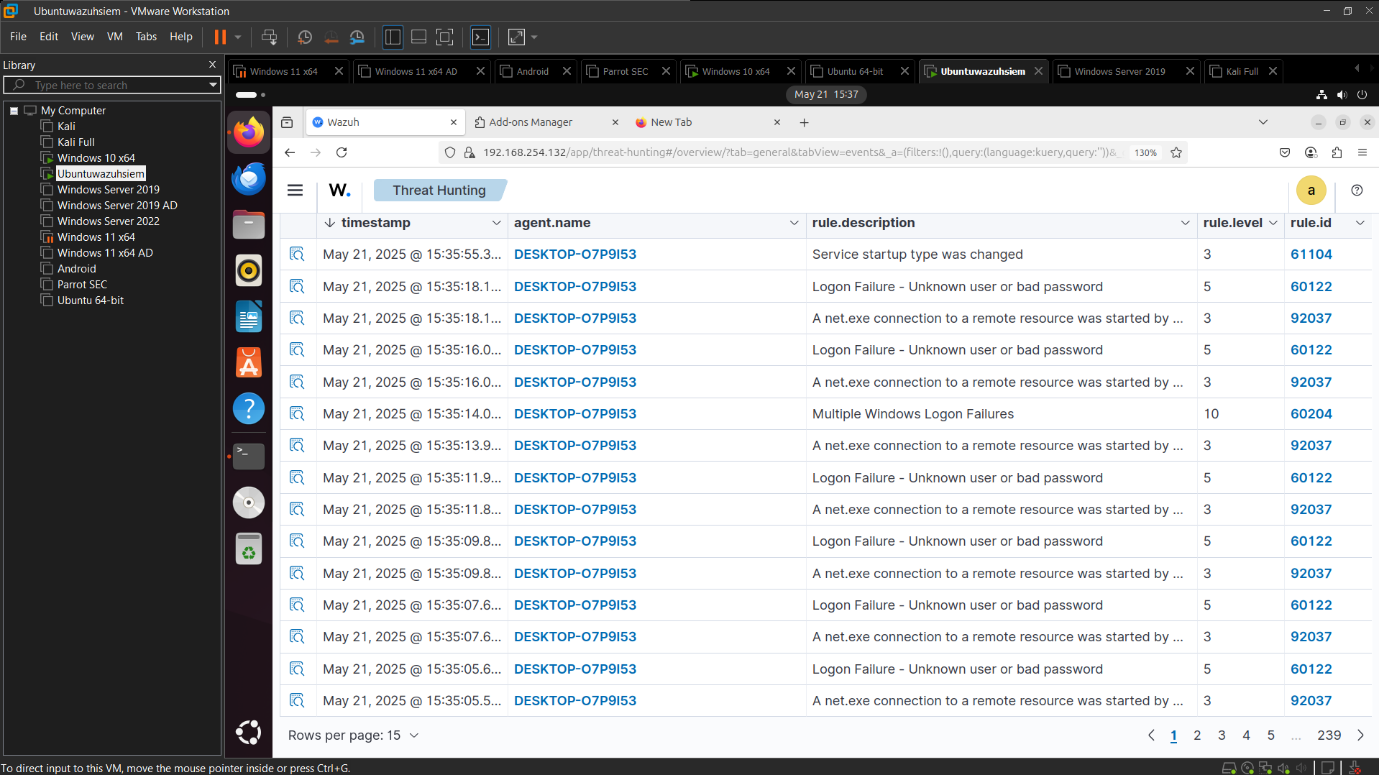
Assignment: Create a Detection Report

Scenario 1: Bruite Force Followed by Privilegde login

Explain= Brute force are simply list of password and username this list used for find login Password

