****

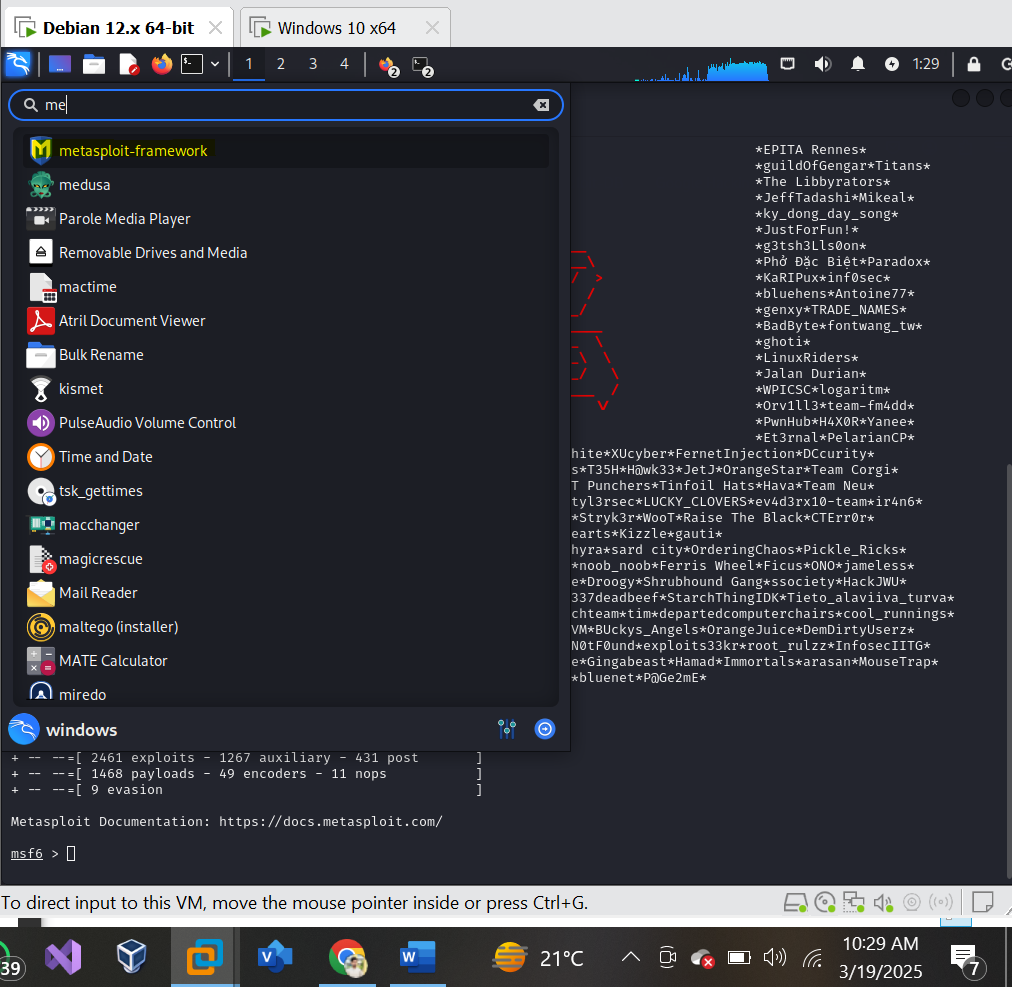
|  |
| --- |
| *BS Cyber Security Department AU* |

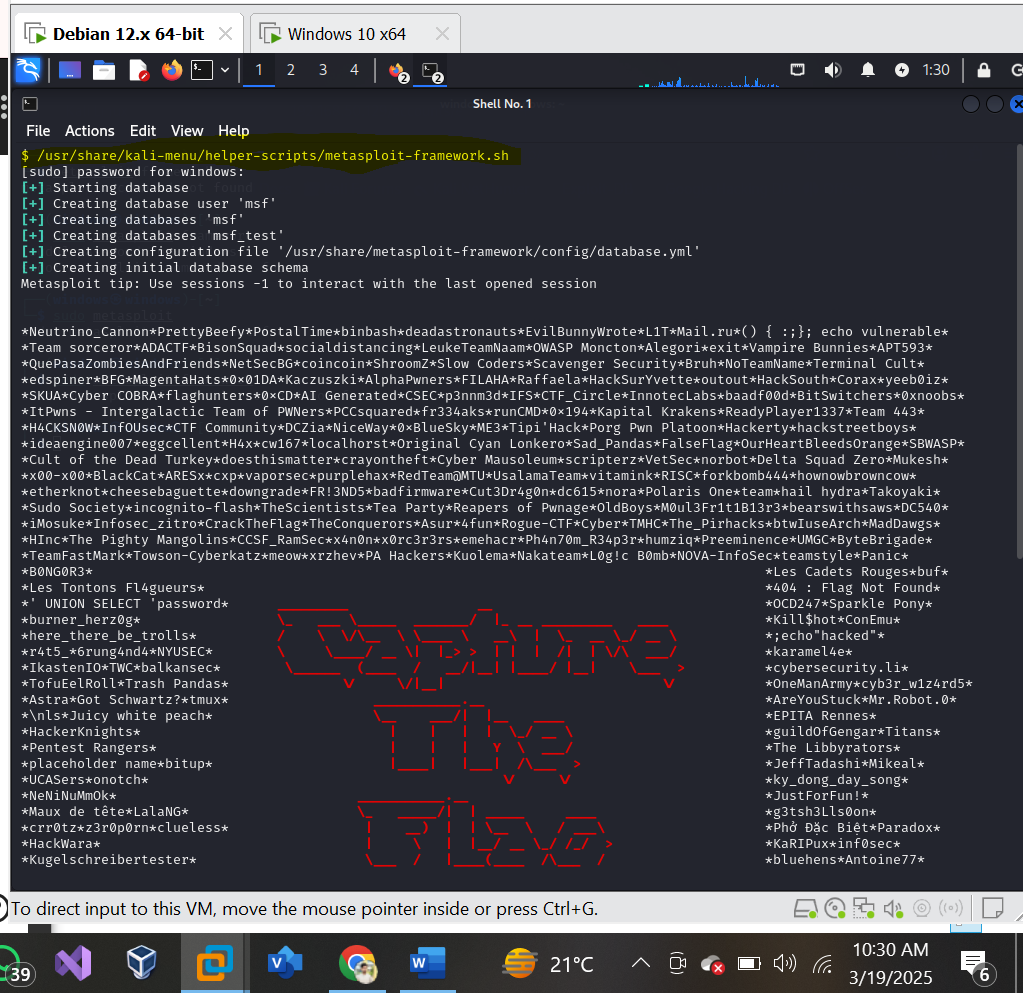
|  |  |
| --- | --- |
| **Registration ID** | **233026** |
| **Submitted By** | **Muhammad Sohaib Rafiq** |
| **Submitted To** | **Iram Fatima Hashmi** |
| **Date of Submission** | **12/02/2024** |
| **Lab NO.** | **5** |
| **Subject** | **NS LAB** |

