**SIEM Foundation – Building Cyber Defense Labs**

Introduction

Welcome To Srinda SIEM Internship

Hello Evryyone My Name Is Harvik Bharat Kumar Prajapati I currunty Doing Internship At Shrida SIEM Internship and Hand s On Prectice on Soc Analyst and Detection Report

Objective Phase1:Setup My Soc lab Simulate Basic Attacks, Configure log Surces and detect real threats

I was use SIEM tool Wazuh I am First install Ubuntu after Ubuntu install it Deploy Wazuh Server in Ubuntu

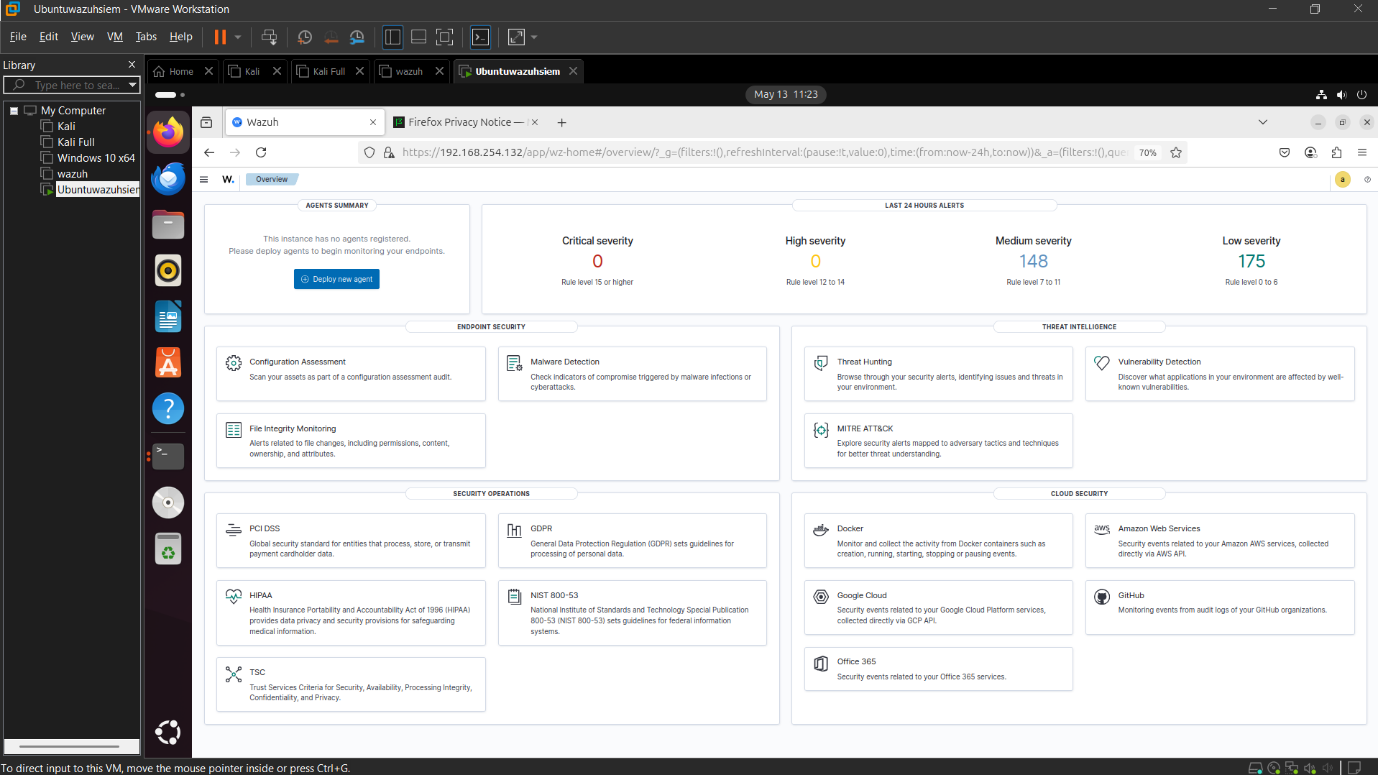
Command use by Me

Sudo apt install Curl

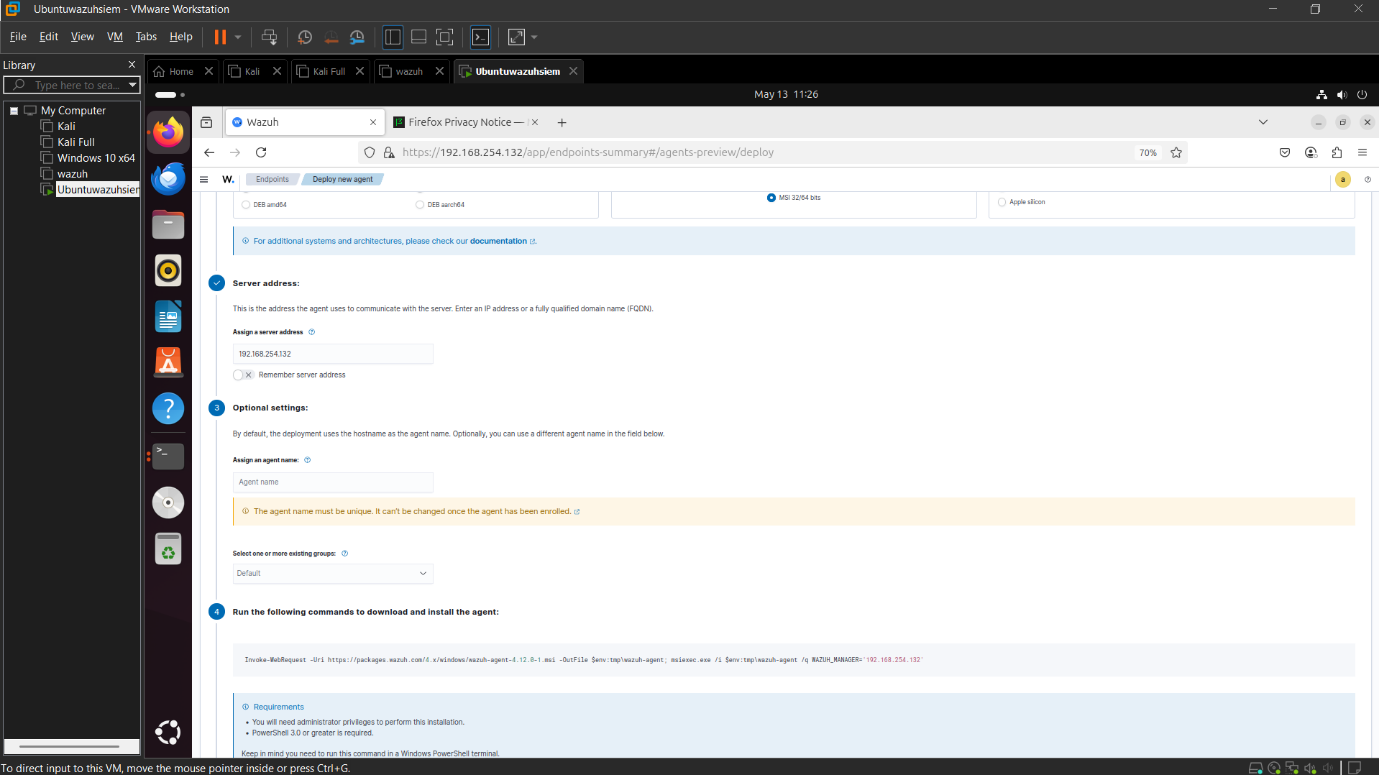
Sudo apt install default-jdk

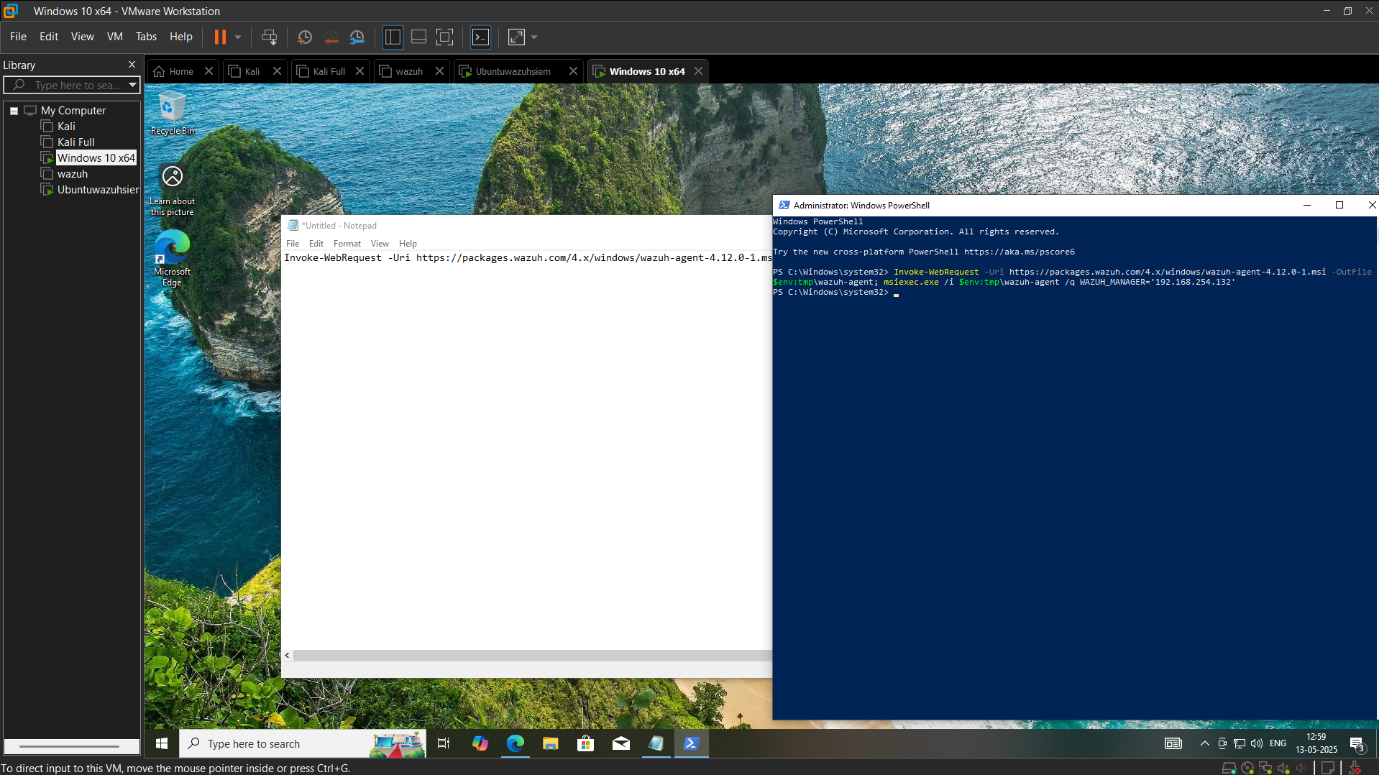
curl -sO <https://packages.wazuh.com/4.12/wazuh-install.sh>

bash wazuh-install.sh -a



Lets Setup wazuh Client





External download syslog xml file <https://wazuh.com/resources/blog/emulation-of-attack-techniques-and-detection-with-wazuh/sysmonconfig.xml>

