

LAB 1: Setting Up Environment

Purpose

We will use Kali Linux to simulate the Internet, and the Windows machine will be fooled by it.

Getting the Virtual Machine

You can download the files you need here:

[IAM302 Malware Analys \(https://my.sharepoint.com/:f:/g/personal/dinhmh_fpt_edu_vn/Es7sIL1BYNVMpjfwJUi7k2wB5y_E_pMkqoUGYmng5rCJxA?e=8hmDJh \)](https://my.sharepoint.com/:f:/g/personal/dinhmh_fpt_edu_vn/Es7sIL1BYNVMpjfwJUi7k2wB5y_E_pMkqoUGYmng5rCJxA?e=8hmDJh)

The two files you need are:

- kali-linux-2019.3-vmware-i386.7z (or a later version)
- Win2008Malware.7z

Extracting the Virtual Machine

Right-click the **Win2008-Target.7z**, **kali-linux-2019.3-vmware-i386.7z** file, click **7-Zip**, and click "**Extract Files...**". In the "Extract to:" box, enter the path to the folder you prepared,

Starting your Win2008-Target Virtual Machine

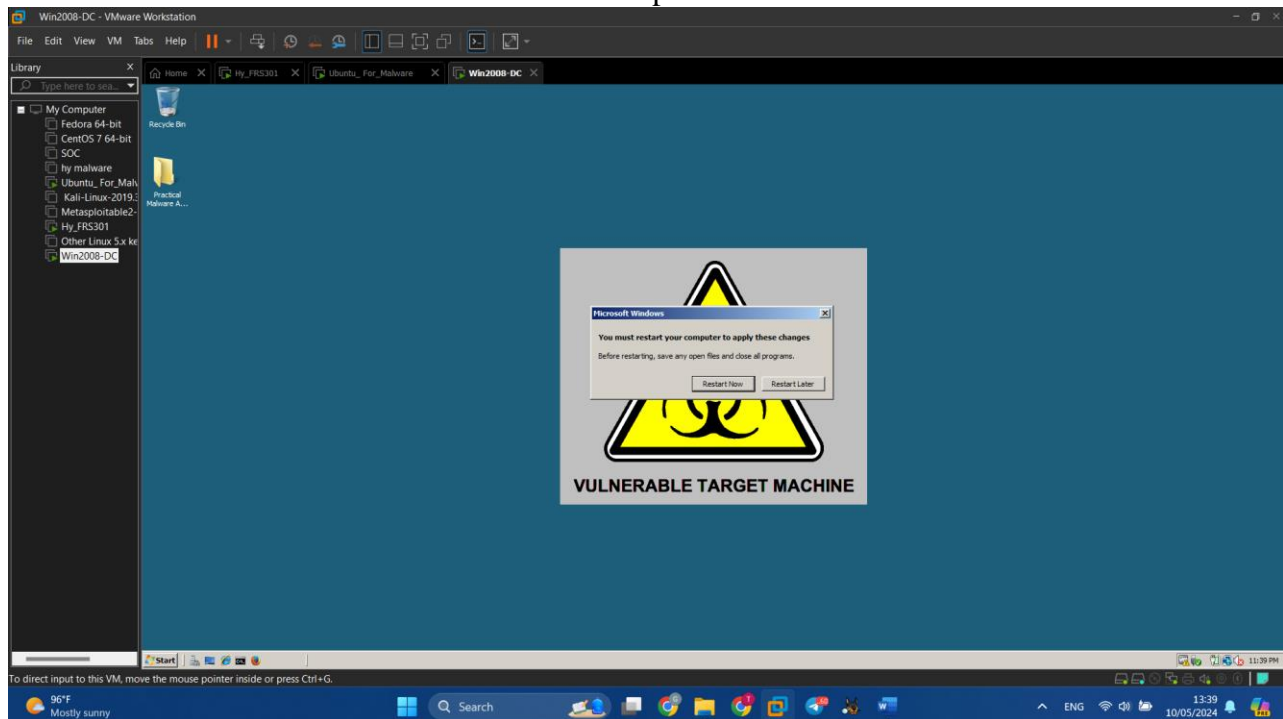
To log in, you need to send a **Ctrl+Alt+Delete** to the virtual machine. On a Windows host, you can usually press **Ctrl+Alt+Insert** to do that.

If that doesn't work, hunt through the VMware menus to send a Ctrl+Alt+Delete.

Log in as **Administrator** with a password of **P@ssw0rd**

When the server starts, it opens some windows by default. Close all windows.

