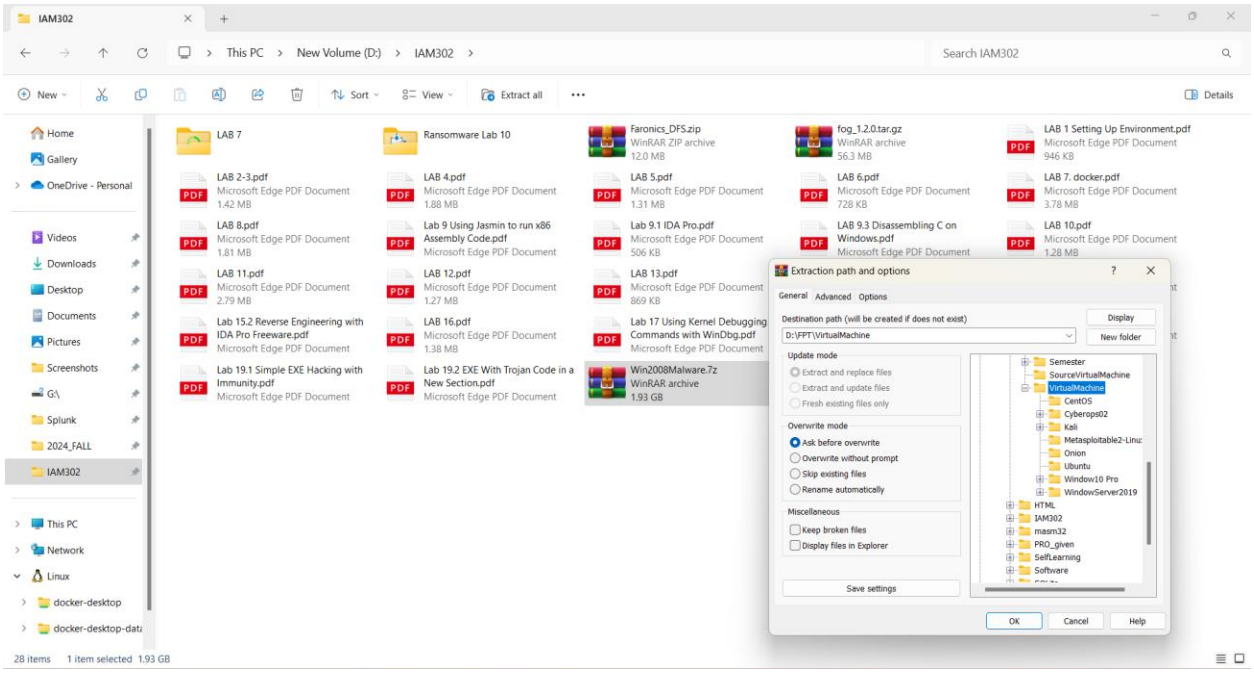
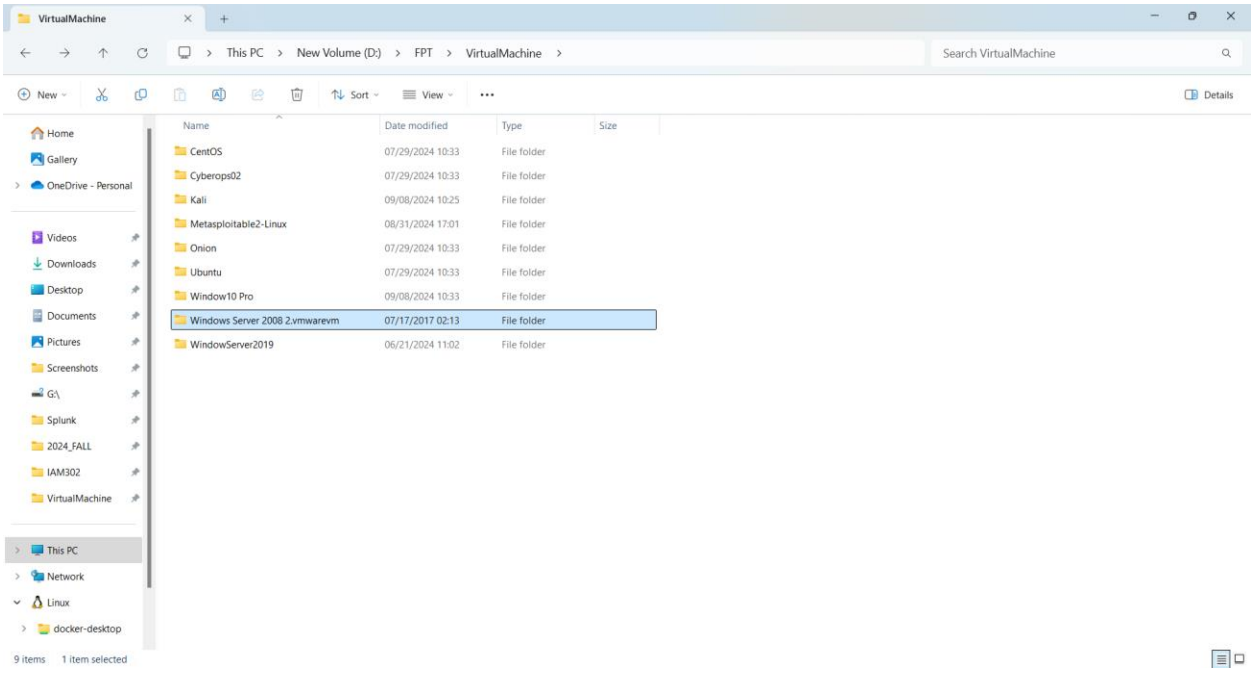
LAB 1: Setting Up Environment

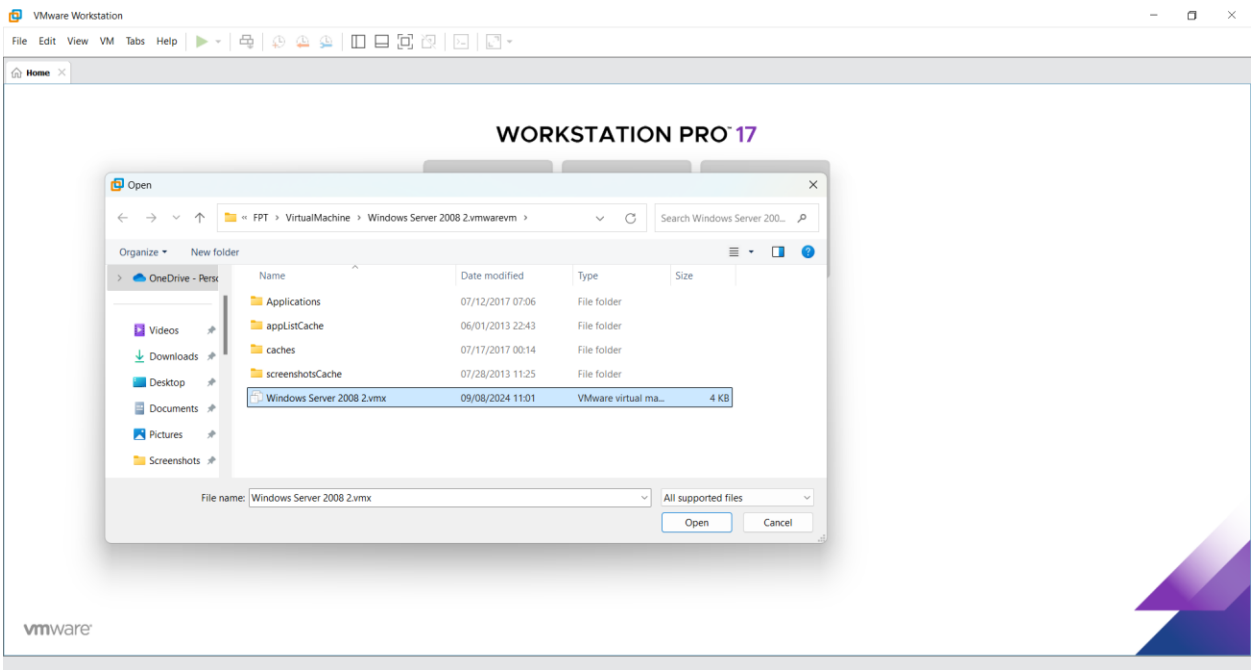
Purpose: We will use Kali Linux to simulate the Internet, and the Windows machine will be fooled by it.

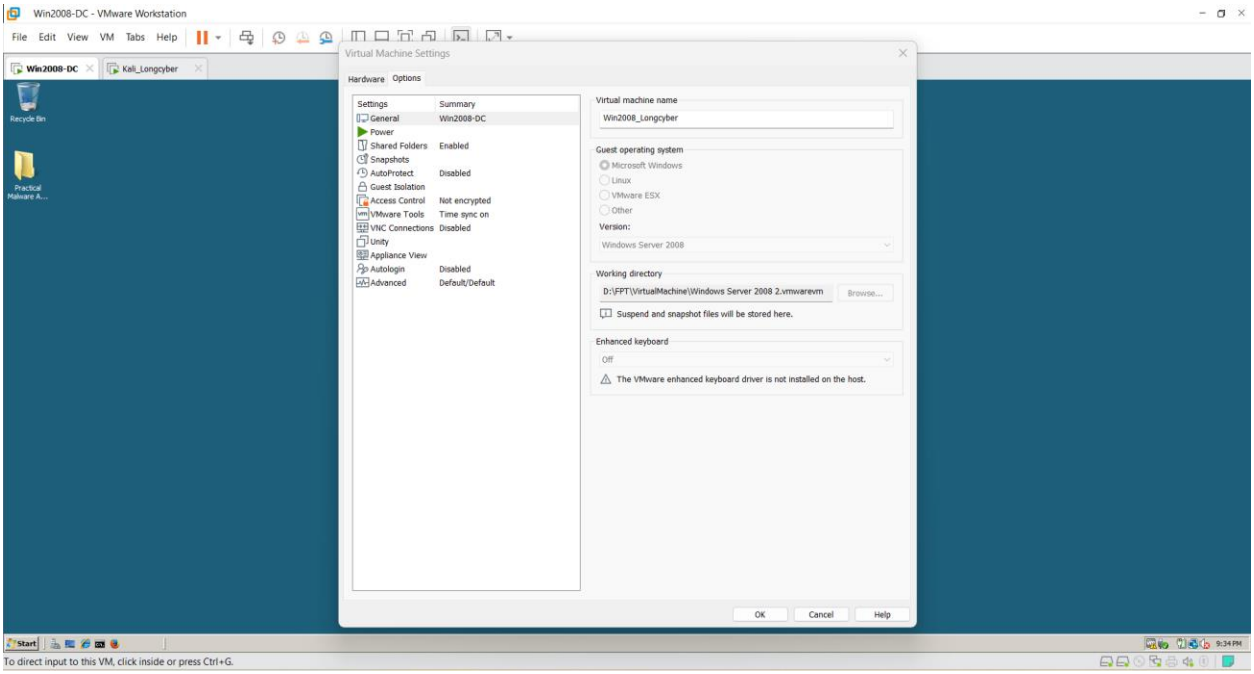
Extracting the Virtual Machine: Right-click the Win2008-Target.7z, kali-linux-2019.3-vmwarei386.7z file, click 7-Zip, and click "Extract Files...". In the "Extract to:" box, enter the path to the folder you prepared.



