****

|  |
| --- |
| *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** |

A mid-sized tech company is facing continuous TCP SYN scans and

exploit attempts on ports 21 (FTP), 22 (SSH), and 80 (HTTP). You have

to detect these activities and generate alerts. Submit rules you created

and relevant alert log entries.



### Step 2: Create a Custom Rule File

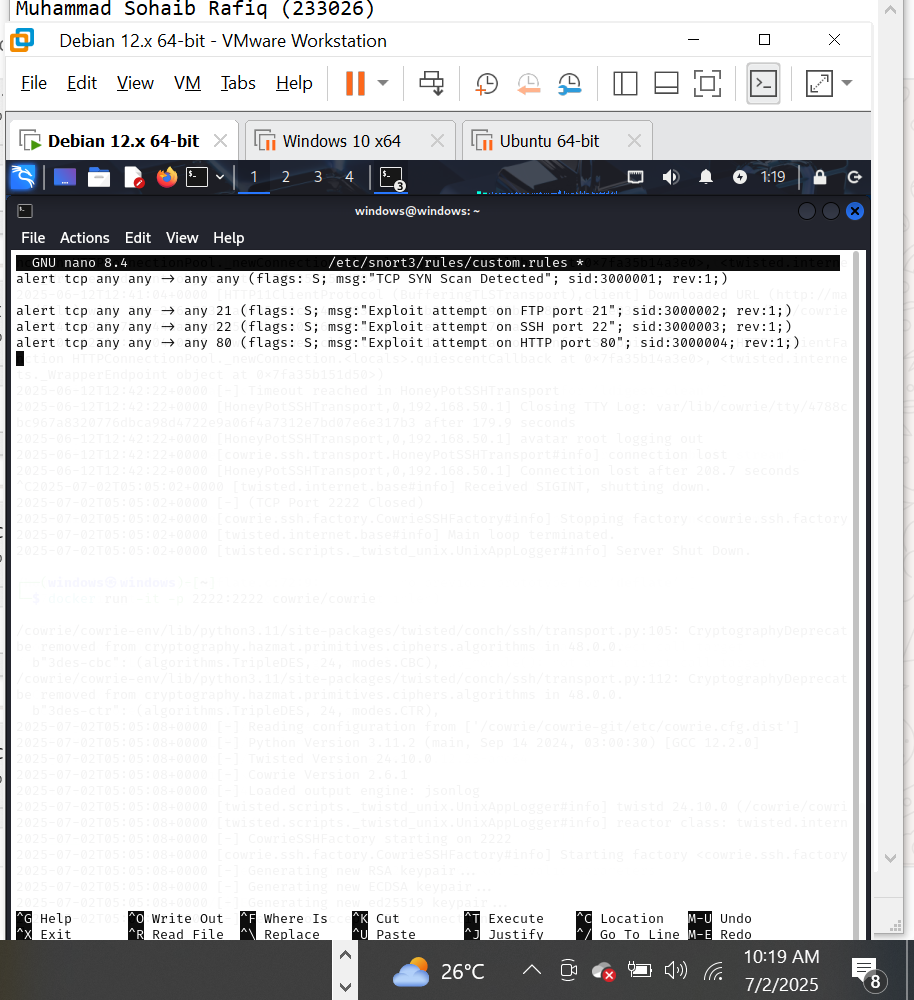
Create a custom rule file to hold your alert rules:

bash

Copy code

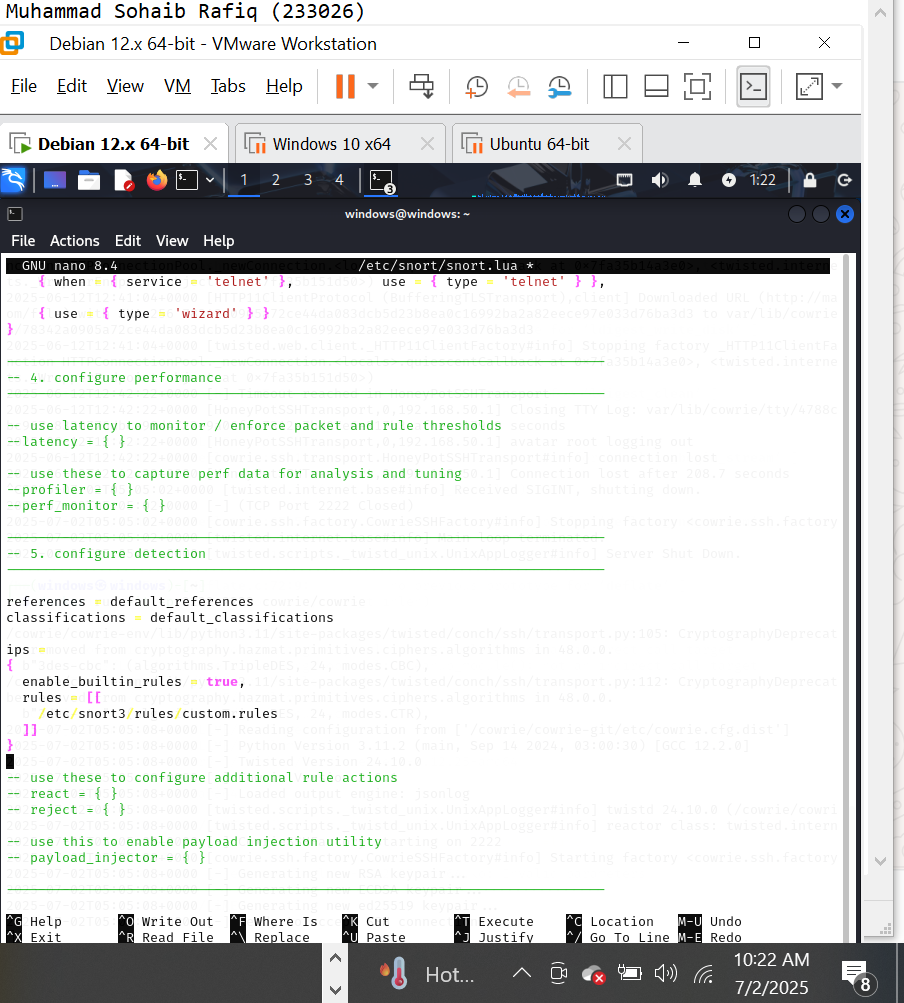
sudo mkdir -p /etc/snort3/rules

sudo nano /etc/snort3/rules/custom.rules



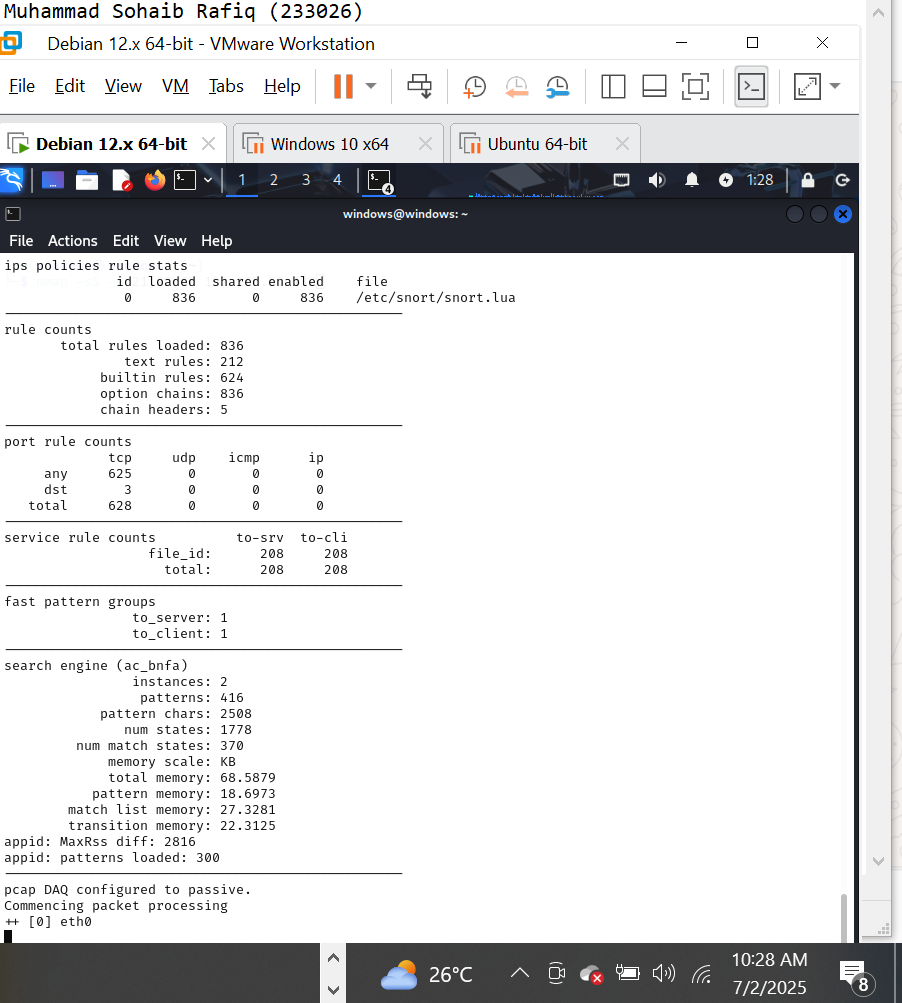
### Step 3: Tell Snort to Load Your Rule File

Edit the main Snort 3 Lua config file:



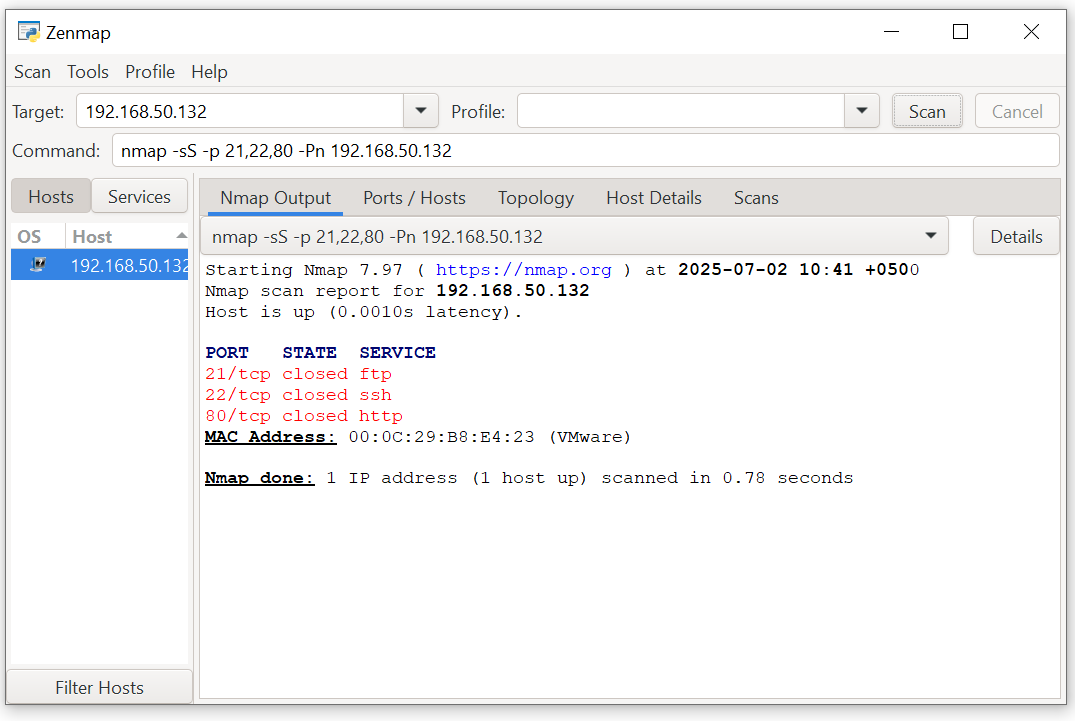
Step 4: Run Snort in IDS Mode with Your Rules

