****

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

|  |  |
| --- | --- |
| **Registration ID** | **233026** |
| **Submitted By** | **Muhammad Sohaib Rafiq** |
| **Submitted To** | **Iram Fatima Hashmi** |
| **Date of Submission** | **07/02/2025** |
| **Lab NO.** | **1** |
| **Subject** | **NS LAB** |

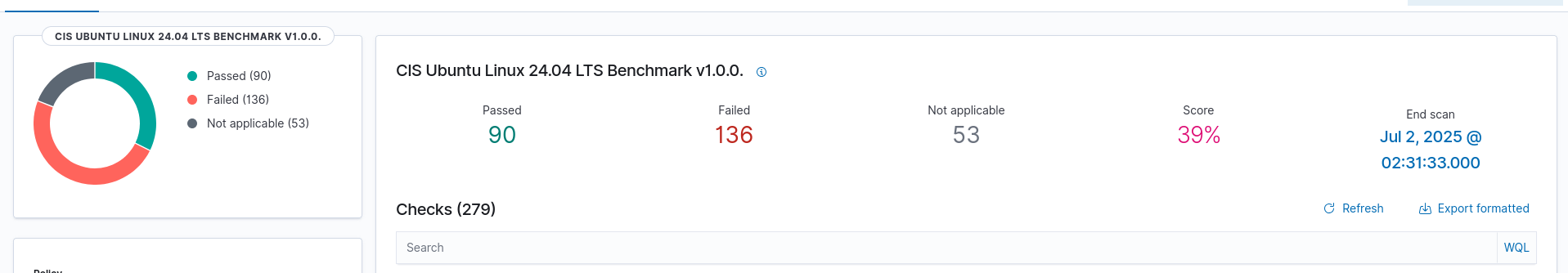
**c) A non-privileged user accessed /etc/shadow and initiated SSH to another**

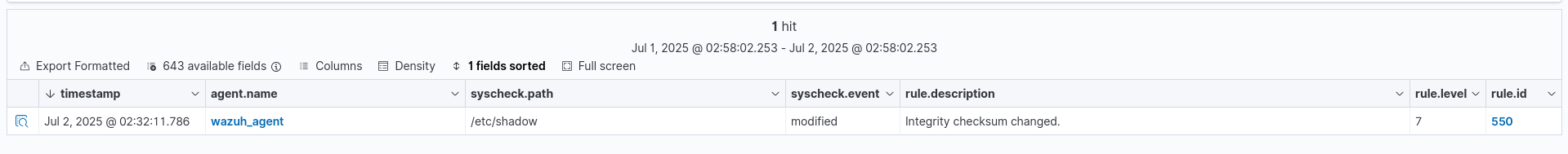
**internal server. You must configure Wazuh to detect such behavior and**

