LAB 1: Setting Up Environment

Purpose

We will use Kali Linux to simulate the Intenet, 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://fptuniversity-my.sharepoint.com/:f:/g/personal/dinhmh_fpt_edu_vn/Es7sIL1BYNVMpjfwJUi7k2wB5y_E_pMkqoUGYmng5rCJxA?e=8hmDJh)

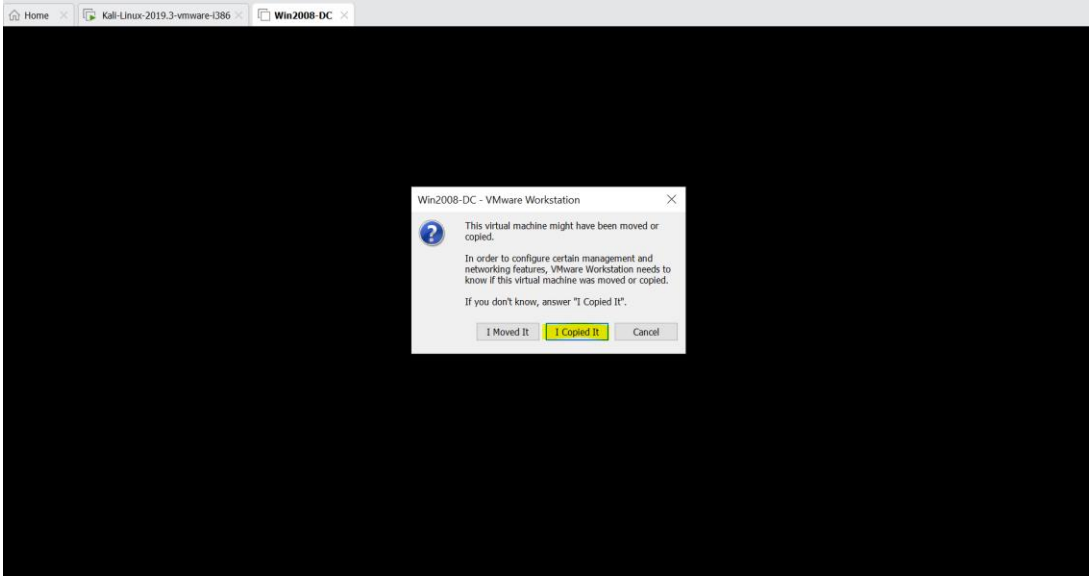
The two files you need are:

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

Extracting the Virtual Machine

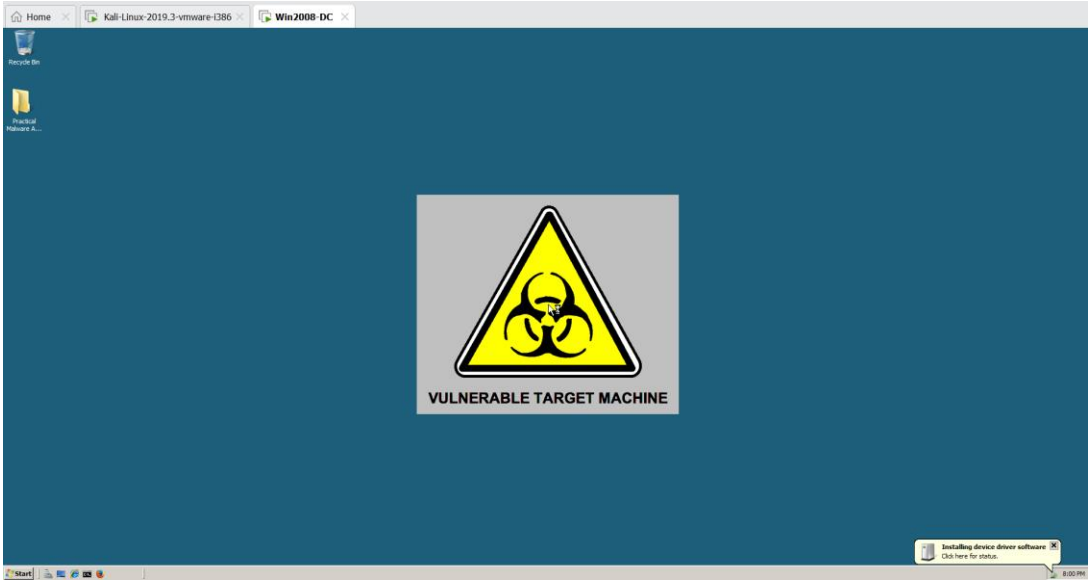
Right-click the **Win2008-Target.7z, kali-linux-2019.3-vmware-i386.7z** file, click **7-Zip**, and click "**Extract Files...**". In the "Extract to:" box, enter the path to the folder you prepared,

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.

