CNIT 126 Proj 3: Using INetSim on Kali Linux (20 pts.)

What You Need for This Project

- A computer with VMware Player. You can use any host OS you like, and if you prefer to use some other virtual machine software like VirtualBox or Xen, that's fine too. You can download VMware Player here:

  https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/12_0|PLAYER-1252|product_downloads

- The instructions below assume you are using Windows 10. You can use VMware on the Mac and other operating systems, but the steps may be somewhat different.

Purpose

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

Start Your Host Machine

If you are working in S214, select a machine to be your primary machine for the semester. You'll want to keep using the same machine as much as possible, because your virtual machines will be there. Power on your computer. Boot to the operating system named "Win 10-S214". Log on as **Student** with no password.

Making Your VM (Virtual Machines) Folder

Click **Start**, "**File Explorer**", "**This PC**". Find the "**VMs-S214**" drive and double-click it to open it.

In the VMs-S214 window, right-click the empty space and click **New**, **Folder**. Name the folder "**YOUR NAME VMs**" replacing YOUR NAME with your own name.

Getting the Virtual Machine 7-Zip Archive Files

You can download the files you need here:

http://games.samsclass.info/secret/download-vms.htm

You need a username and password to view that page. The username and password are written on the blackboard in the hacking lab, and you can get them from your instructor.

The two files you need are:

- Kali Linux 32 bit VM PAE: Kali-Linux-2016.2-vm-i686.7z (or a later version)
- Windows 2008 Server: Win2008-Target.7z

If you don't have broadband Internet access, you can get these files on a DVD labelled "8K2" in the hacking lab.

Getting 7-Zip

You need 7-Zip on your host machine. If you don't have it, download it from 7-zip.org

If you are using a Mac, get Ez7z

Extracting the Kali Virtual Machine

Make a folder for your Kali virtual machine on the VMs-S214 partition or some other available partition. I recommend making a folder with your name on it, and a subfolder within it named Kali.

DO NOT PUT VIRTUAL MACHINES ON THE C: DRIVE IN S214. They fill the drive and make the machine unusable, and will be deleted.

Right-click the **Kali-Linux-2016.2-vm-i686.7z** file, click **7-Zip**, and click "**Extract Files...**". In the "Extract to:" box, enter the path to the folder you prepared, such as "G:\YOURNAME\Kali". Click **OK**.

Extracting the Windows Server 2008 Virtual Machine

Right-click the **Win2008-Target.7z** file, click **7-Zip**, and click "**Extract Files...**". In the "Extract to:" box, enter the path to the folder you prepared, such as "G:\YOURNAME\Srv08". Click **OK**.

> ***DO NOT PUT VIRTUAL MACHINES ON THE C: DRIVES IN S214!***
>
> *They fill the drive and make the machines stop working. Virtual machines left on the desktop, Documents folder, or other C: drive locations may be deleted at any time, as needed to keep the machines working.*

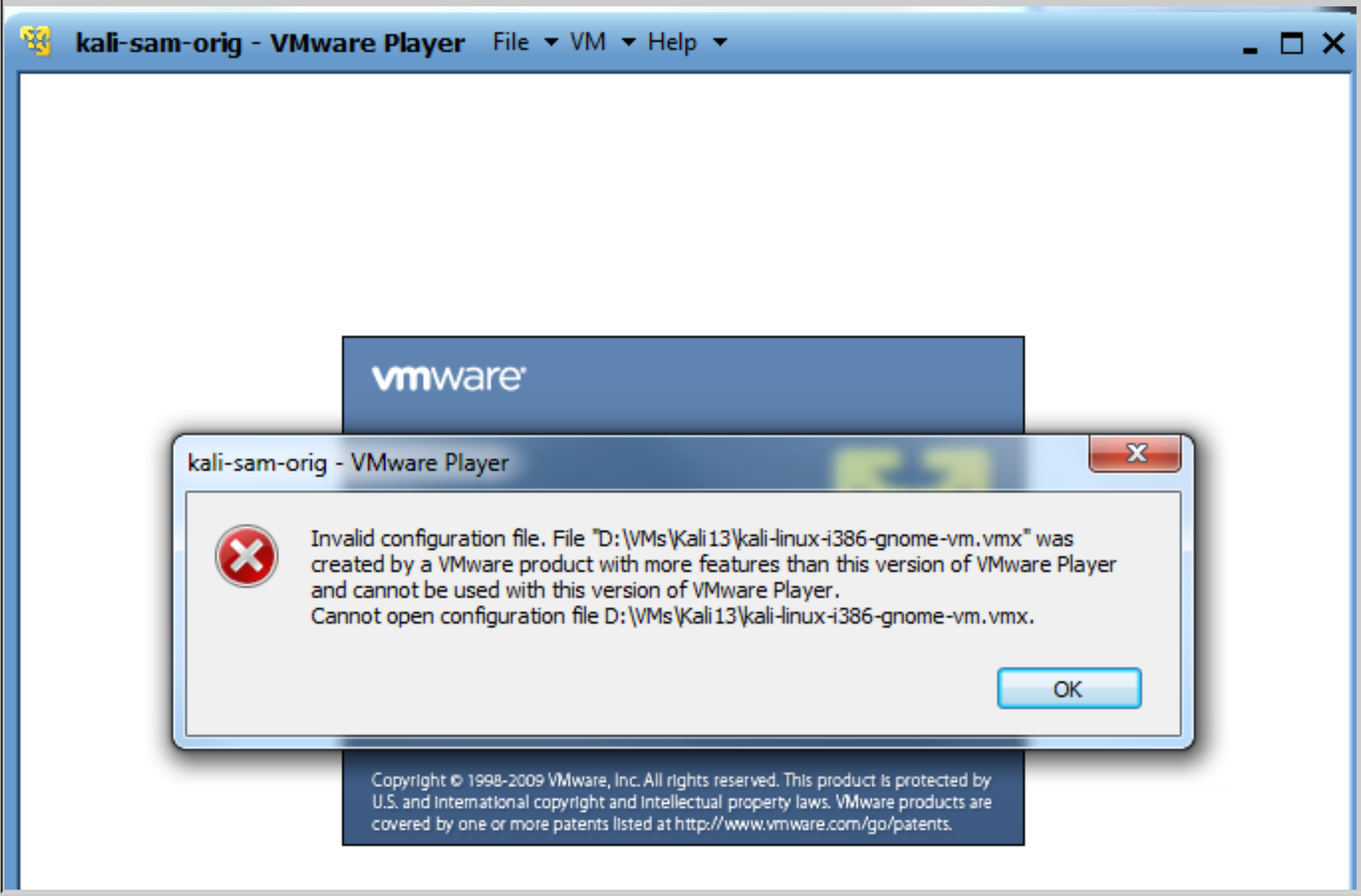
Starting your Win2008-Target Virtual Machine

In the VMware Player window, click "**Open a Virtual Machine**". Browse to the VMs-S214 drive amd open the folder with your name on it. Open the "Win2008-Target" folder and double-click the "**Windows Server 2008 2.vmx**" file.