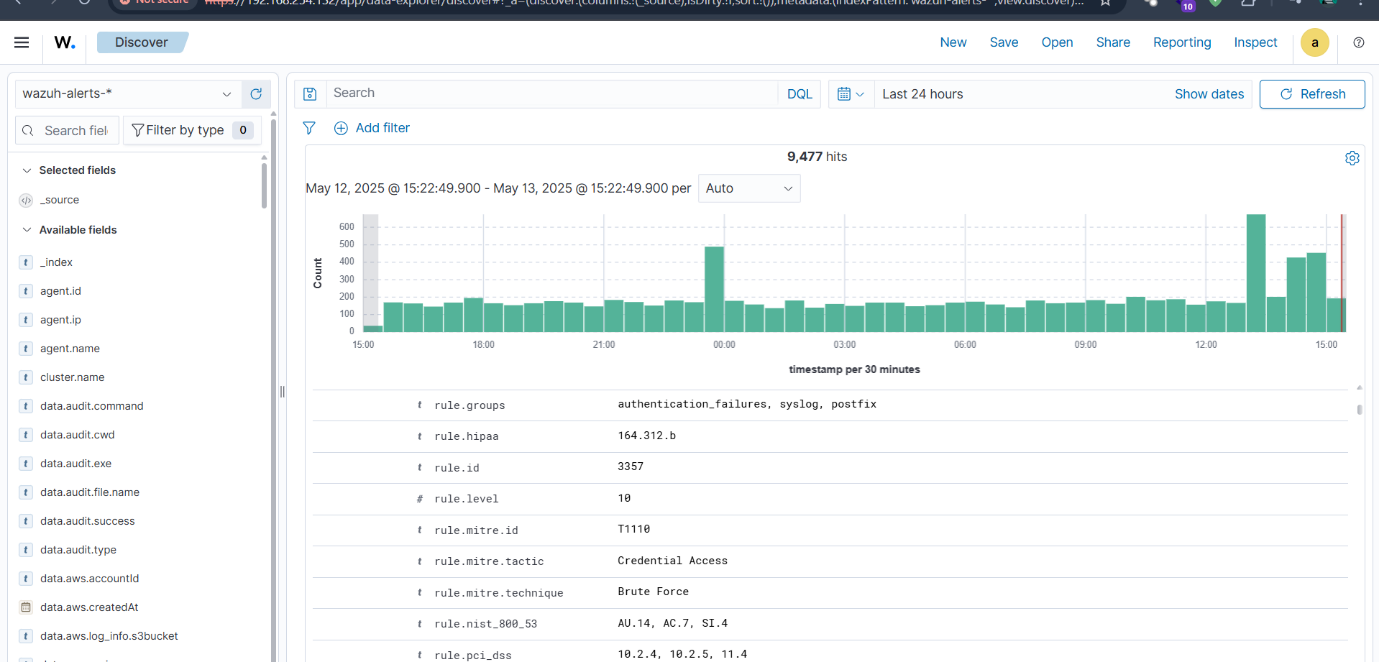
Download xml file in syslog folder

Use this Commad in powershell

sysmon.exe -accepteula -i sysmonconfig.xml

if Fasing error

Set-ExecutionPolicy Unrestricted after retry sysmon.exe -accepteula -i sysmonconfig.xml



**What is SIEM And Why is Matters?**

**Define SIEM (Security Information and Event Management)**.

**SIEM Fundamentals**

A **SIEM (Security Information and Event Management)** system is a vital security tool that provides a comprehensive view of an organization's security posture. It achieves this by collecting and aggregating log data from diverse sources like network devices, servers, and applications. Key functions include normalizing this data into a common format, correlating events to identify potential threats, generating alerts for critical incidents, and offering reporting and dashboard capabilities.

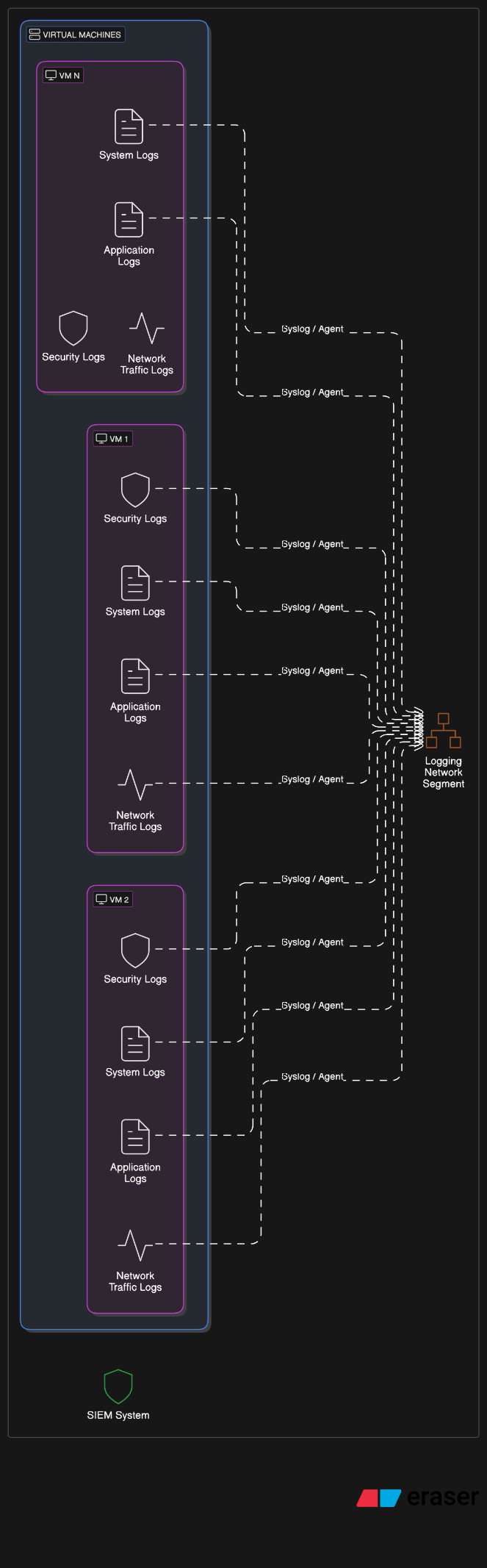
In the real world, SIEMs are crucial for:

* **Log Collection**: Centralizing logs from numerous sources for monitoring and forensic analysis.
* **Alerting**: Automatically notifying security teams about suspicious activities, like multiple failed logins, enabling rapid response.
* **Correlation**: Linking seemingly unrelated events to uncover complex attack patterns, such as an advanced persistent threat (APT) moving through different stages of an attack.

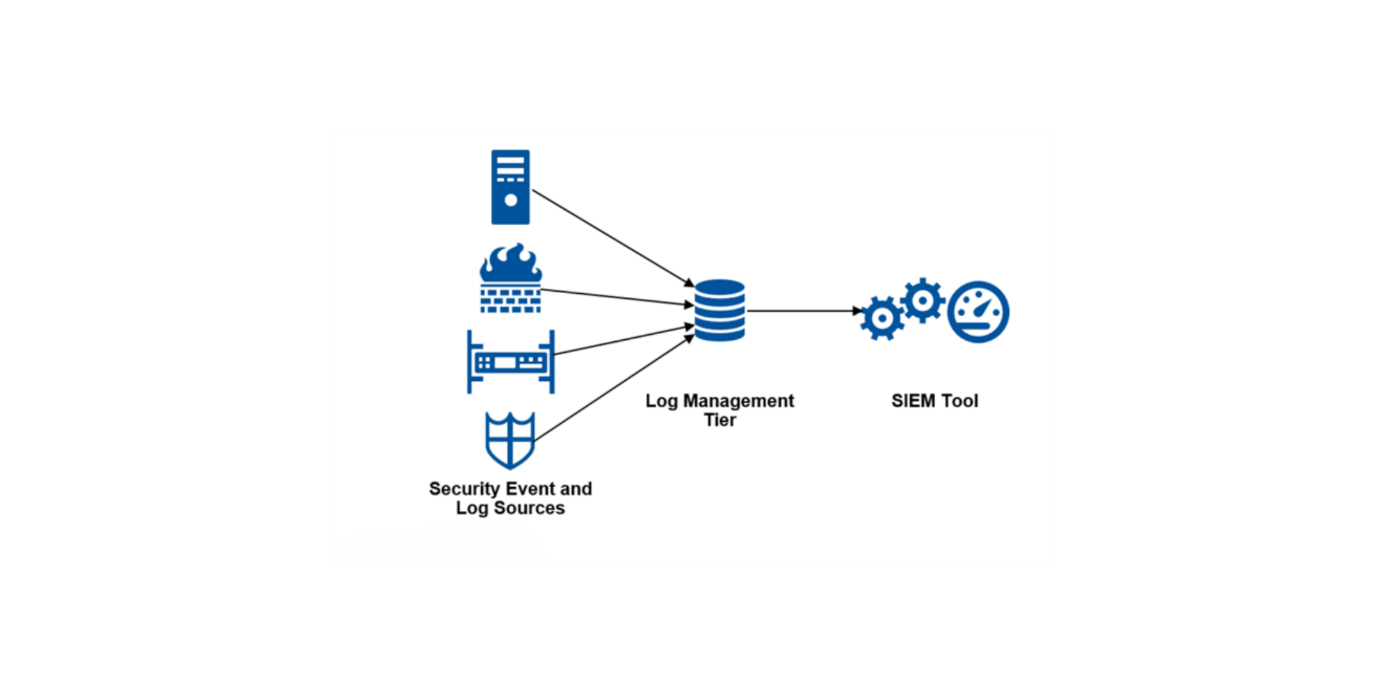
Critically, SIEMs play a significant role in detecting the early stages of cyber attacks. By monitoring for initial compromise indicators (e.g., phishing link clicks, malware execution) and subsequent activities like an attacker establishing a foothold or attempting privilege escalation, a SIEM helps organizations intervene before major damage occurs. This proactive detection is key to modern cybersecurity defense.

\***Lab Setup :**

Use Tool vmware ubuntu os deploy Wazuh sever and windows 10 as a agent and Syslog are share logs in wazuh server As SIEM



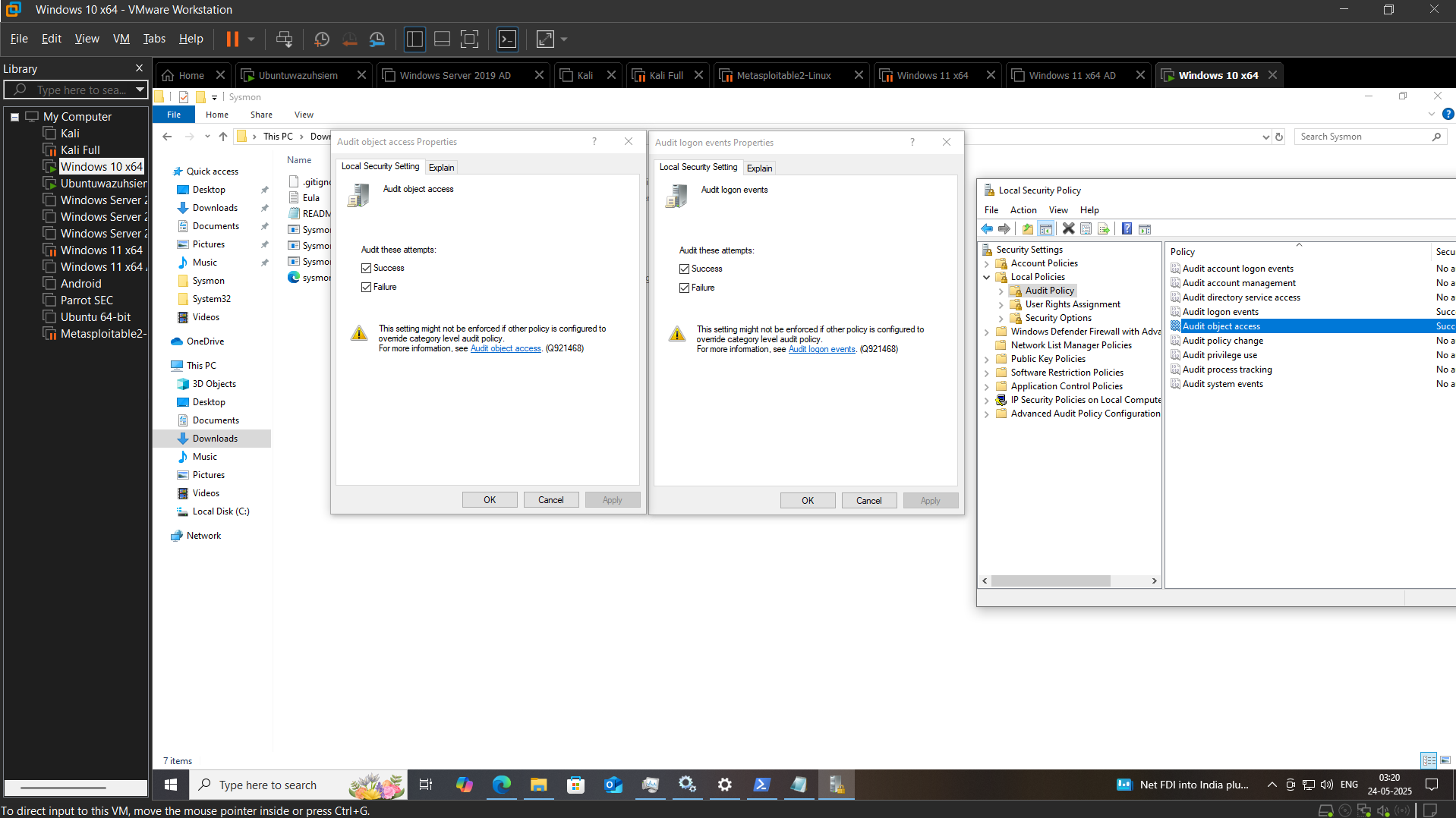




**\*Log Source Configration**

**Enable Auditing and Install Sysmon**

* **Enable Auditing**:
  + Open the **Local Security Policy** (windows+r secpol.msc).
  + Navigate to **Local Policies > Audit Policy**.