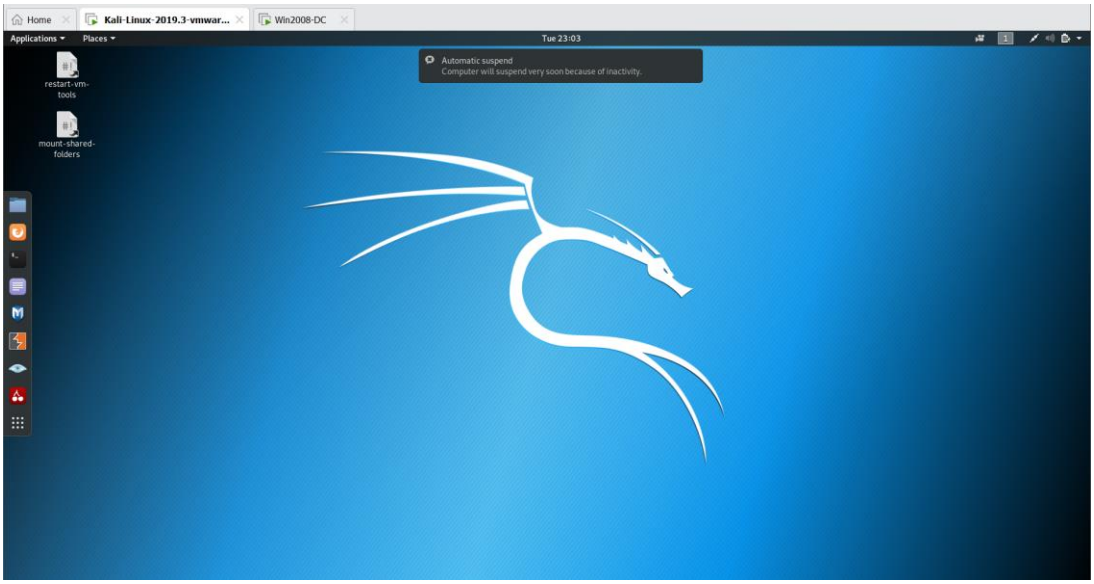
Log in as **Administrator** with a password of **P@ssw0rd**
When the server starts, it opens some windows by default. Close all windows.
You should see the Windows Server 2008 desktop as shown below:



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

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# dhclient
root@kali:~# dhclient -v
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/00:0c:29:09:a6:15
Sending on   LPF/eth0/00:0c:29:09:a6:15
Sending on   Socket/fallback
DHCPREQUEST for 192.168.70.133 on eth0 to 255.255.255.255 port 67
DHCPACK of 192.168.70.133 from 192.168.70.254
RTNETLINK answers: File exists
bound to 192.168.70.133 -- renewal in 832 seconds.
root@kali:~#
```

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

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
DHCPACK of 192.168.70.133 from 192.168.70.254
RTNETLINK answers: File exists
bound to 192.168.70.133 -- renewal in 832 seconds.
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.70.138  netmask 255.255.255.0  broadcast 192.168.70.255
        inet6 fe80::20c:29ff:fe09:a615  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:09:a6:15  txqueuelen 1000  (Ethernet)
        RX packets 268  bytes 113993 (111.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 195  bytes 17514 (17.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 46  bytes 2750 (2.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 46  bytes 2750 (2.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

Checking for a Web server

On your Linux machine, in a Terminal window, execute this command:
lsof -i :80

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# lsof -i :80
root@kali:~#
```