In the VMware Player window, click the green "**Play virtual machine**" button.

Troubleshooting

If you see the message shown below, you need to update VMware Player. An updated version of VMware Player is on the S13 disk.



Invalid configuration file. File "D:\VMs\Kali13\kali-linux-i386-gnome-vm.vmx" was created by a VMware product with more features than this version of VMware Player and cannot be used with this version of VMware Player.
Cannot open configuration file D:\VMs\Kali13\kali-linux-i386-gnome-vm.vmx.

Copyright © 1998-2009 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

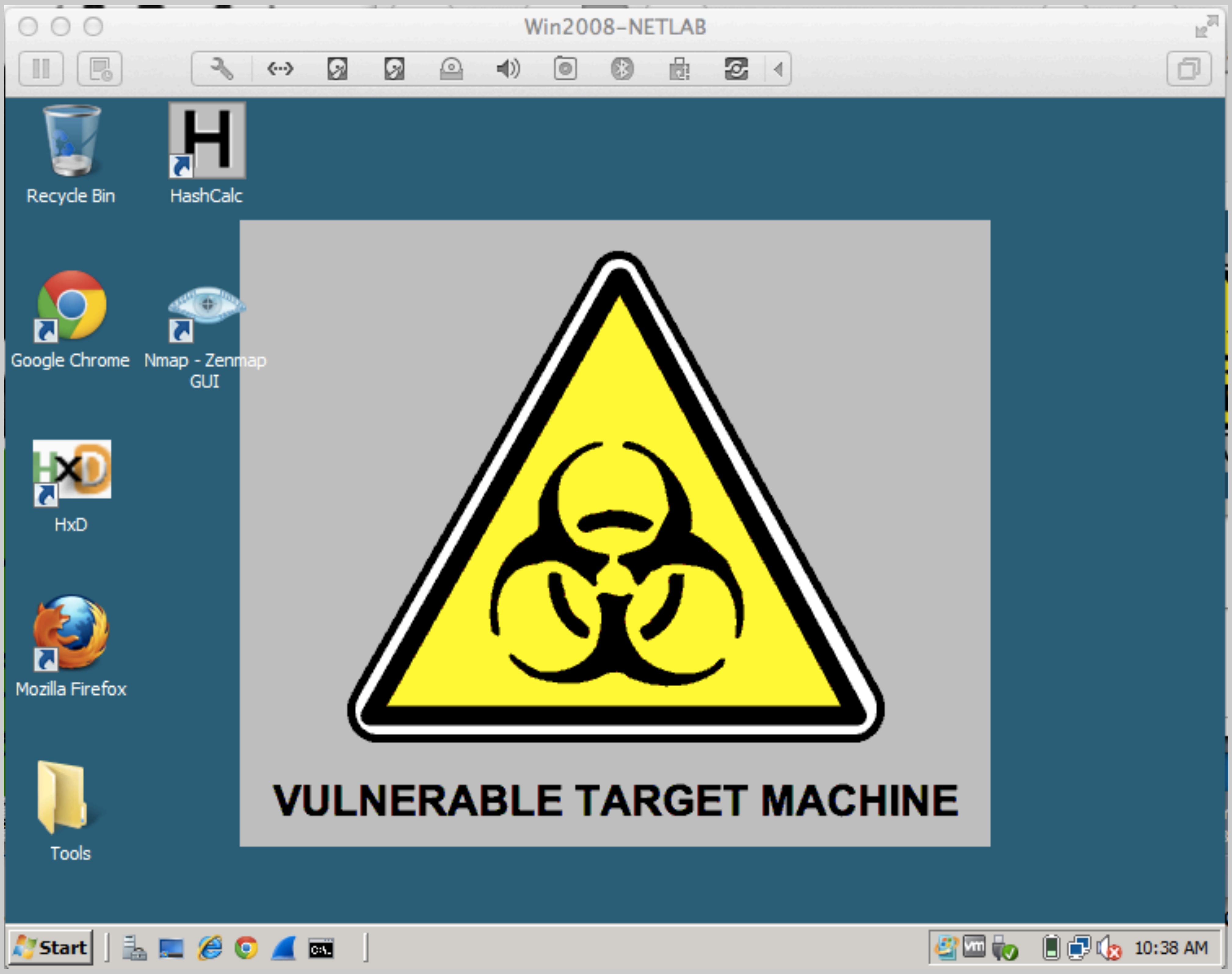
VMware Player will pop up several dialog boxes, asking whether this machine was moved or copied, telling you details about the processor, etc. Just accept the default choice for all those boxes.

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:



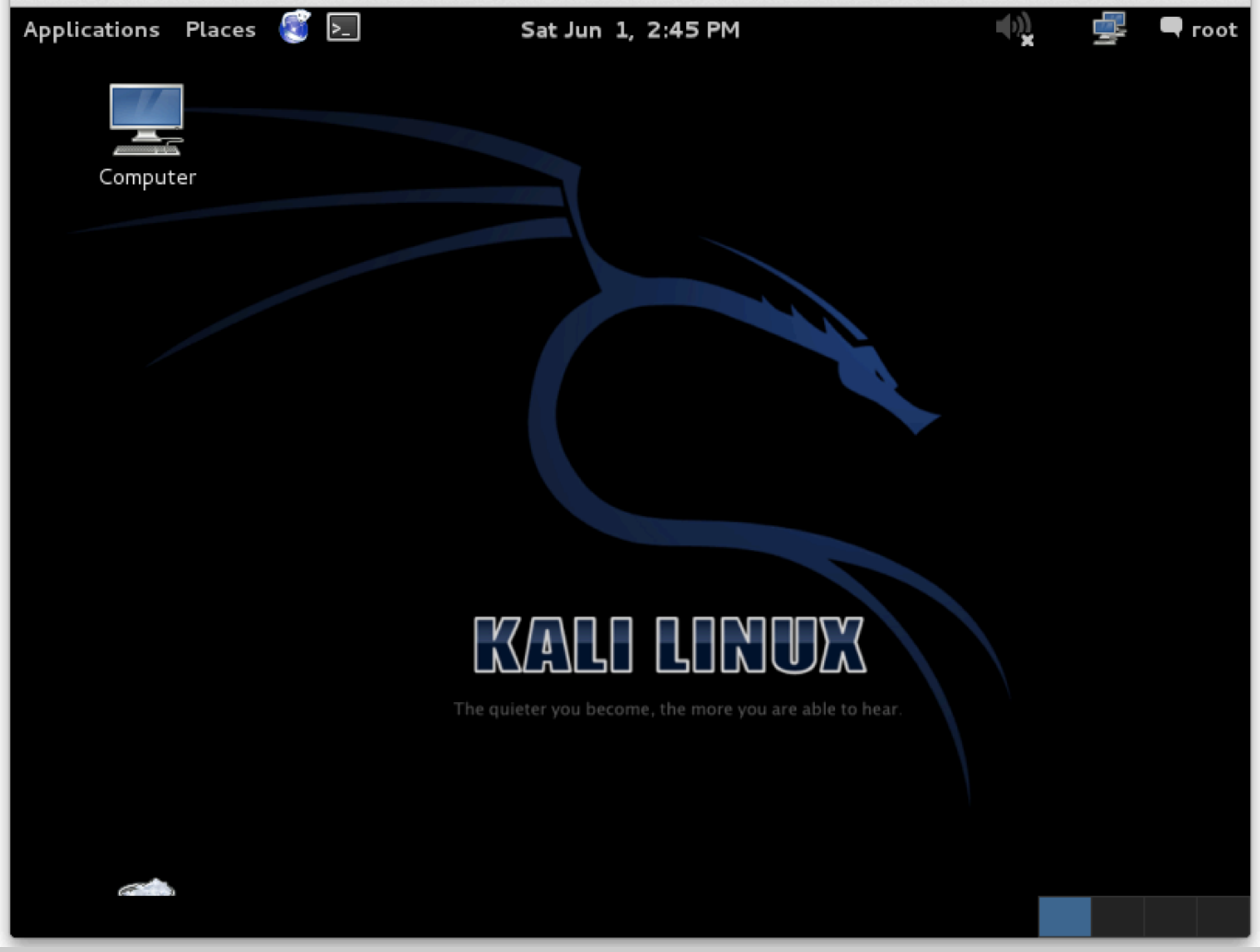
Starting the Kali Linux Machine and Adjusting Networking

Start the Attacker Linux machine in VMware Player.

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 Player window showing your Kali Linux desktop, on the top left, click **Player**, **Manage**, "**Virtual Machine 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 opens IceWeasel, a free version of FireFox
- A rectangular black icon that opens a Terminal window
- The date and time

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:

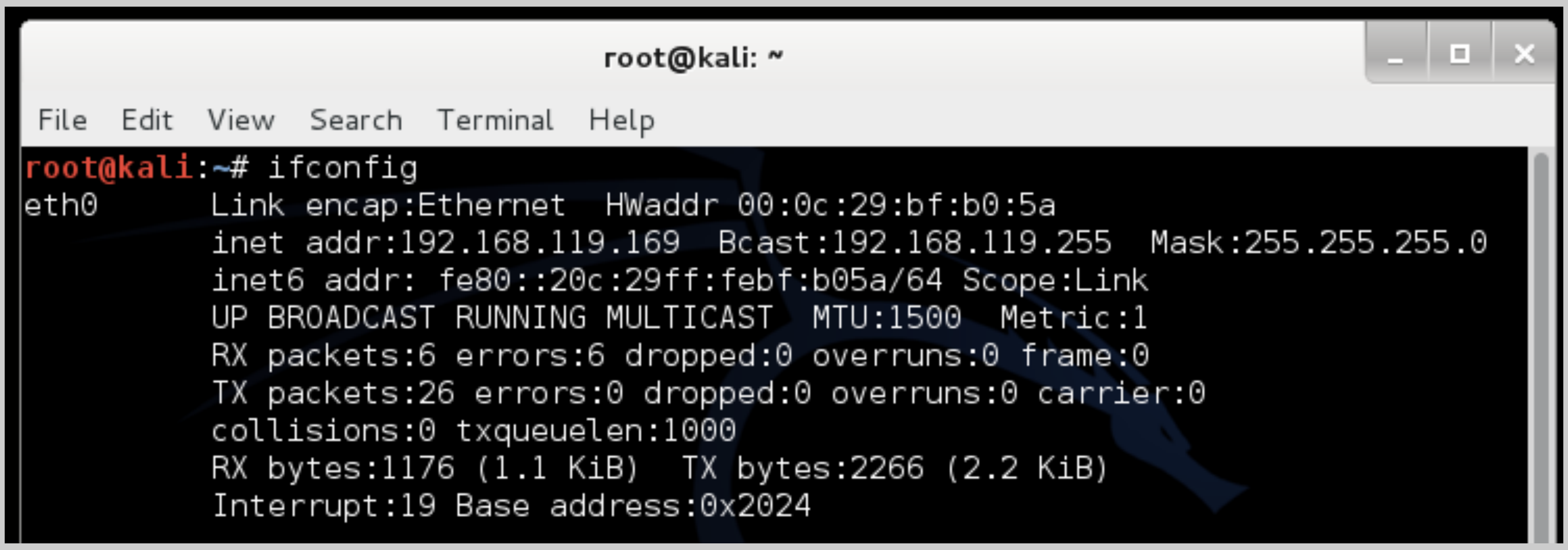
```
dhclient -v
```

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 192.168.119.169.



```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:bf:b0:5a
          inet addr:192.168.119.169  Bcast:192.168.119.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:febf:b05a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:6 dropped:0 overruns:0 frame:0
          TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1176 (1.1 KiB)  TX bytes:2266 (2.2 KiB)
          Interrupt:19 Base address:0x2024
```