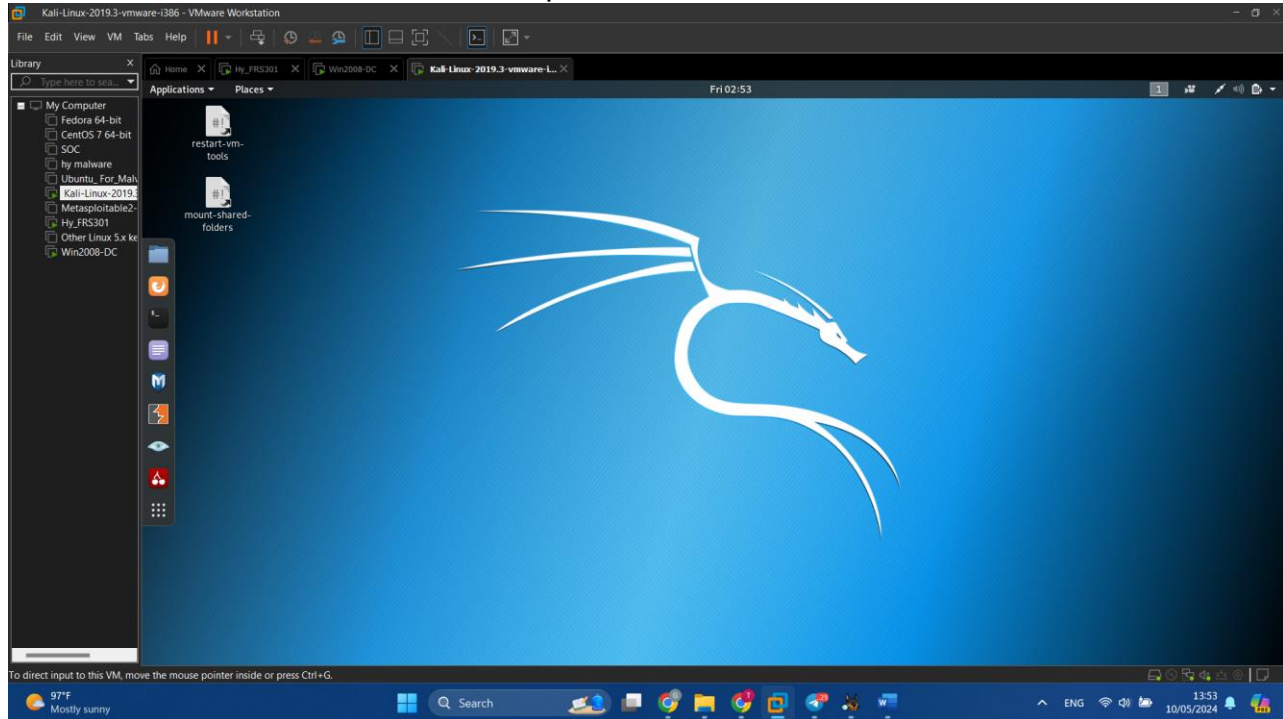
You should see the Windows Server 2008 desktop as shown below:



Starting the Kali Linux Machine and Adjusting Networking

Start the Attacker Linux machine in VMware. If you don't see a user named "root", click Other....

Log in to Kali with the username **root** and a password of **toor**
You should see the Kali Linux desktop as shown below:



Setting the Kali Linux VM to NAT Networking

In the VMware window showing your Kali Linux desktop, on the top left, click VM, "Settings".

In the "Virtual Machine Settings" box, on the left side, click "Network Adapter".

On the right side, click "NAT". Click **OK**.

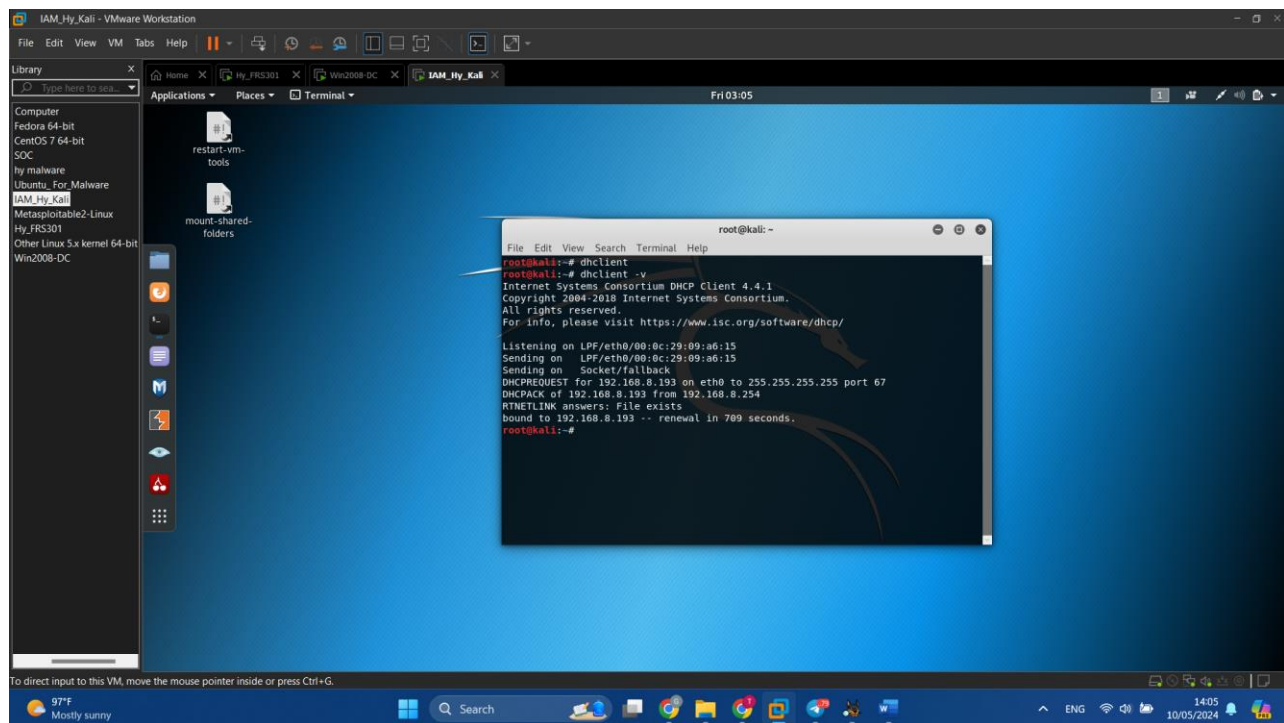
At the top left of the Kali Linux desktop, find these items:

- "Applications" menu
- "Places" menu
- A blue icon that FireFox ESR
- A rectangular black icon that opens a Terminal window

At the top left of the Kali Linux desktop, click the rectangular black icon to open a **Terminal window**.

In the **Terminal window**, type in this command to get a new IP address, and then press the Enter key:

dhclient -v

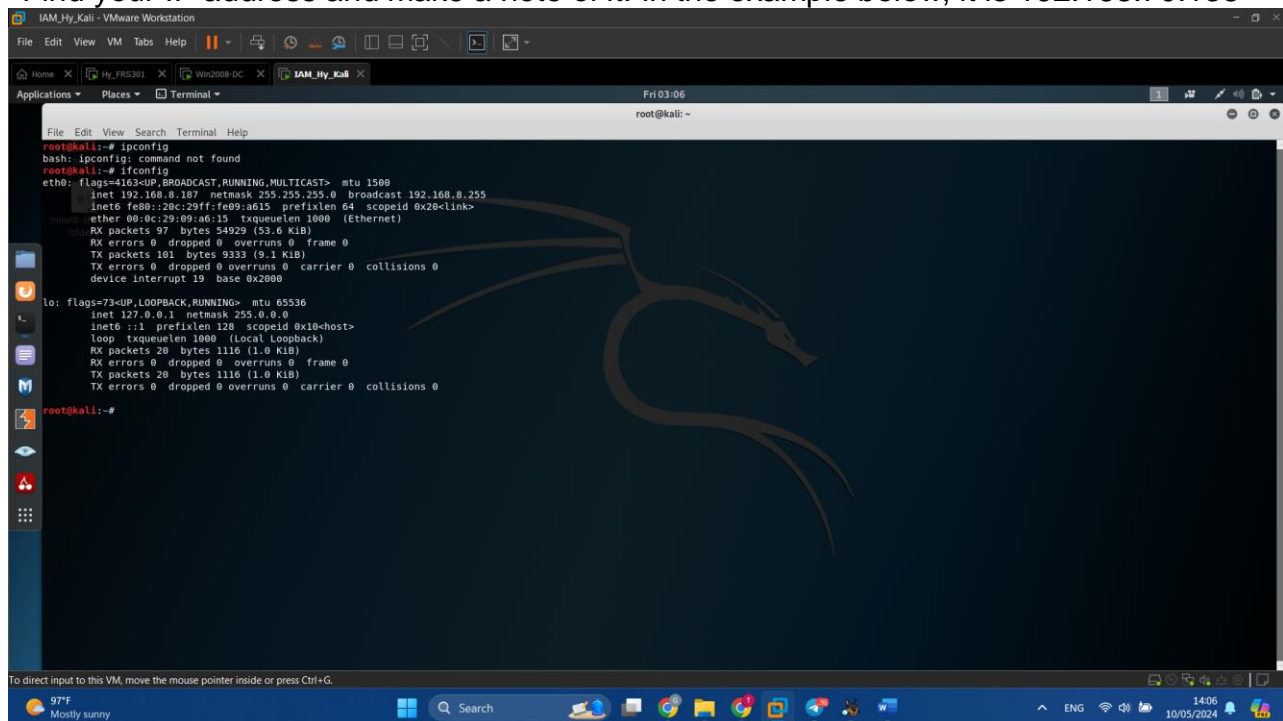


Finding the Kali Machine's IP Address

On your Kali Linux machine, in a Terminal window, execute this command:

ifconfig

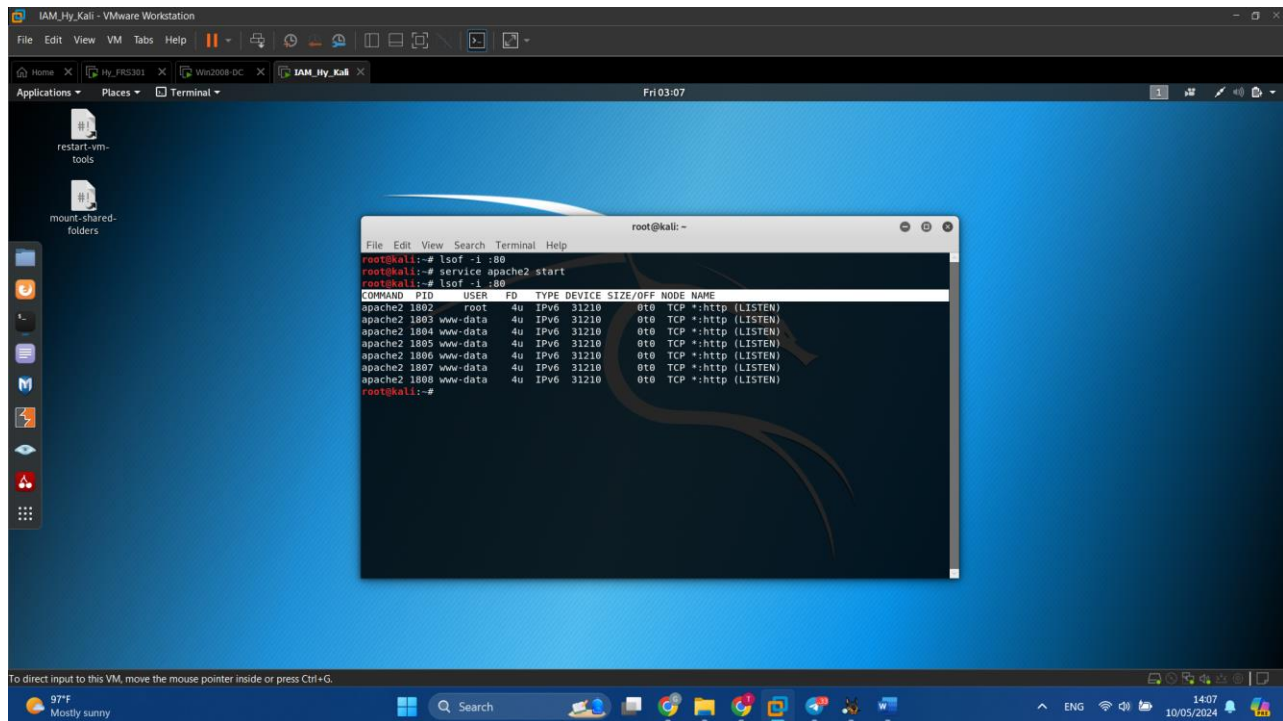
Find your IP address and make a note of it. In the example below, it is 192.168.70.138



Checking for a Web server

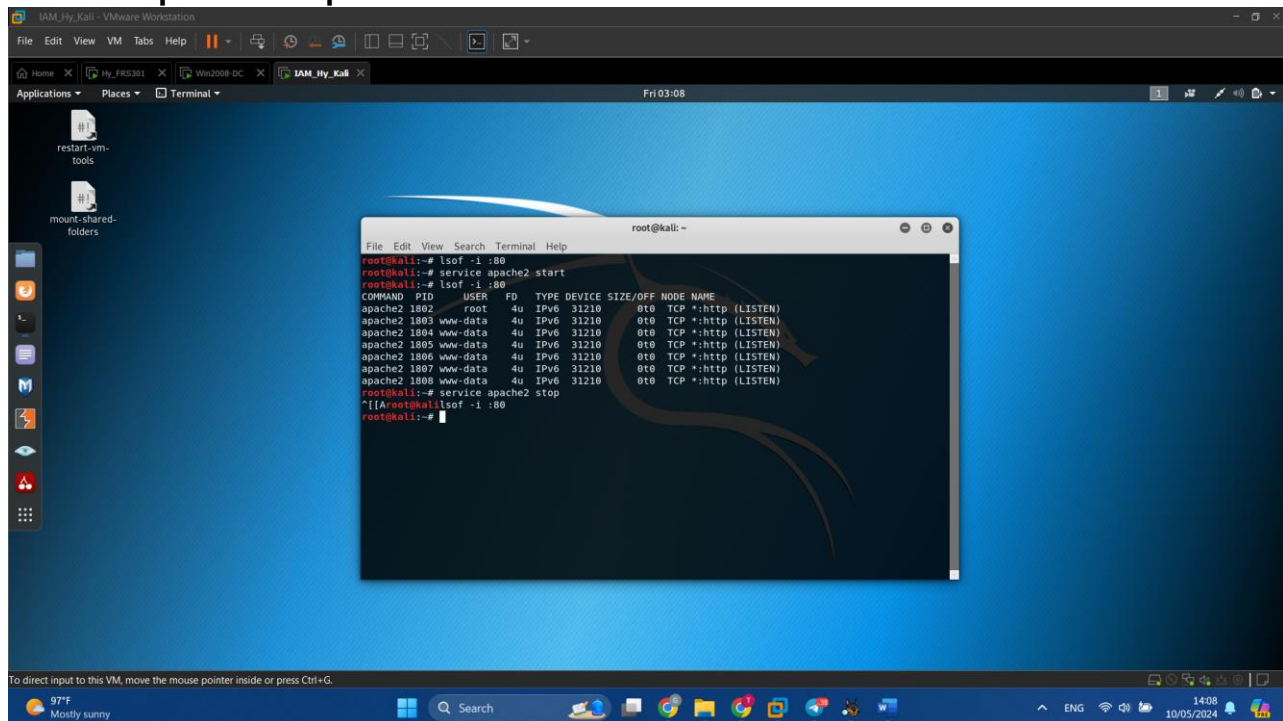
On your Linux machine, in a Terminal window, execute this command:

Isot -i :80



This command shows processes listening on port 80. If you see apache2 processes, as shown below, execute this command to stop apache:
service apache2 stop

service apache2 stop

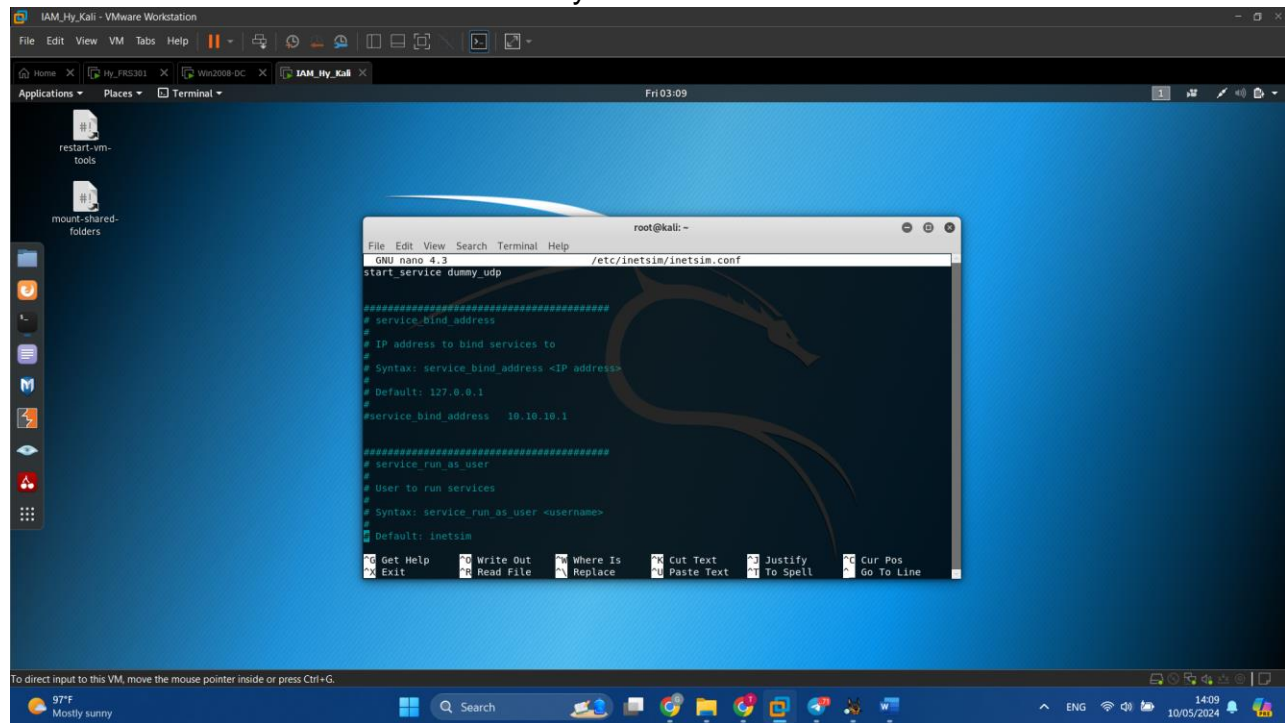


Configuring inetsim

inetsim is included in Kali Linux 2 already. But it needs some configuration. On your Linux machine, in a Terminal window, execute these commands:

```
cp /etc/inetsim/inetsim.conf /etc/inetsim/inetsim.conf.orig  
nano /etc/inetsim/inetsim.conf
```


Scroll down about 3 screens. Find the **service_bind_address** section shown below. All these lines are comments because they start with the # character



The screenshot shows a VMware Workstation window titled 'IAM_Hy_Kali - VMware Workstation'. Inside the VM, the desktop is blue with a Kali Linux dragon logo. A terminal window is open, running the nano text editor on the file /etc/inetsim/inetsim.conf. The terminal output shows the following configuration:

```
root@kali: ~  
GNU nano 4.3 /etc/inetsim/inetsim.conf  
start_service dummy_udp  
  
#####  
# service_bind_address  
#  
# IP address to bind services to  
# Syntax: service_bind_address <IP address>  
# Default: 127.0.0.1  
#service_bind_address 10.10.10.1  
  
#####  
# service_run_as_user  
#  
# User to run services  
# Syntax: service_run_as_user <username>  
# Default: inetsim
```

The bottom of the screen shows the Windows taskbar with the date 10/05/2024 and time 14:09.