winlogbeat https://www.elastic.co/downloads/beats/winlogbeat

**Configure Winlogbeat**

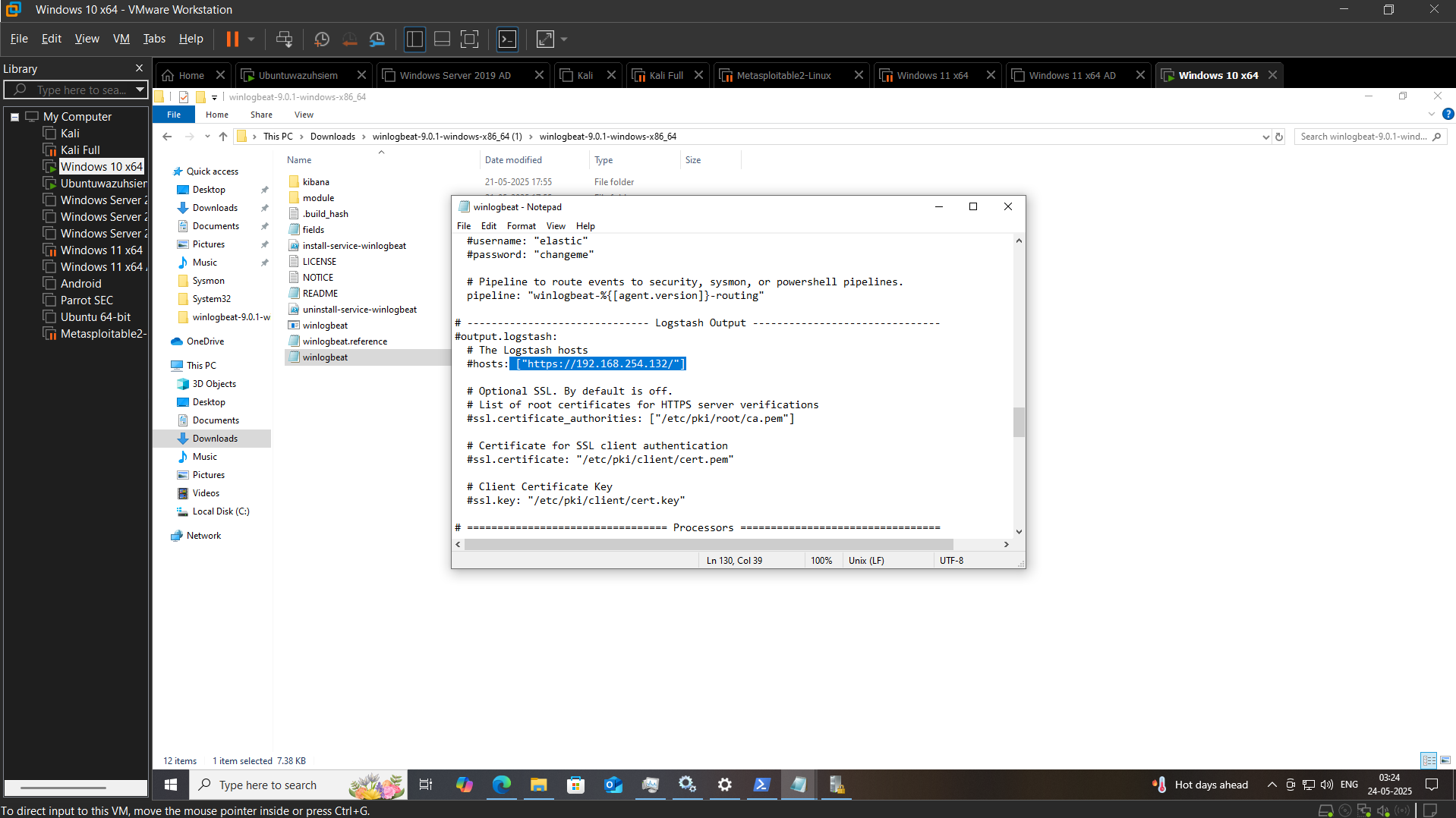
* + Open the **winlogbeat.yml** configuration file in a text editor.