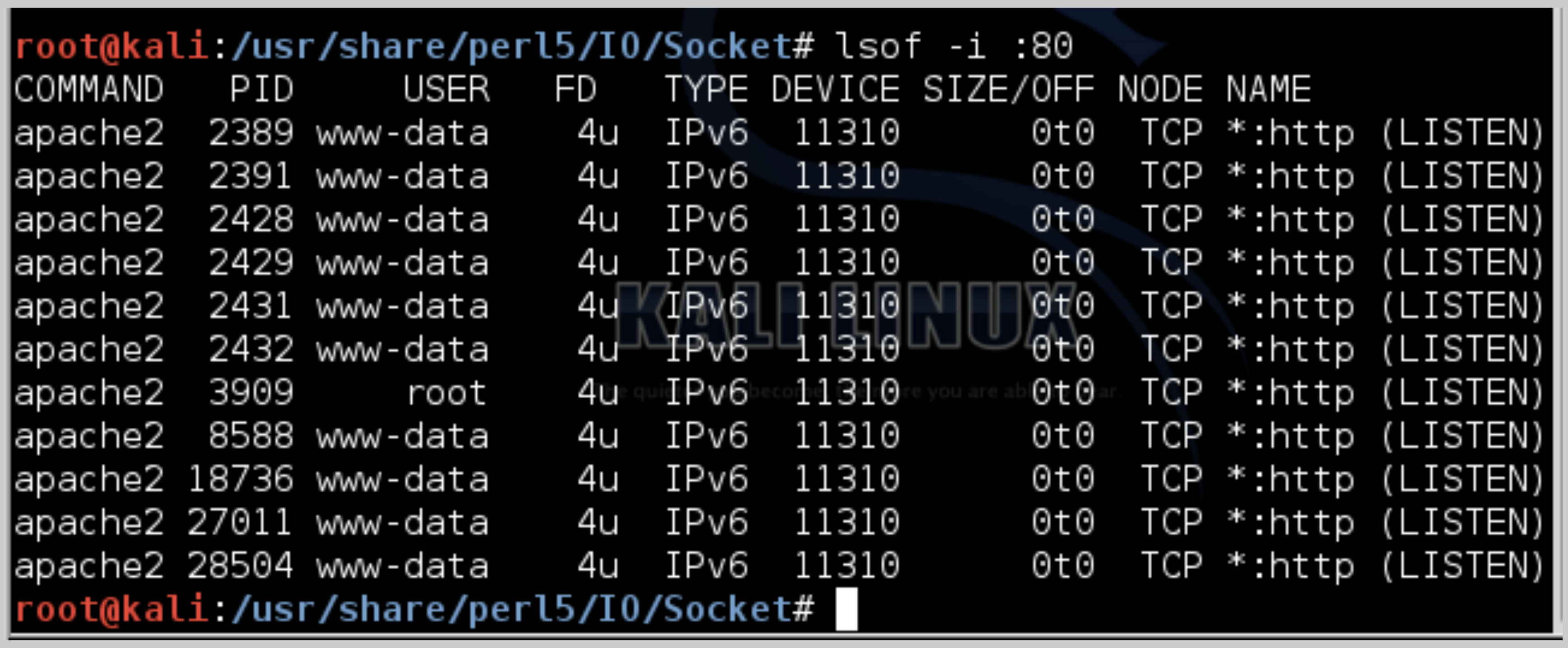
Checking for a Web server

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
```



```
root@kali:/usr/share/perl5/IO/Socket# lsof -i :80
COMMAND    PID     USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
apache2   2389 www-data    4u  IPv6  11310      0t0  TCP *:http (LISTEN)
apache2   2391 www-data    4u  IPv6  11310      0t0  TCP *:http (LISTEN)
apache2   2428 www-data    4u  IPv6  11310      0t0  TCP *:http (LISTEN)
apache2   2429 www-data    4u  IPv6  11310      0t0  TCP *:http (LISTEN)
apache2   2431 www-data    4u  IPv6  11310      0t0  TCP *:http (LISTEN)
apache2   2432 www-data    4u  IPv6  11310      0t0  TCP *:http (LISTEN)
apache2   3909     root    4u  IPv6  11310      0t0  TCP *:http (LISTEN)
apache2   8588 www-data    4u  IPv6  11310      0t0  TCP *:http (LISTEN)
apache2  18736 www-data    4u  IPv6  11310      0t0  TCP *:http (LISTEN)
apache2  27011 www-data    4u  IPv6  11310      0t0  TCP *:http (LISTEN)
apache2  28504 www-data    4u  IPv6  11310      0t0  TCP *:http (LISTEN)
root@kali:/usr/share/perl5/IO/Socket#
```

Configuring inetsim

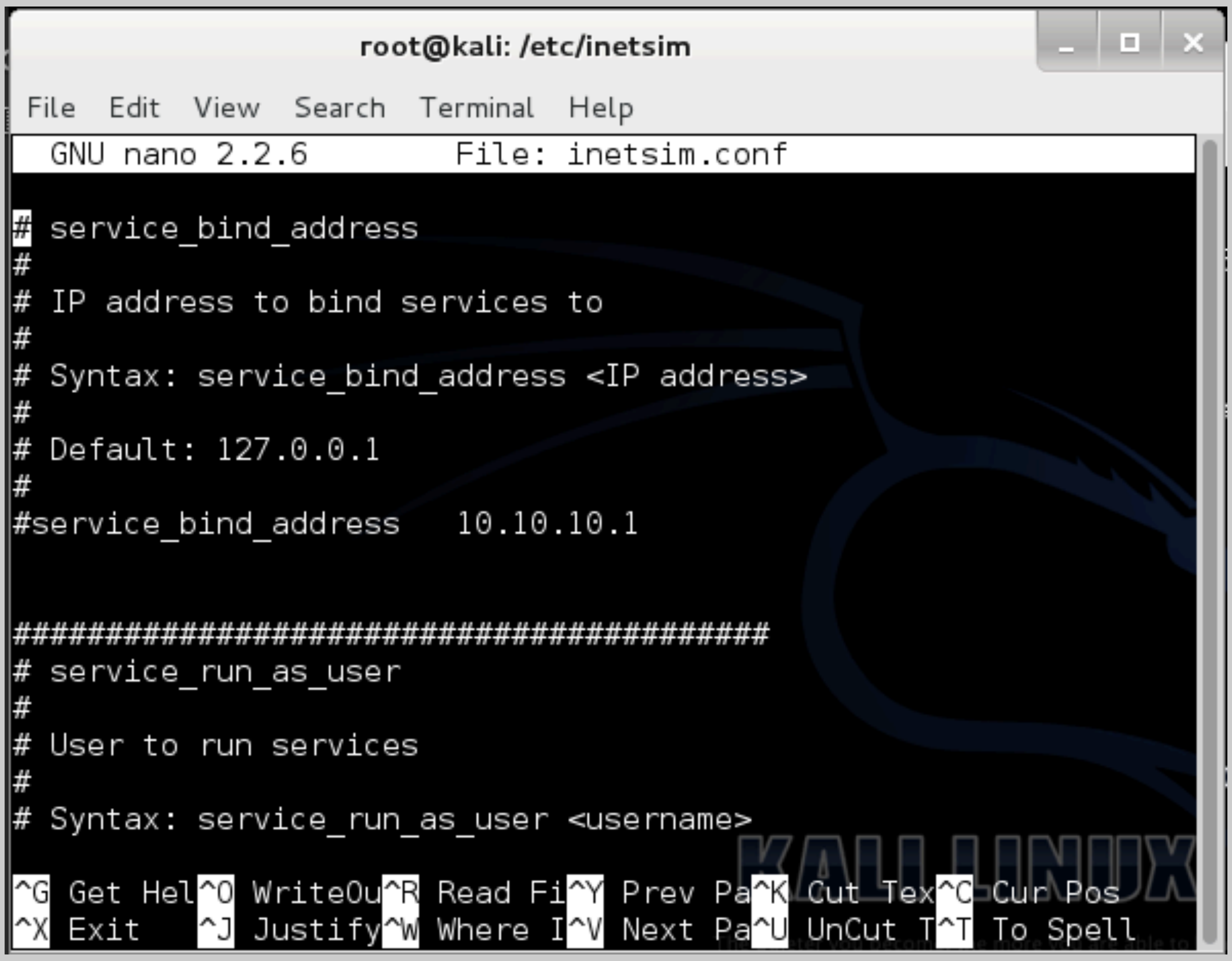
inetsim is included in Kali Linux 2 already. But it needs some configuration.

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.