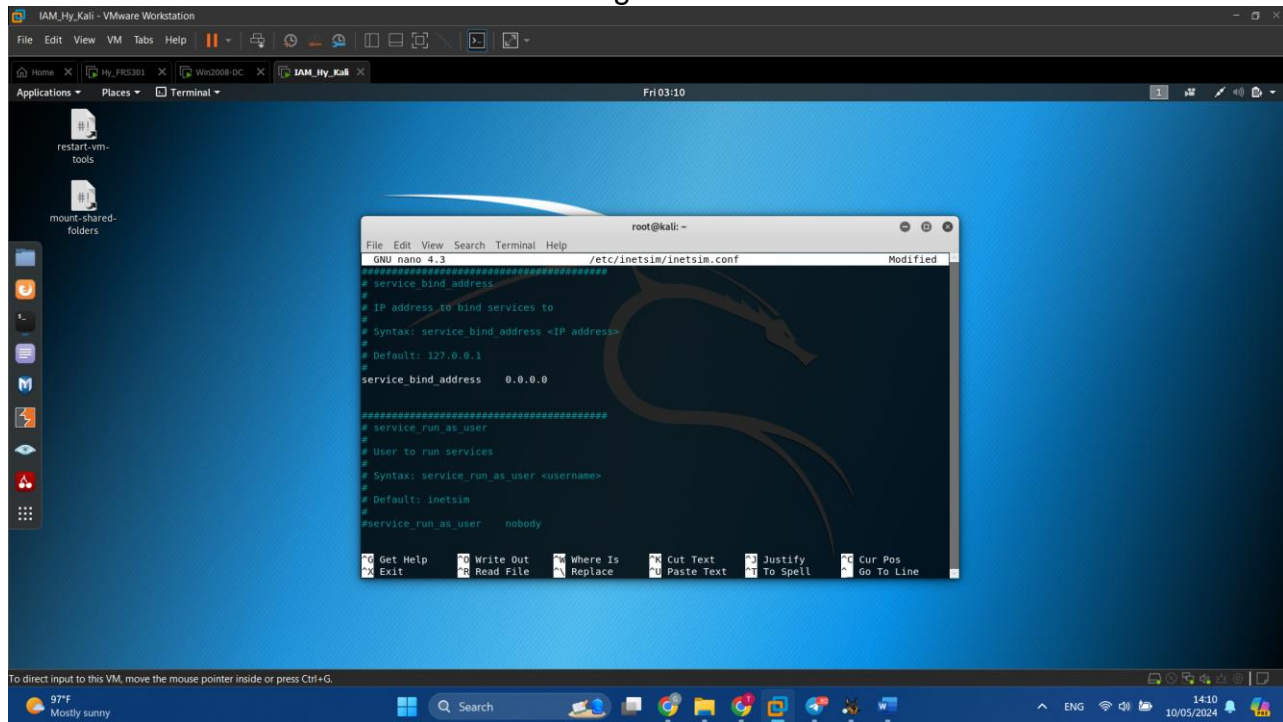
Change this line:

#service_bind_address 10.10.10.1

to this

service_bind_address 0.0.0.0

as shown below. This sets inetsim listening on all Kali's IP addresses.



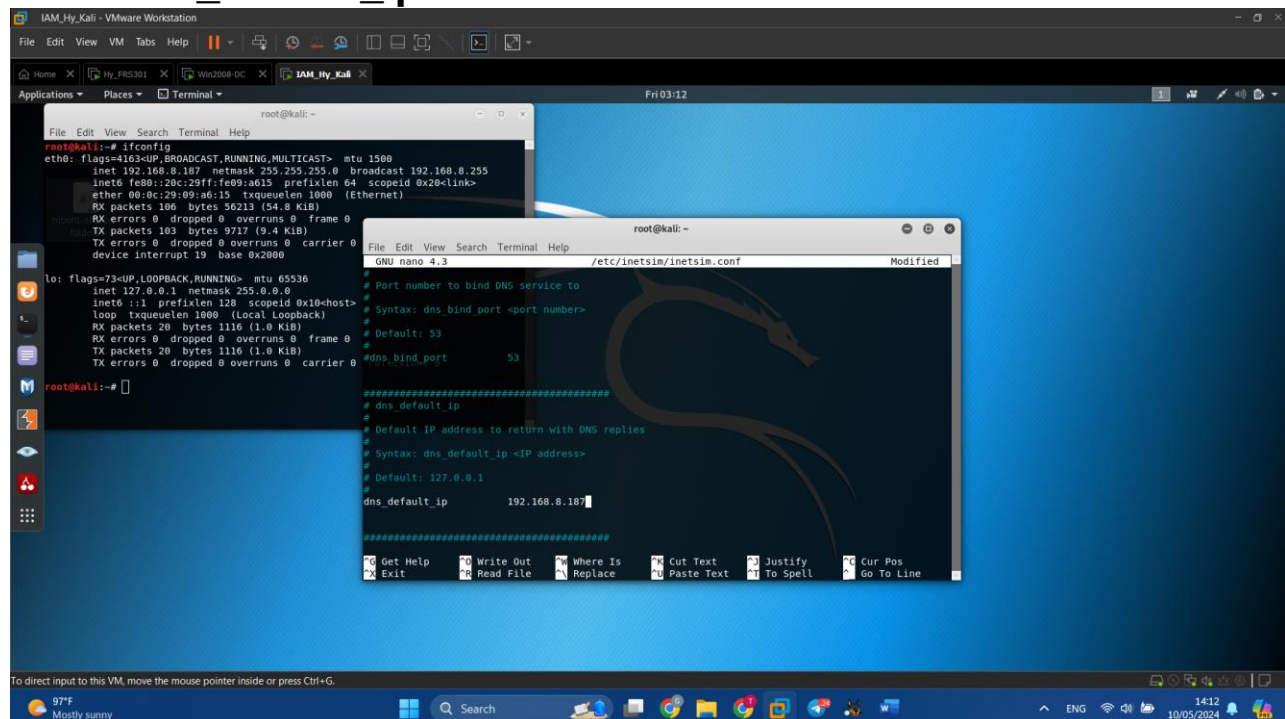
Don't forget to delete the # at the start of the line!