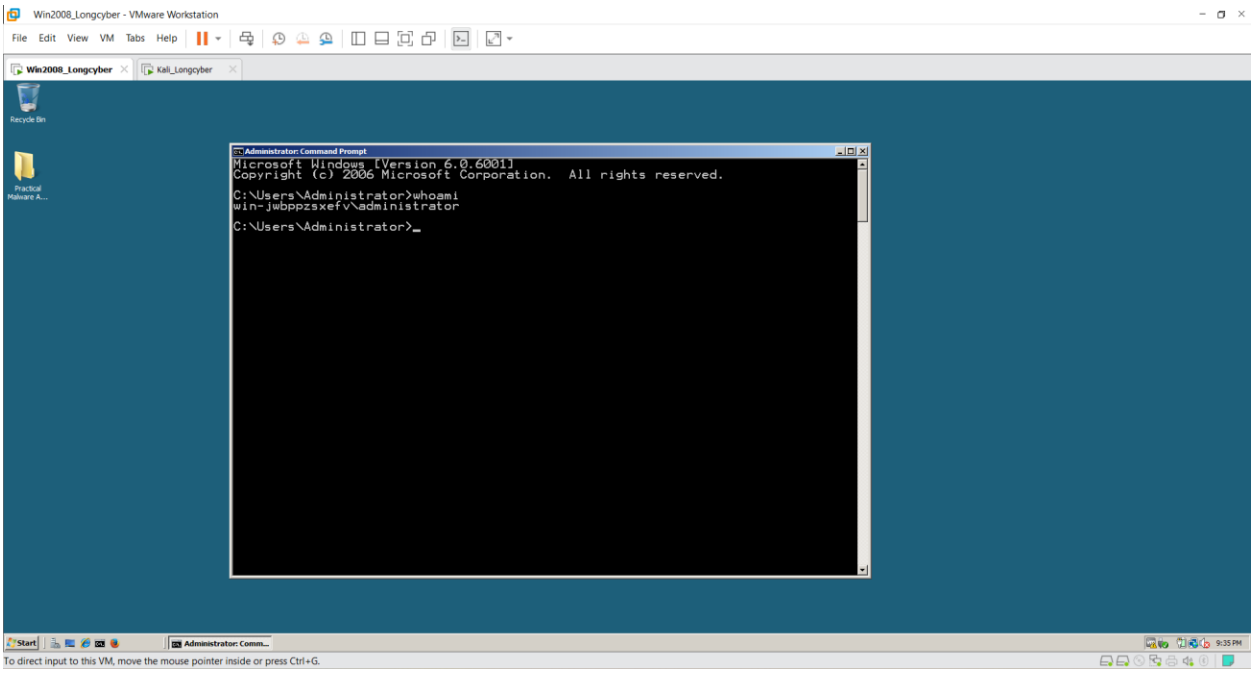


Starting your Win2008-Target Virtual Machine

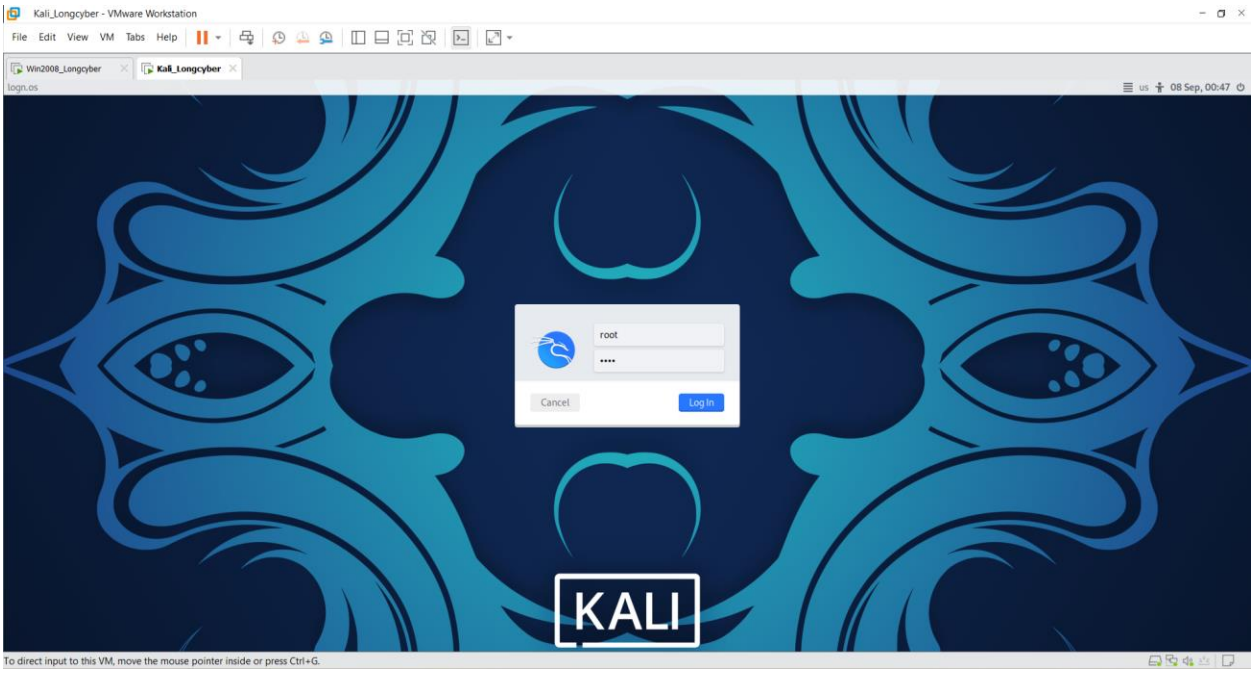


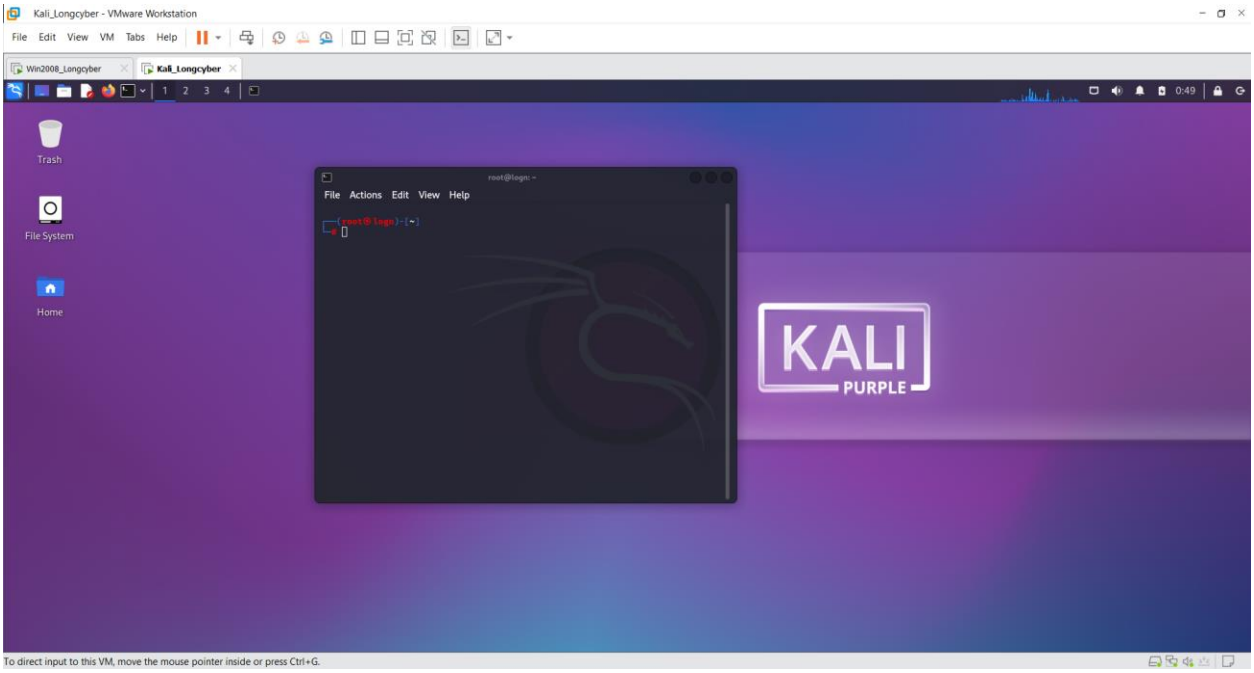

Win2008-DC - VMware Workstation
File Edit View VM Tabs Help
Win2008-DC
Kali_Longcyber
Recycle Bin
Practical Malware A...
Virtual Machine Settings
Hardware Options
Settings Summary
General Win2008-DC
Power
Shared Folders Enabled
Snapshots
AutoProtect Disabled
Guest Isolation
Access Control Not encrypted
VMware Tools Time sync on
VNC Connections Disabled
Unity
Appliance View
Autologin Disabled
Advanced Default/Default
Virtual machine name
Win2008_Longcyber
Guest operating system
Microsoft Windows
Linux
VMware ESX
Other
Version:
Windows Server 2008
Working directory
D:\FPT\VirtualMachine\Windows Server 2008 2.vmwarevm
Browse...
Suspend and snapshot files will be stored here.
Enhanced keyboard
Off
The VMware enhanced keyboard driver is not installed on the host.
OK
Cancel
Help
Start
9:34 PM
To direct input to this VM, click inside or press Ctrl+G.