**generate alerts. Submit screenshots of test events you generated and**

**show correlated alerts.**

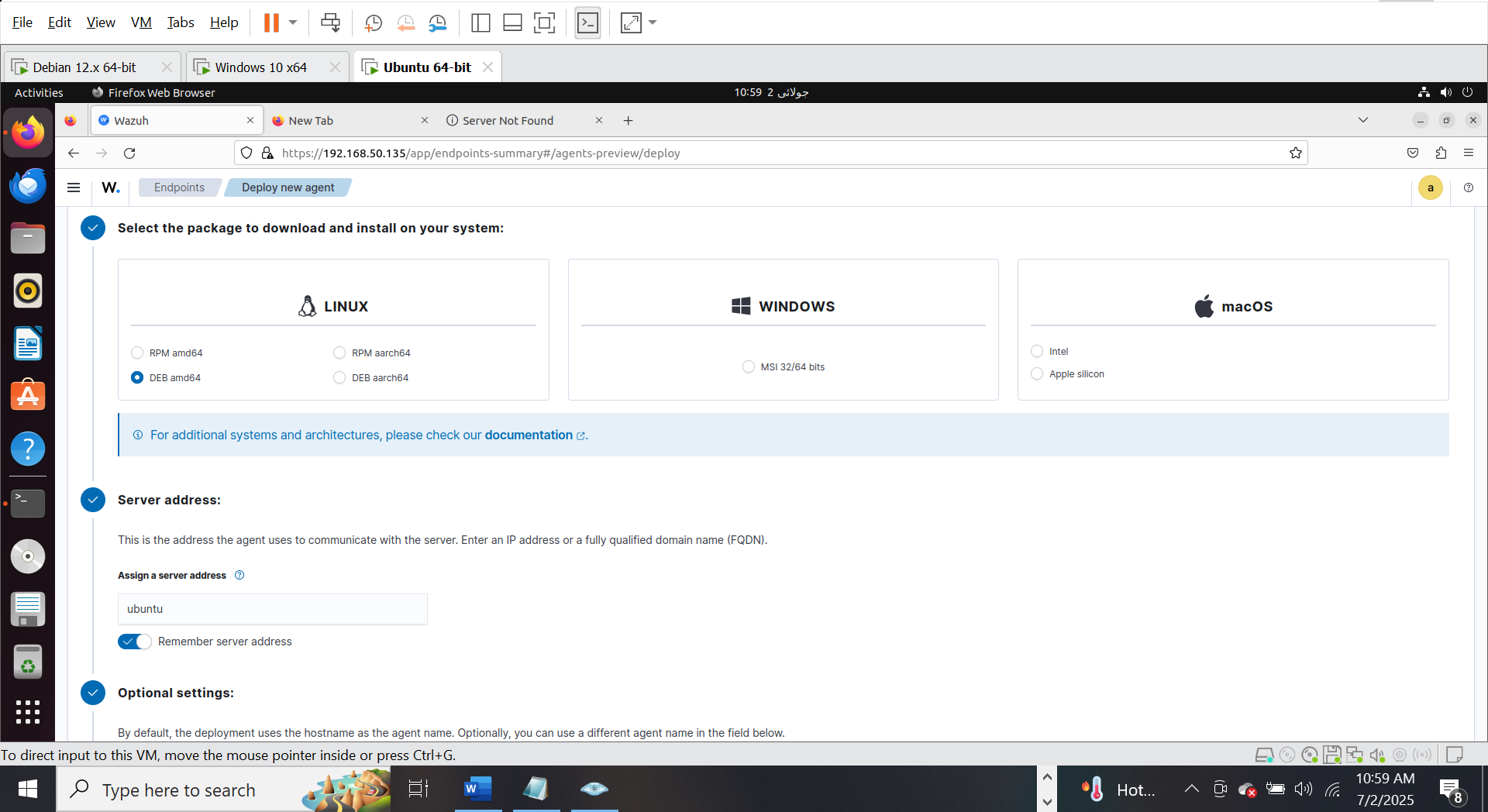