```
  GNU nano 2.2.6          File: inetsim.conf

# 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>

^G Get Hel^O WriteOu^R Read Fi^Y Prev Pa^K Cut Tex^C Cur Pos
^X Exit   ^J Justify^W Where I^V Next Pa^U UnCut T^T To Spell
```

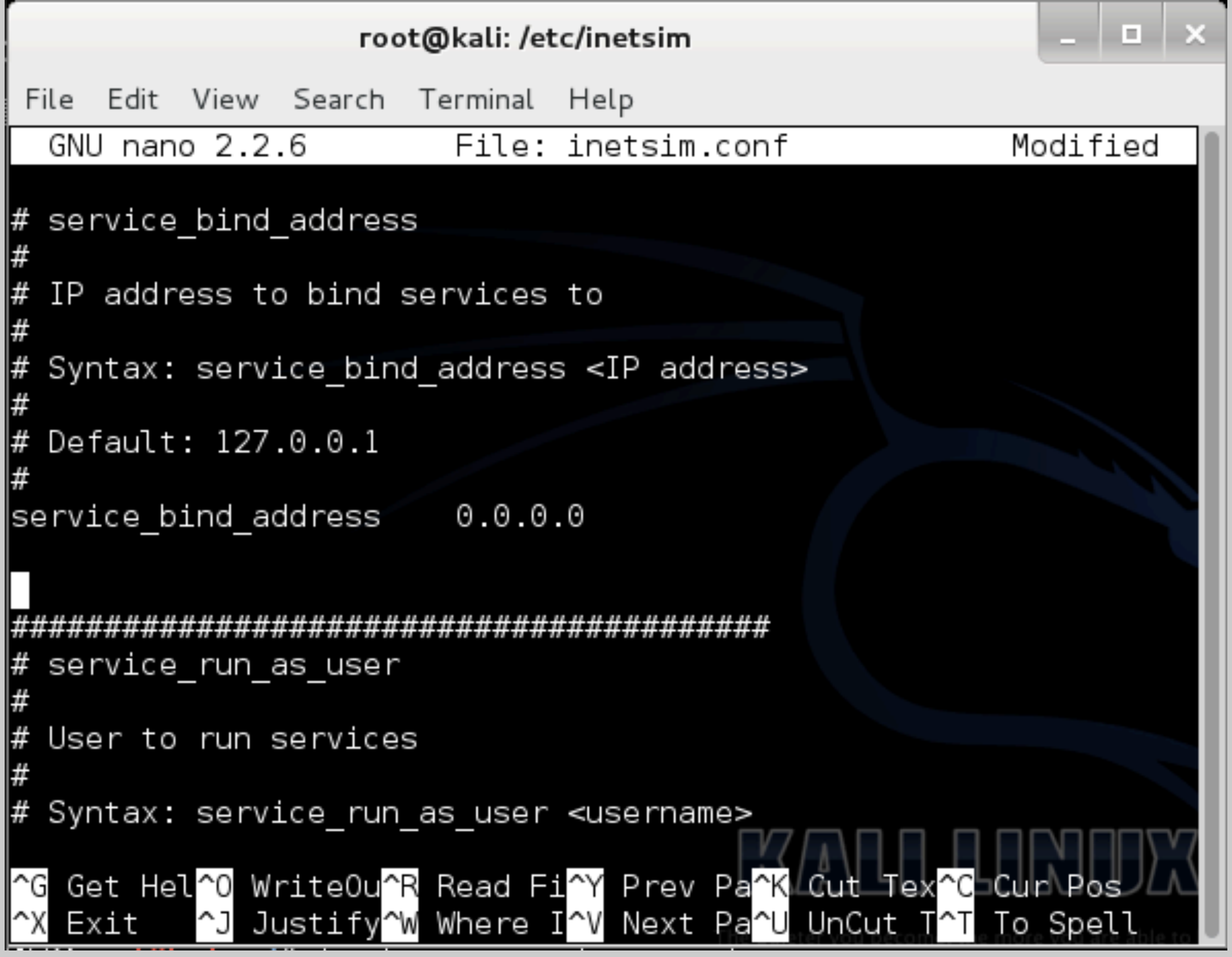
Change this line:

```
#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.



```
GNU nano 2.2.6        File: inetsim.conf                    Modified

# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address    0.0.0.0


#########################################
# service_run_as_user
#
# User to run services
#
# Syntax: service_run_as_user <username>

^G Get Hel^O WriteOu^R Read Fi^Y Prev Pa^K Cut Tex^C Cur Pos
^X Exit   ^J Justify^W Where I^V Next Pa^U UnCut T^T To Spell
```

