you want to brute-force.** For example:
   - If you are brute-forcing a password, highlight the password field in the request.
   - Click **Add §** to surround it with Burp's markers, like this: `username=admin&password=§password§`.
5. Ensure that the right parameter is selected to be brute-forced. You can adjust the markers manually if necessary.

Step 5: Set Payloads for Brute-Force

1. After selecting the parameter, go to the **Payloads** tab.
2. In the **Payload Sets** section, select **Payload Set 1** (or any other number, depending on how many payloads you need to use).
3. **Choose the type of payload:**
   - For **password brute-forcing**, you might use a **Simple list**.
   - Select **Simple list**, then click the **Load** button to load a wordlist (such as a dictionary file or a list of common passwords).
   - If you're brute-forcing numbers, choose **Numbers**.
   - **Battering Ram**: If you're brute-forcing multiple fields with the same payload.
   - **Pitchfork**: If you're brute-forcing multiple fields with different payloads.
4. **Load a payload:**
   - If you're brute-forcing a password, you might load a wordlist like `rockyou.txt` or create your own custom list.
   - If you're brute-forcing something like a username or other field, load the corresponding list for that field.

Step 6: Configure the Intruder Attack Type

1. Select the **Attack Type**:
   - **Sniper**: Used when you're testing one payload on one parameter at a time (useful for brute-forcing a single field like the password).
   - **Battering Ram**: Used when you're testing the same payload across multiple parameters.
   - **Pitchfork**: Use different payloads for different parameters (useful for brute-forcing both the username and password).
   - **Cluster Bomb**: Used for combining multiple payloads across different parameters in all possible combinations.
2. For a simple **password brute-force**, **Sniper** is usually the best option.

Step 7: Start the Brute-Force Attack

1. Once the configuration is complete, click on **Start Attack** at the top of the **Intruder** tab.
2. Burp Suite will begin sending requests with the payloads you specified and display the results in real-time.

Step 8: Monitor Results

1. While the attack is running, you'll see a live update of the request responses, including:
   - **Status Code**: This tells you if the request was successful (e.g., a 200 status might mean successful login, while a 403 might indicate failure).
   - **Response Length**: This can help indicate a successful login (the response size might be different for successful vs. failed attempts).
   - **Response Body**: You may also analyze the body for messages like "Incorrect password" or "Welcome back!" to identify successful login attempts.
2. Look for anomalies or differences in the response that indicate a successful brute-force attempt.

Step 9: Analyze the Results

1. After the attack completes, review the results.
2. Look for successful attempts:
   - Look for any responses that might indicate a successful login, such as a different HTTP status code or response body.
3. You can stop the attack at any time by clicking **Stop Attack**.

Additional Tips:

- **Rate Limiting**: Be mindful of rate limits and account lockout mechanisms that could block you after too many failed attempts.
- **Ethical Use**: Make sure you have explicit permission to perform penetration testing on the target. Unauthorized brute-forcing can be illegal and unethical.

This is a basic guide to using Burp Suite Intruder for brute-forcing a login form. Would you like more details on any specific step?