Objetive=I was find login faild event repidaly try wrong password

Tool Used = Siem = Wazuh and syslog for log forwarding



Analyst Notes / recommedations

find login faild event repidaly try wrong password

yes some time deley to detect

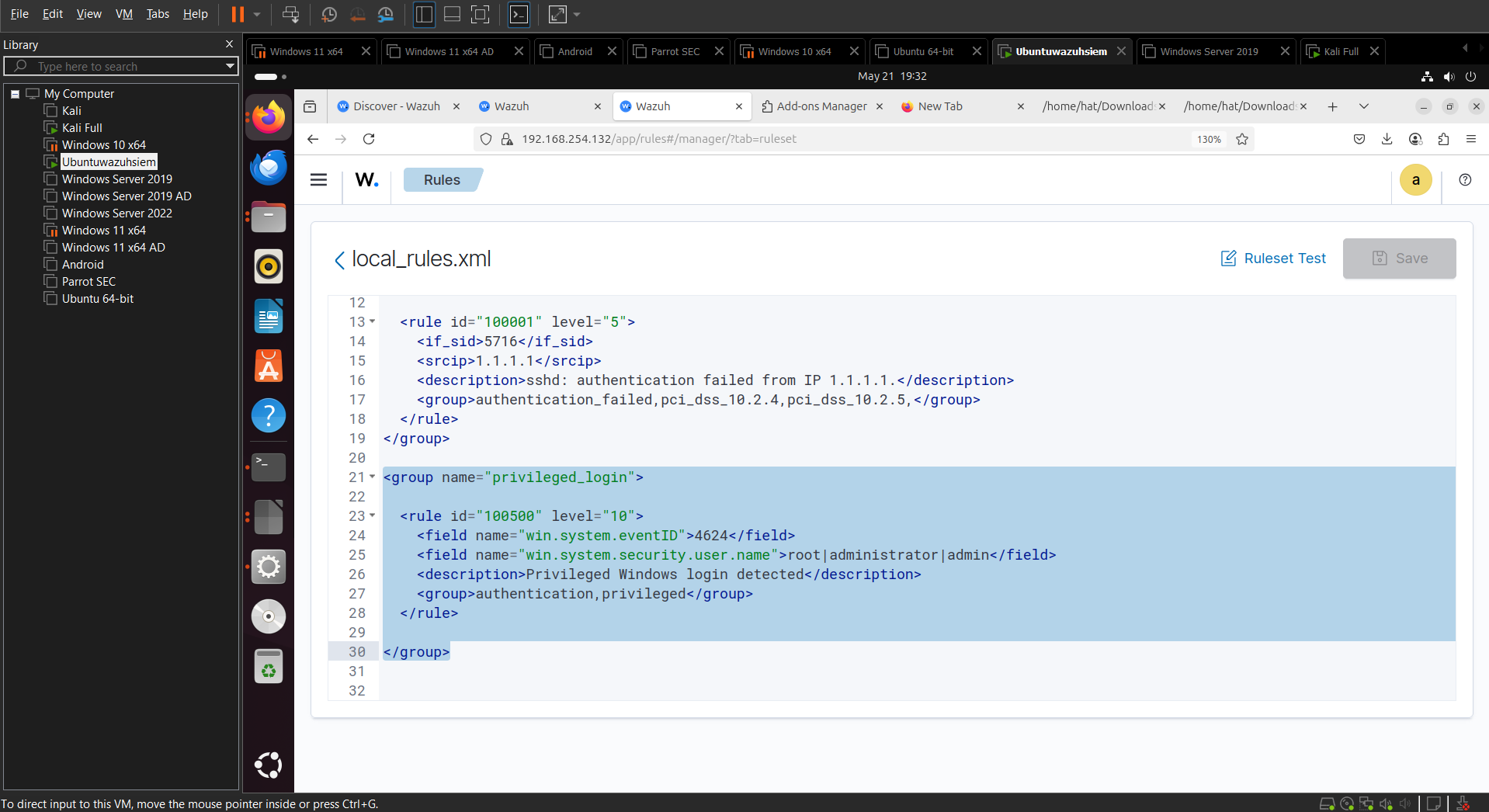
Detection Status

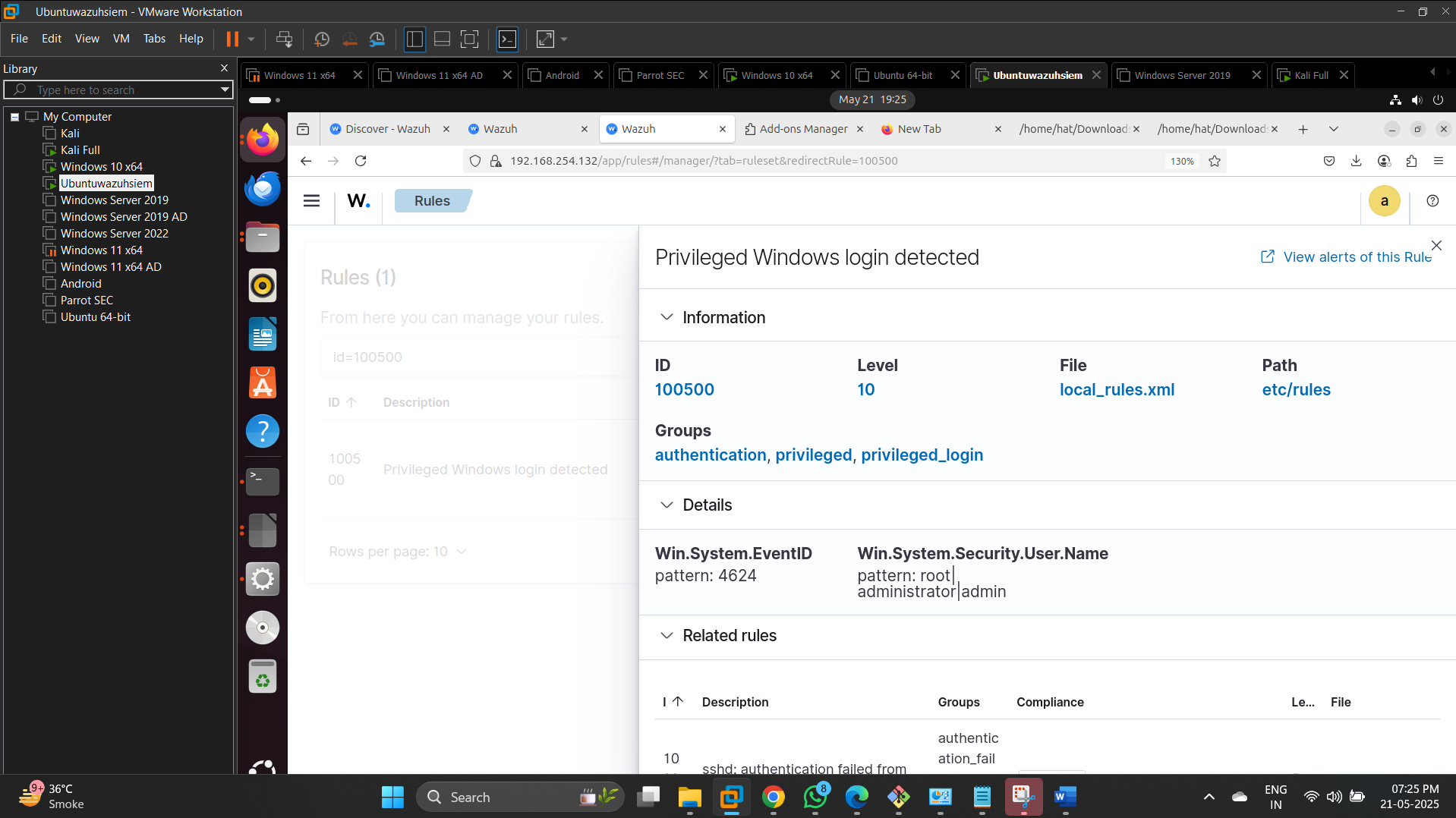
Successfully Triggered

Scenario 2 = Suspicious logon time – After-hour Admin Activity

Explain= after 9 am to 7 pm someone try to login detect it in alert after hour login