**Wazuh logs:**

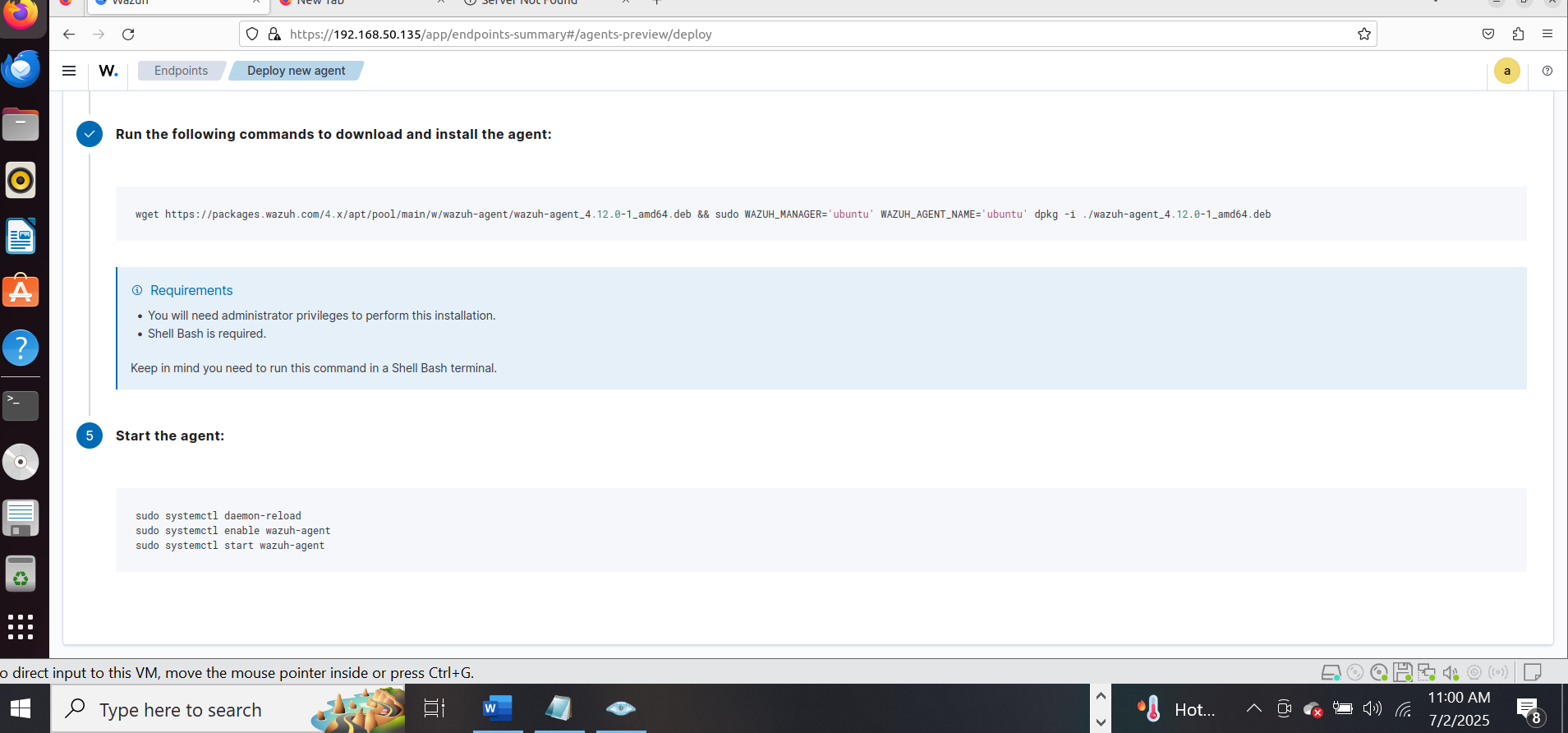




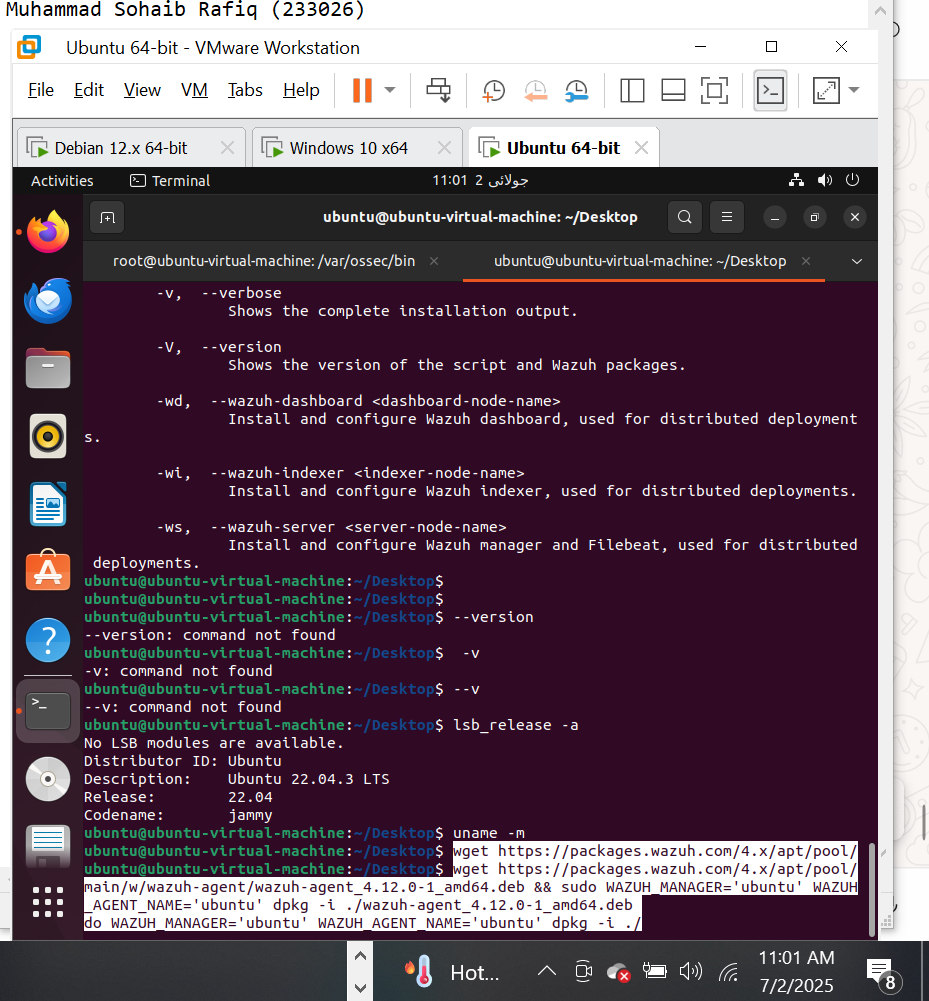
**Adding the new agent on the wazhu:**