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: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# lsof -i :80
root@kali:~# service apache2 start
root@kali:~# lsof -i :80
COMMAND  PID     USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
apache2 2744     root    4u  IPv6  38723      0t0  TCP *:http (LISTEN)
apache2 2745 www-data    4u  IPv6  38723      0t0  TCP *:http (LISTEN)
apache2 2746 www-data    4u  IPv6  38723      0t0  TCP *:http (LISTEN)
apache2 2747 www-data    4u  IPv6  38723      0t0  TCP *:http (LISTEN)
apache2 2748 www-data    4u  IPv6  38723      0t0  TCP *:http (LISTEN)
apache2 2749 www-data    4u  IPv6  38723      0t0  TCP *:http (LISTEN)
apache2 2750 www-data    4u  IPv6  38723      0t0  TCP *:http (LISTEN)
root@kali:~#
```

service apache2 stop

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# lsof -i :80
root@kali:~# service apache2 start
root@kali:~# lsof -i :80
COMMAND  PID     USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
apache2 2744     root    4u  IPv6  38723      0t0  TCP *:http (LISTEN)
apache2 2745 www-data    4u  IPv6  38723      0t0  TCP *:http (LISTEN)
apache2 2746 www-data    4u  IPv6  38723      0t0  TCP *:http (LISTEN)
apache2 2747 www-data    4u  IPv6  38723      0t0  TCP *:http (LISTEN)
apache2 2748 www-data    4u  IPv6  38723      0t0  TCP *:http (LISTEN)
apache2 2749 www-data    4u  IPv6  38723      0t0  TCP *:http (LISTEN)
apache2 2750 www-data    4u  IPv6  38723      0t0  TCP *:http (LISTEN)
root@kali:~# service apache2 stop
root@kali:~# lsof -i :80
root@kali:~#
```

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

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
  GNU nano 4.3                /etc/inetsim/inetsim.conf
start_service chargen_udp
start_service dummy_tcp
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

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line
```

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.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
  GNU nano 4.3                /etc/inetsim/inetsim.conf                Modified
start_service chargen_udp
start_service dummy_tcp
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    0.0.0.0


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

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line
```

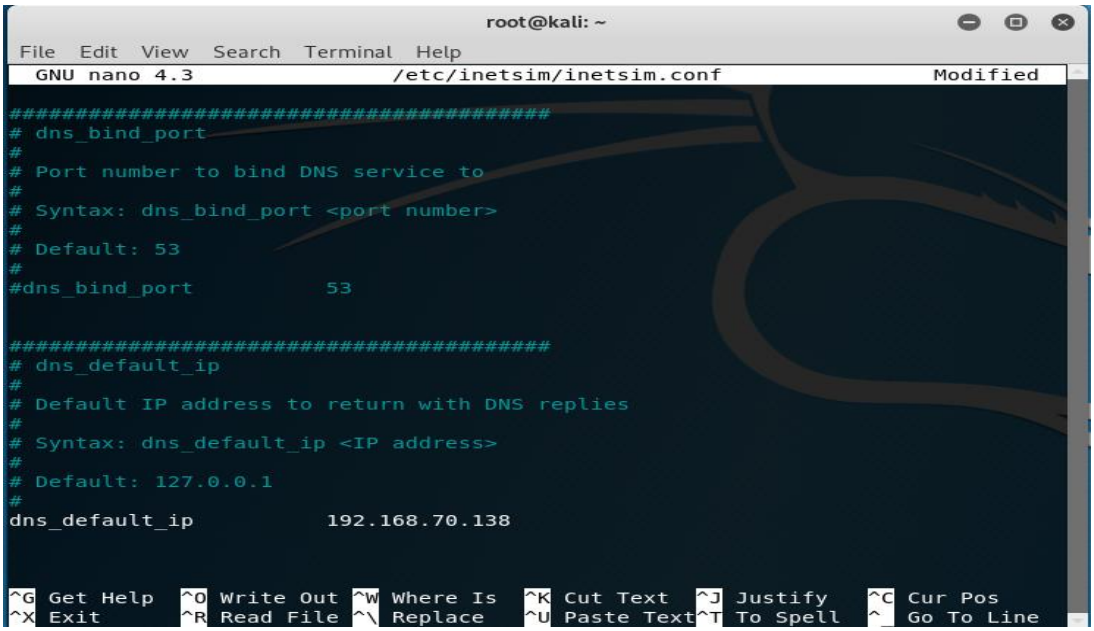
Don't forget to delete the # at the start of the line!