Now snort working listing in IDS mode:

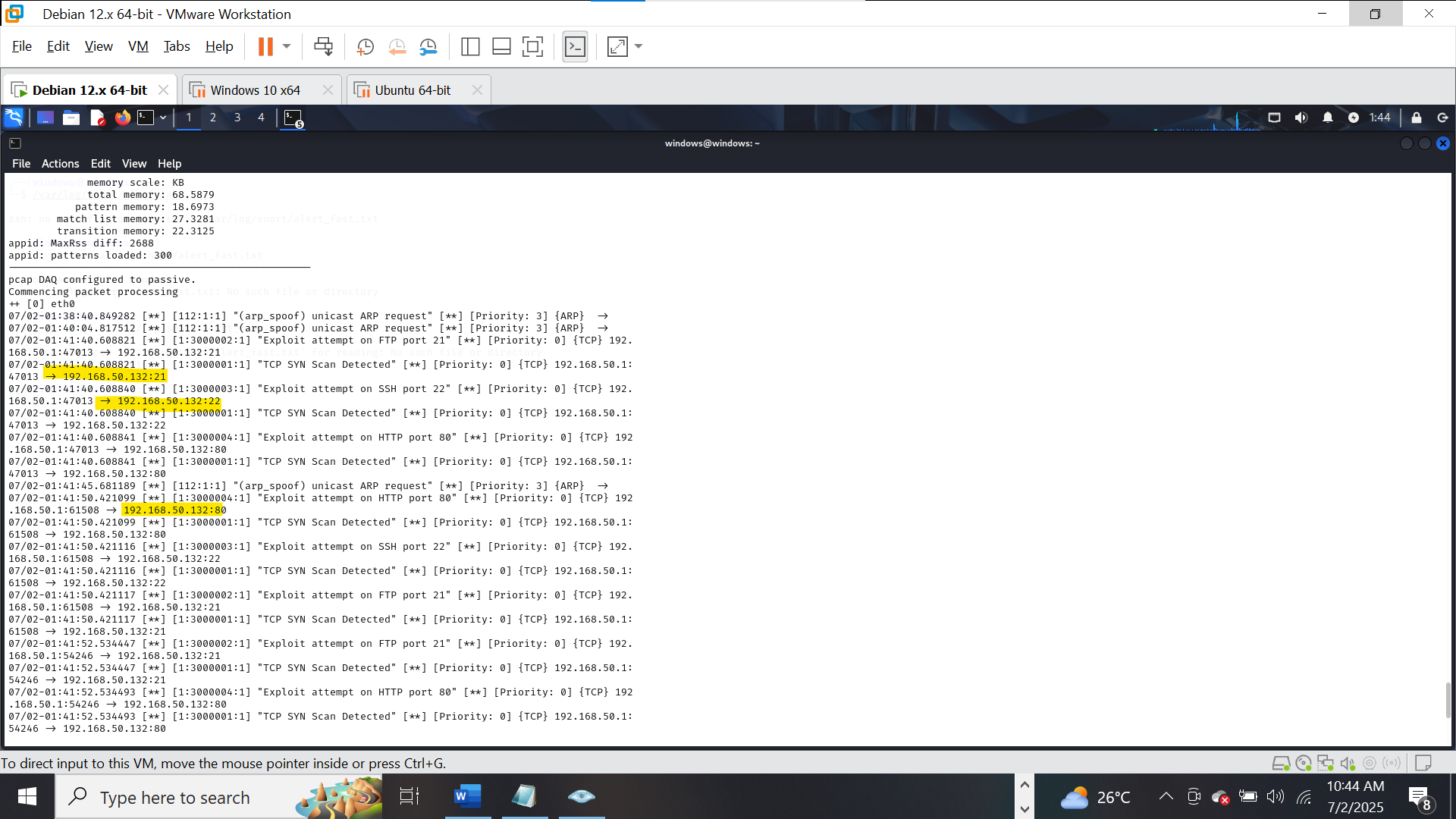


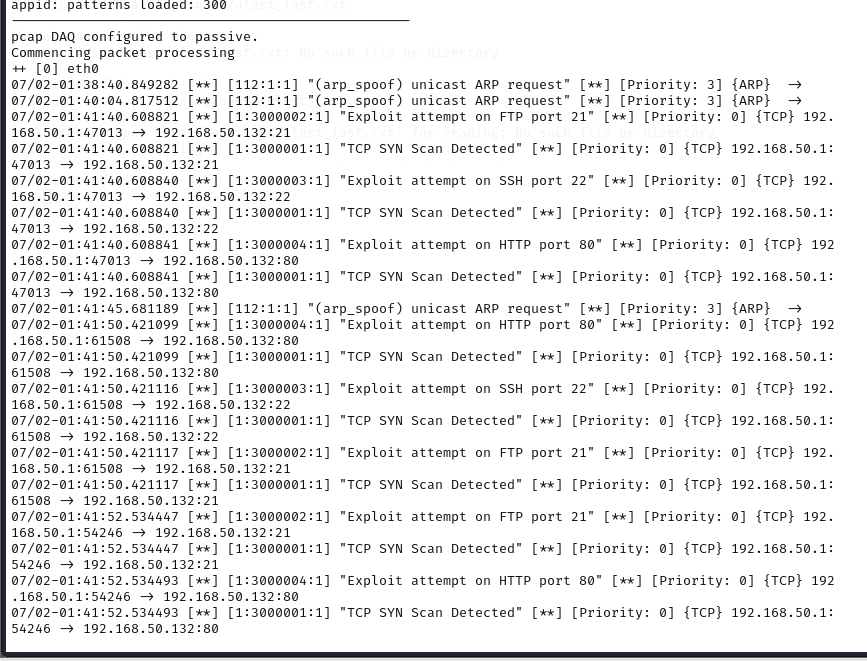
Simulate Alerts

Scanning from windows:



Snort Alerts:





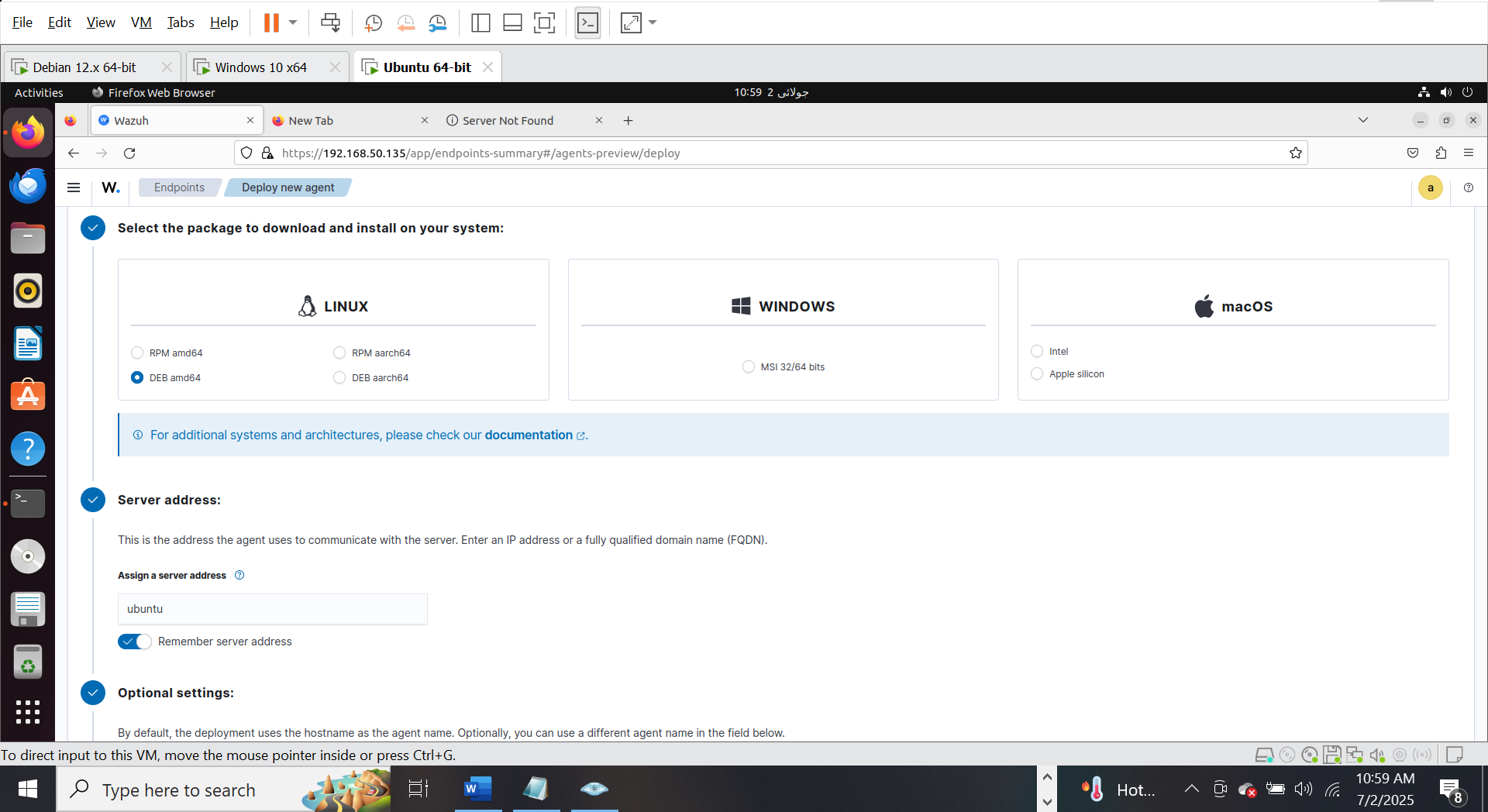
**c) A non-privileged user accessed /etc/shadow and initiated SSH to another**