**Adding the new agent on the wazhu:**

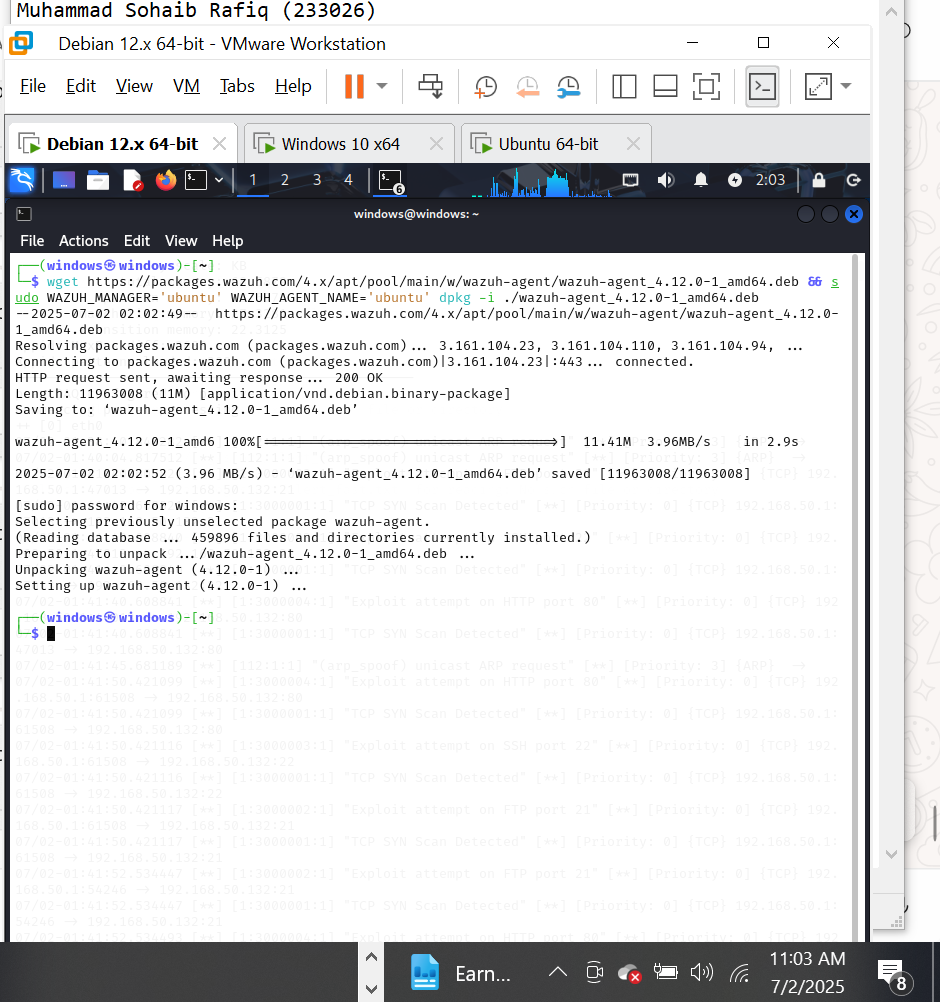
****

****

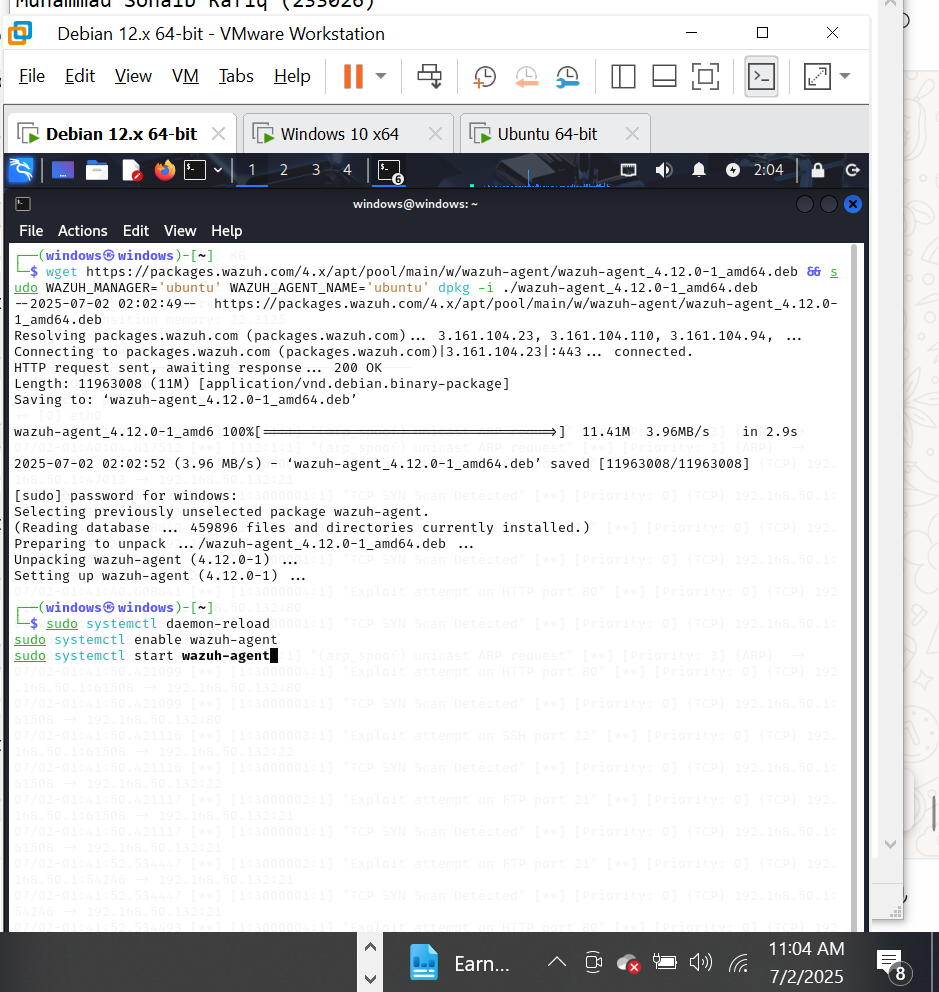