Scroll down another several screens to find the **dns_default_ip** section shown below. Find this line:

#dns_default_ip 10.10.10.1

Remove the # at the start of the line, and replace the IP address with the IP address of your Kali Linux machine, as shown below:

dns_default_ip 192.168.70.138

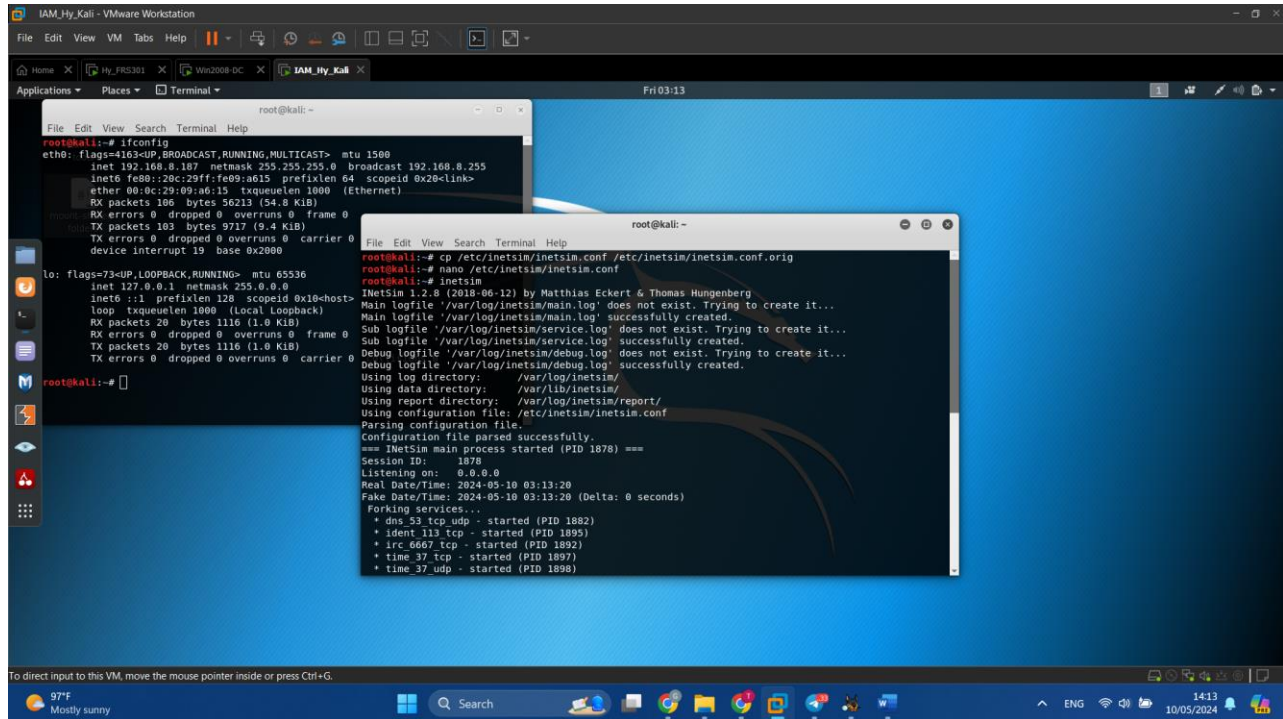


Use your correct IP address instead of "192.168.70.138"

Save the file with **Ctrl+X, Y, Enter**.

To start inetsim, on your Linux machine, in a Terminal window, execute this command:

Inetsim



Start Your Windows VM

Start your Windows Server 2008 virtual machine, and set it to NAT networking.

Installing Nmap

In your Windows Server 2008 virtual machine, click **Start** and look for Nmap. It should be there. If not, open a Web browser and go to <http://nmap.org/> to get it.