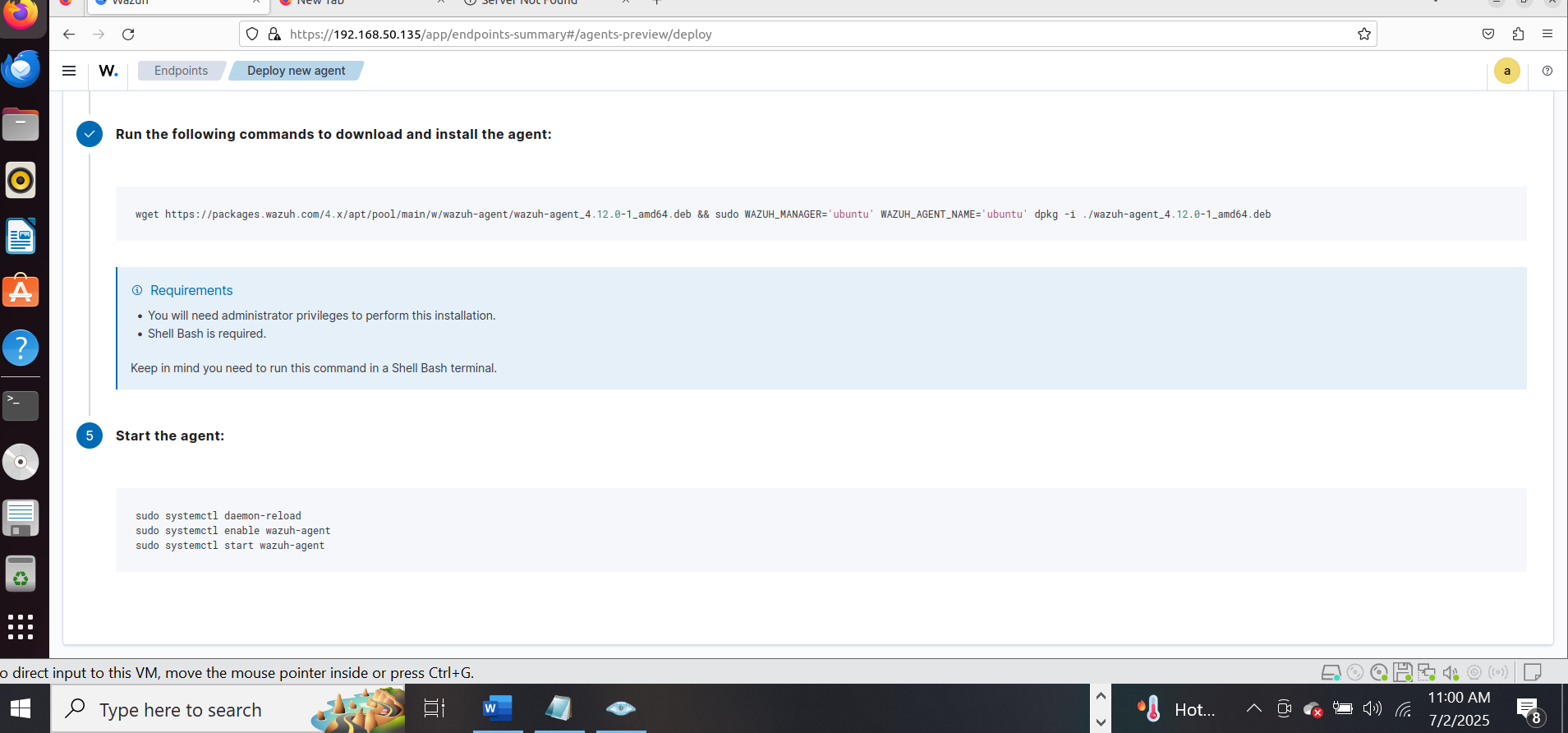
**internal server. You must configure Wazuh to detect such behavior and**