**On the ubuntu terminal:**

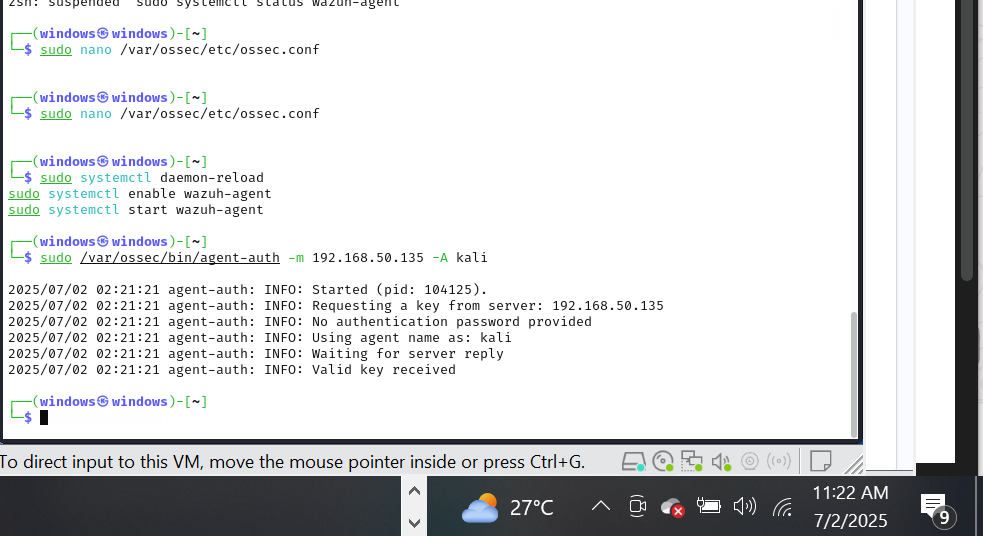
****

**I am facing error on the same ubuntu where my wazhub server is install so I