Win2008_Longcyber - VMware Workstation
File Edit View VM Tabs Help
Win2008_Longcyber
Kali_Longcyber
Recycle Bin
Practical Malware A...
VULNERABLE TARGET MACHINE
Start
9:34 PM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



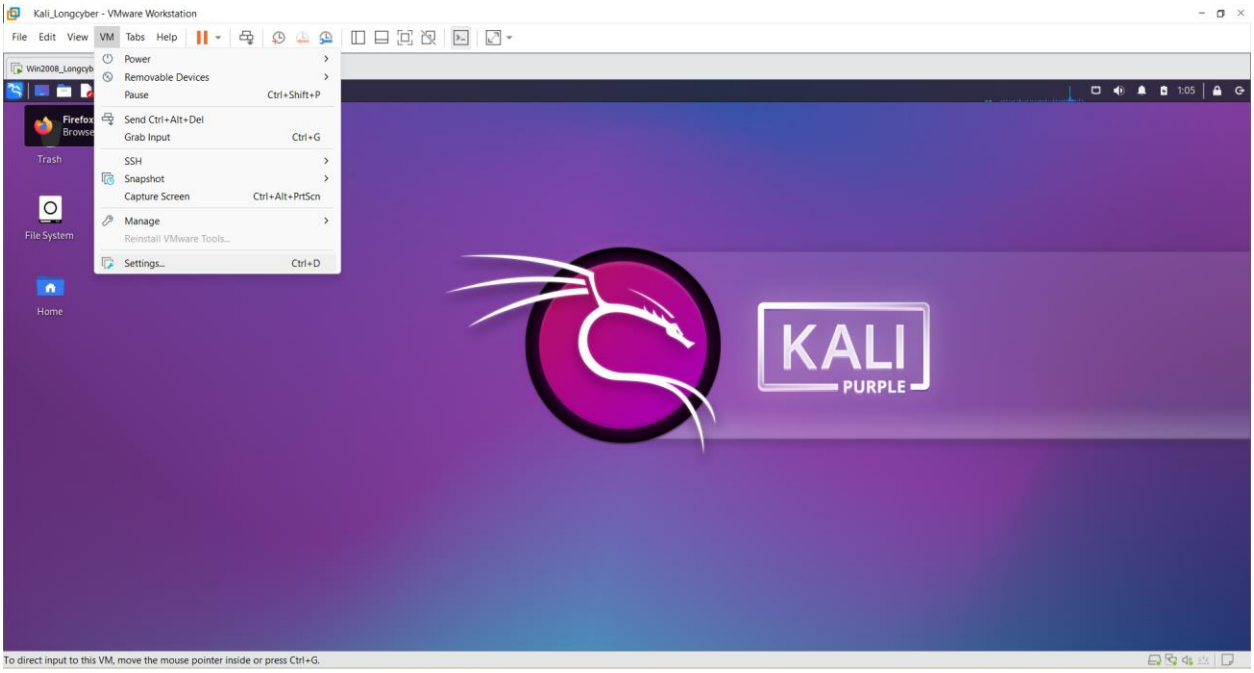
Starting the Kali Linux Machine and Adjusting Networking

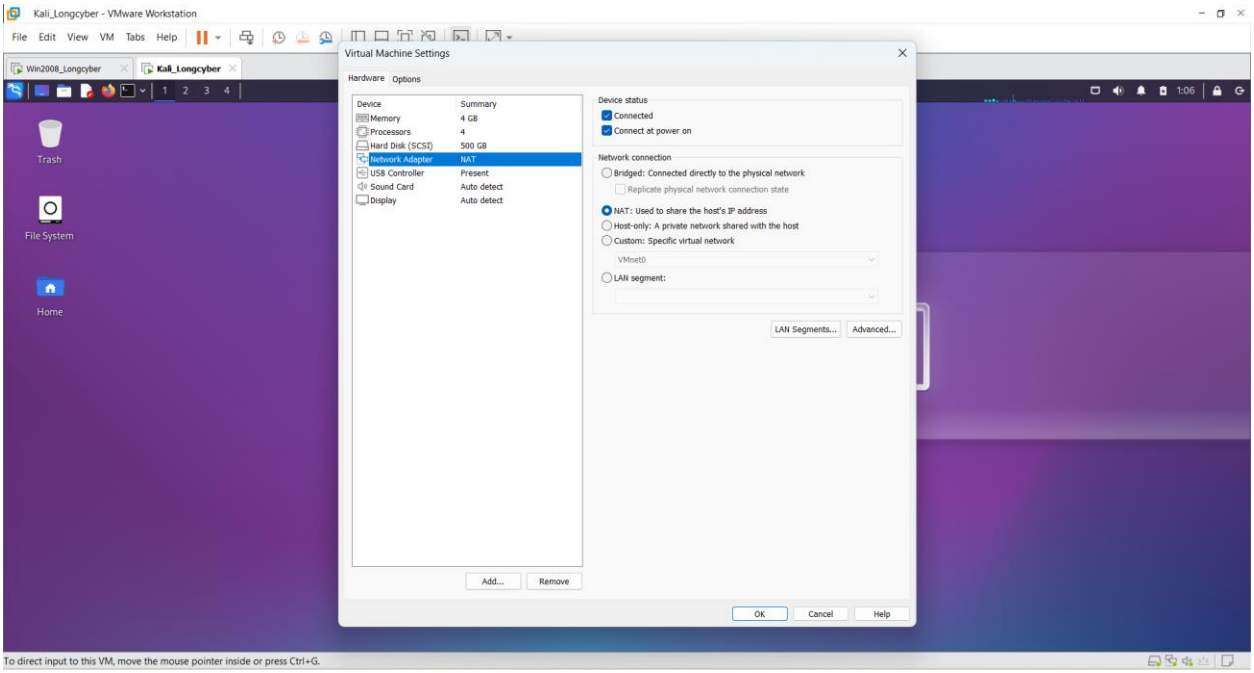




Setting the Kali Linux VM to NAT Networking

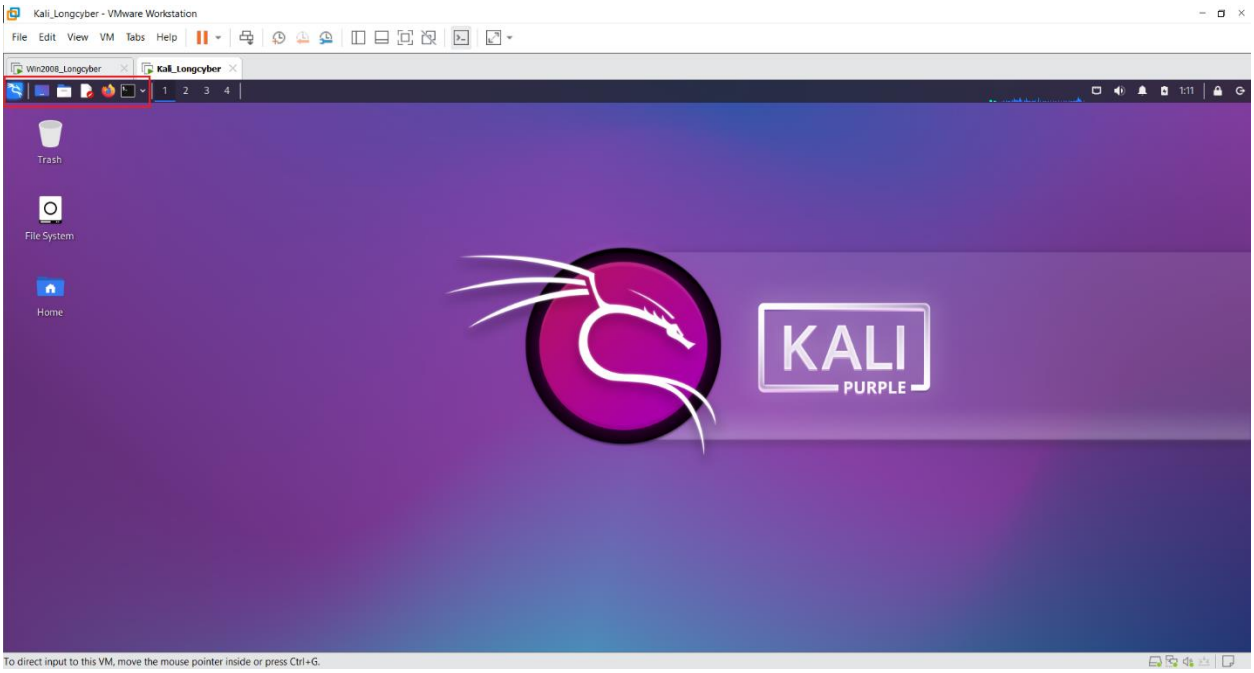
In the VMware window showing your Kali Linux desktop, on the top left, click VM, “Settings". In the "**Virtual Machine Settings**" box, on the left side, click "**Network Adapter**". On the right side, click "**NAT**". Click **OK**.





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

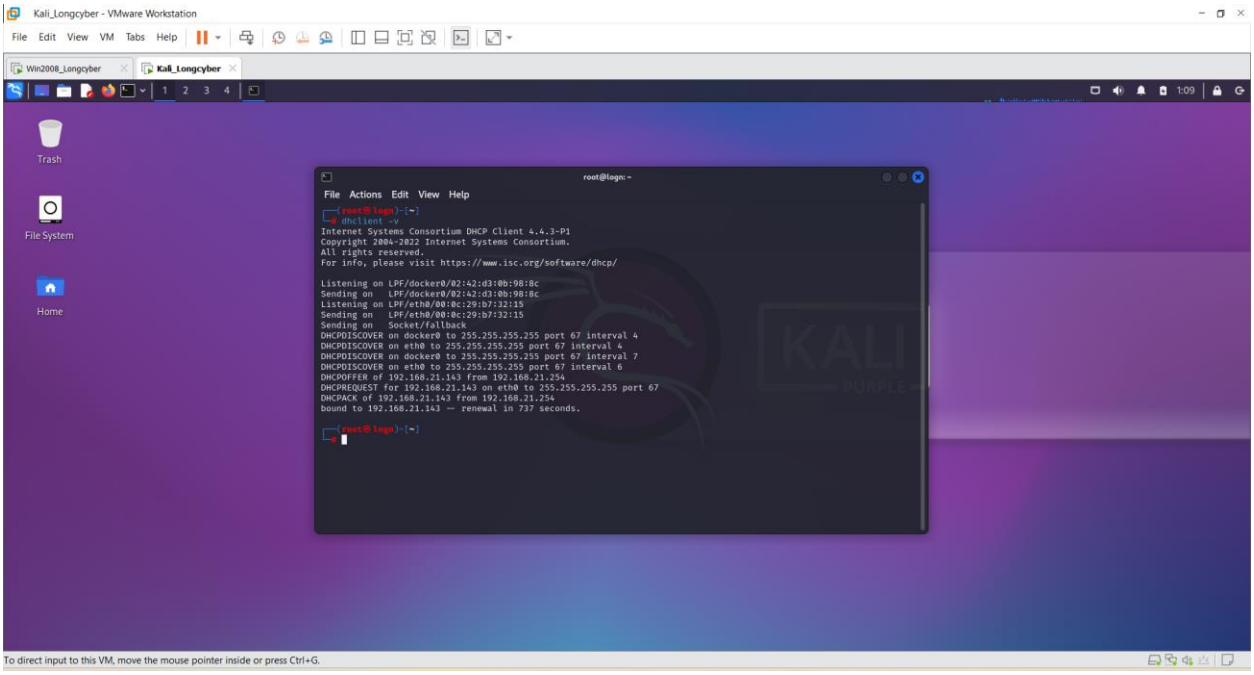
- "Applications" menu
- "Places" menu
- A blue icon that FireFox ESR
- A rectangular black icon that opens a Terminal window