1. **Start Winlogbeat**

Start-Service winlogbeat

1. **Verify Winlogbeat is Running**

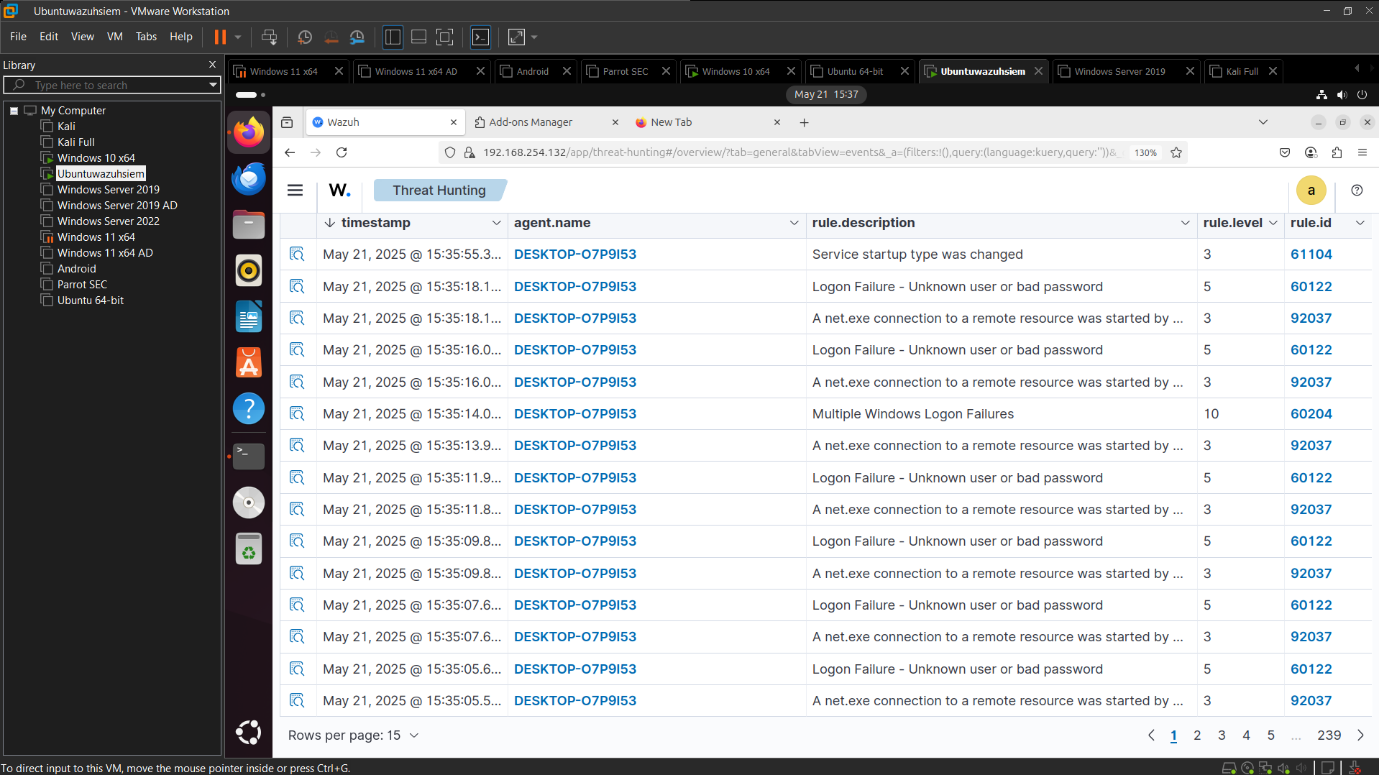
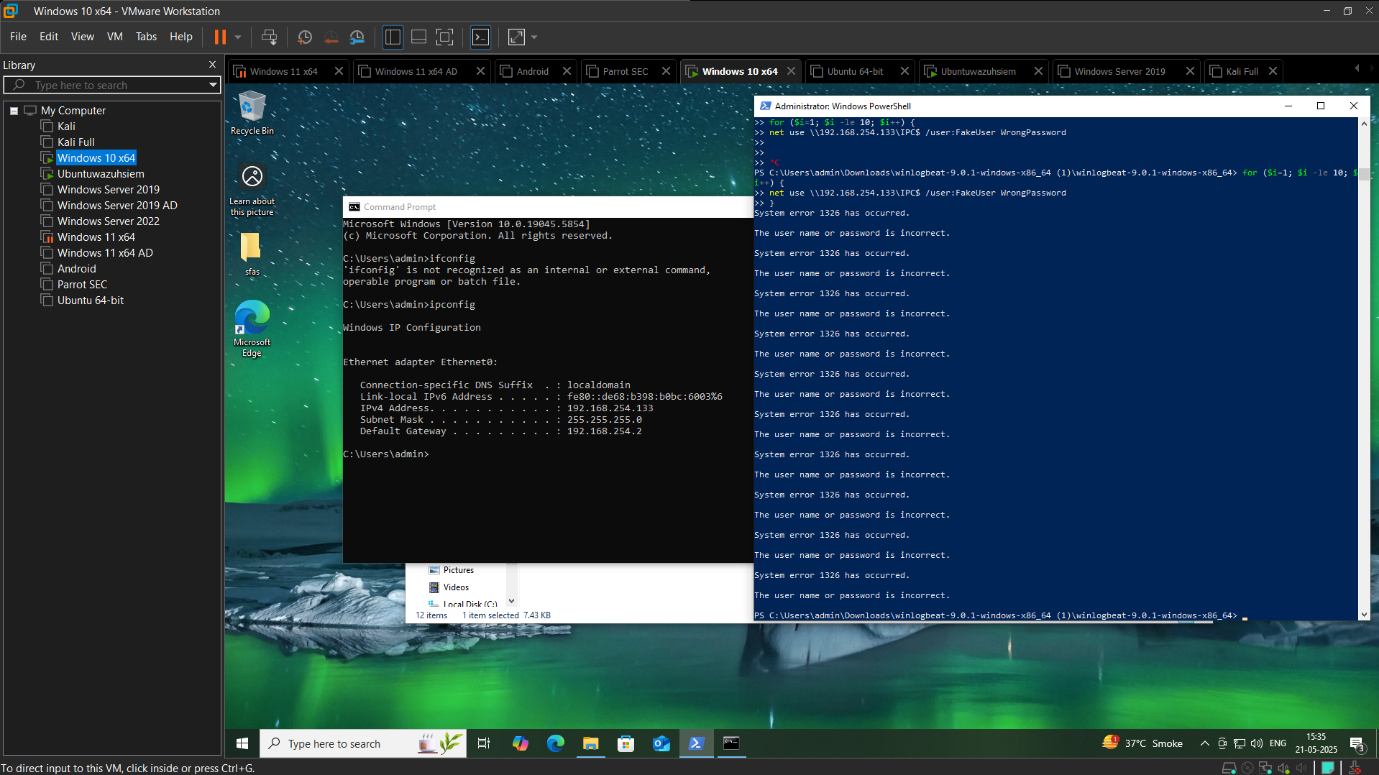
Get-Service winlogbeat