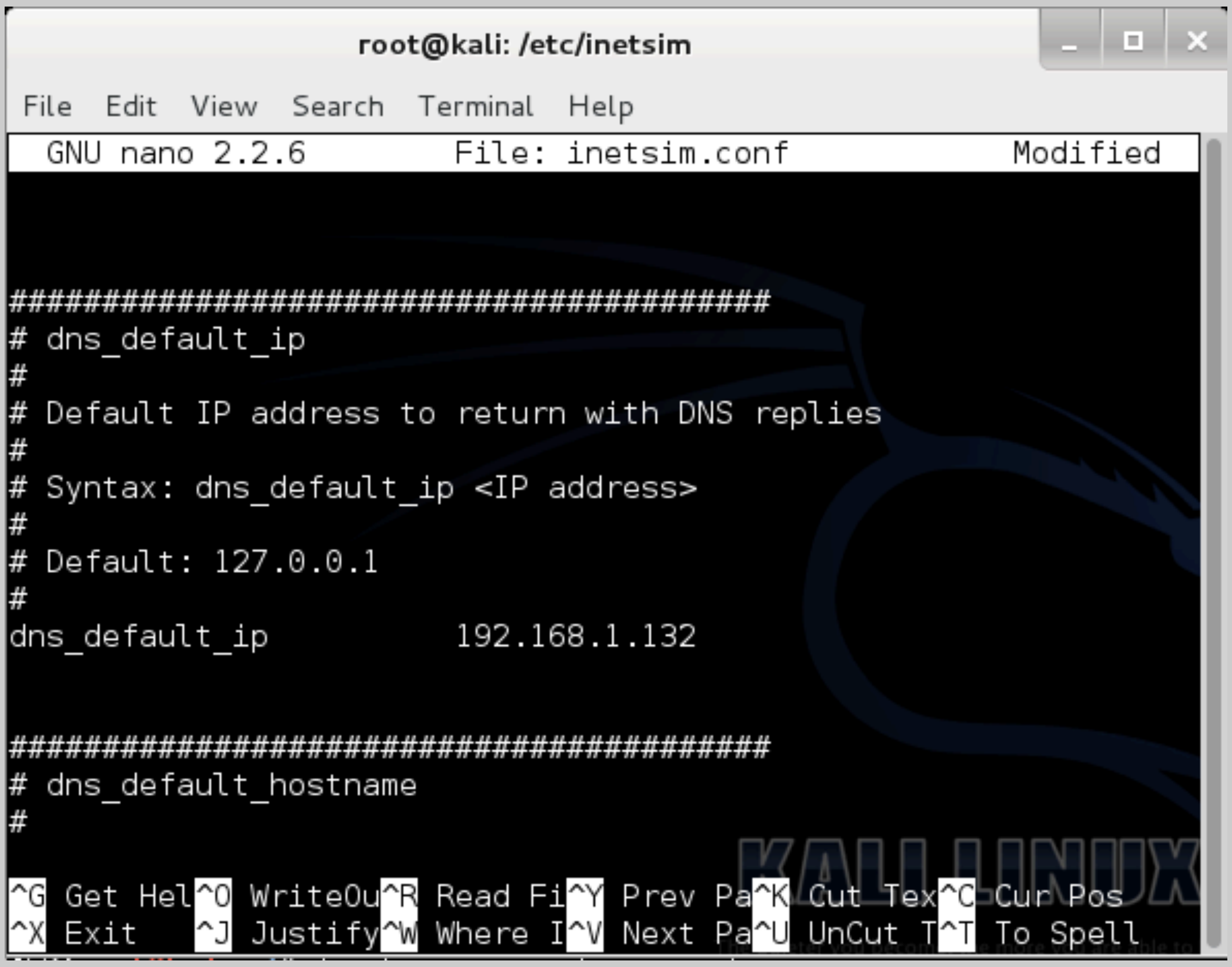
Don't forget to delete the # at the start of the line!

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 192.168.1.132
```



```
GNU nano 2.2.6        File: inetsim.conf                    Modified



#########################################
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
dns_default_ip          192.168.1.132


#########################################
# dns_default_hostname
#

^G Get Hel^O WriteOu^R Read Fi^Y Prev Pa^K Cut Tex^C Cur Pos
^X Exit   ^J Justify^W Where I^V Next Pa^U UnCut T^T To Spell
```

Use your correct IP address instead of "192.168.1.132"

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.

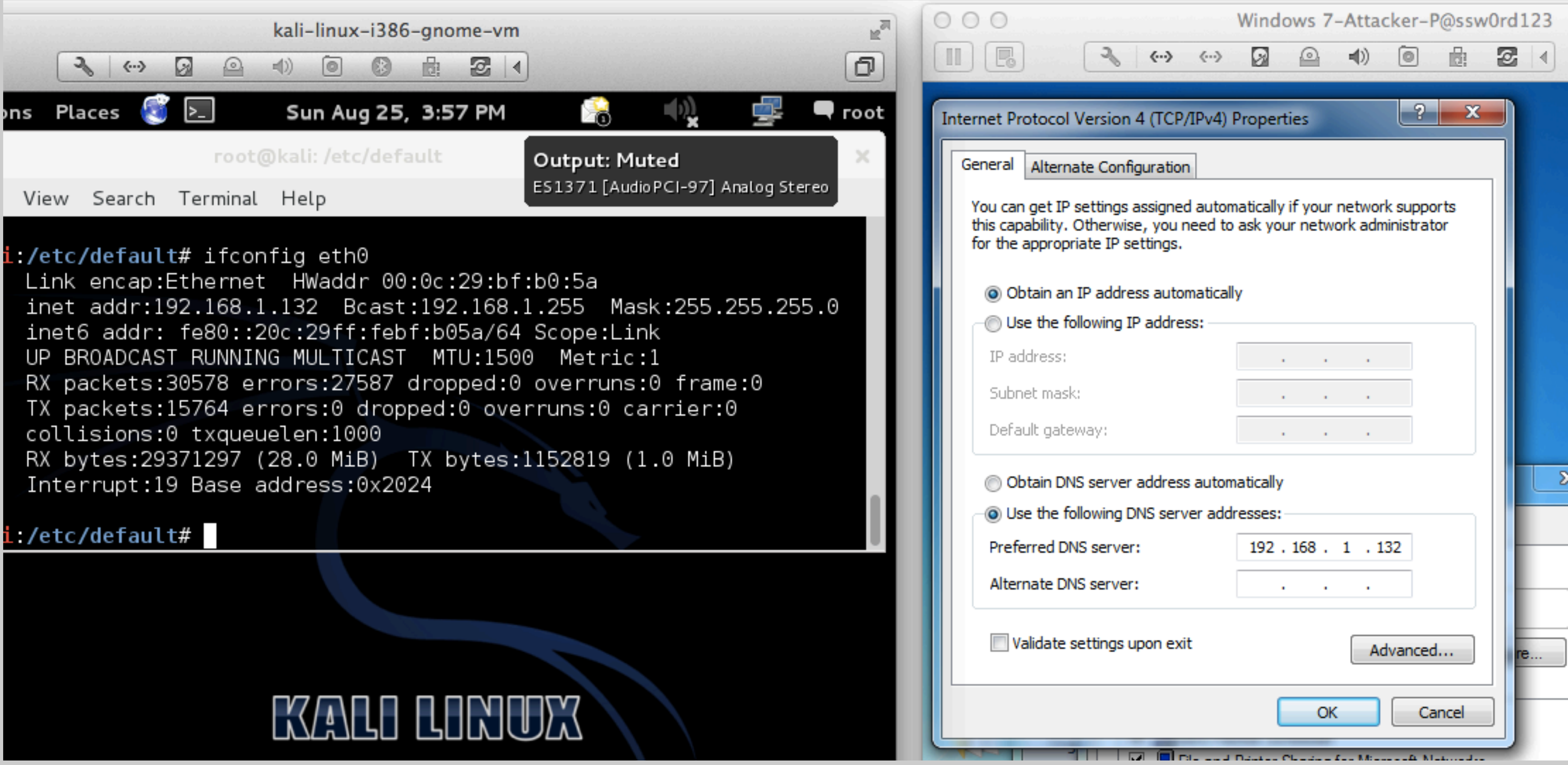
Setting the DNS Server

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.