Objective = detect priviled esclution





Analyst Notes / recommedations

Other side try to login is detect by privilideg esculision

yes some time deley to detect

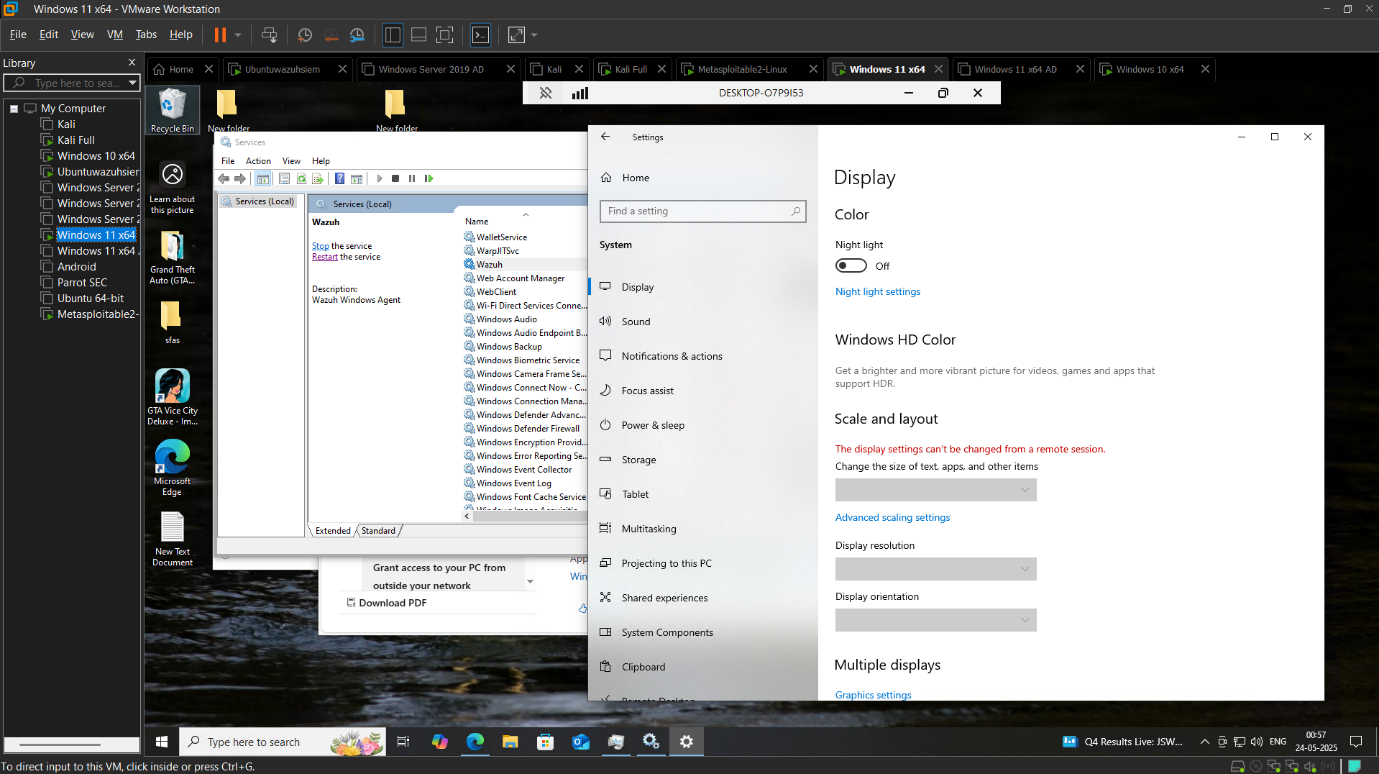
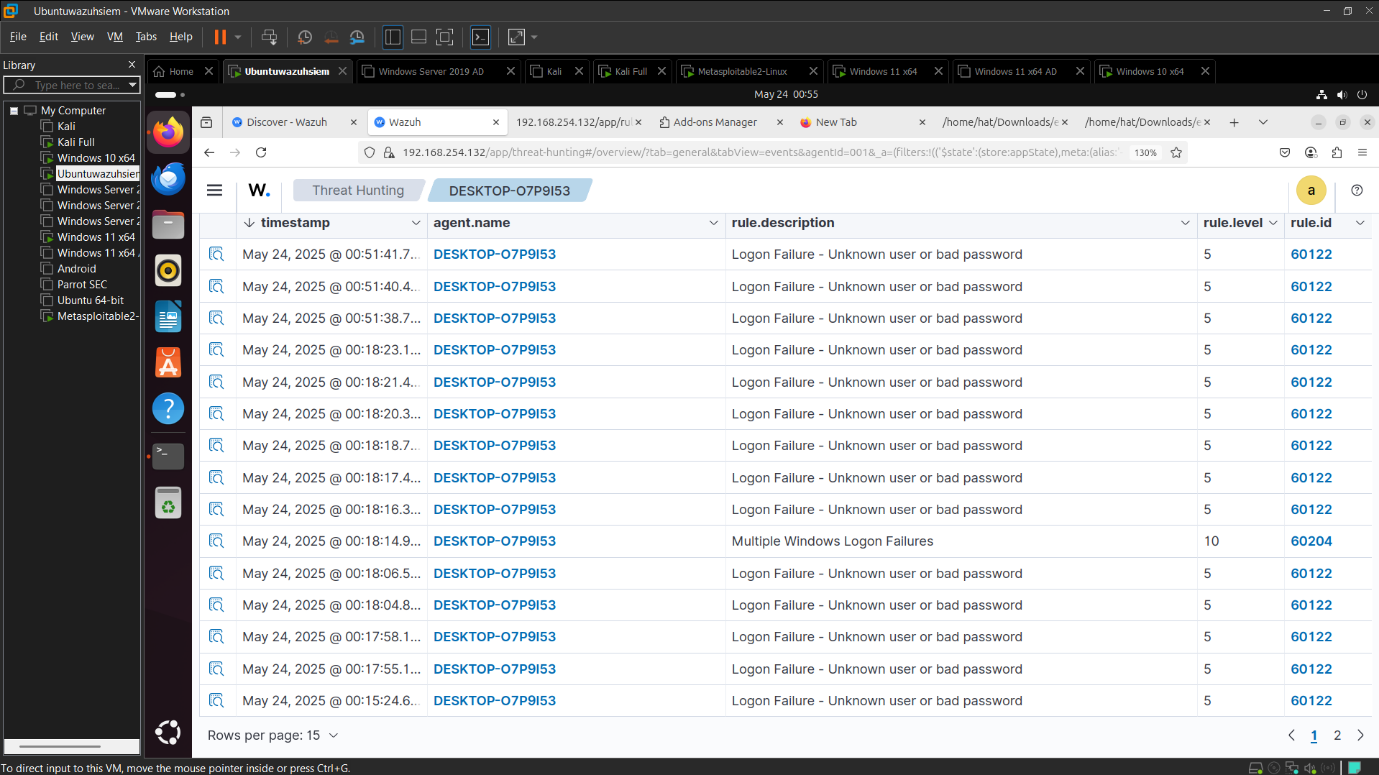
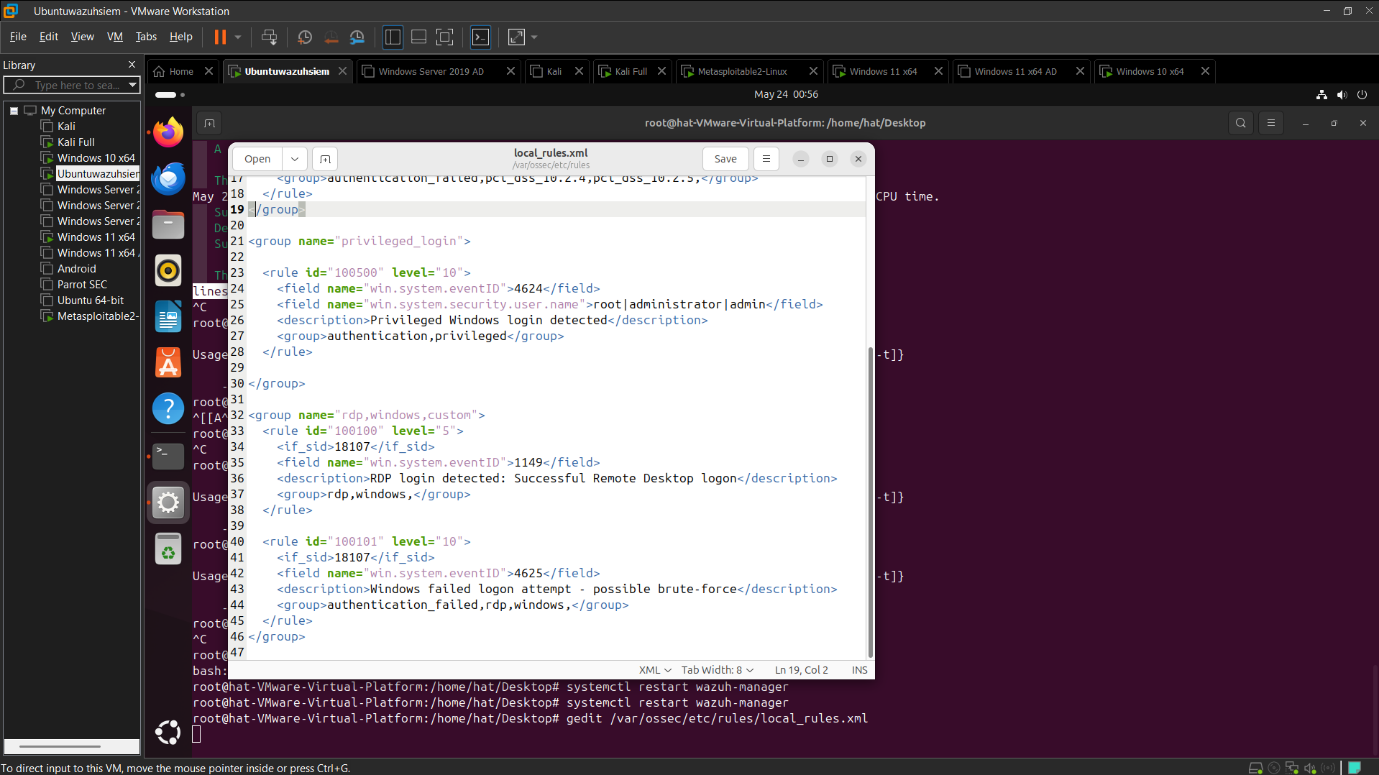
Detection Status