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

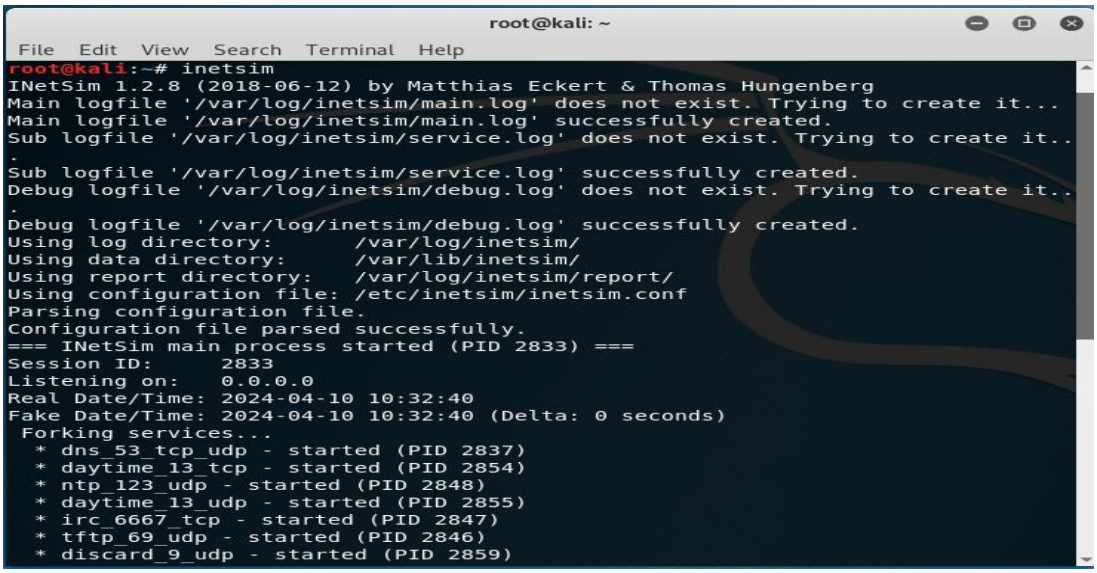


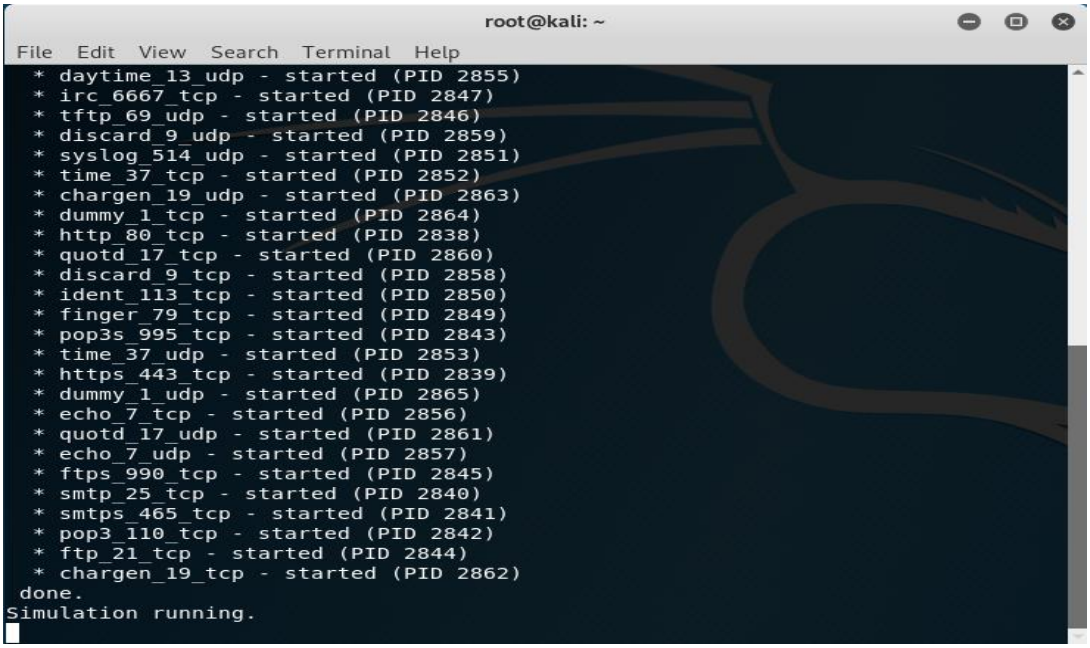
Use your correct IP address instead of "192.168.70.138"

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.