**\*Detection Use case 1 -Brute force**

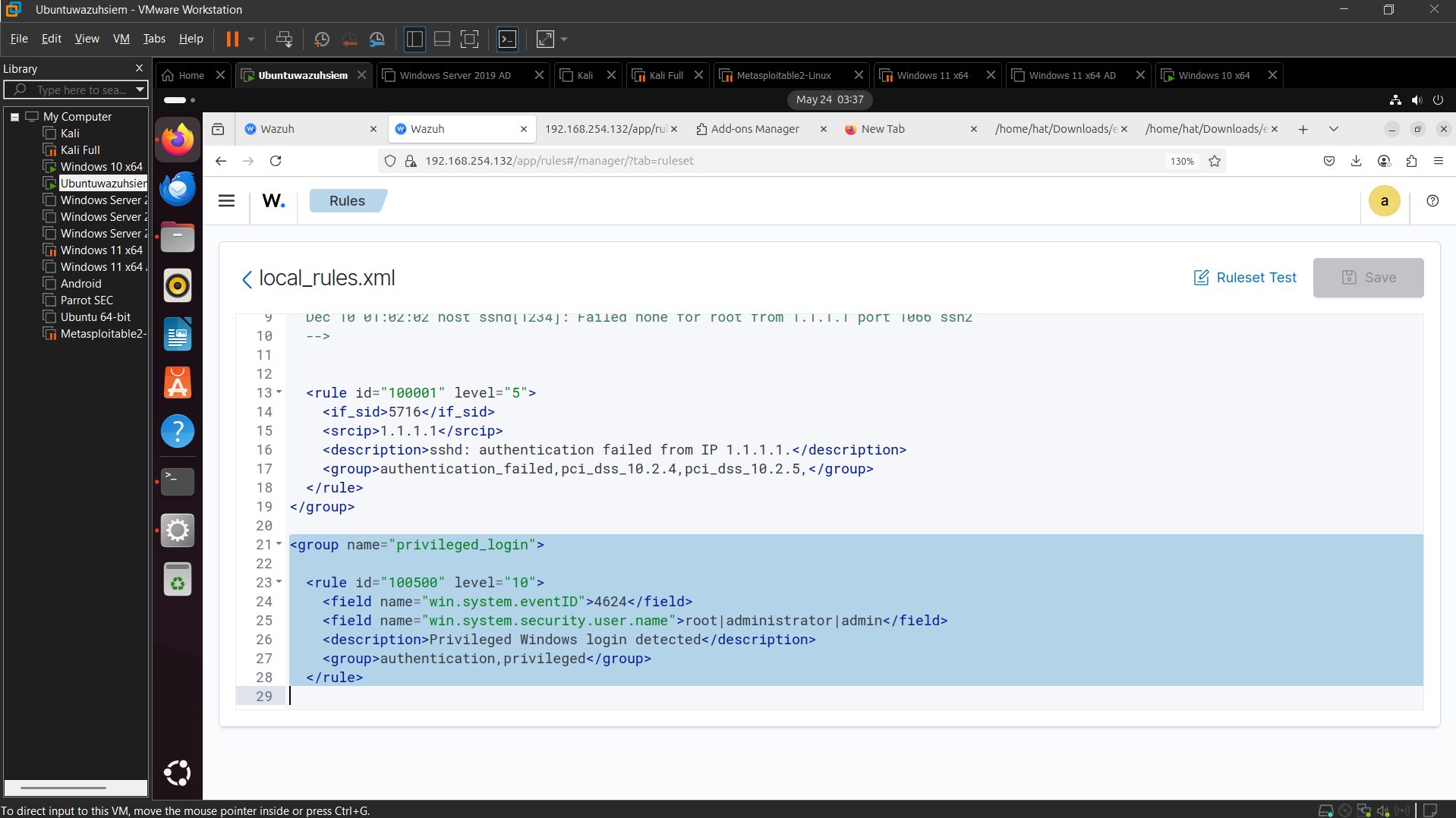
**Event IDs Involved:**

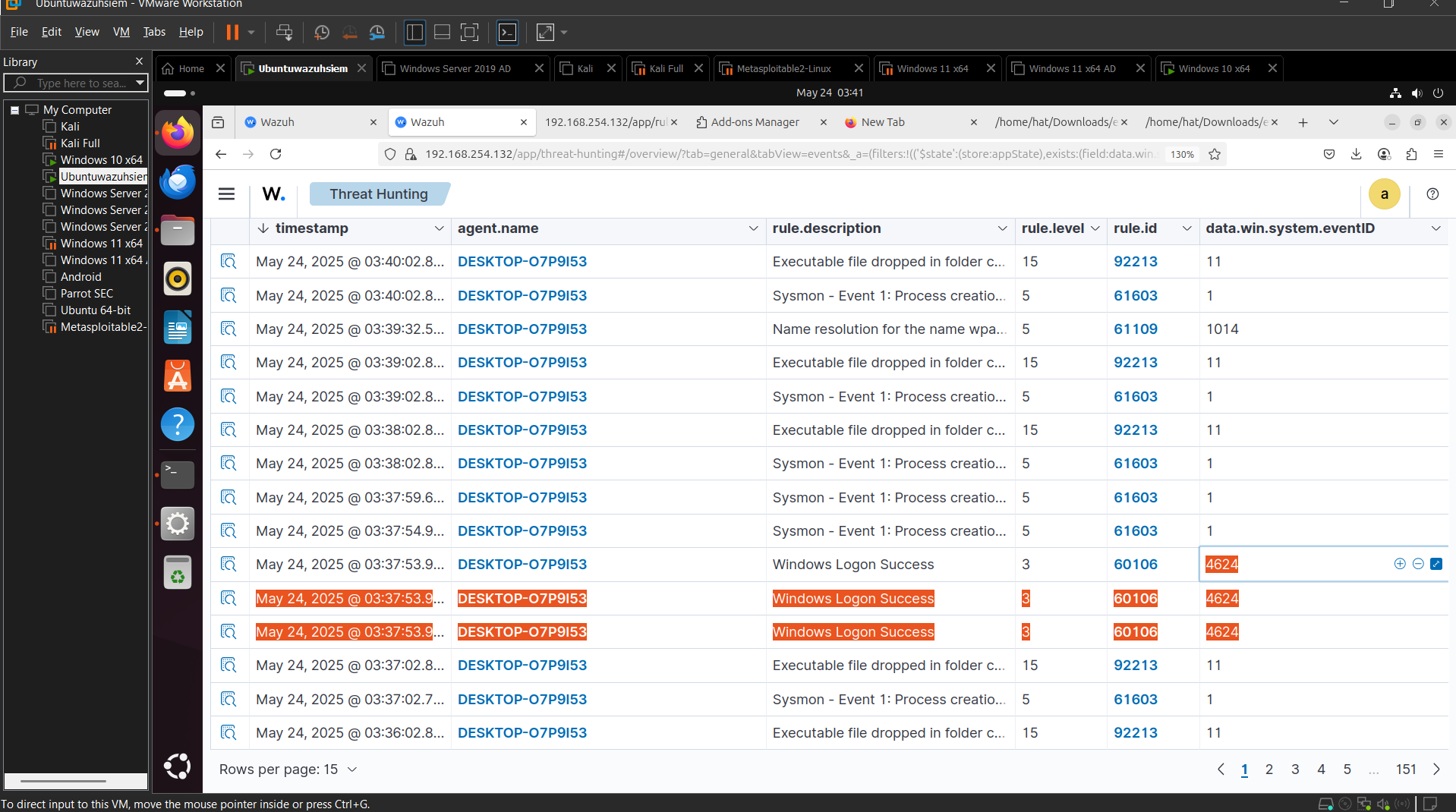
* **4625**: Failed login attempt
* **6624**: Security group management event