```
i:/etc/default# ifconfig eth0
  Link encap:Ethernet  HWaddr 00:0c:29:bf:b0:5a
  inet addr:192.168.1.132  Bcast:192.168.1.255  Mask:255.255.255.0
  inet6 addr: fe80::20c:29ff:febf:b05a/64 Scope:Link
  UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
  RX packets:30578 errors:27587 dropped:0 overruns:0 frame:0
  TX packets:15764 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:29371297 (28.0 MiB)  TX bytes:1152819 (1.0 MiB)
  Interrupt:19 Base address:0x2024

i:/etc/default# 
```

Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

IP address: . . .
Subnet mask: . . .
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

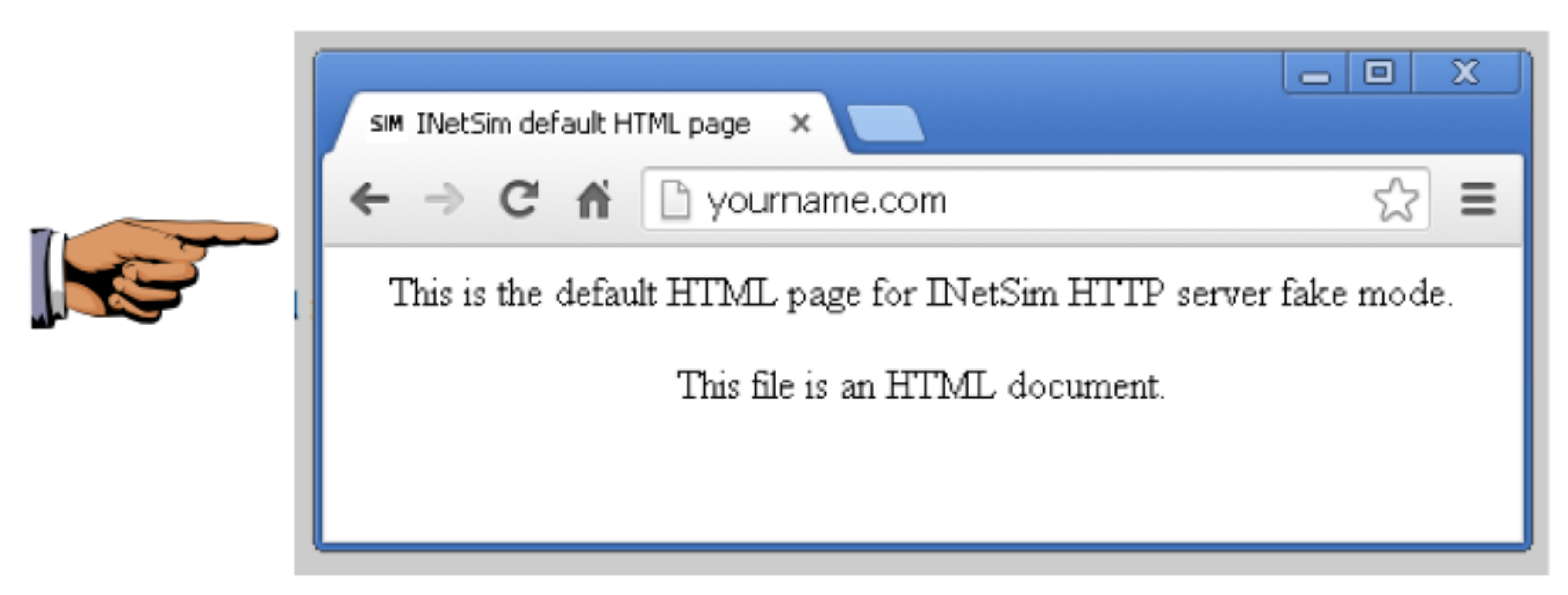
Preferred DNS server: 192 . 168 . 1 . 132
Alternate DNS server: . . .

□ Validate settings upon exit

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:



This is the default HTML page for INetSim HTTP server fake mode.

This file is an HTML document.

Saving a Screen Image

Make sure the Web browser shows these two things:

- **YOUR NAME** in the URL
- The "**INetSim HTTP server**" message

Click the taskbar at the bottom of your host Windows 10 desktop, to make the host machine listen to the keyboard, instead of the virtual machine.

Press the **PrintScrn** key in the upper-right portion of the keyboard. That will copy the whole desktop to the clipboard.

YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT!

On the host machine, not the virtual machine, click **Start**.

Type **mspaint** into the Search box and press the Enter key.

Click in the untitled - Paint window, and press **Ctrl+V** on the keyboard. The desktop appears in the Paint window.

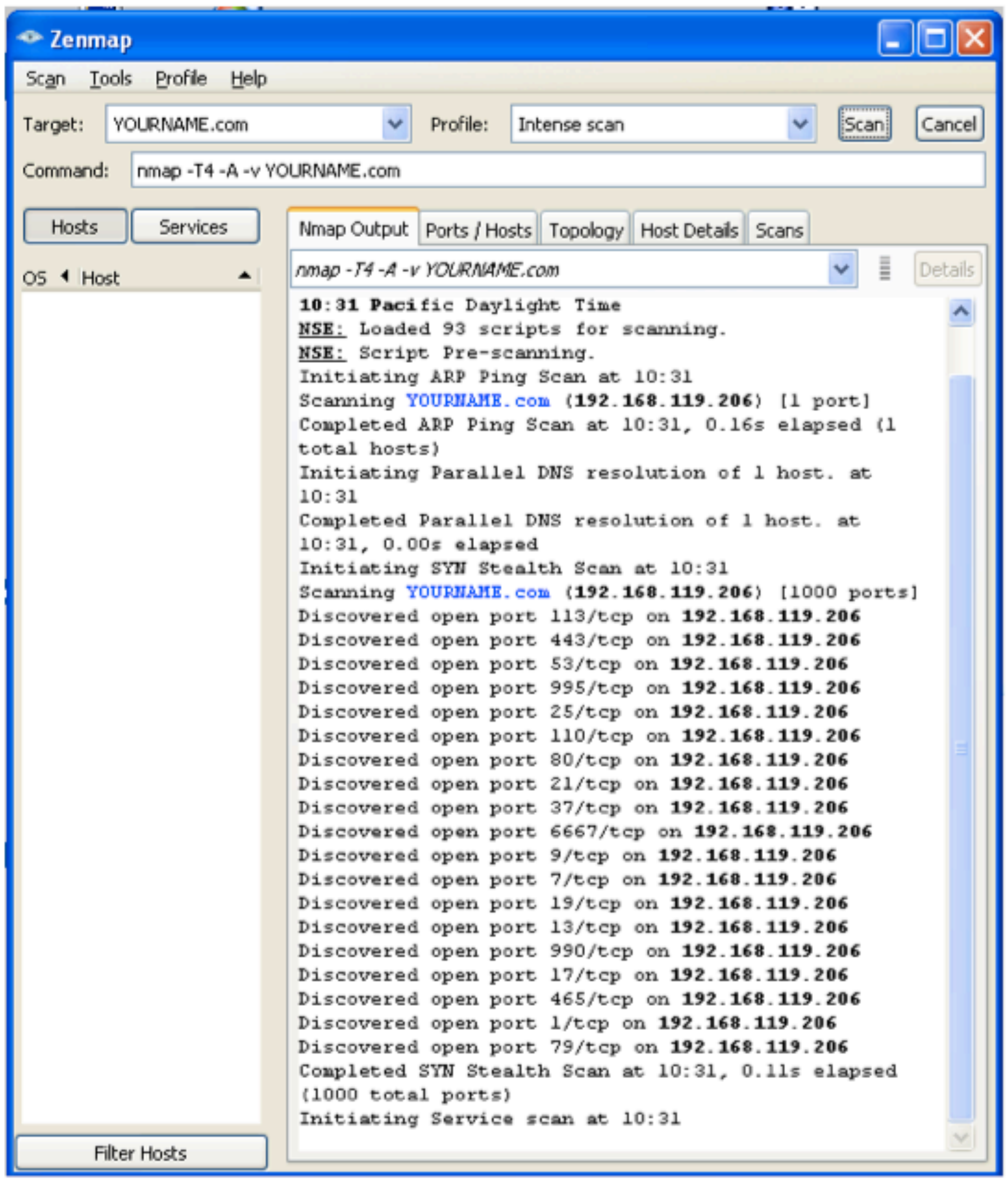
Save the document with the filename "**YOUR NAME Proj 3a**", replacing "YOUR NAME" with your real name.

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.



Target: YOURNAME.com

Profile: Intense scan

Command: nmap -T4 -A -v YOURNAME.com