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

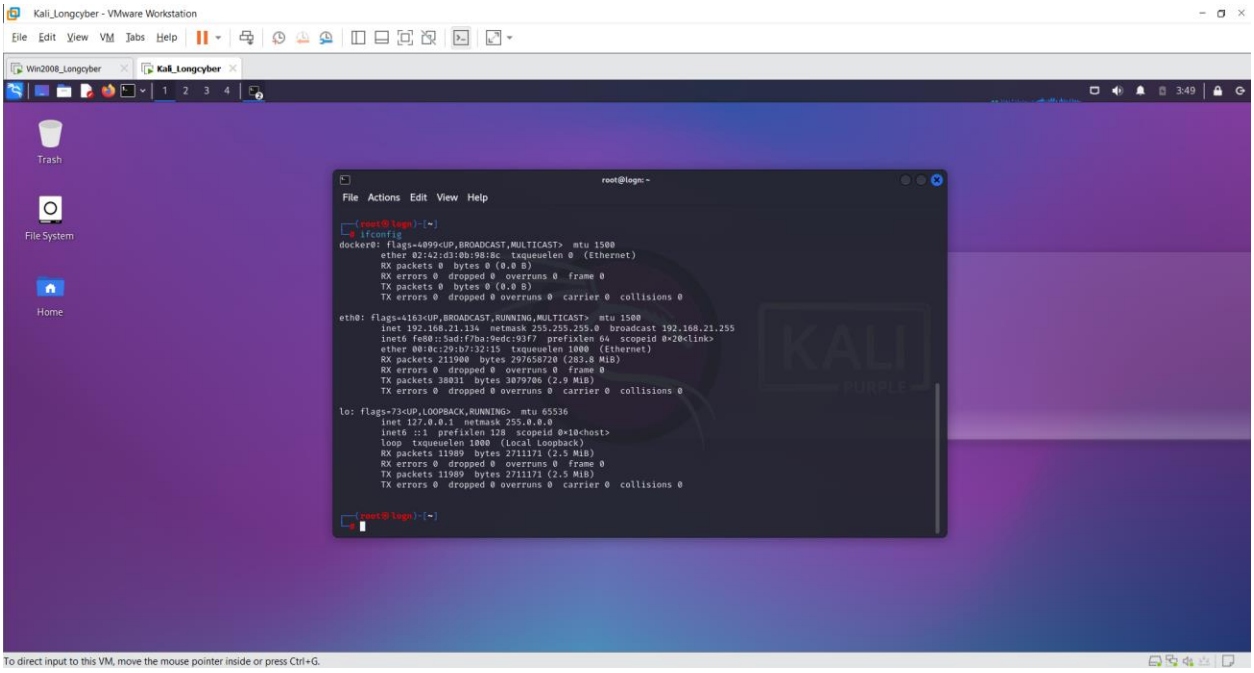


Finding the Kali Machine's IP Address

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

ifconfig

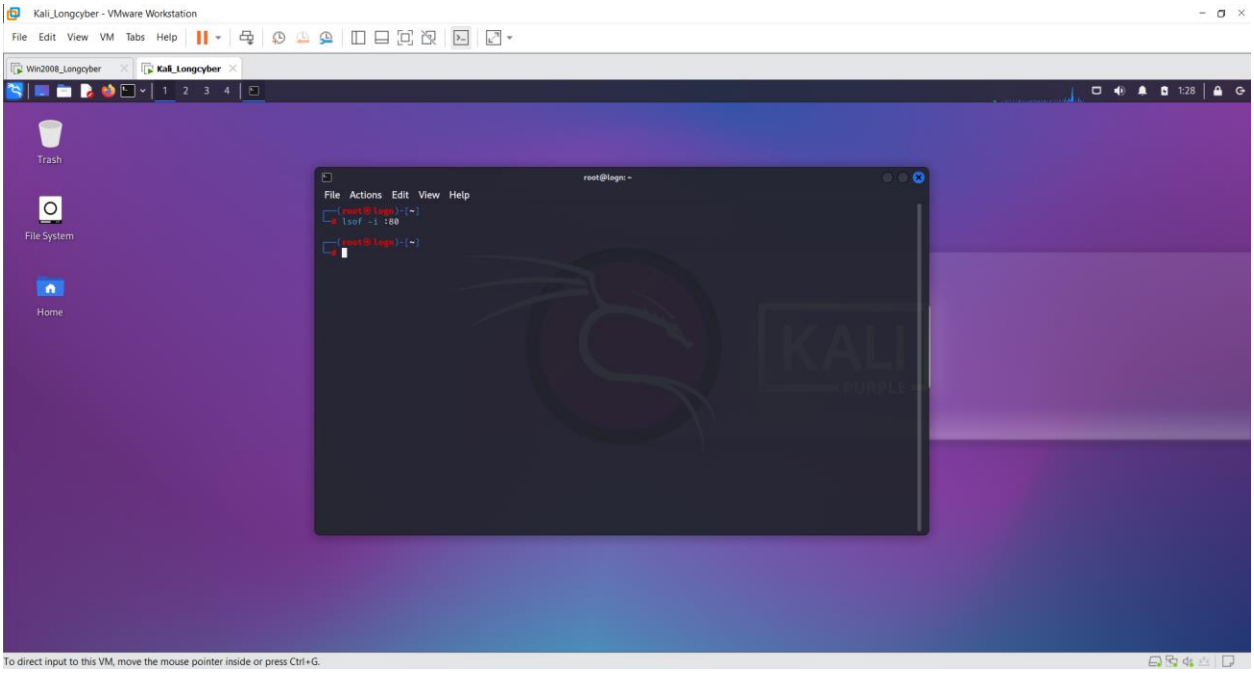
Find your IP address and make a note of it. In the example below, it is **192.168.21.134**



Checking for a Web server

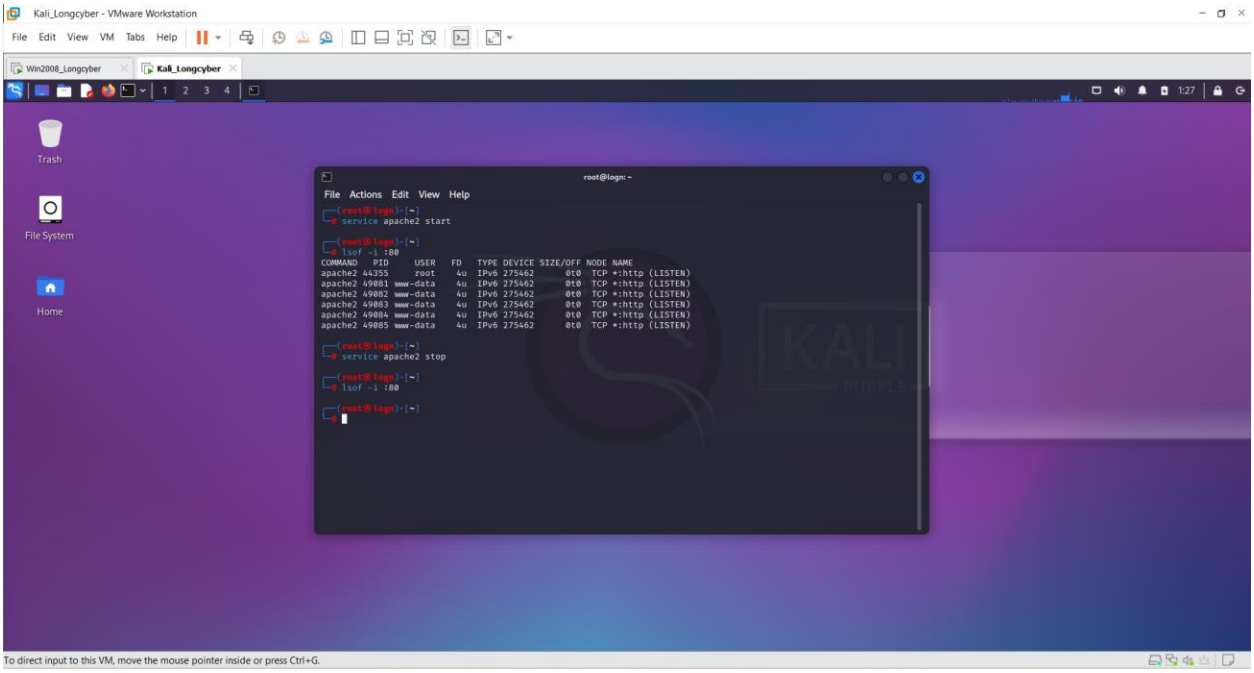
On your Linux machine, in a Terminal window, execute this command:

lsof -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



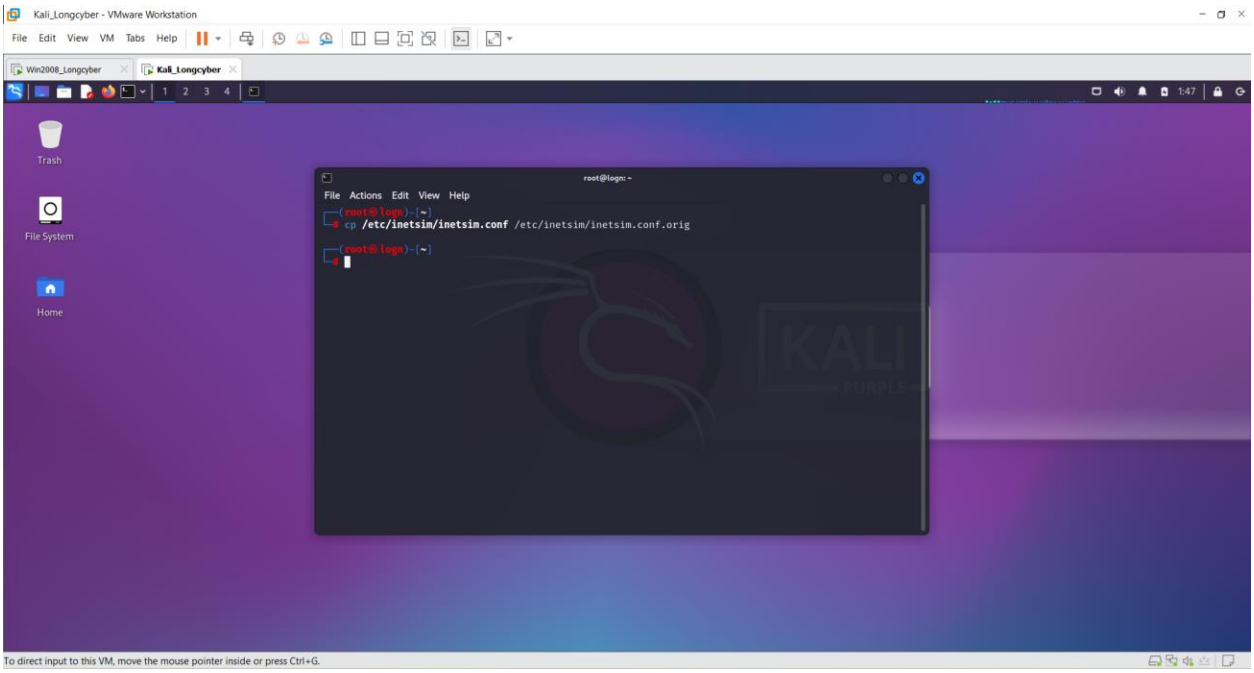
Configuring inetsim

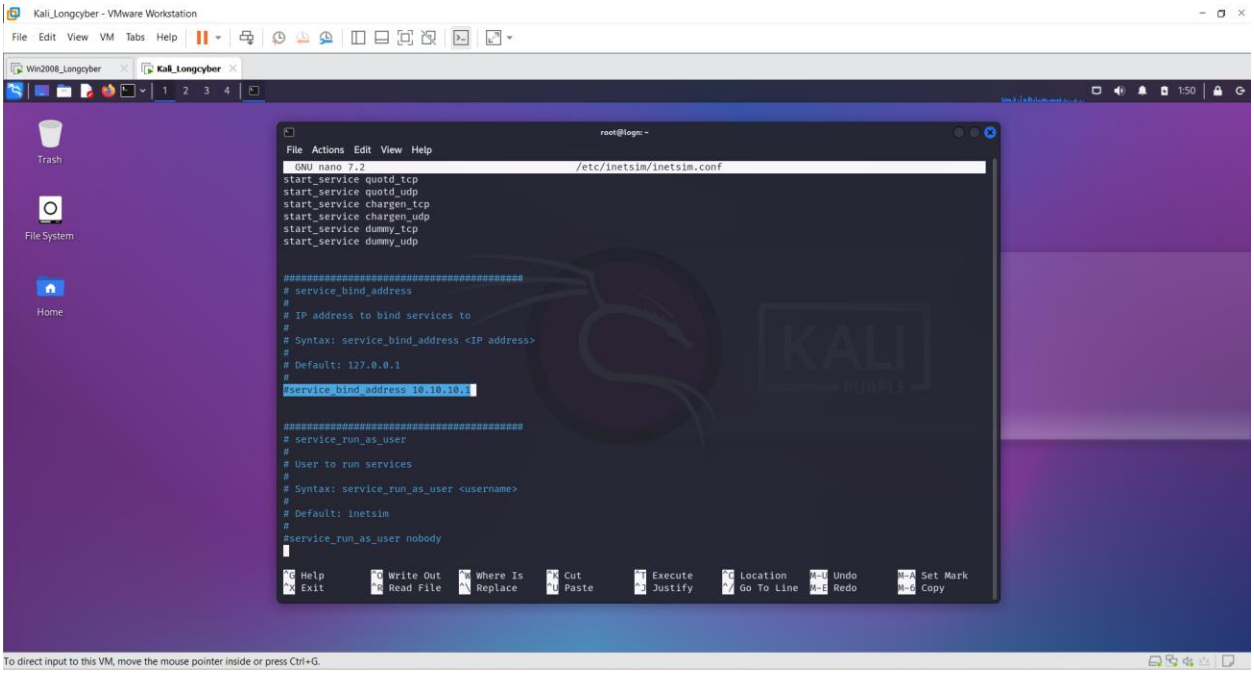
inetsim is included in Kali Linux 2 already. But it needs some configuration. On your Linux machine, in a Terminal window, execute these commands:

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.





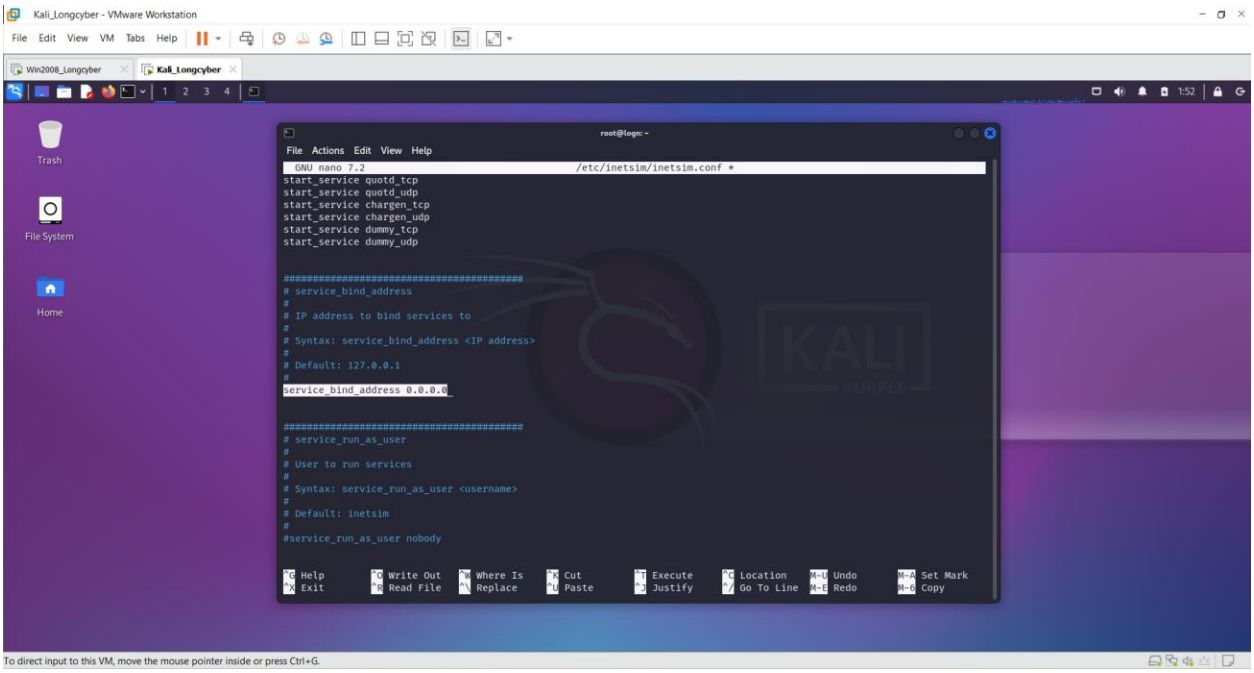
Change this line:

#service_bind_address 10.10.10.1

to this

service_bind_address 0.0.0.0

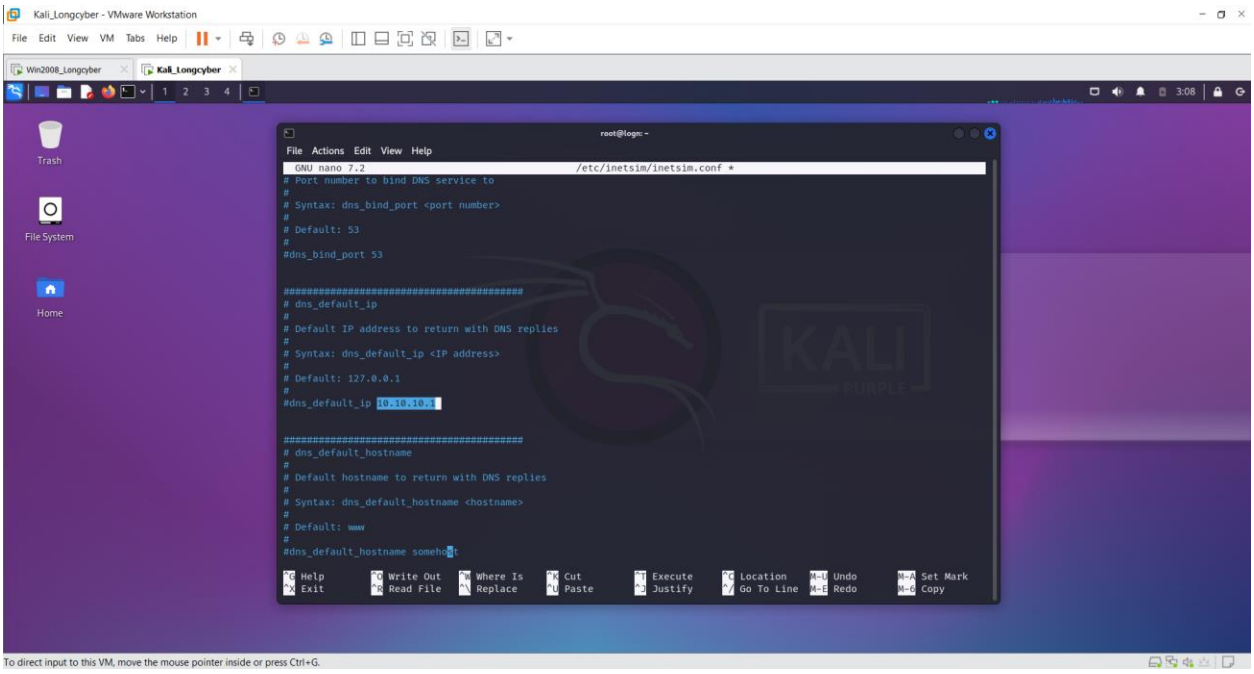
as shown below. This sets inetsim listening on all Kali's IP addresses.