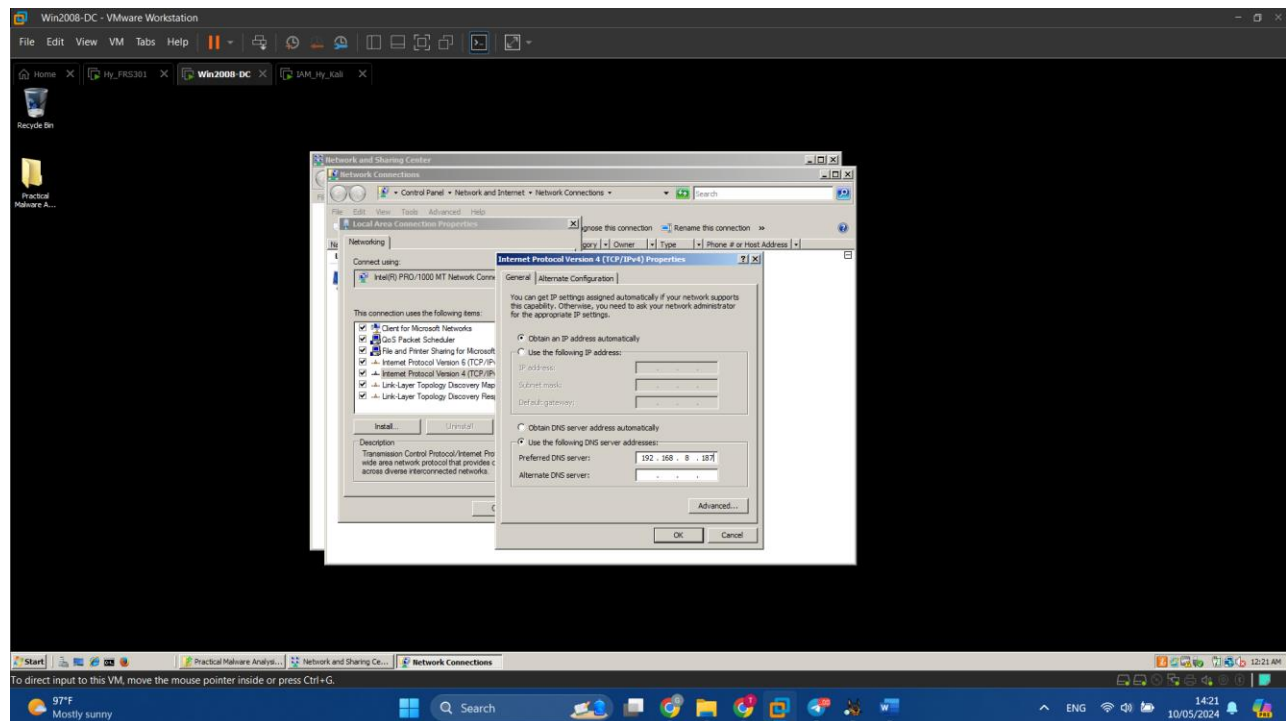
Setting the DNS Server

On your Windows VM, click **Start**. Right-click **Network** and click **Properties**.

On the left side, click "Manage network connections". Right-click "**Local Area Connection**" and click **Properties**.

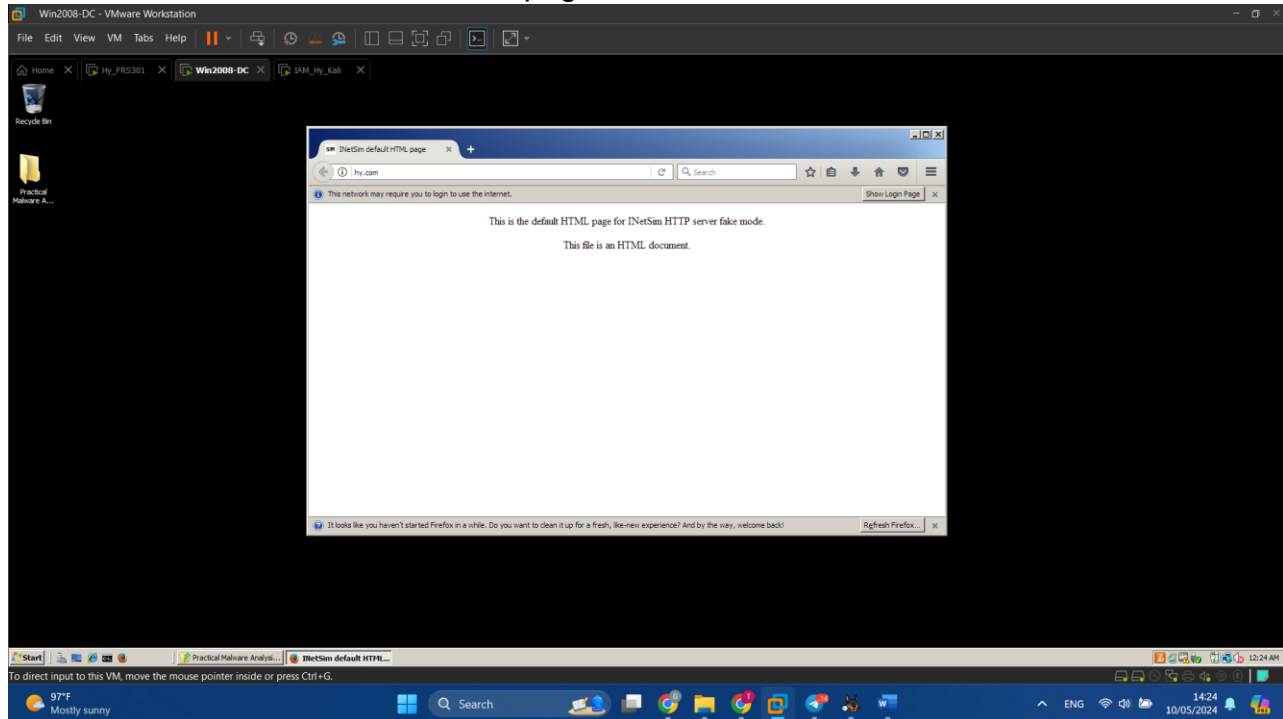
Double-click "**Internet Protocol Version 4(TCP/IPv4)**".

Set your DNS server to the Kali Linux machine's IP address, as show below. Then click **OK** twice.



Viewing an HTTP Web Page

Open a Web browser on the Windows VM and go to this URL: **http://YOURNAME.com**, replacing "YOURNAME" with your real name.
You see the INetSim default HTML page, as shown below:



Scanning YOURNAME.com

Start Nmap. Enter a Target of **YOURNAME.com**, replacing "YOURNAME" with your own name.

Click the **Scan** button.

You should see a lot of open ports, as shown below.