Partially triggered

Scenario 3 : Leteral Movement with attempt via RDP

Objective : Detect many login Faild

Tool Wazuh and syslog



Analyst Notes / recomendatiom

Altemp to login via rdp

Detect faild login logs

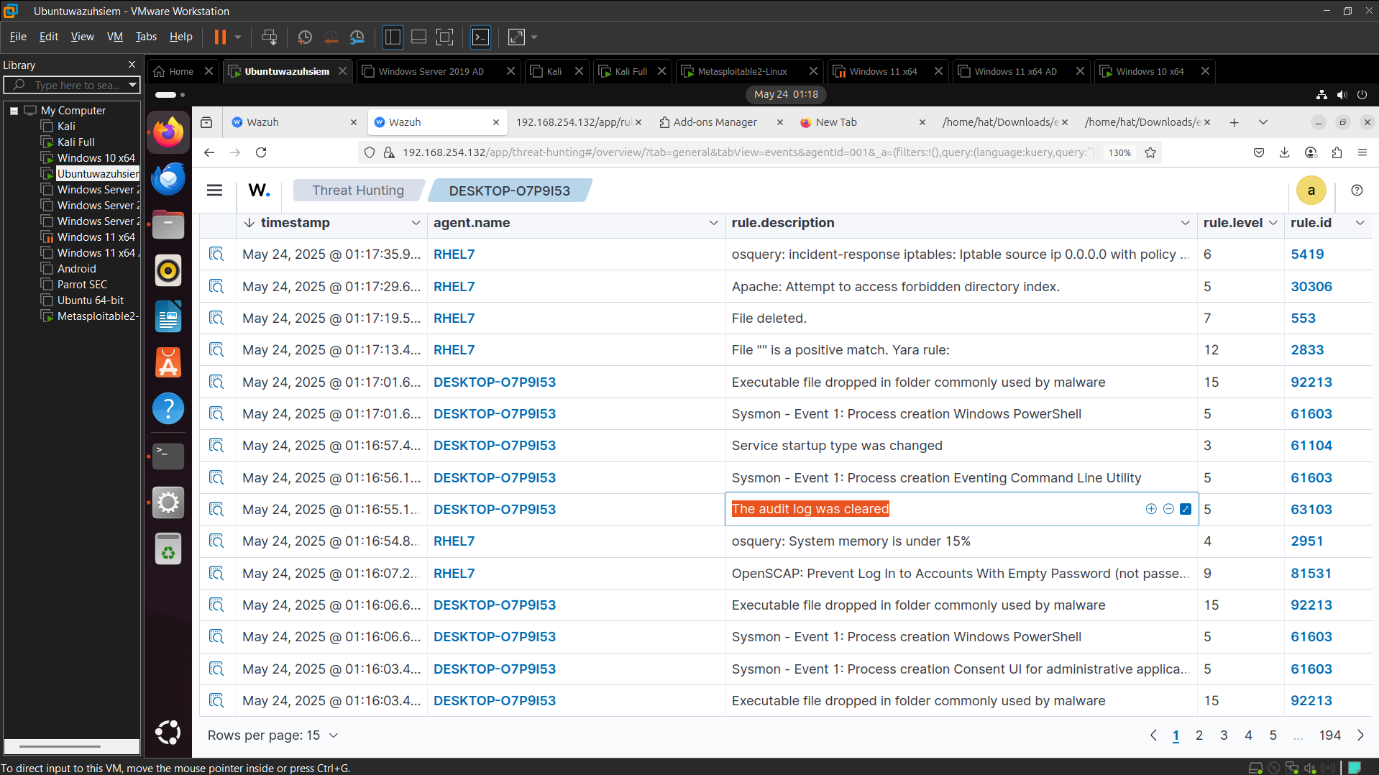
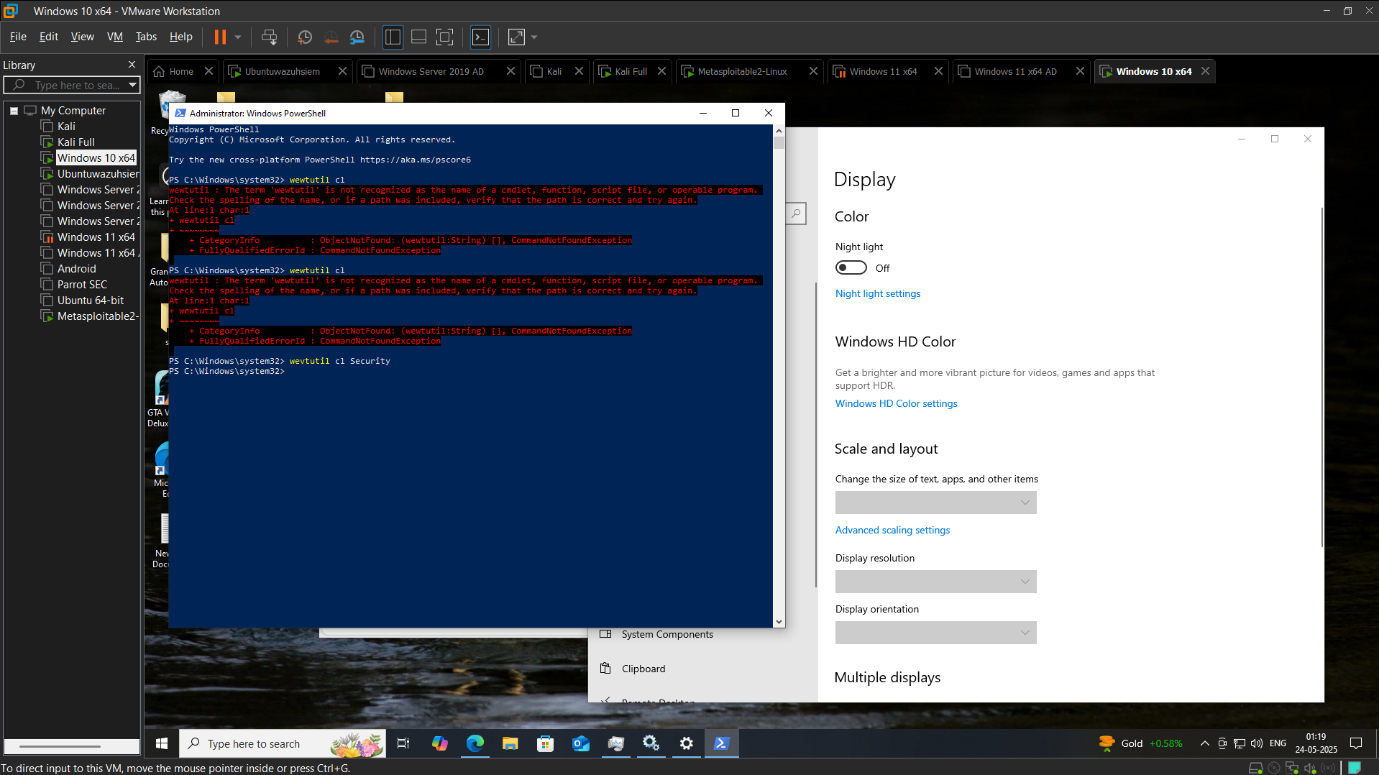
**Detection Status**