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

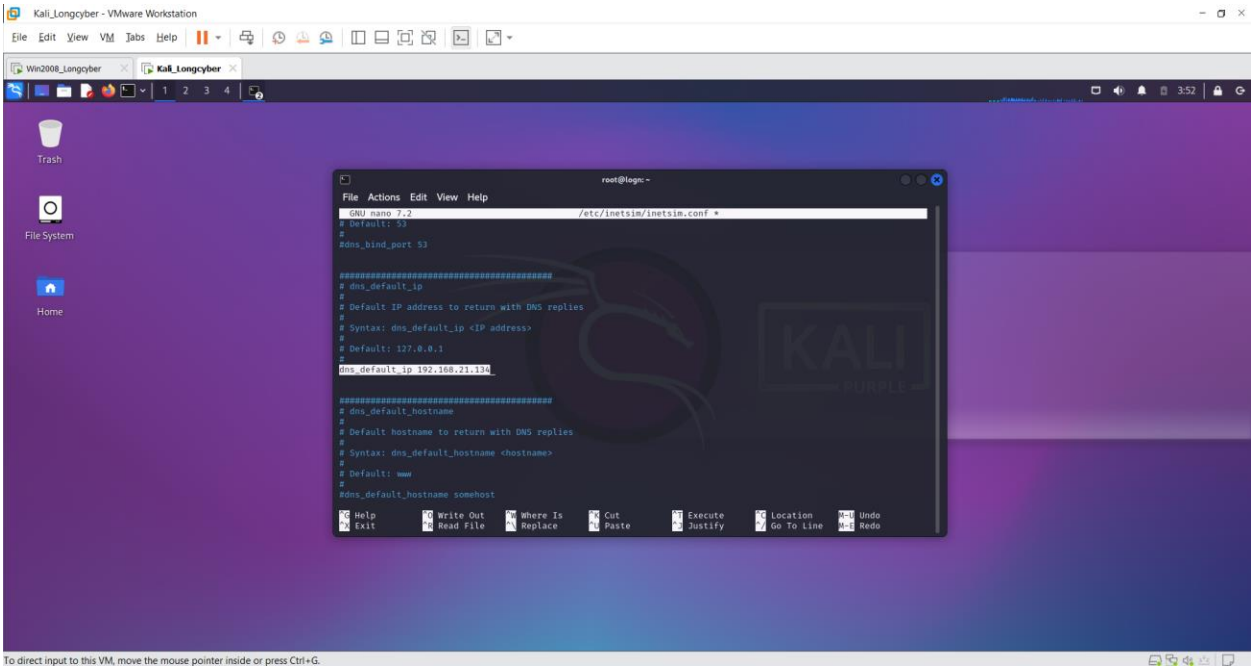
Scroll down another several screens to find the **dns_default_ip** section shown below. Find this line:

#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 192.168.21.134

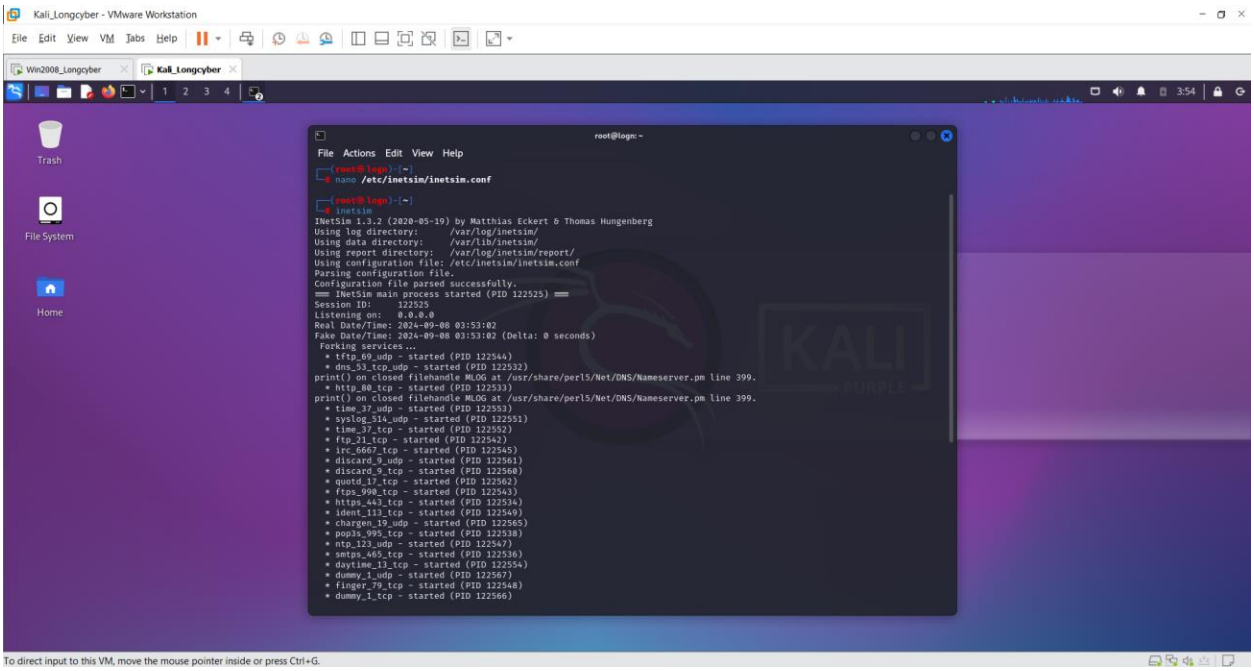


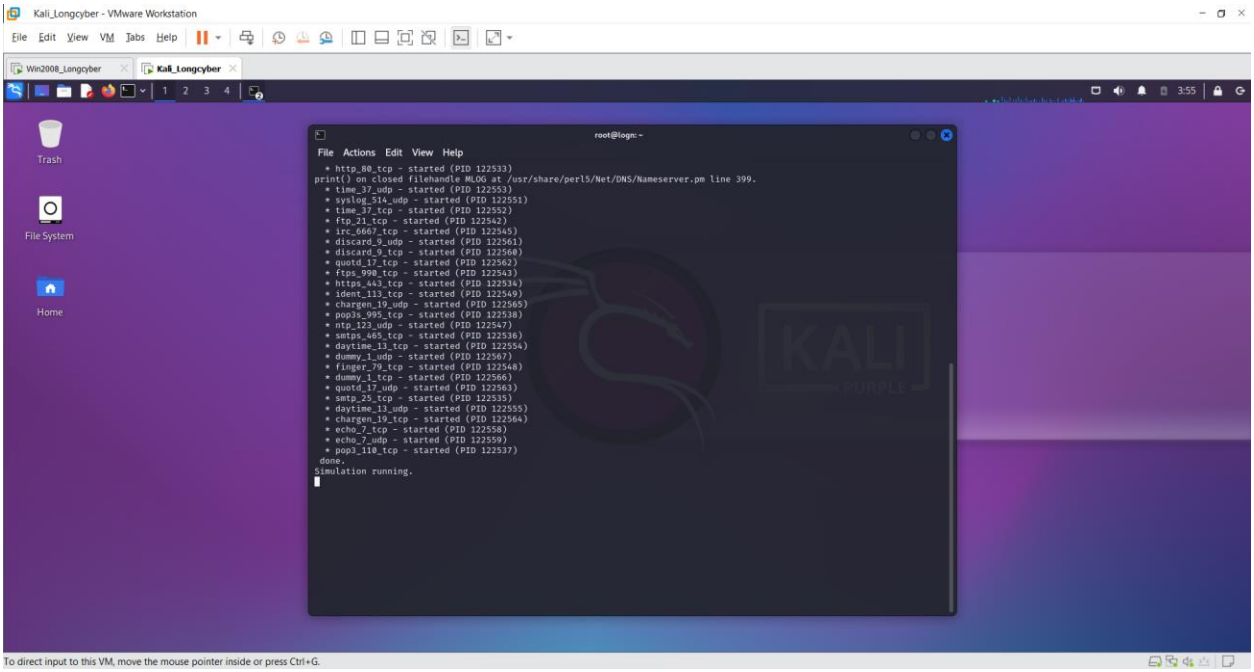
Use your correct IP address instead of "**192.168.21.134**"