```
nmap -T4 -A -v YOURNAME.com
10:31 Pacific Daylight Time
NSE: Loaded 93 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 10:31
Scanning YOURNAME.com (192.168.119.206) [1 port]
Completed ARP Ping Scan at 10:31, 0.16s elapsed (1
total hosts)
Initiating Parallel DNS resolution of 1 host. at
10:31
Completed Parallel DNS resolution of 1 host. at
10:31, 0.00s elapsed
Initiating SYN Stealth Scan at 10:31
Scanning YOURNAME.com (192.168.119.206) [1000 ports]
Discovered open port 113/tcp on 192.168.119.206
Discovered open port 443/tcp on 192.168.119.206
Discovered open port 53/tcp on 192.168.119.206
Discovered open port 995/tcp on 192.168.119.206
Discovered open port 25/tcp on 192.168.119.206
Discovered open port 110/tcp on 192.168.119.206
Discovered open port 80/tcp on 192.168.119.206
Discovered open port 21/tcp on 192.168.119.206
Discovered open port 37/tcp on 192.168.119.206
Discovered open port 6667/tcp on 192.168.119.206
Discovered open port 9/tcp on 192.168.119.206
Discovered open port 7/tcp on 192.168.119.206
Discovered open port 19/tcp on 192.168.119.206
Discovered open port 13/tcp on 192.168.119.206
Discovered open port 990/tcp on 192.168.119.206
Discovered open port 17/tcp on 192.168.119.206
Discovered open port 465/tcp on 192.168.119.206
Discovered open port 1/tcp on 192.168.119.206
Discovered open port 79/tcp on 192.168.119.206
Completed SYN Stealth Scan at 10:31, 0.11s elapsed
(1000 total ports)
Initiating Service scan at 10:31
```

Saving a Screen Image

Make sure the Nmap window shows these two things:

- A long list of open ports is visible in the Nmap window, as shown above.

  Note: If you wait too long, the scan will complete and scroll to the bottom. Drag the scroll bar back to the top to capture the image shown above.

- **YOUR NAME** in the Target field

Click the taskbar at the bottom of your host Windows 10 desktop, to make the host machine listen to the keyboard, instead of the virtual machine.

Press the **PrintScrn** key to copy the whole desktop to the clipboard.

YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT!

Paste the image into Paint.

Save the document with the filename "**YOUR NAME Proj 3b**", replacing "YOUR NAME" with your real name.

Turning in your Project

Email the images showing the secret messages to cnit.126sam@gmail.com with the subject line: **Proj 3 from YOUR NAME**

Sources

http://www.inetsim.org/packages.html

http://securitygoth.blogspot.com/

http://danielabrantes.blogspot.com/2013/05/sendemail-invalid-sslversion-specified.html

Last modified 1-30-17