**LAB: REMOTE HACKING OF WINDOWS VIA METASPLOIT**

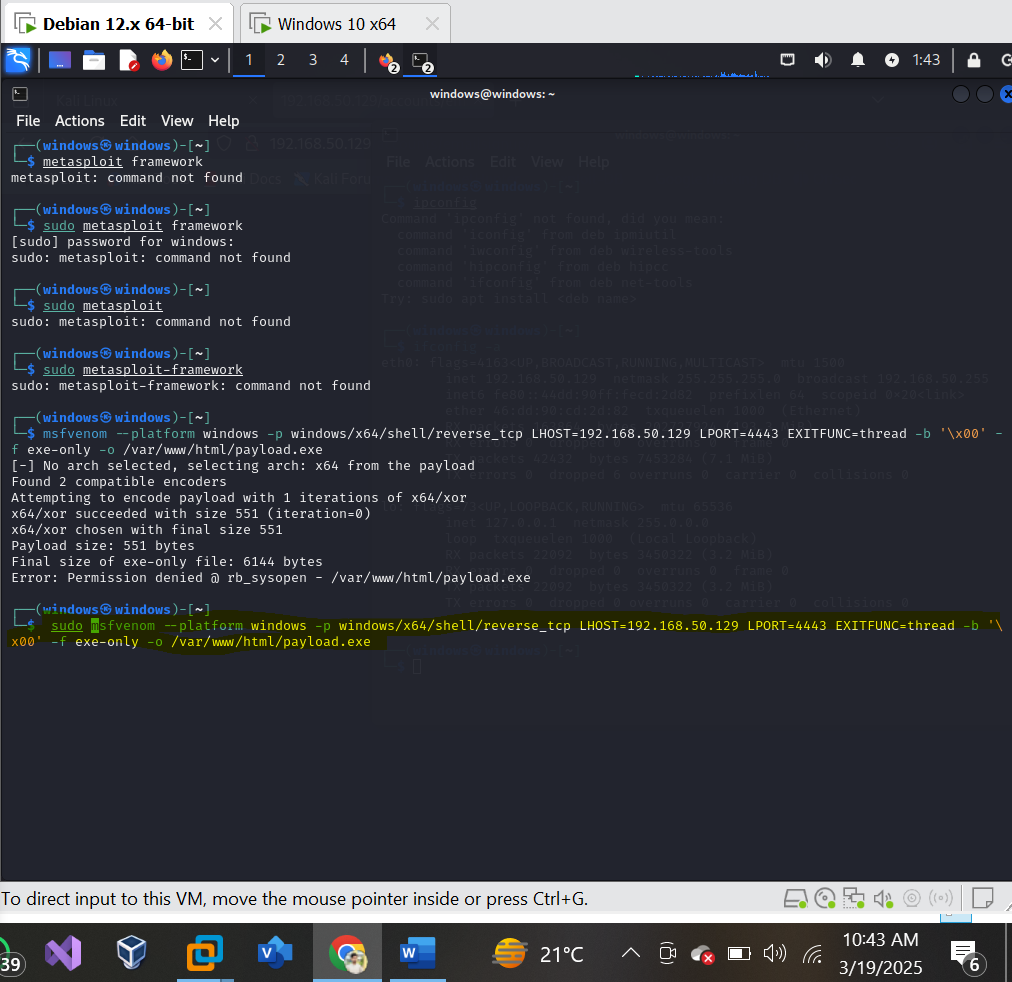
***1. Create Malicious Exe:***

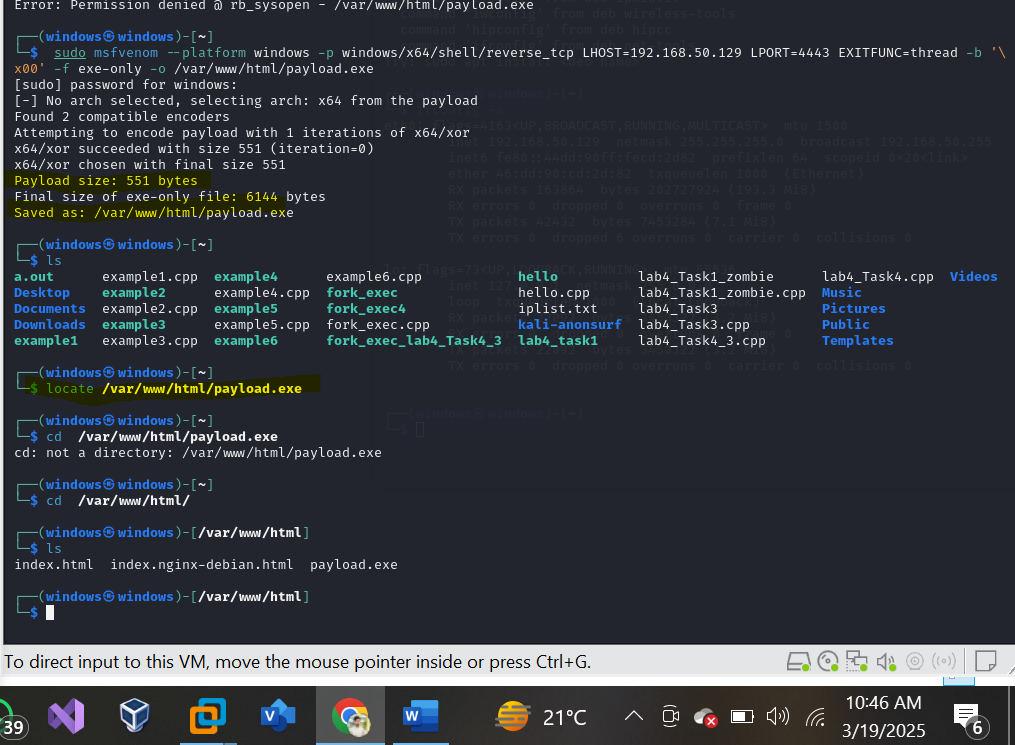
Starting the Metasploit-framework:





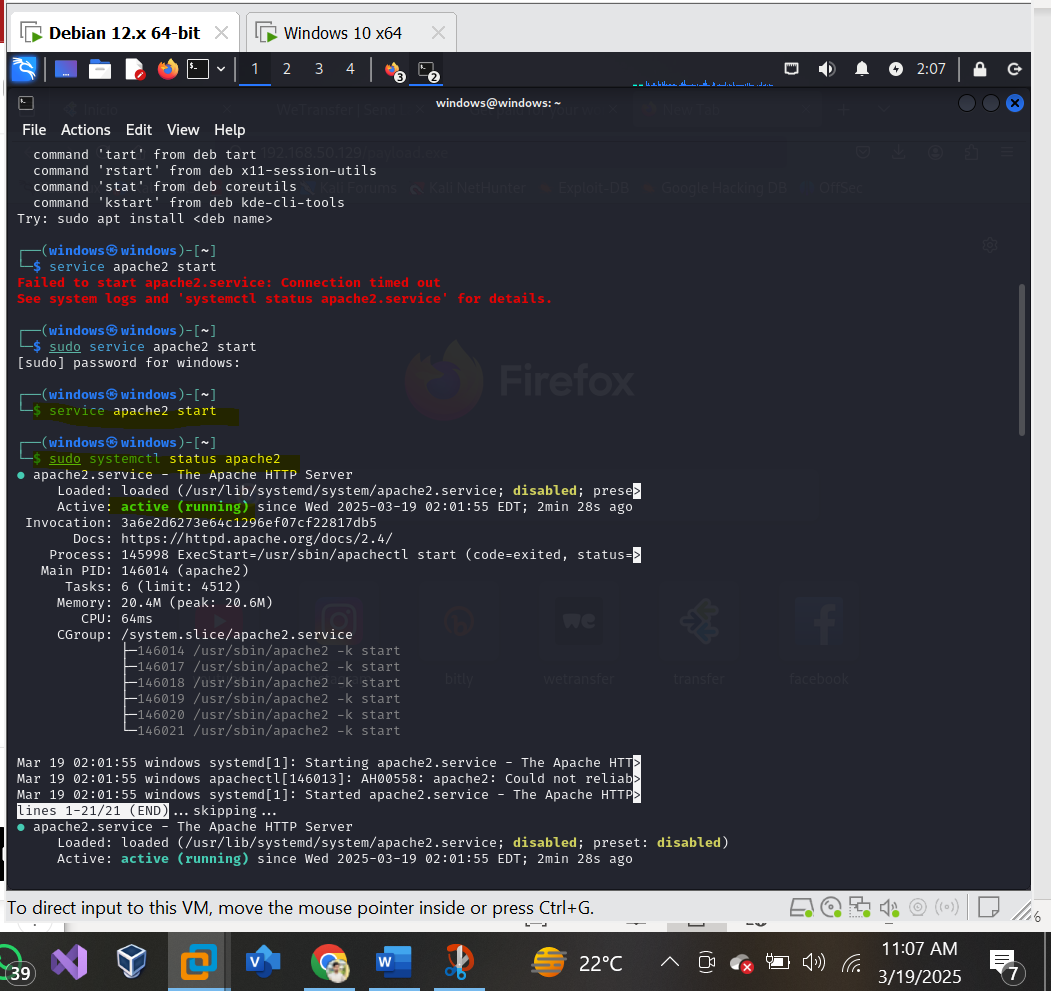
Creating the payload with this command: that contains a reverse\_tcp\_meterpreter Shell:

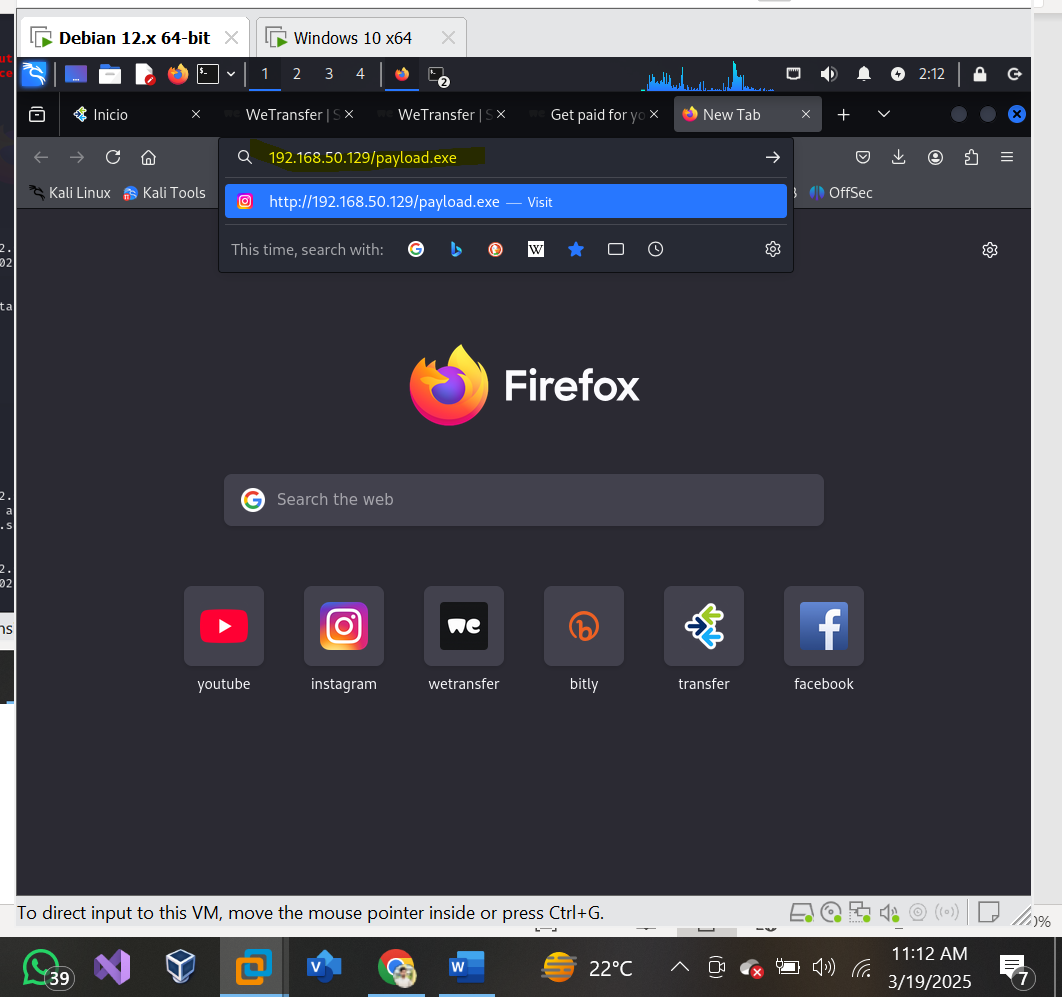




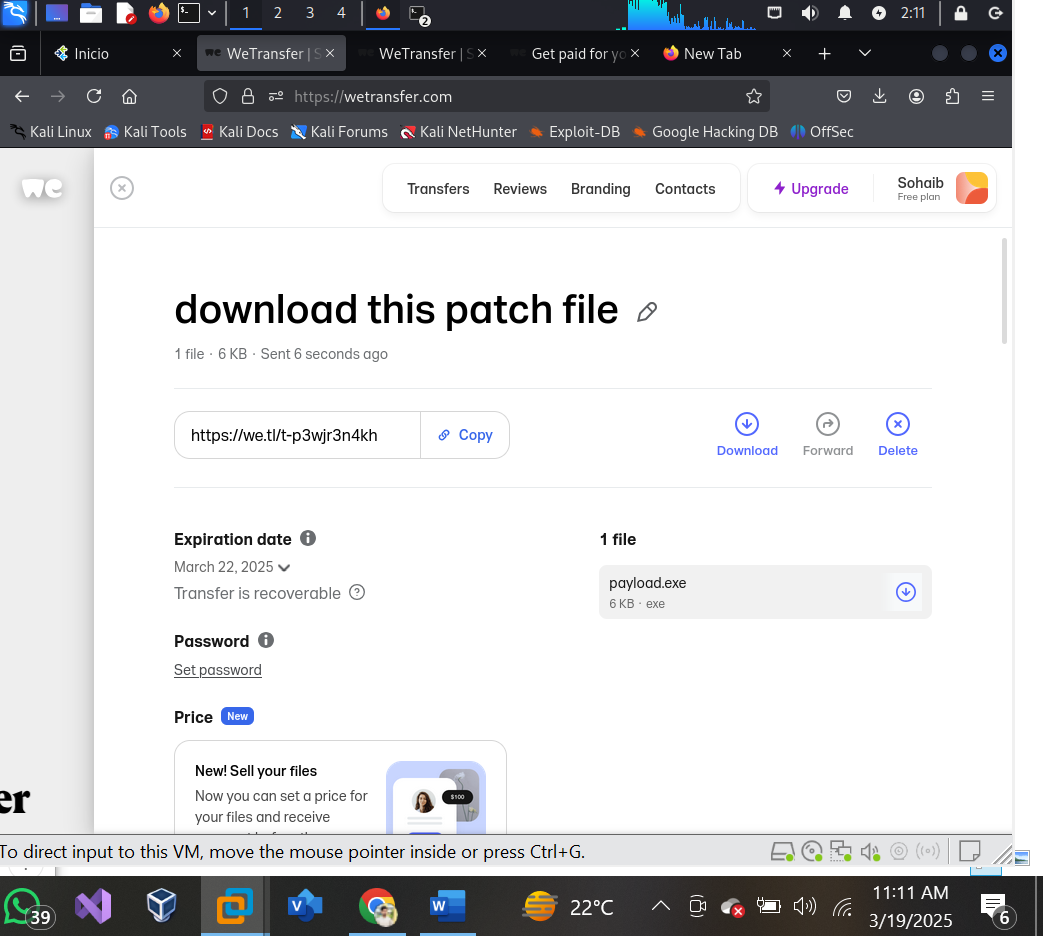
**2. Send the exe to victim:**

**Method:**

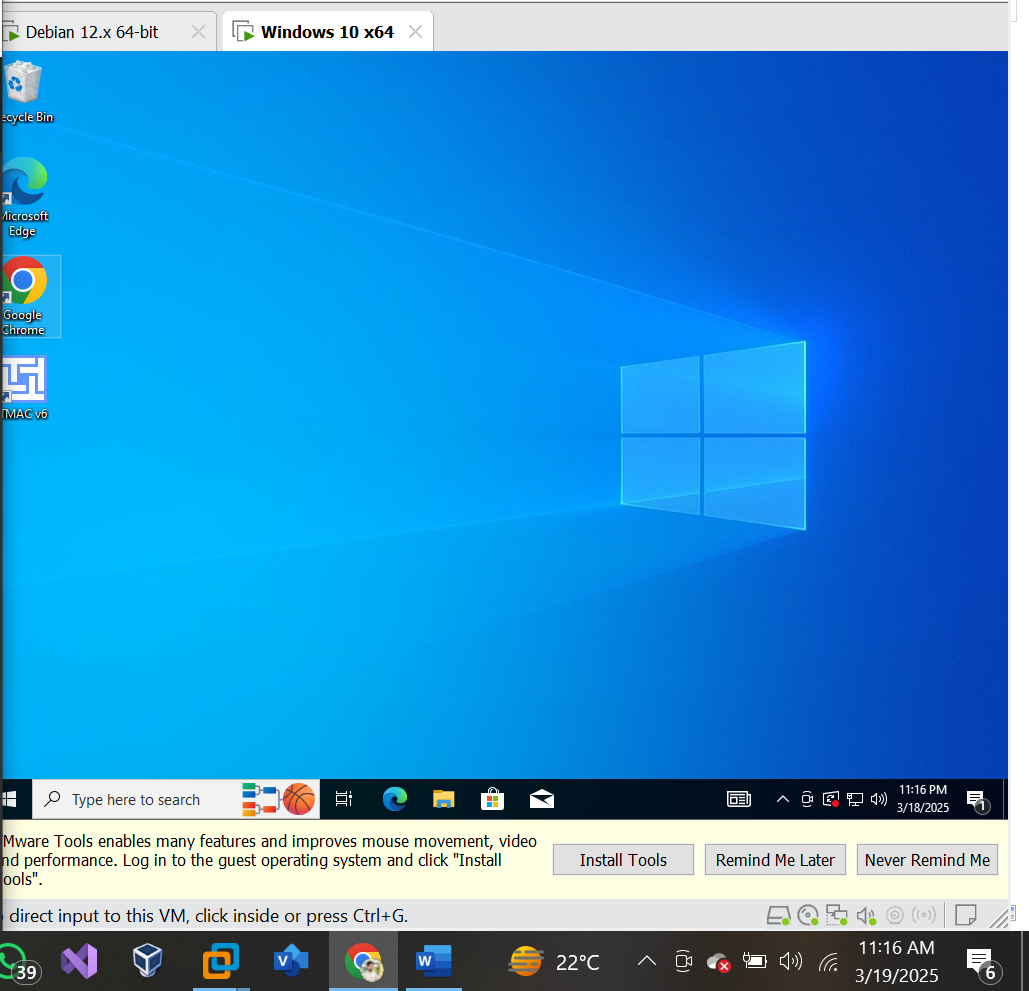