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

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

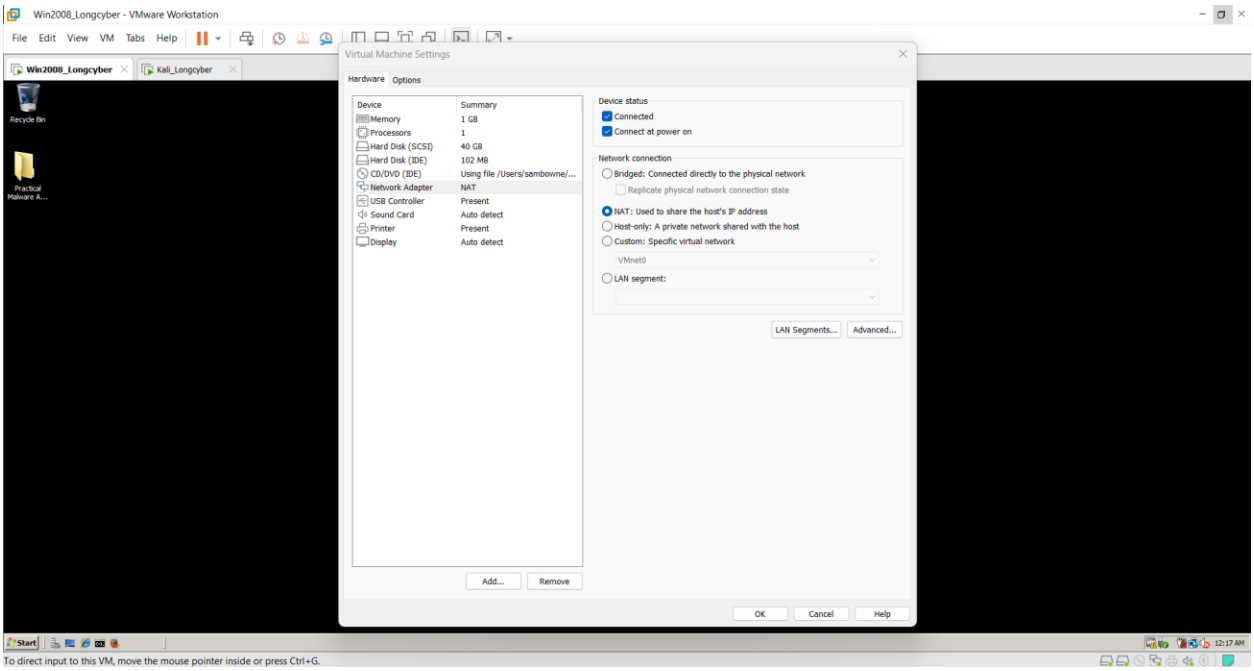
Inetsim





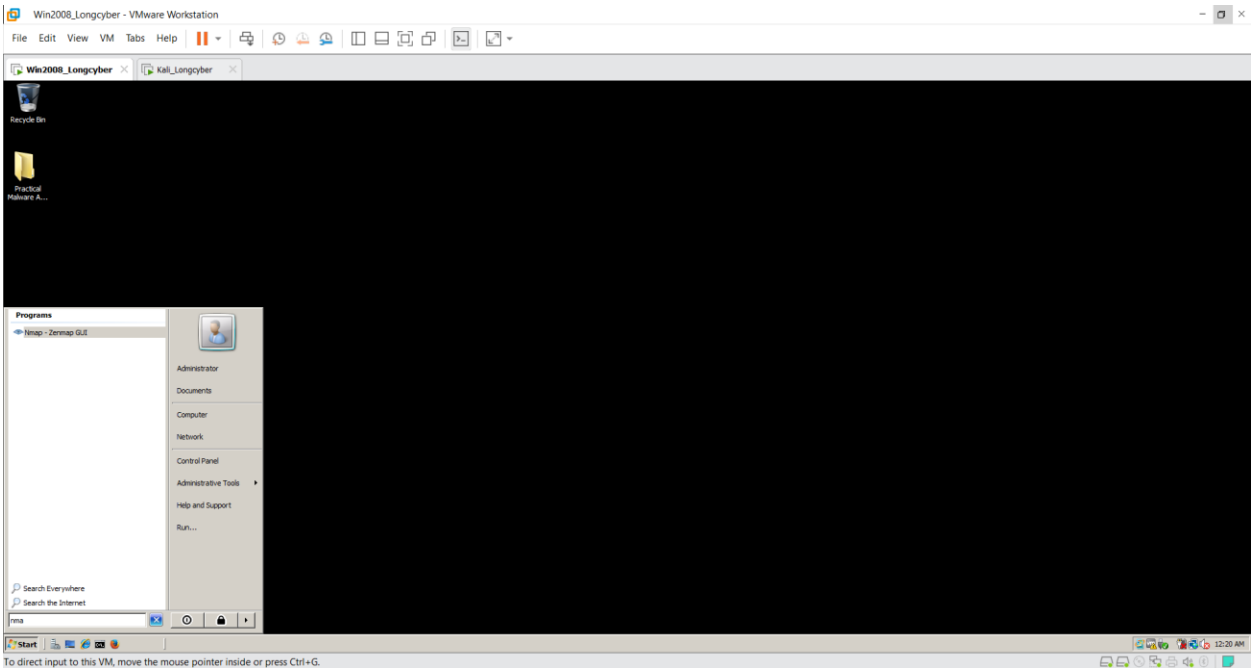
Start Your Windows VM

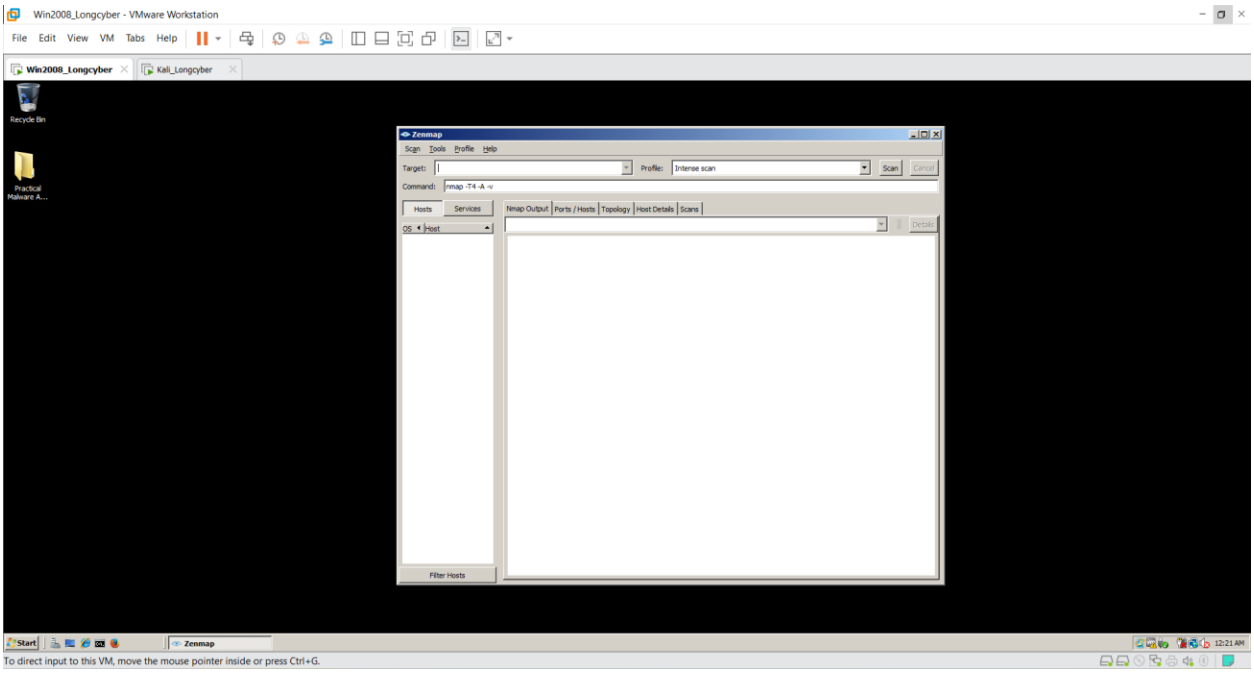
Start your Windows Server 2008 virtual machine, and set it to NAT networking.



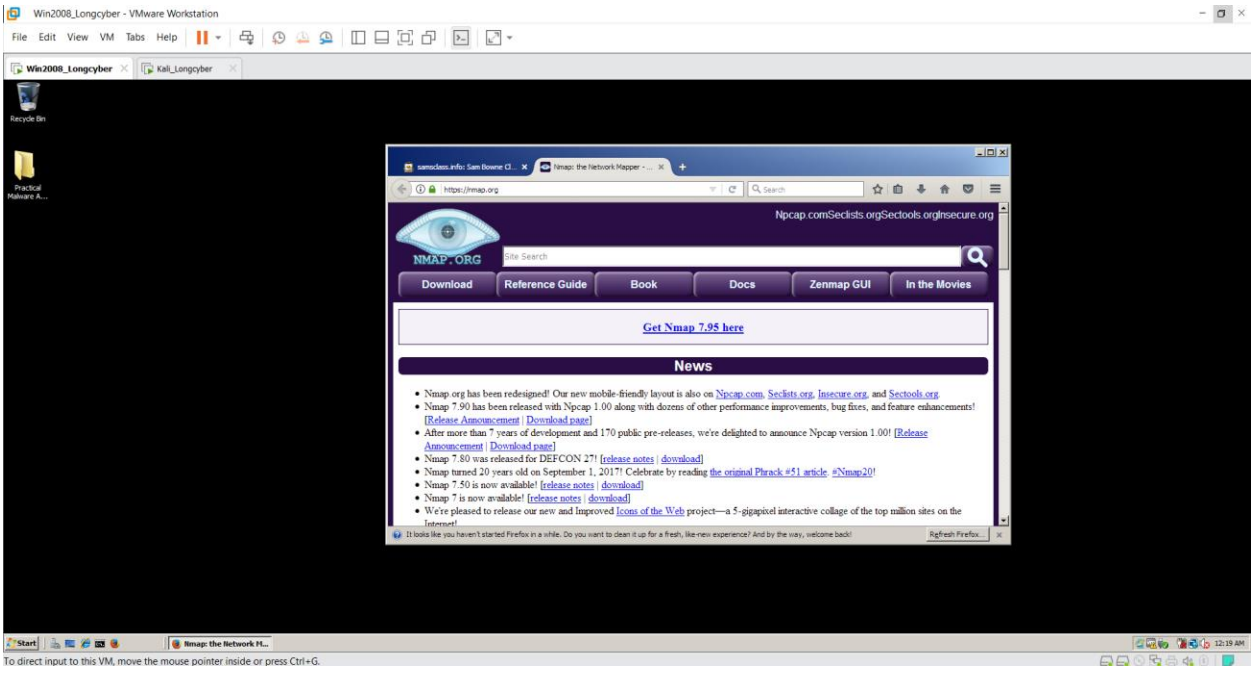
Installing Nmap

In your Windows Server 2008 virtual machine, click **Start** and look for Nmap. It should be there.



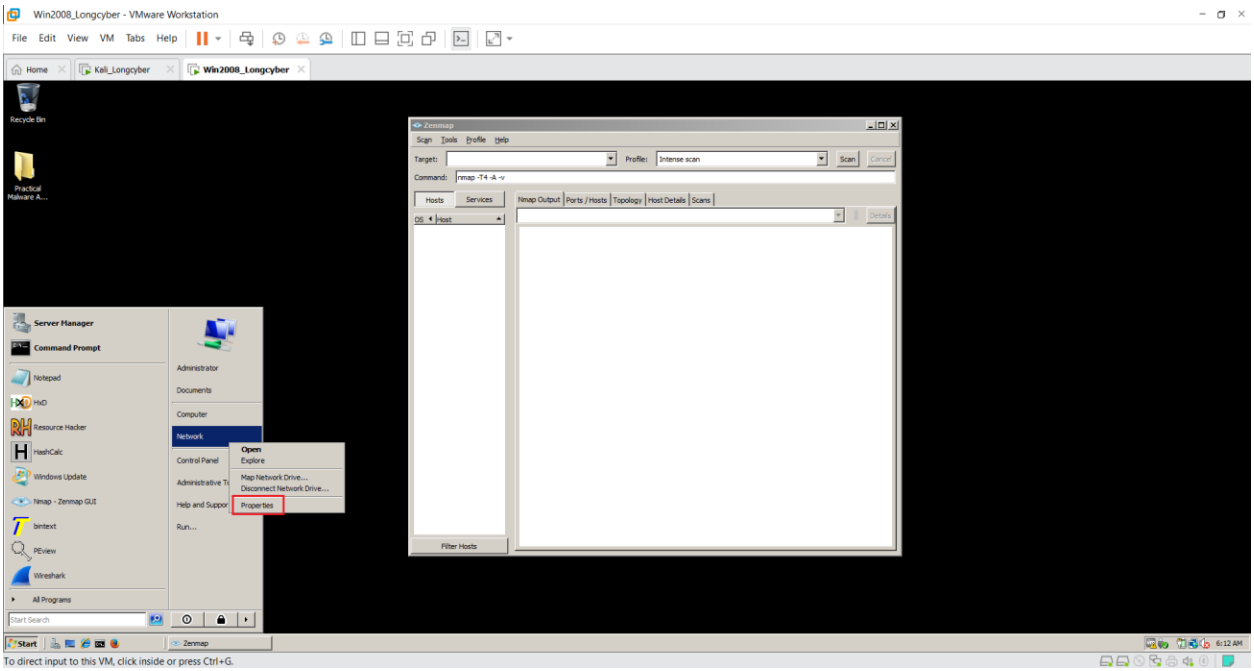


If not, open a Web browser and go to https://nmap.org/ to get it.