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

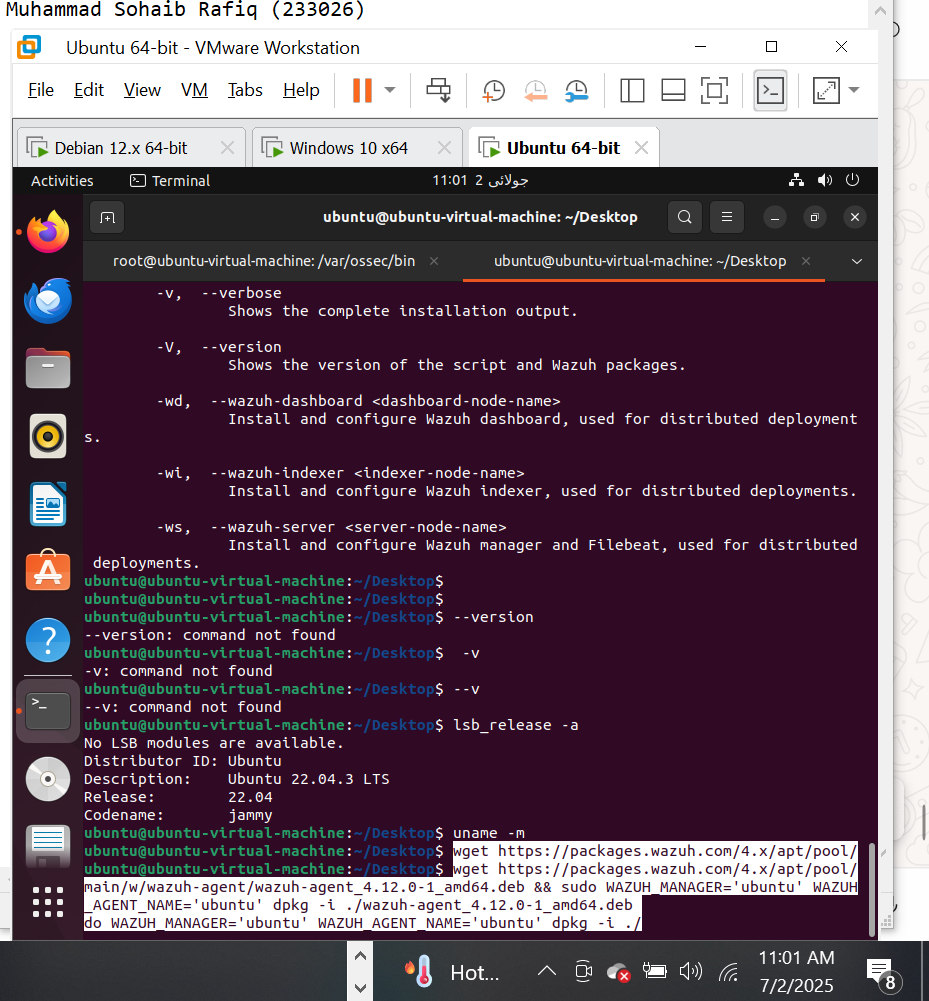
**show correlated alerts.**

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

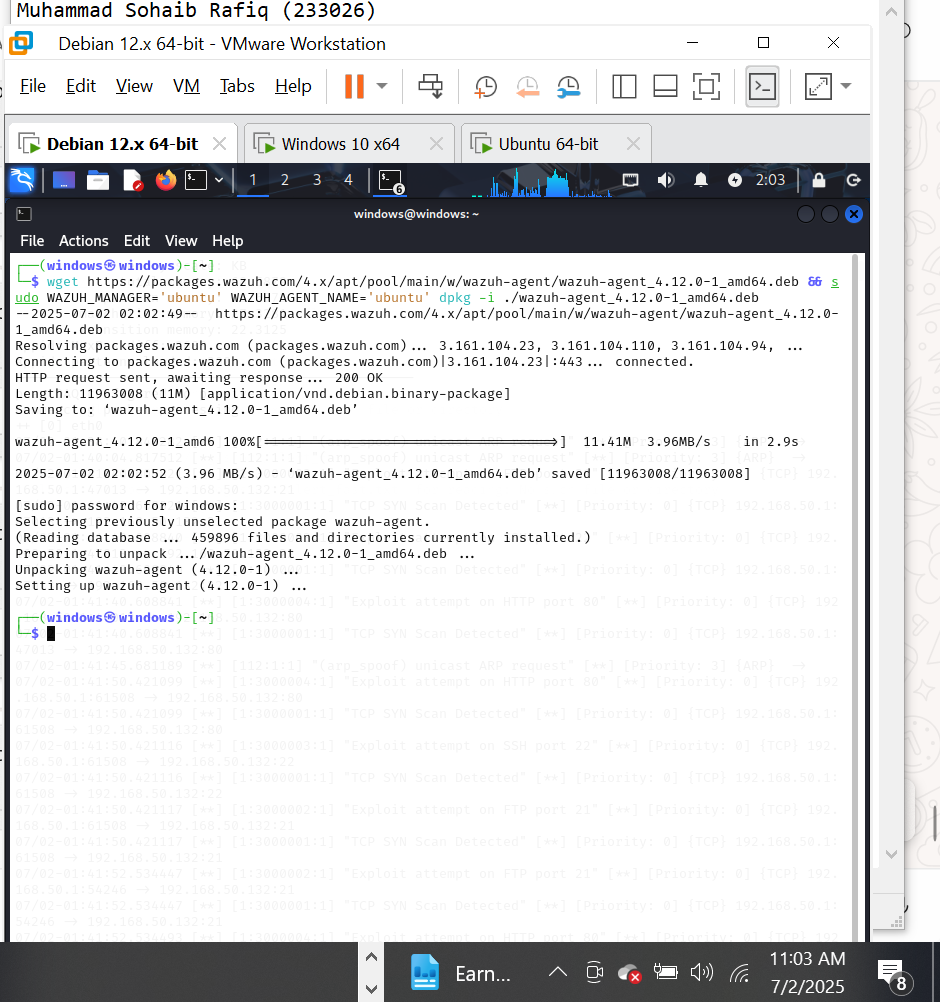
****

****

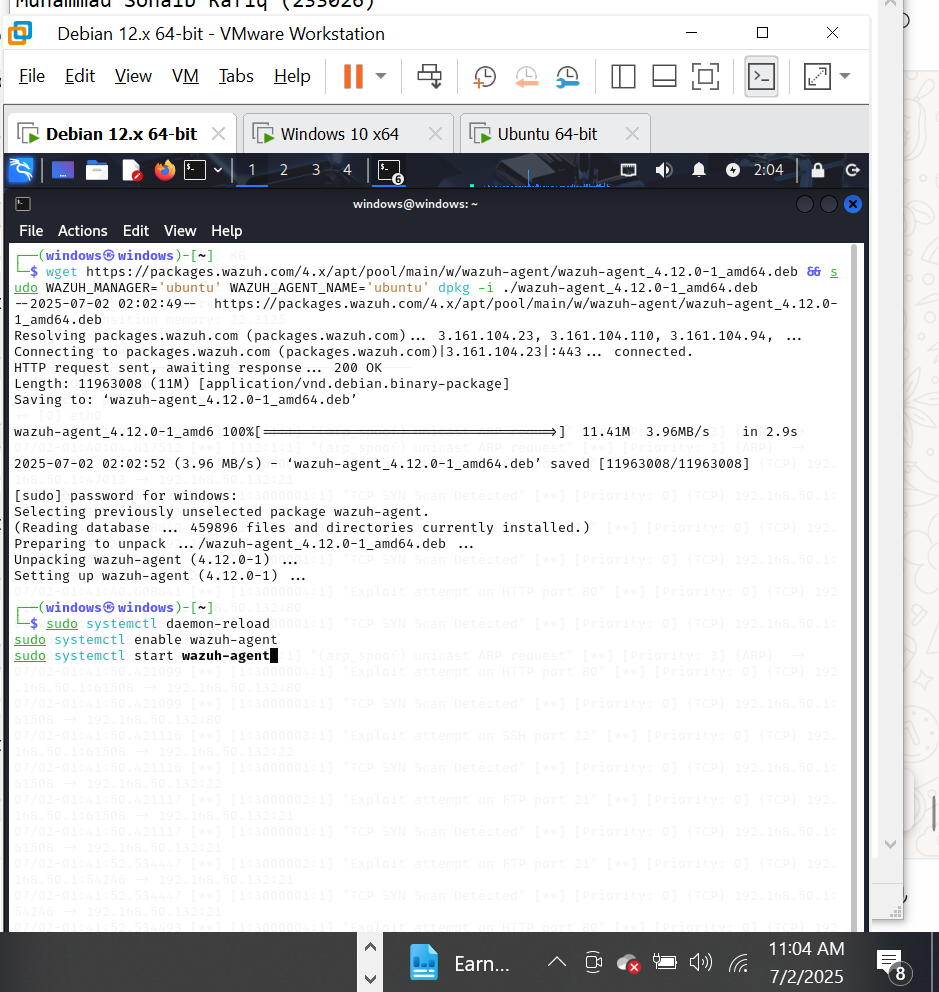
**On the ubuntu terminal:**

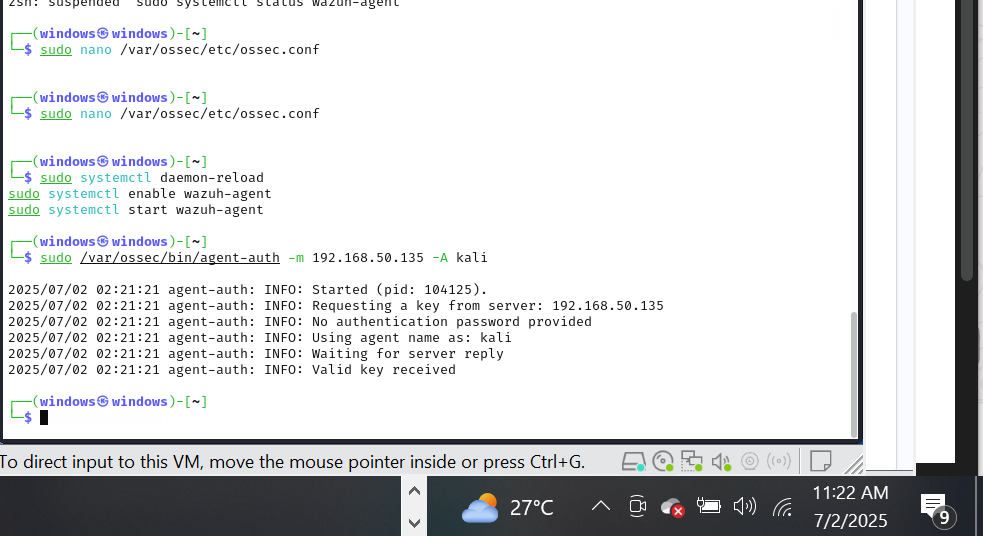