****

****

**Method1:**

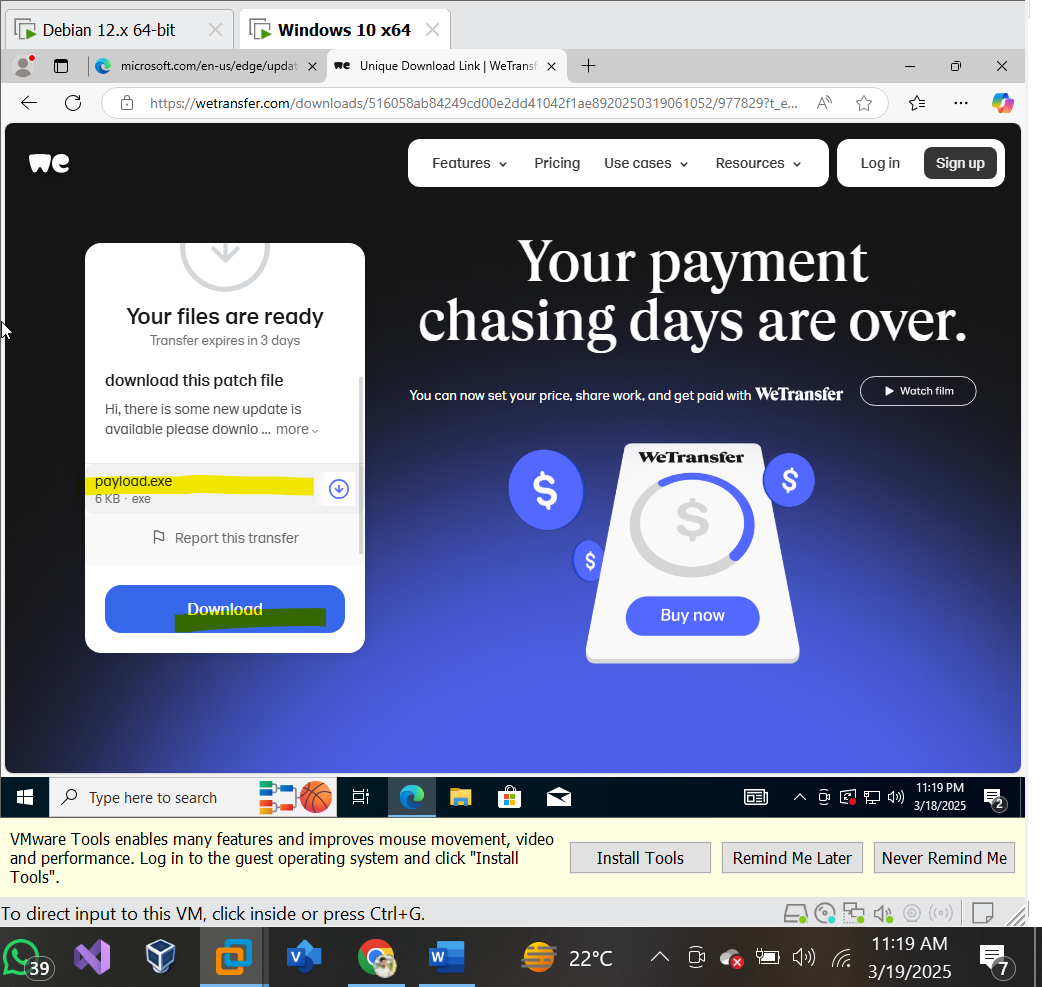
****

**Sending it to the victim machine:**



Disabling the anti-virus:

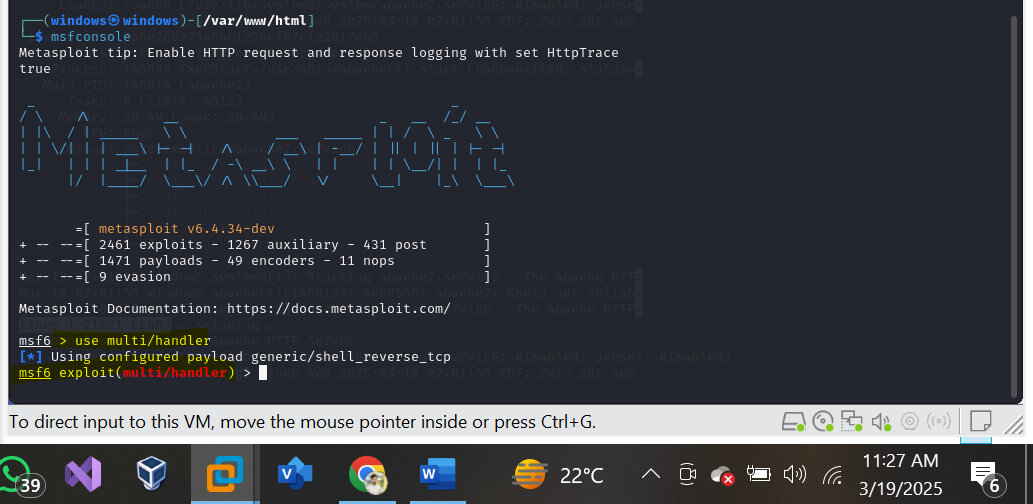
Transferring the payload.exe to the victim machine:

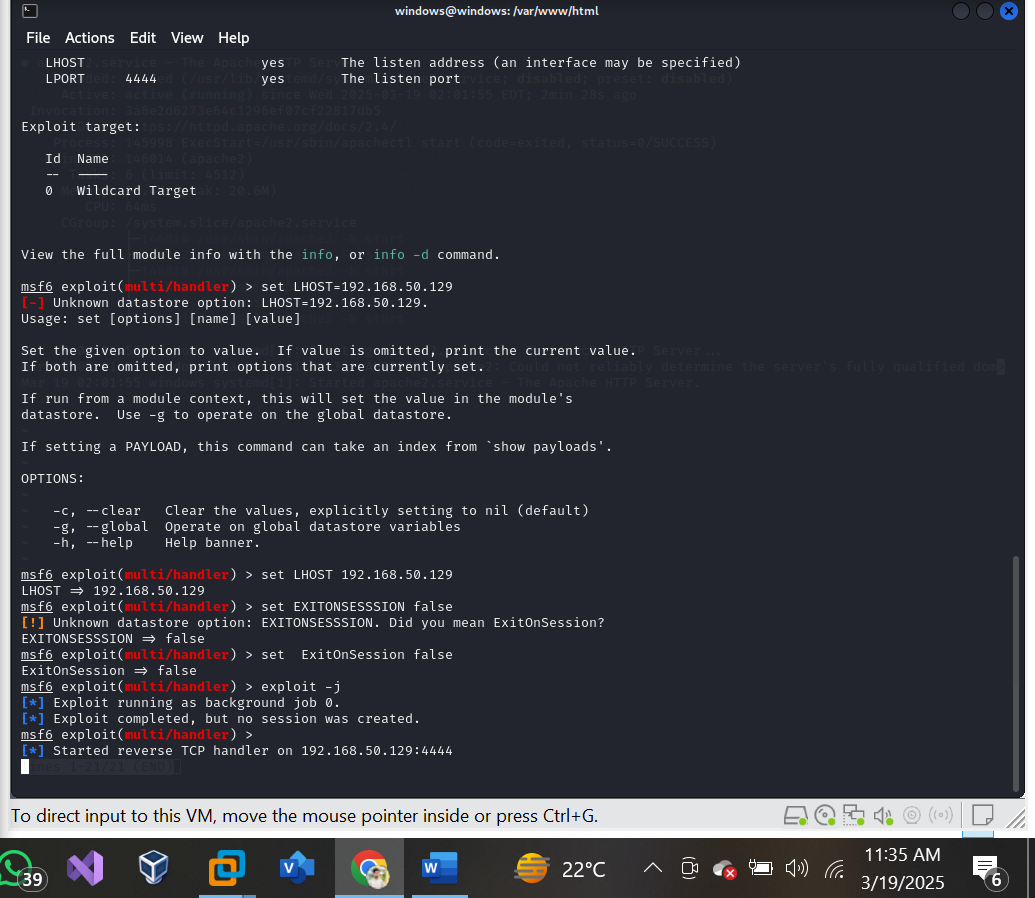




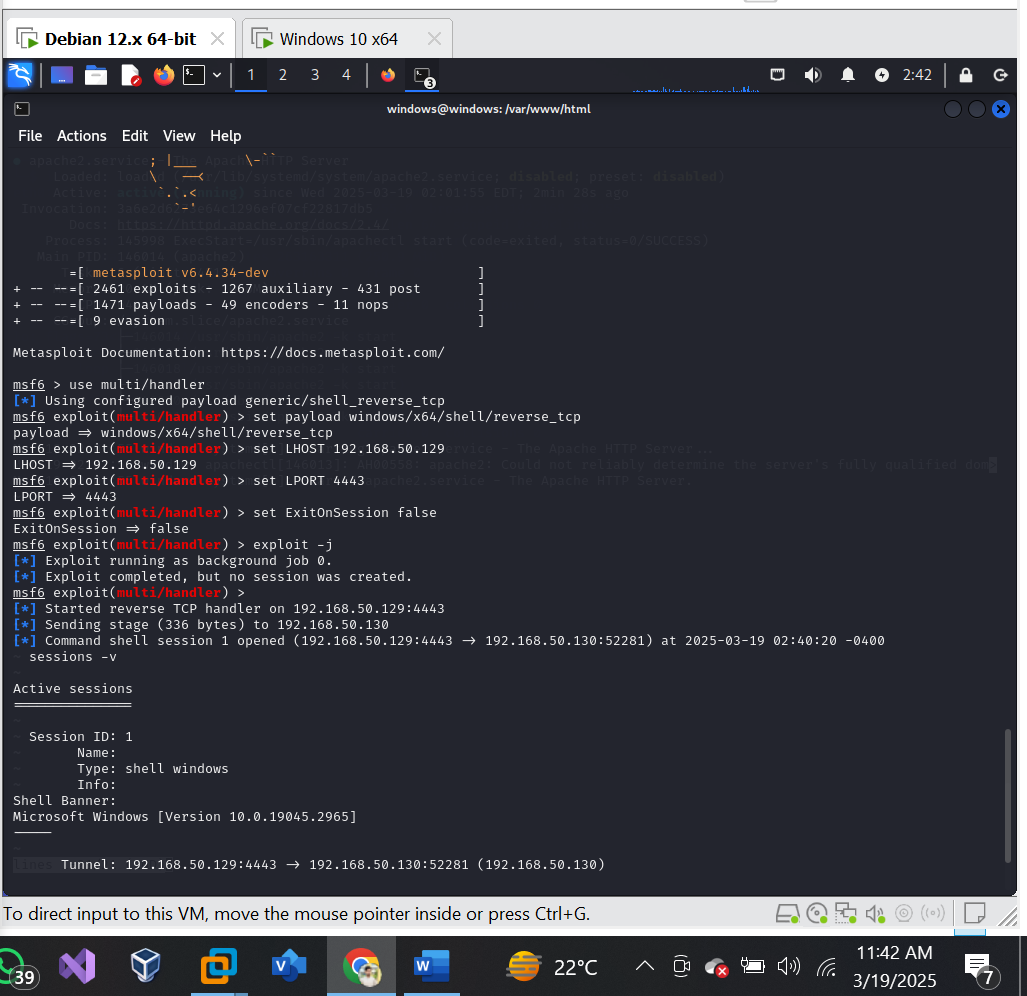
The payload file is successfully transferred to the victim successfully.