install the agent on the kali linux:**

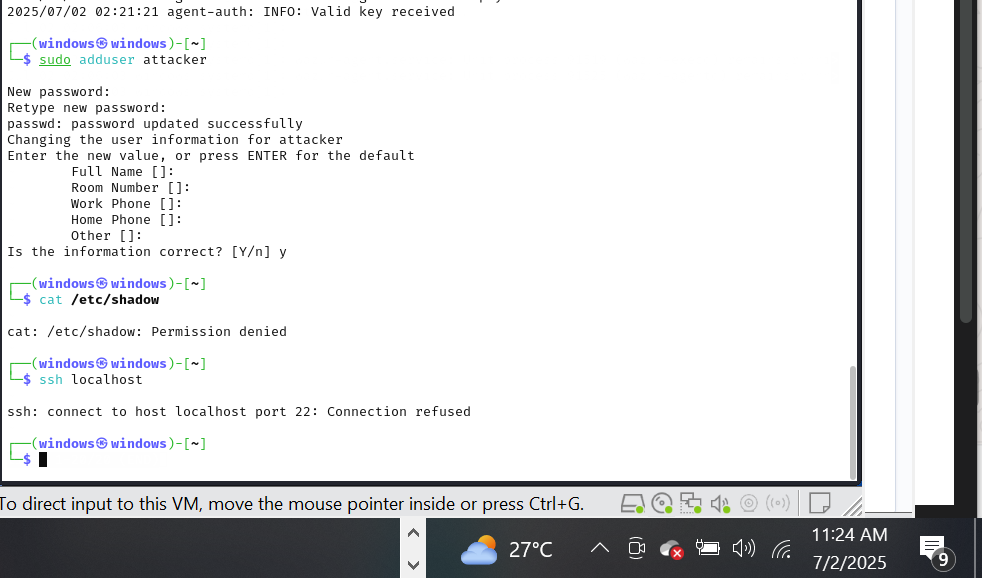
****

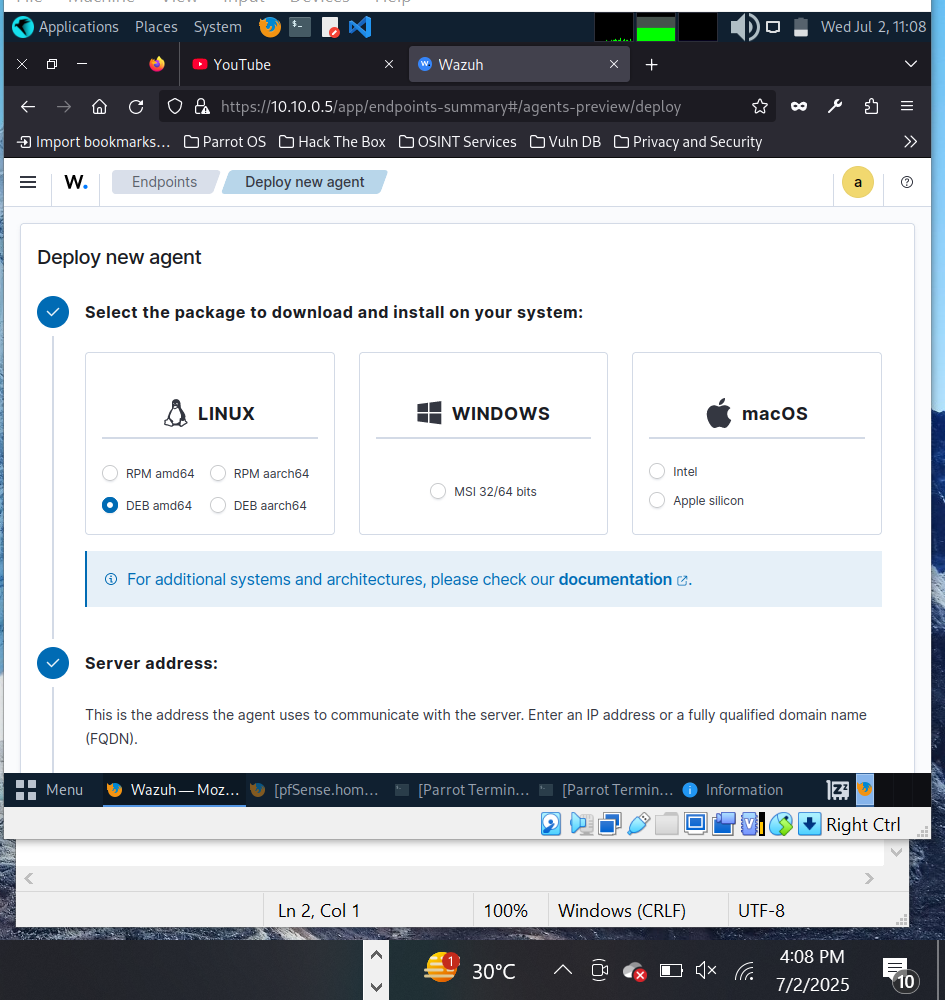
Staring the agent:

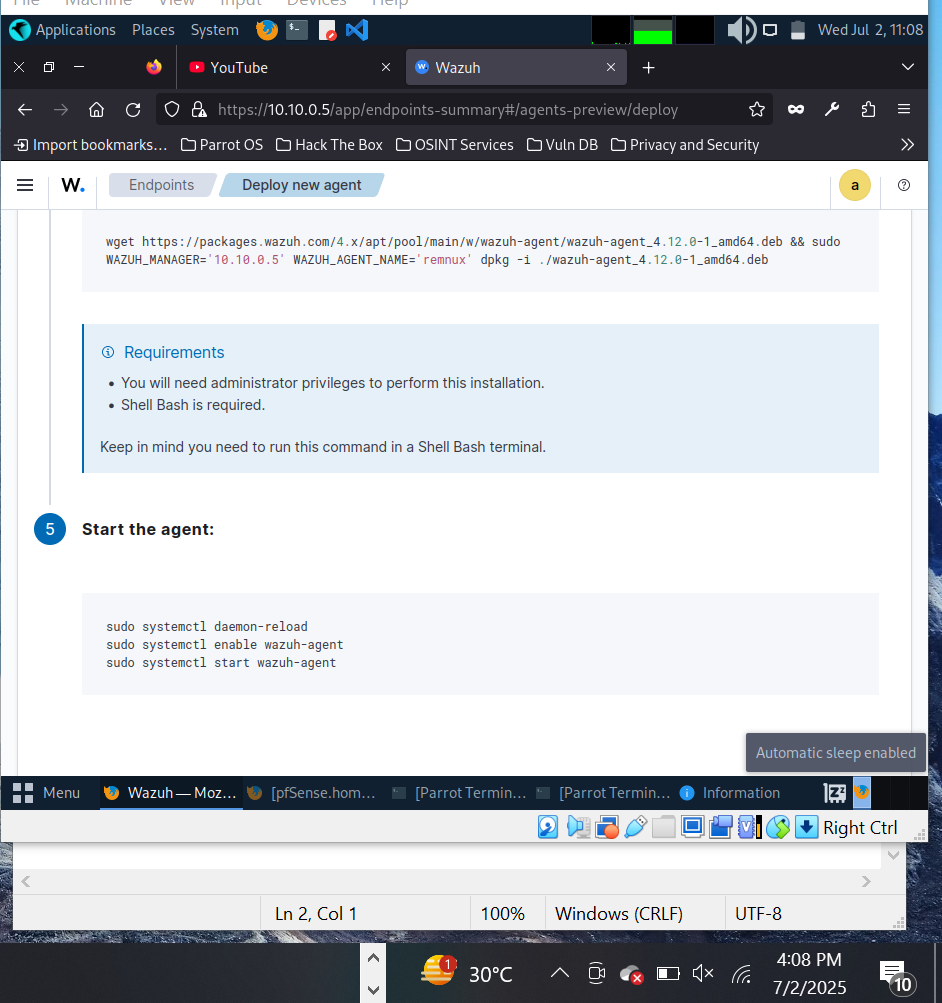




Perfrom the attacks the attempts are failed but the wazuh still monitor them :







**Wazuh logs:**