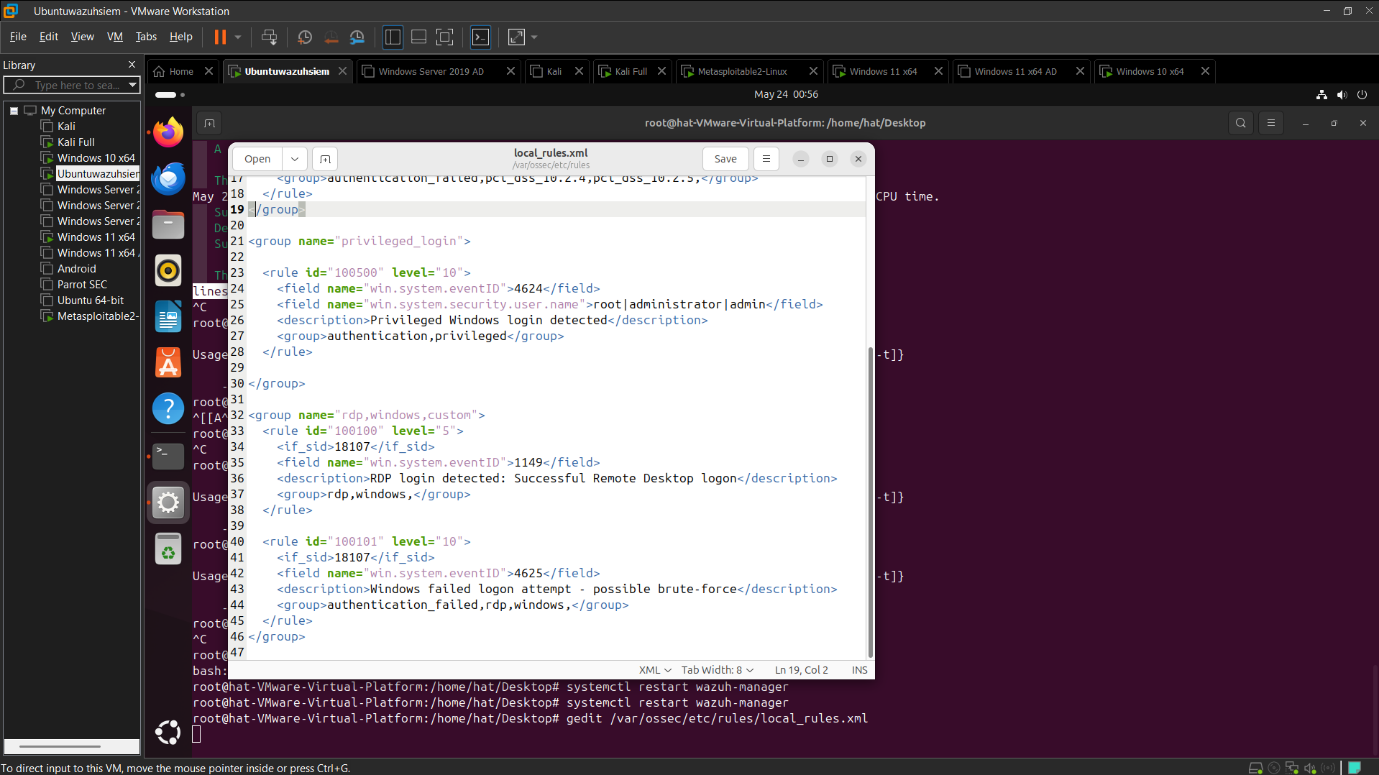
\*Detection Use case 2 After-hour login

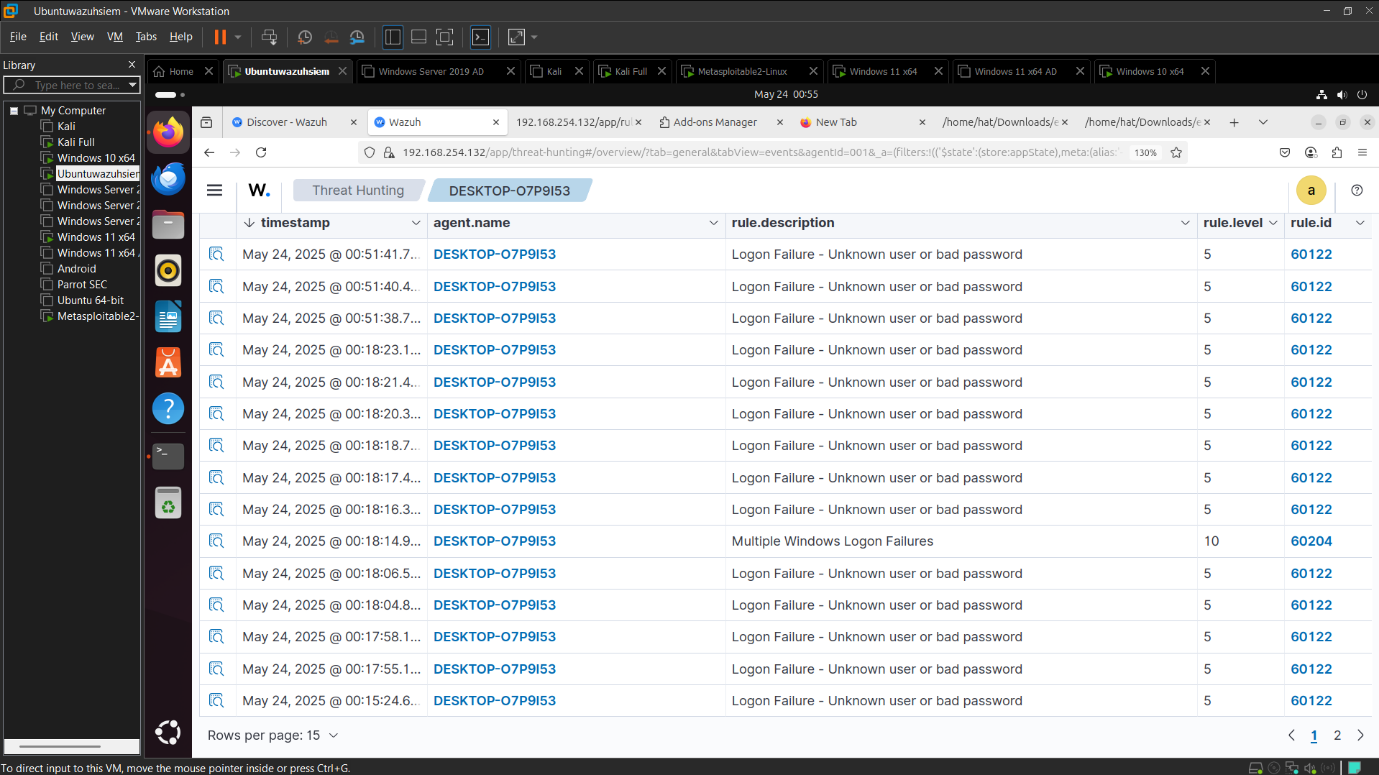
Bussiness hour 9 Am To 7 Pm

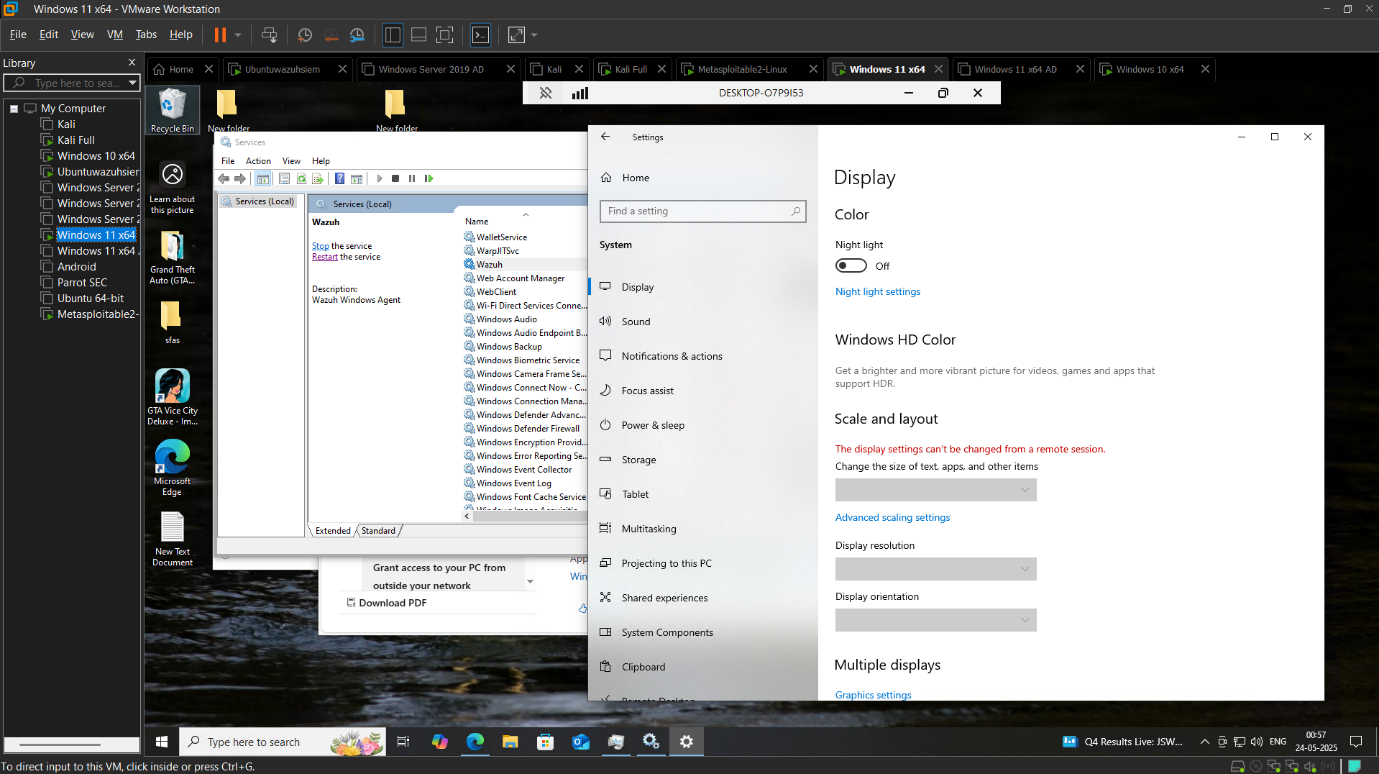




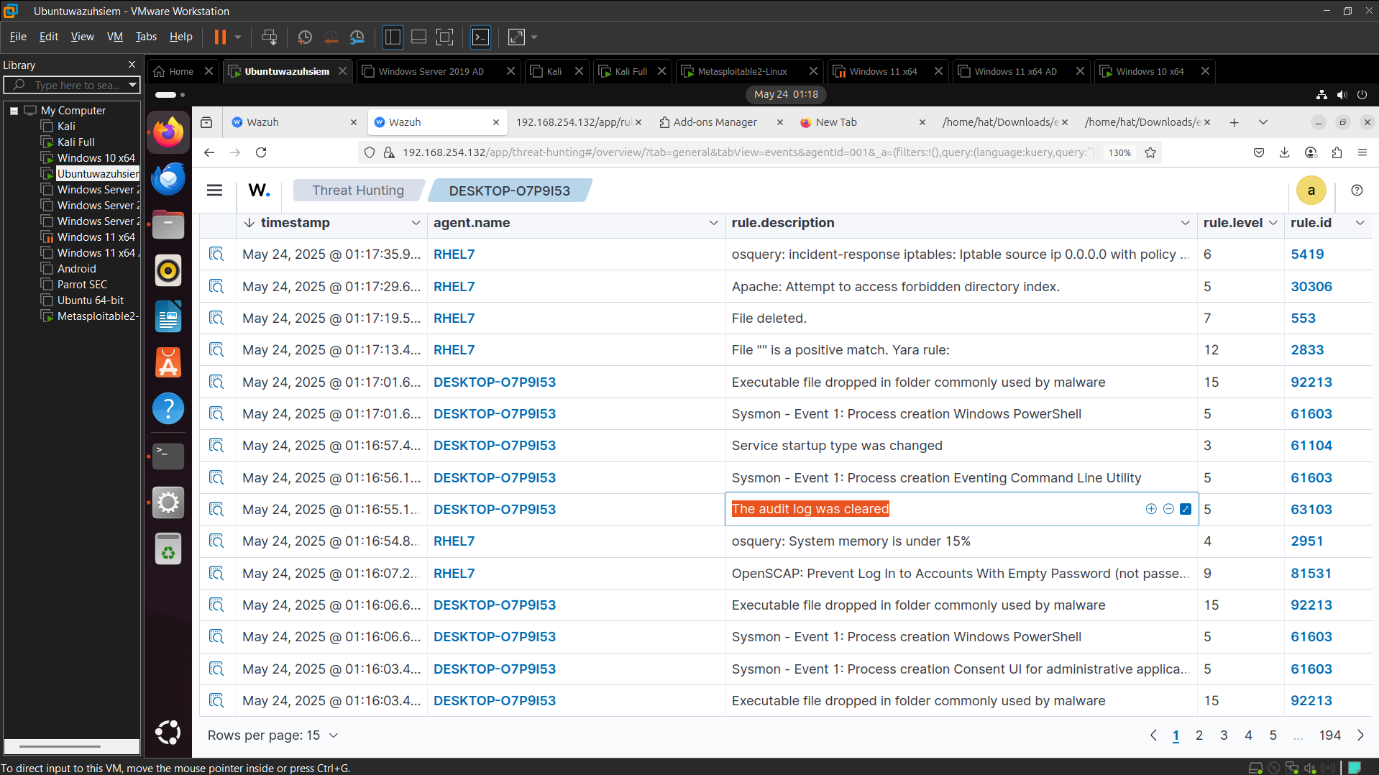
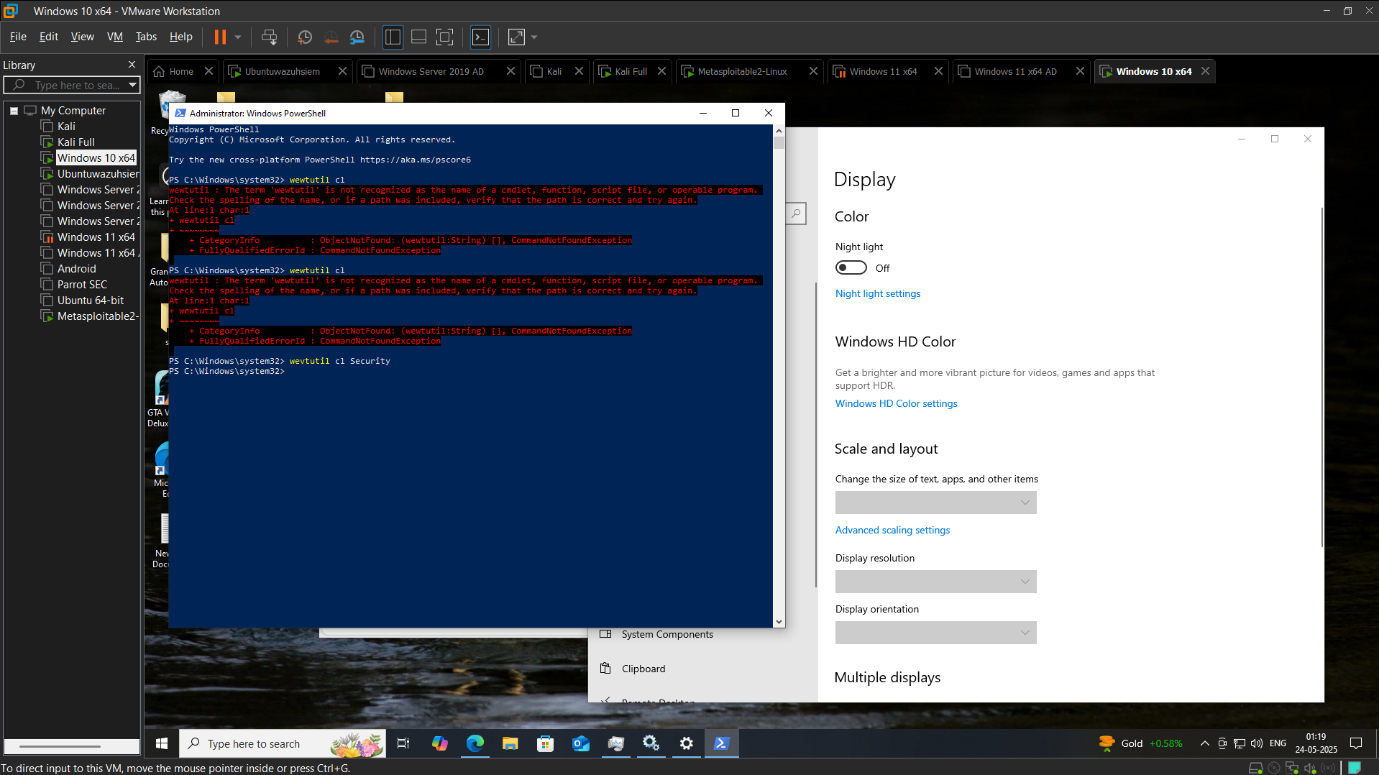
Detection Use Case 3 – RDP Lateral Movement







Detection Use case 4 Log Tampering



**Reflection Questions Evaulations**

Reflections & Evulautions Qiestions

**1. What is the role of SIEM in modern cybersecurity?**

SIEM (Security Information and Event Management) plays a central role in detecting and responding to security threats. It collects, correlates, and analyzes logs from various systems to identify unusual behavior, generate alerts, and help analysts investigate incidents. Without SIEM, it would be nearly impossible to sift through the vast amount of security data organizations generate every day.

**2. What challenges did you face while setting up your lab?**

One of the biggest challenges was getting Wazuh to start properly. I encountered a configuration error due to incorrectly formatted rules in the local\_rules.xml file. It took a bit of trial and error to understand that all rules must be inside a <group> tag. Also, figuring out how to pull specific event logs from Windows and send them to Wazuh took some extra research.

**3. What are the differences between Sysmon logs and Windows Security logs?**

Sysmon logs give more detailed, low-level visibility into what’s happening on a system, like process creation, network connections, and file changes. In contrast, Windows Security logs focus more on high-level user actions like logins, policy changes, or failed login attempts. Both are useful, but Sysmon is often better for detecting stealthy attacks like lateral movement or privilege escalation.

**4. How does a brute force attack appear in logs? Mention specific Event IDs.**

A brute force attack usually shows up as a series of **Event ID 4625** entries (failed logon attempts) in the Windows Security log. If the attacker succeeds, you may also see an **Event ID 4624** (successful logon) shortly after. A large number of 4625s from the same IP or targeting the same account is a red flag.