Successess Fully Triggered

Scenario 4: log Teampering Simulations

Detect clear logs

Wazuh and sysloh



Analyst Notes/recomedention

Clear log Alert triggers

Detection Status

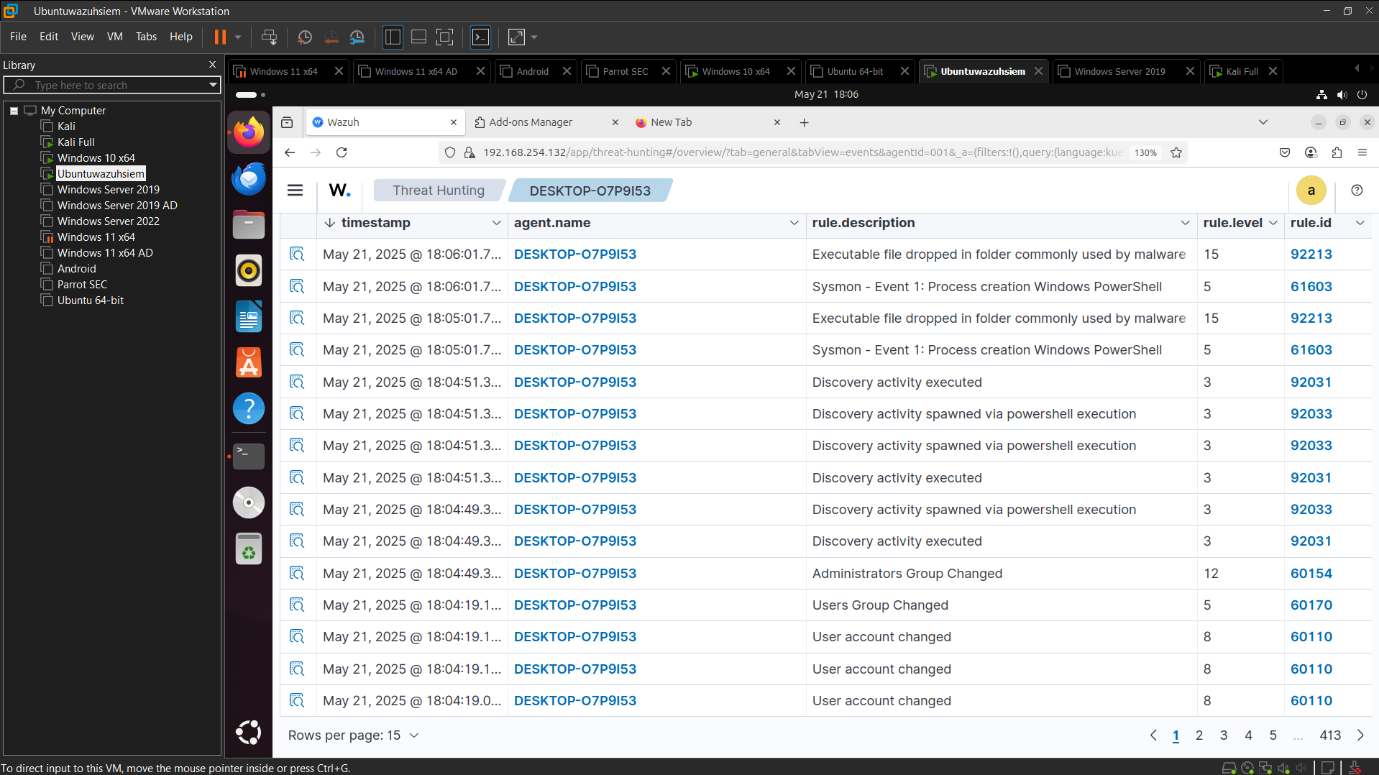
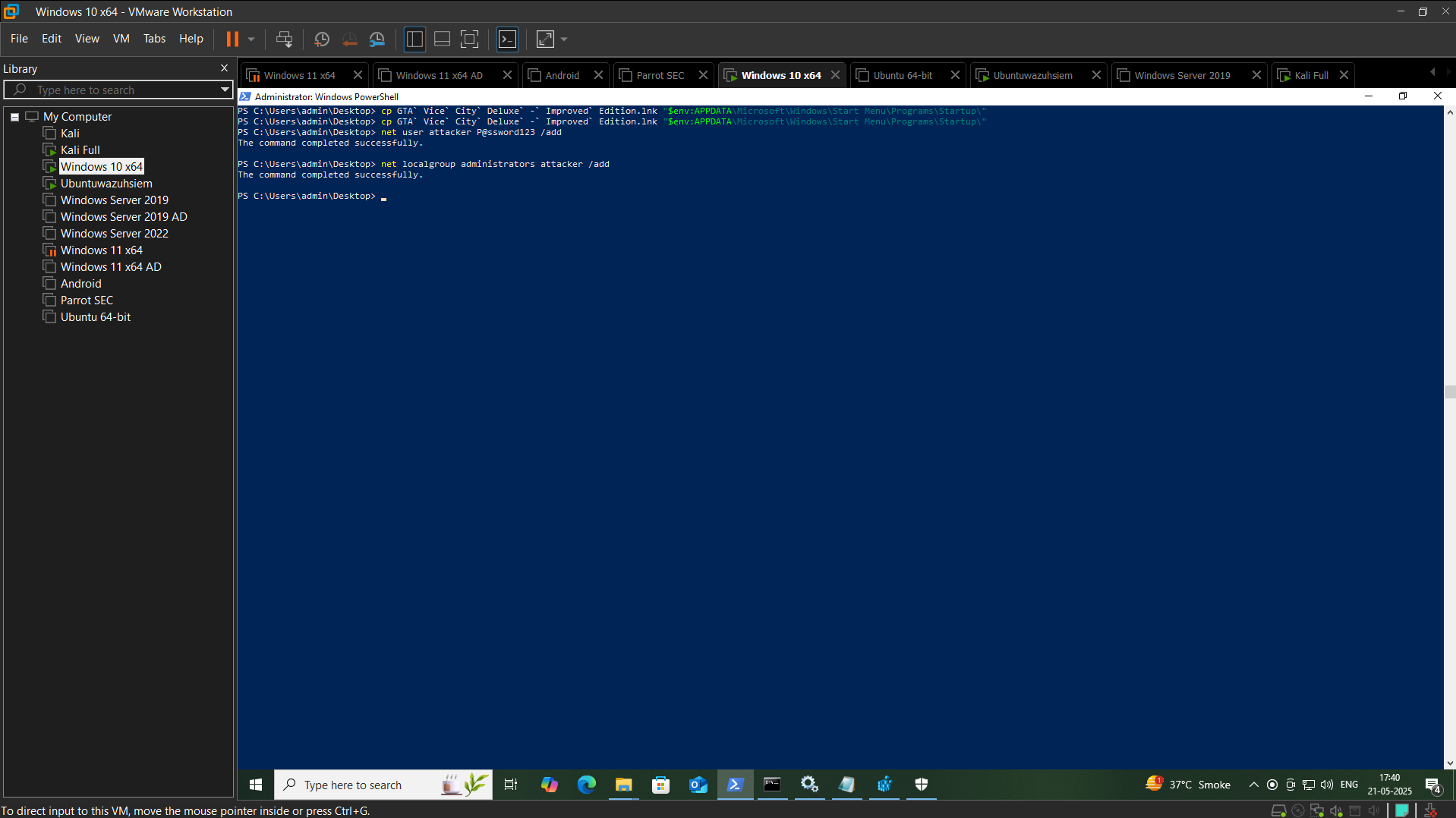
Success fully Triggered

Scenario 5 Hidden User Account Creations

Objective find new user create alert logs

Log source Syslog

Lab Setup Wazuh in Ubuntu



Analyst Notes /recomedation

Alert are triggered user account and group are changerd

Detection Status

Successfully Triggered