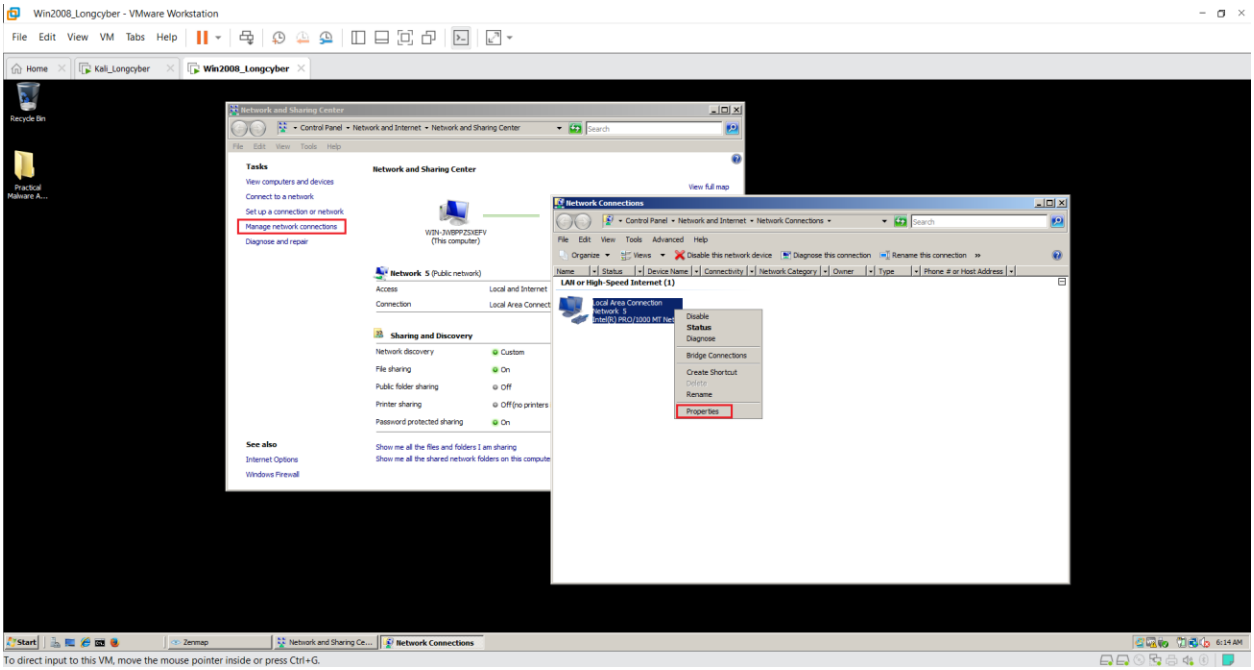


Setting the DNS Server

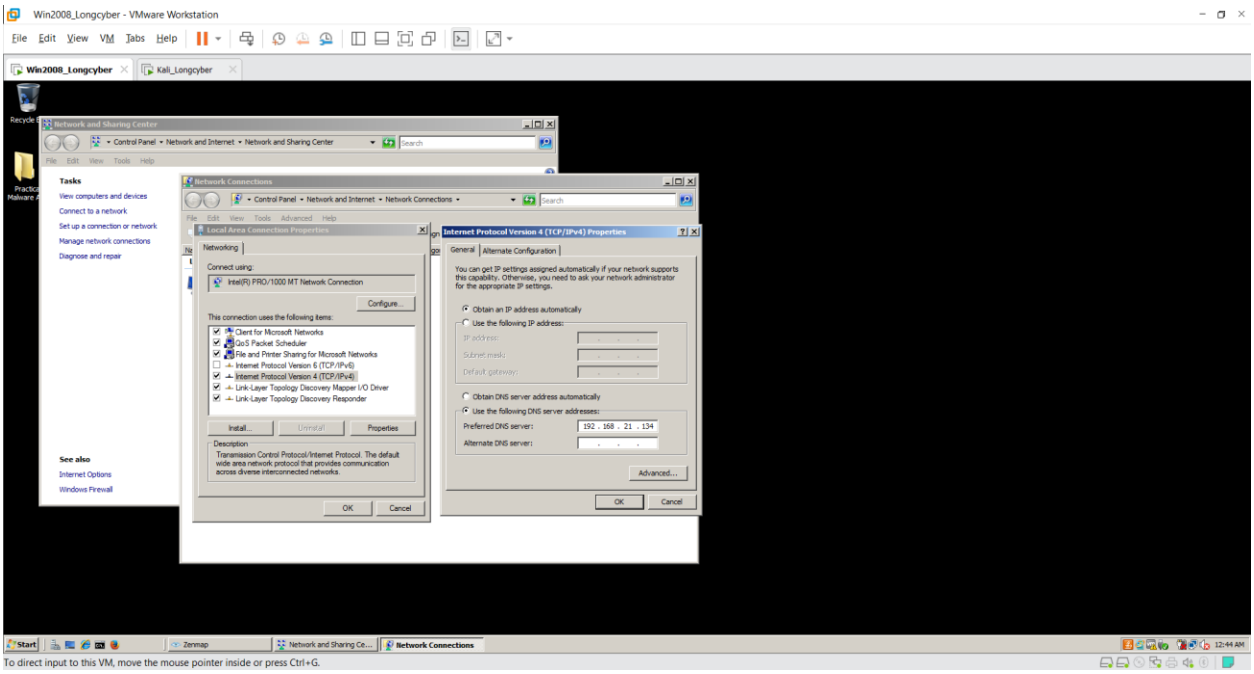
On your Windows VM, click **Start**. Right-click **Network** and click **Properties**.



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

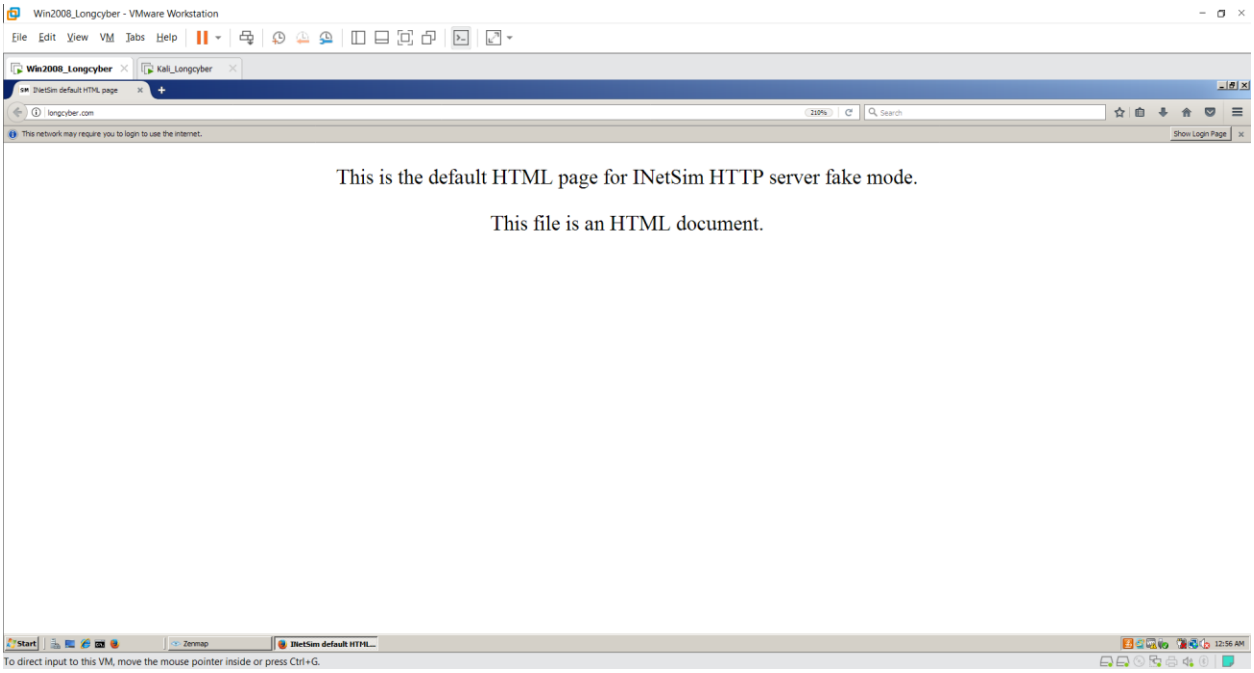


Double-click "**Internet Protocol Version 4(TCP/IPv4)**". Set your DNS server to the Kali Linux machine's IP address, as show below. Then click **OK** twice.



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:

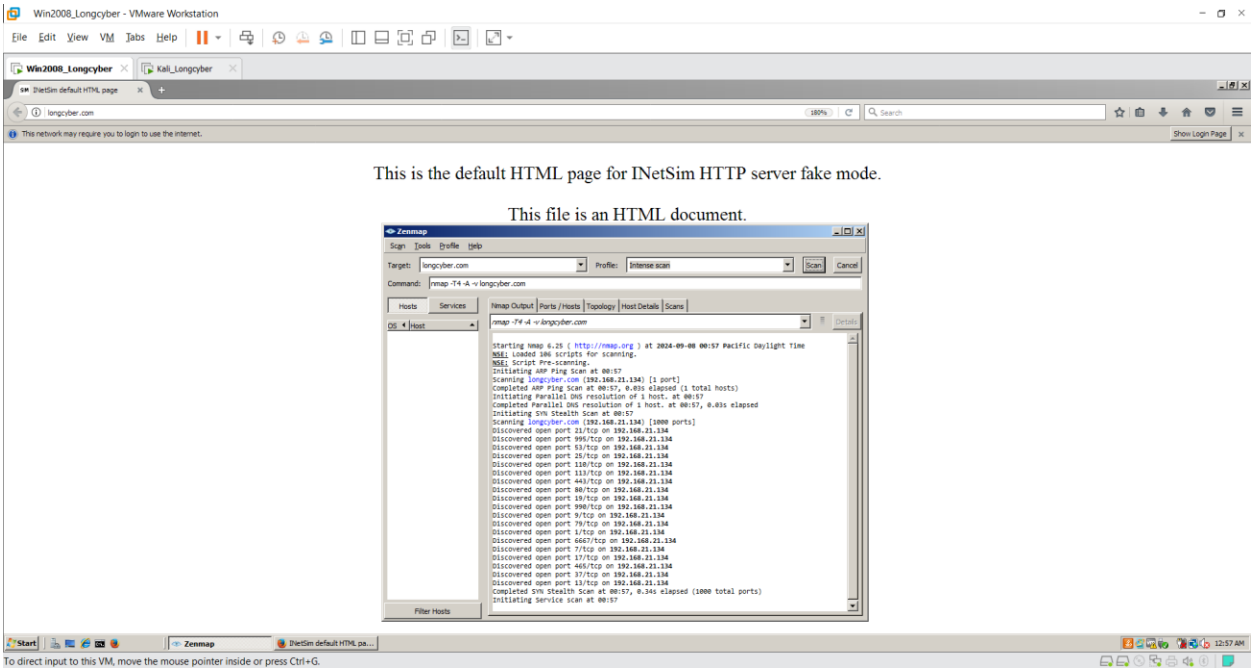


Scanning YOURNAME.com

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.


Win2008_Longcyber - VMware Workstation
File Edit View VM Tabs Help
Win2008_Longcyber
Kali_Longcyber
INetSim default HTML page
longcyber.com
This network may require you to login to use the internet.
Show Login Page
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
Zenmap
Scan Tools Profile Help
Target: longcyber.com
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v longcyber.com
Hosts
Services
OS
Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Filter Hosts
Start
Zenmap
INetSim default HTML pa...
12:57 AM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.