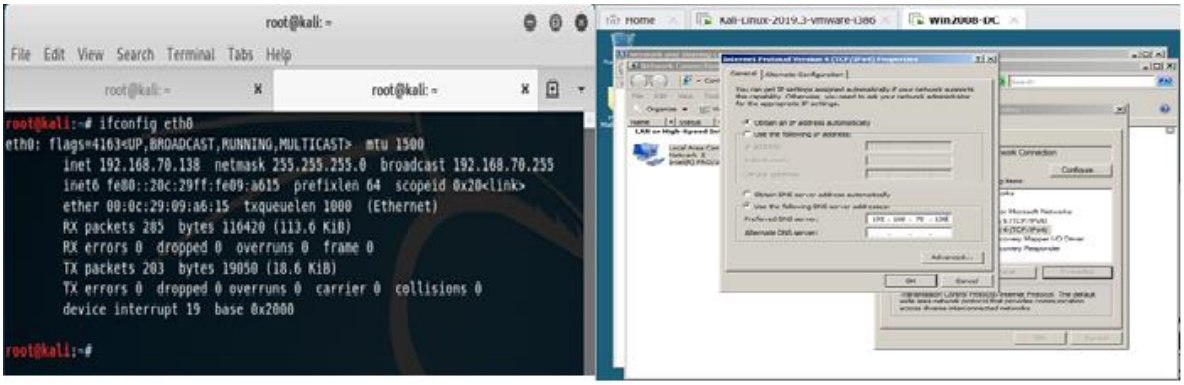
Installing Nmap

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.

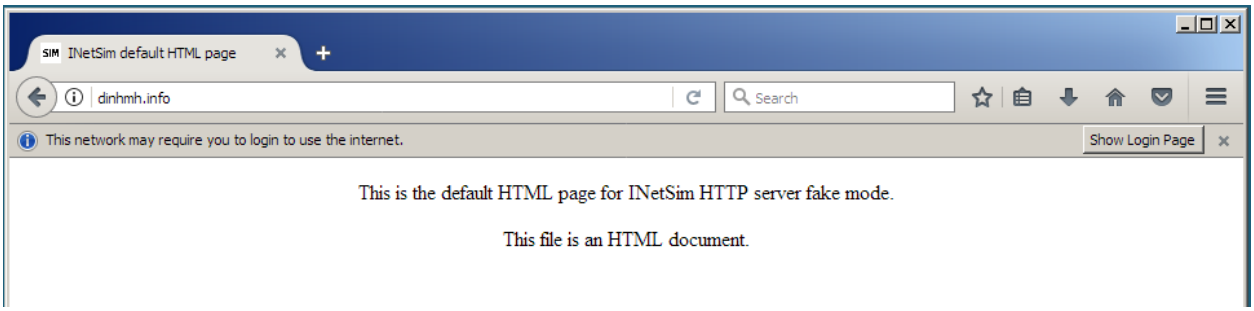
Setting the DNS Server

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.



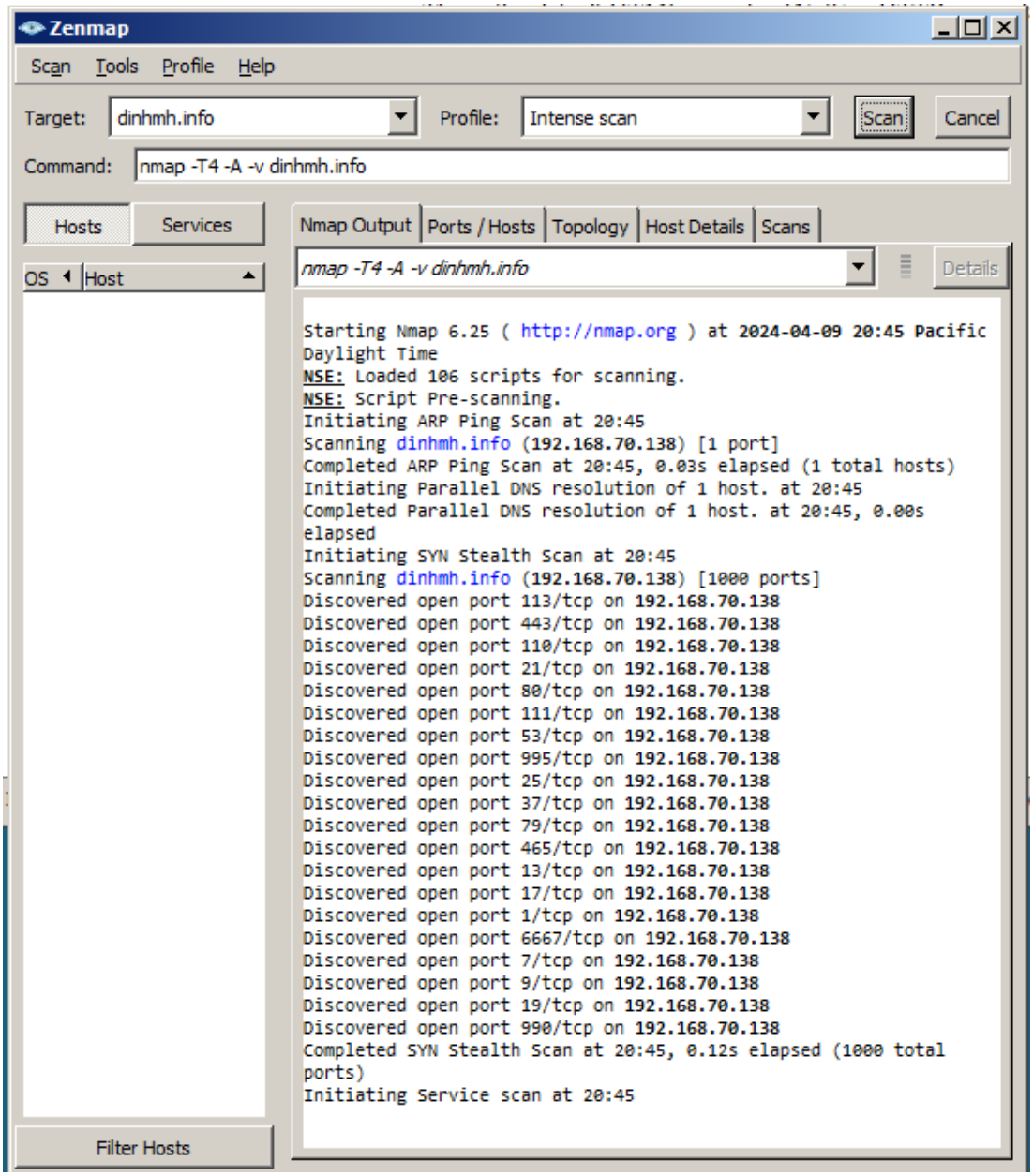
Viewing an HTTP Web Page

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.


Zenmap
Scan Tools Profile Help
Target: dinhmh.info
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v dinhmh.info
Hosts
Services
OS
Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v dinhmh.info
Details
Starting Nmap 6.25 (http://nmap.org) at 2024-04-09 20:45 Pacific Daylight Time
NSE: Loaded 106 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 20:45
Scanning dinhmh.info (192.168.70.138) [1 port]
Completed ARP Ping Scan at 20:45, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:45
Completed Parallel DNS resolution of 1 host. at 20:45, 0.00s elapsed
Initiating SYN Stealth Scan at 20:45
Scanning dinhmh.info (192.168.70.138) [1000 ports]
Discovered open port 113/tcp on 192.168.70.138
Discovered open port 443/tcp on 192.168.70.138
Discovered open port 110/tcp on 192.168.70.138
Discovered open port 21/tcp on 192.168.70.138
Discovered open port 80/tcp on 192.168.70.138
Discovered open port 111/tcp on 192.168.70.138
Discovered open port 53/tcp on 192.168.70.138
Discovered open port 995/tcp on 192.168.70.138
Discovered open port 25/tcp on 192.168.70.138
Discovered open port 37/tcp on 192.168.70.138
Discovered open port 79/tcp on 192.168.70.138
Discovered open port 465/tcp on 192.168.70.138
Discovered open port 13/tcp on 192.168.70.138
Discovered open port 17/tcp on 192.168.70.138
Discovered open port 1/tcp on 192.168.70.138
Discovered open port 6667/tcp on 192.168.70.138
Discovered open port 7/tcp on 192.168.70.138
Discovered open port 9/tcp on 192.168.70.138
Discovered open port 19/tcp on 192.168.70.138
Discovered open port 990/tcp on 192.168.70.138
Completed SYN Stealth Scan at 20:45, 0.12s elapsed (1000 total ports)
Initiating Service scan at 20:45
Filter Hosts