**5. How would you detect a login outside normal business hours?**

You can detect off-hours logins by correlating **Event ID 4624** (successful logons) with time-of-day logic in your SIEM. For example, setting a rule that flags logons outside of 9 AM – 7 PM. You could also compare logons against a known baseline of user behavior to detect anomalies.

**6. Describe how RDP lateral movement is tracked in event logs.**

RDP lateral movement can be seen through a combination of events. **Event ID 1149** shows a successful RDP connection. You might also see **Event IDs 4624** (logon), **4778** (reconnect), or **4779** (disconnect). By mapping the source and destination IPs along with the user accounts, you can trace RDP use across systems.

**7. What is the risk of log tampering, and how can we detect it?**

Log tampering is when an attacker tries to erase or alter logs to hide their tracks. This is dangerous because it can blind defenders to an ongoing or past breach. We can detect it by monitoring for Event IDs like **1102** (log cleared), using file integrity monitoring (FIM), or comparing expected log volume to actual logs. SIEMs like Wazuh can alert us when logs are suddenly missing or altered.

**8. What improvements would you make in your lab setup if given more time?**

If I had more time, I would automate more of the Wazuh agent deployment and expand logging to include Sysmon. I’d also fine-tune my rules and maybe integrate email or Slack alerts for real-time notifications. A dashboard with visualizations of failed logons and RDP activity would make monitoring much easier too.

**9. How will this phase help you in real-world interviews or jobs?**

It gave me hands-on experience with a real SIEM, which is something employers often ask about. I now understand how to configure log collection, write detection rules, and troubleshoot issues. More importantly, I learned how to approach a problem methodically, which is crucial in any security job.

**10. What was your biggest takeaway from Phase 1?**

My biggest takeaway was realizing how much visibility logs can give into system activity — if you know what to look for. Learning to detect real-world threats like brute force attacks or RDP lateral movement using logs felt empowering. It showed me how defenders use tools like Wazuh to stay one step ahead of attackers.