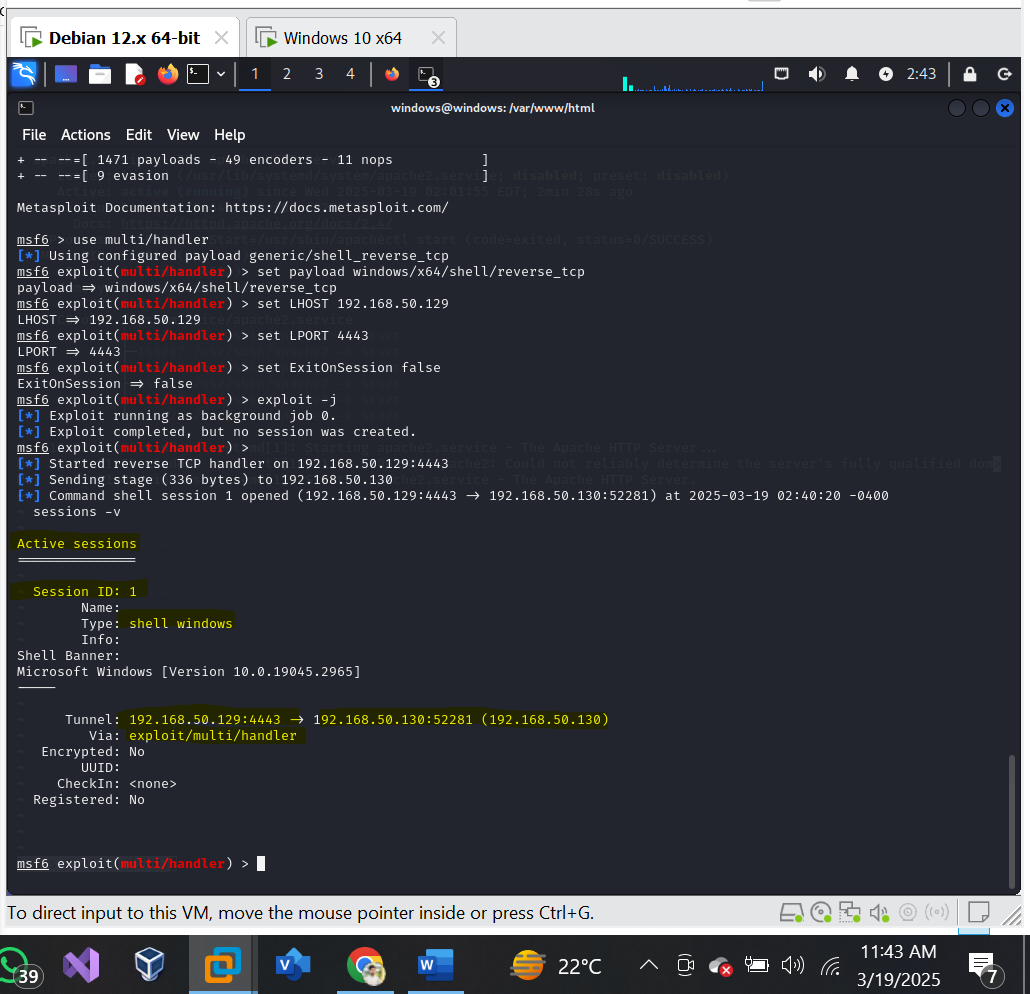
**3. Turning on listener:**

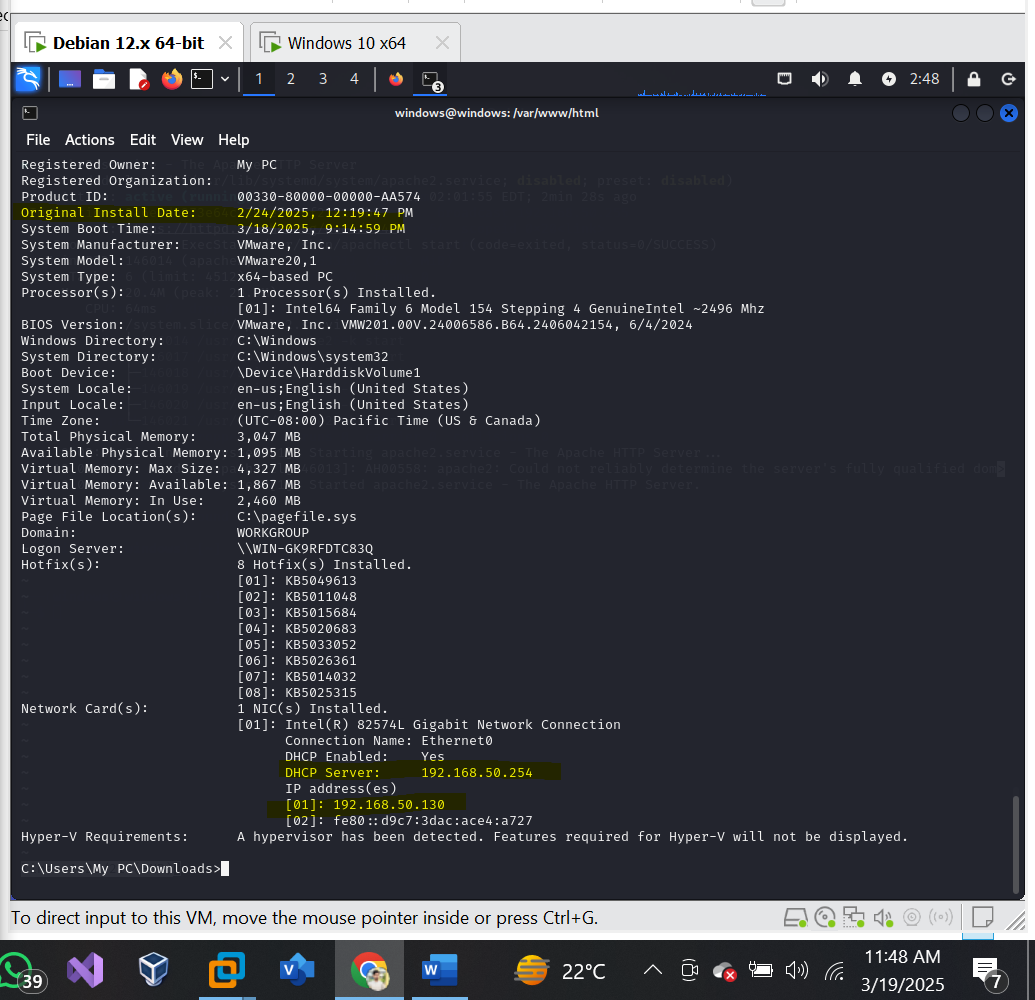
****

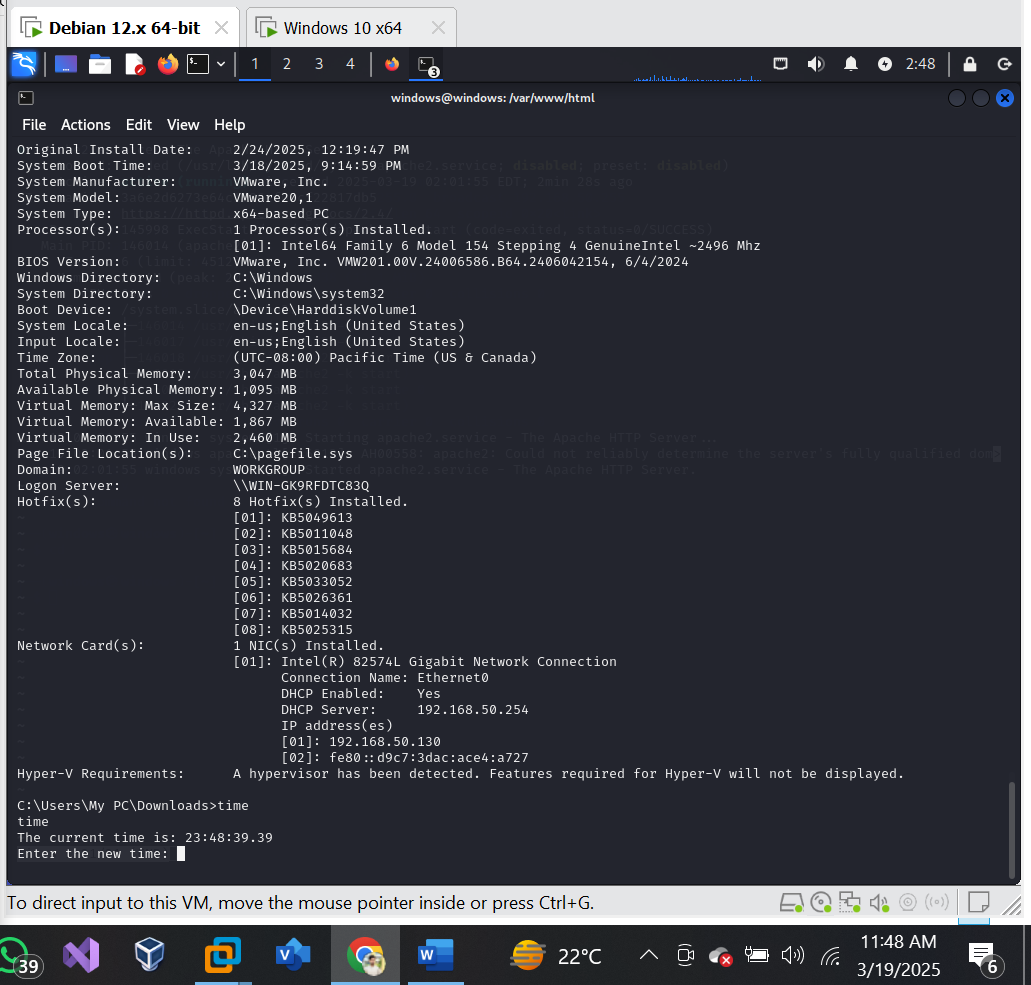
****

**4. Exploitation:**

****

****

****

****