****

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

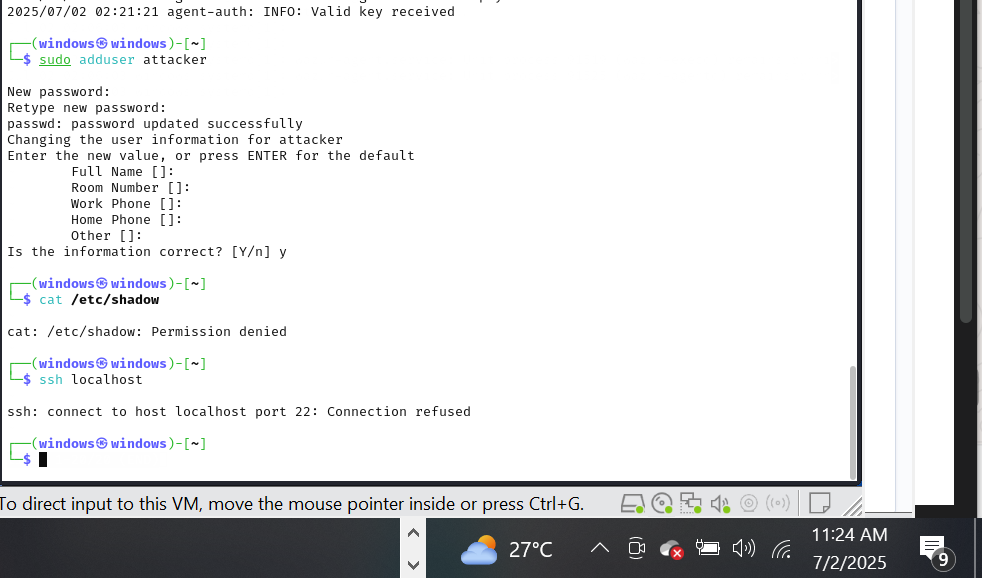
****

Staring the agent:





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



The process is same but unfortunately the wazuh give me this error and due the short time I am moving the next questions because wazuh I showing and error so there are no alerts :



I will fix it later:

**b) One internal machine is communicating with known malicious IPs. You are**

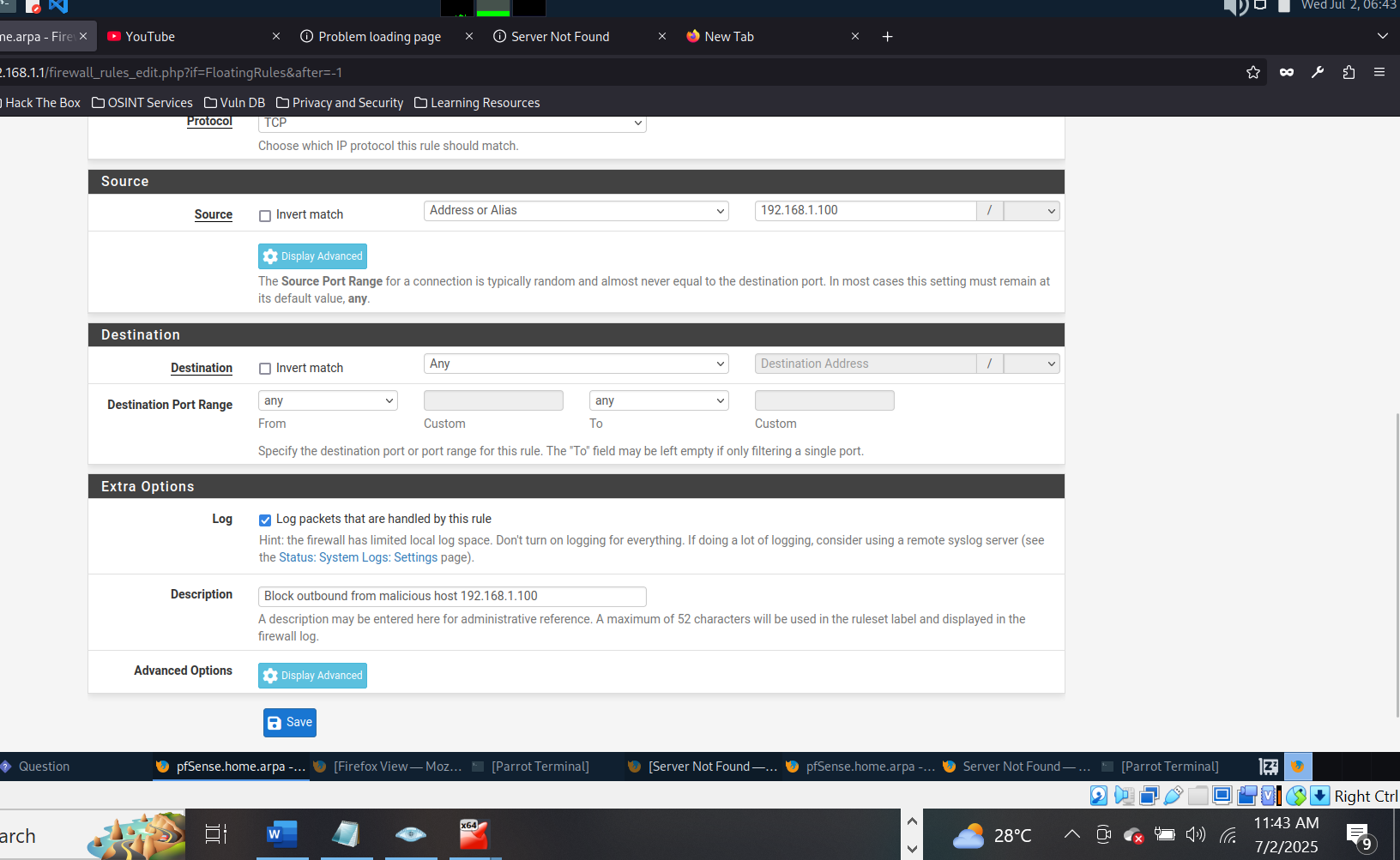
**to use PFsense to isolate this host by blocking all outbound traffic from**

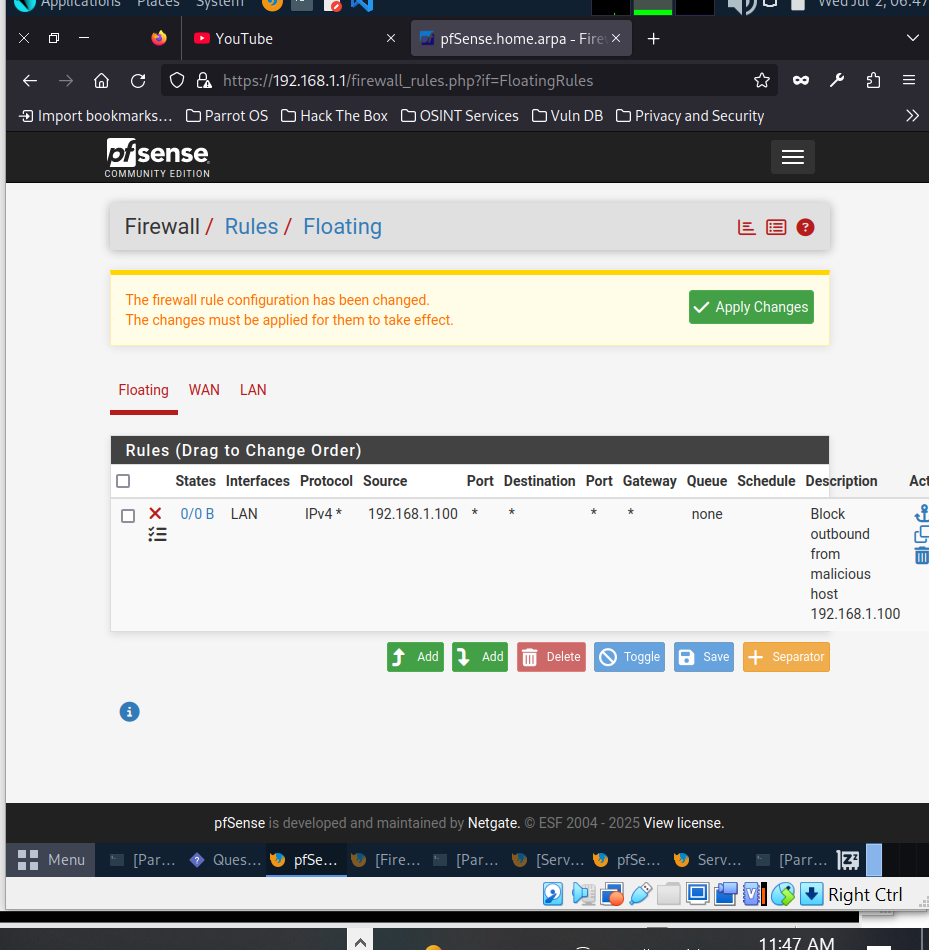
**that host while keeping the rest of the network operational. Submit**

**screenshots of firewall rules you configured and logs of blocked traffic.**

Creating the PfSense rules:







Testing:

