Splunk and Wazuh SIEM Setup, Configuration, and Testing Documentation

Salamova Gunel

# Introduction

This documentation details the setup, configuration, and testing of two SIEM toolsSplunk En- terprise (community edition) and Wazuhon an Ubuntu server, along with the deployment of their respective agents on Windows 10 and Kali Linux target machines. It also covers the sim- ulation of brute-force attacks on these targets using a Kali Linux attacker machine, with the resulting logs captured and analyzed by both Splunk and Wazuh instances, each configured on separate snapshots of the Ubuntu server.

# 2 Lab Setup

The lab environment was configured as follows:

• SIEM Server: Ubuntu Server with two network interfaces:

– NAT interface: 192.168.19.137 (for internet access)

– Host-only interface: 192.168.254.129 (gateway for internal network)

• Target 1: Windows 10 (192.168.254.150) with vulnerable services enabled:

– SMBv1

– LLMNR

– SSH (OpenSSH Server)

– RDP

• Target 2: Kali Linux (192.168.254.140) with vulnerable services enabled:

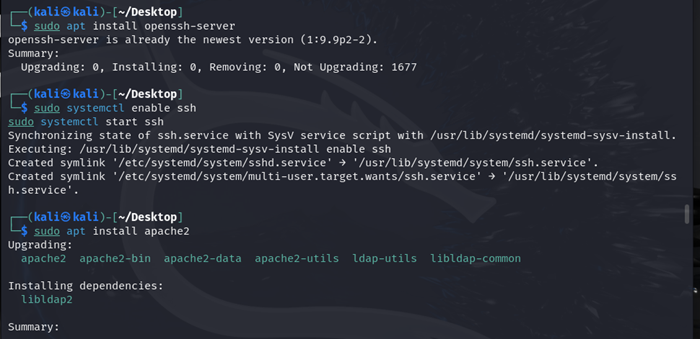
– SSH

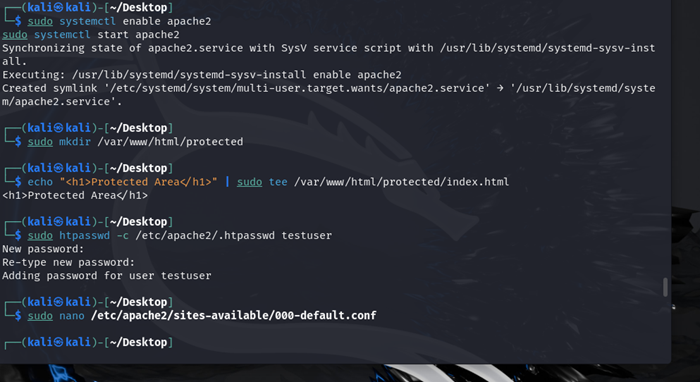
– FTP (vsftpd)

– Apache2

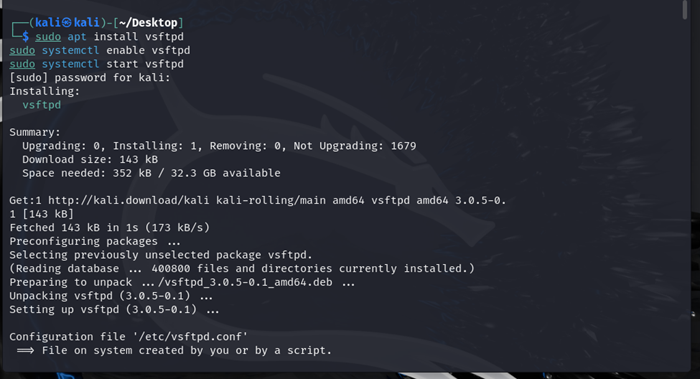
• Attacker: Kali Linux (192.168.254.130)

All machines were connected to the same internal network (192.168.254.0/24), with the Ubuntu









server acting as the gateway for internet access. Splunk and Wazuh were installed on separate

snapshots to ensure isolation.

# Splunk SIEM Setup on Ubuntu Server

The Splunk SIEM was installed on an Ubuntu server snapshot with the IP address 192.168.254.129 (host-only interface) and 192.168.19.137 (NAT interface for internet access). The following steps were performed:

## Step 1: Download Splunk Enterprise

* Accessed the Splunk website ([https://www.splunk.com/en\_us/download/splunk-enterpr](https://www.splunk.com/en_us/download/splunk-enterprise.html) [html](https://www.splunk.com/en_us/download/splunk-enterprise.html)) and registered for a free community edition account. - Downloaded the Splunk Enter-

prise package for Linux (64-bit .tgz file) using wget:

wget -O splunk-9.2.1-78803dd9f5ec-Linux-x86\_64.tgz \ "https://download.splunk.com/products/splunk/releases/9.2.1/linux/splun

## Step 2: Install Splunk

* Extracted the downloaded .tgz file to the /opt directory:

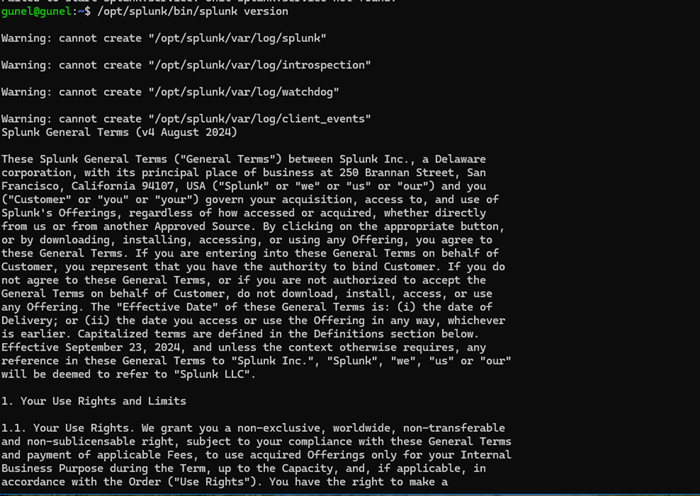
sudo tar -xvzf splunk-9.2.1-78803dd9f5ec-Linux-x86\_64.tgz -C /opt

* This created the directory /opt/splunk.

## Step 3: Start Splunk and Set Admin Credentials

* Navigated to the Splunk bin directory and started Splunk:

cd /opt/splunk/bin sudo ./splunk start



* During the first startup, accepted the license agreement and set an admin username and pass- word:
  + Username: splunk
  + Password: salam123
* Splunk started and listened on port 8000 for the web interface.

## Step 4: Enable Splunk to Start on Boot

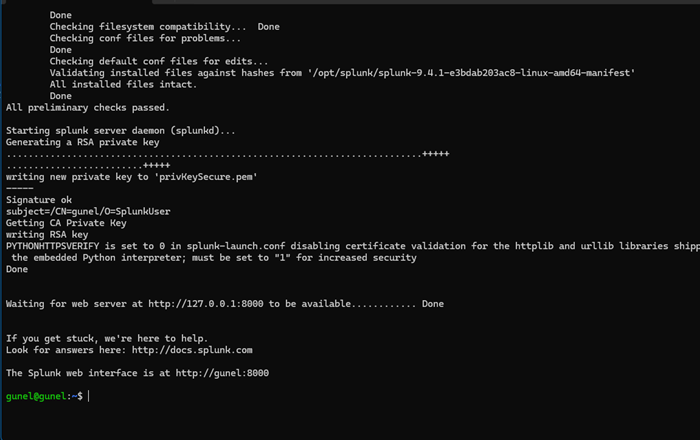
* Configured Splunk to start automatically on system boot:

sudo /opt/splunk/bin/splunk enable boot-start

## Step 5: Access the Splunk Web Interface

* Opened a web browser on a machine with access to the Ubuntu server and navigated to:

[http://192.168.254.129:8000](http://192.168.254.129:8000/)



* Logged in using the admin credentials set earlier. - Verified that the Splunk dashboard was accessible and ready for configuration.

## Step 6: Configure Receiving Port for Forwarders

* In the Splunk web interface, navigated to Settings > Forwarding and Receiving.
* Configured a new receiving port to accept data from forwarders:
  + Port: 9997
  + Protocol: TCP
* Saved the configuration to allow Splunk to receive logs from forwarder agents.

# Splunk Forwarder Agent Setup on Target Machines

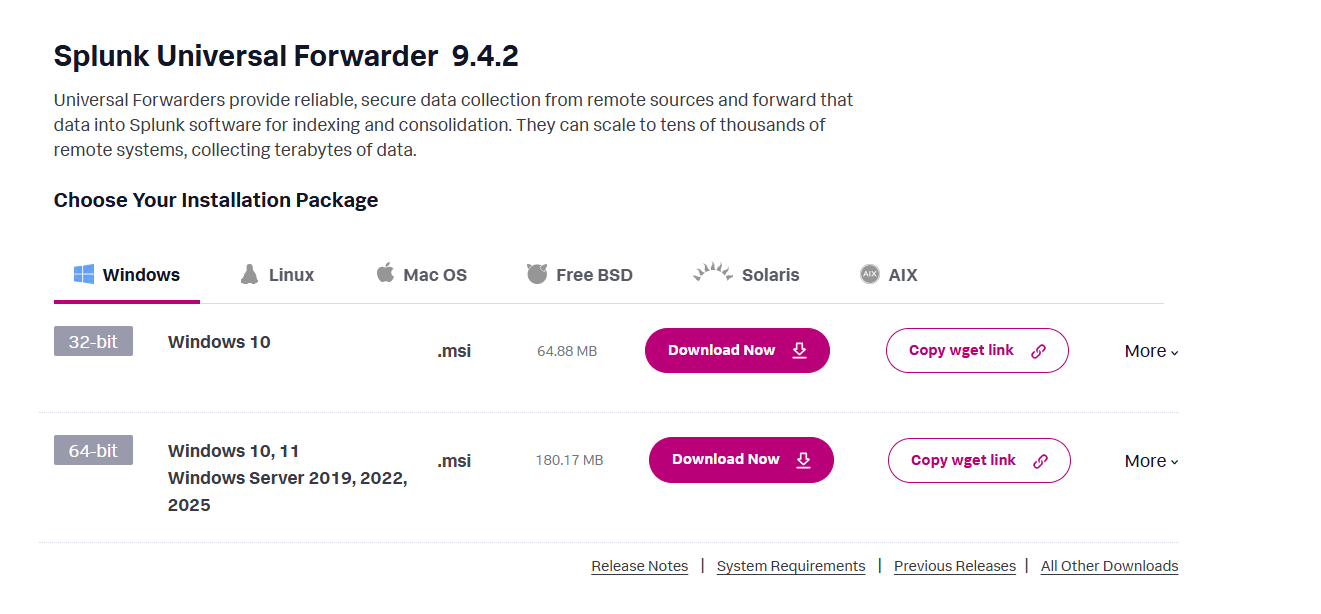
Splunk forwarder agents were installed on the Windows 10 (192.168.254.150) and Kali Linux (192.168.254.140) target machines to send logs to the Splunk SIEM instance.

## Windows 10 Target (192.168.254.150)

### Step 1: Download Splunk Universal Forwarder

* + - * On the Windows 10 machine, downloaded the Splunk Universal Forwarder for Windows (64- bit .msi file) from the Splunk website:

https://download.splunk.com/products/universalforwarder/releases/9.2.1/



### Step 2: Install the Forwarder

* + - * Double-clicked the .msi file to start the installation wizard. - Accepted the license agreement and proceeded with the default installation path: C:Files. - During installation, configured the forwarder to connect to the Splunk SIEM instance:
        + Receiving indexer: 192.168.254.129
        + Port: 9997
      * Set a local admin username and password for the forwarder service (e.g., Username: splunk, Password: salam123).

### Step 3: Configure Inputs for Windows Event Logs

* + - * Navigated to the forwarders configuration directory:

C:\Program Files\SplunkUniversalForwarder\etc\system\local

* + - * Edited the inputs.conf file (or created it if it didnt exist) to monitor Windows Security Event Logs:

[WinEventLog://Security] disabled = 0

index = main

sourcetype = WinEventLog:Security

* + - * This configuration ensured that security-related logs, such as failed login attempts, were sent to Splunk.

### Step 4: Start the Forwarder

* + - * Started the Splunk forwarder service:

"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" start

* + - * Verified that the forwarder was running and sending data by checking the Splunk web interface for incoming logs from the Windows 10 machine.

## Kali Linux Target (192.168.254.140)

### Step 1: Download Splunk Universal Forwarder

* + - * On the Kali Linux target, downloaded the Splunk Universal Forwarder for Linux (64-bit .tgz file):

wget -O splunkforwarder-9.2.1-78803dd9f5ec-Linux-x86\_64.tgz \ "https://download.splunk.com/products/universalforwarder/releases/9.2.1

### Step 2: Install the Forwarder

* + - * Extracted the .tgz file to /opt:

sudo tar -xvzf splunkforwarder-9.2.1-78803dd9f5ec-Linux-x86\_64.tgz -C /

* + - * This created the directory /opt/splunkforwarder.

### Step 3: Configure the Forwarder to Send Data

* + - * Navigated to the forwarders bin directory and set the Splunk SIEM instance as the receiver:

cd /opt/splunkforwarder/bin

sudo ./splunk add forward-server 192.168.254.129:9997

* + - * Set the admin credentials for the forwarder:

sudo ./splunk set admin-user admin

* + - * Entered the password (e.g., Splunk@123) when prompted.

### Step 4: Configure Inputs for Syslogs

* + - * Navigated to the forwarders configuration directory:

/opt/splunkforwarder/etc/system/local

* + - * Edited the inputs.conf file to monitor syslogs, including SSH and FTP logs:

[monitor:///var/log/auth.log] disabled = false

index = main

sourcetype = linux\_secure

[monitor:///var/log/vsftpd.log] disabled = false

index = main sourcetype = vsftpd\_log

* + - * This configuration ensured that authentication logs (e.g., SSH failed logins) and FTP logs were sent to Splunk.

### Step 5: Start the Forwarder

* + - * Started the forwarder:

sudo /opt/splunkforwarder/bin/splunk start

* + - * Verified that the forwarder was sending data by checking the Splunk web interface for logs from the Kali Linux machine.

# Wazuh SIEM Setup on Ubuntu Server

Wazuh was installed on a separate snapshot of the Ubuntu server with the IP address 192.168.254.129 (host-only interface) and 192.168.19.137 (NAT interface for internet access) using the assisted installation method. The following steps were performed:

## Step 1: Install Wazuh Server

* Downloaded and ran the Wazuh installation assistant script:

curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh && sudo bash

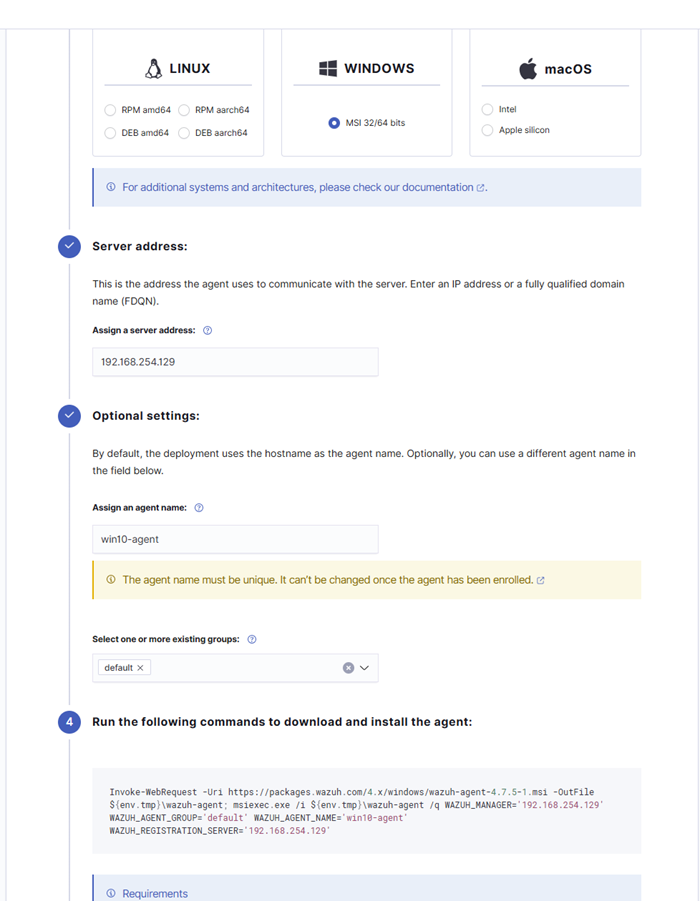
* The script automatically installed and configured the Wazuh manager, indexer, and dashboard on the same host. - After completion, noted the access credentials and IP address provided in the output (e.g., https://192.168.254.129:443, username: admin, password: as displayed). - Accessed the Wazuh dashboard via a web browser at the provided URL and logged in with the credentials.

## Step 2: Verify Installation

- Ensured all services (Wazuh manager, indexer, and dashboard) were running by checking the dashboard interface and verifying the successful setup message.

# Wazuh Agent Setup on Target Machines

Wazuh agents were installed on the Windows 10 (192.168.254.150) and Kali Linux (192.168.254.140) target machines to send logs to the Wazuh manager.



## Windows 10 Target (192.168.254.150)

### Step 1: Download and Install Wazuh Agent

* + - * Downloaded the Wazuh agent for Windows from the Wazuh dashboard under Management

> Agents > Register Agent, using the provided command (e.g., downloading wazuh-agent-4.1 from <https://packages.wazuh.com/4.11/windows/>). - Ran the .msi installer with

administrator privileges and followed the wizard, selecting the default path: C:Files (x86)-agent.

### Step 2: Configure the Wazuh Agent

* + - * Edited the ossec.conf file at C:Files (x86)-agent.conf to specify the Wazuh managers IP:
      * Ensured the agent monitored Windows Security Event Logs by verifying the configuration:

### Step 3: Register and Start the Agent

* + - * Registered the agent using the command provided by the Wazuh dashboard (e.g., "C:Files (x86)-agent-auth.exe" -m 192.168.254.129). - Started the Wazuh agent ser- vice:

net start wazuh

* + - * Verified the agent was connected to the Wazuh manager by checking the Wazuh dashboard under Agents.

## Kali Linux Target (192.168.254.140)

### Step 1: Install Wazuh Agent

* + - * Downloaded and installed the Wazuh agent using the command provided by the Wazuh dash- board (e.g., from [https://packages.wazuh.com/4.7/apt/](https://packages.wazuh.com/4.11/apt/)):

curl -s https://packages.wazuh.com/4.7/apt/pool/main/w/wazuh-agent/waz

### Step 2: Configure the Wazuh Agent

* + - * Edited the ossec.conf file at /var/ossec/etc/ossec.conf to specify the Wazuh managers IP:
      * Ensured the agent monitored syslogs by verifying the configuration:

<localfile>

<log\_format>syslog</log\_format>

<location>/var/log/auth.log</location>

</localfile>

<localfile>

<log\_format>syslog</log\_format>

<location>/var/log/vsftpd.log</location>

</localfile>

### Step 3: Register and Start the Agent

* + - * Registered the agent using the command provided by the Wazuh dashboard (e.g., sudo

/var/ossec/bin/agent-auth -m 192.168.254.129). - Enabled and started the Wazuh agent service:

sudo systemctl enable wazuh-agent sudo systemctl start wazuh-agent

* + - * Verified the agent was connected to the Wazuh manager by checking the Wazuh dashboard under Agents.

# Attack Simulation

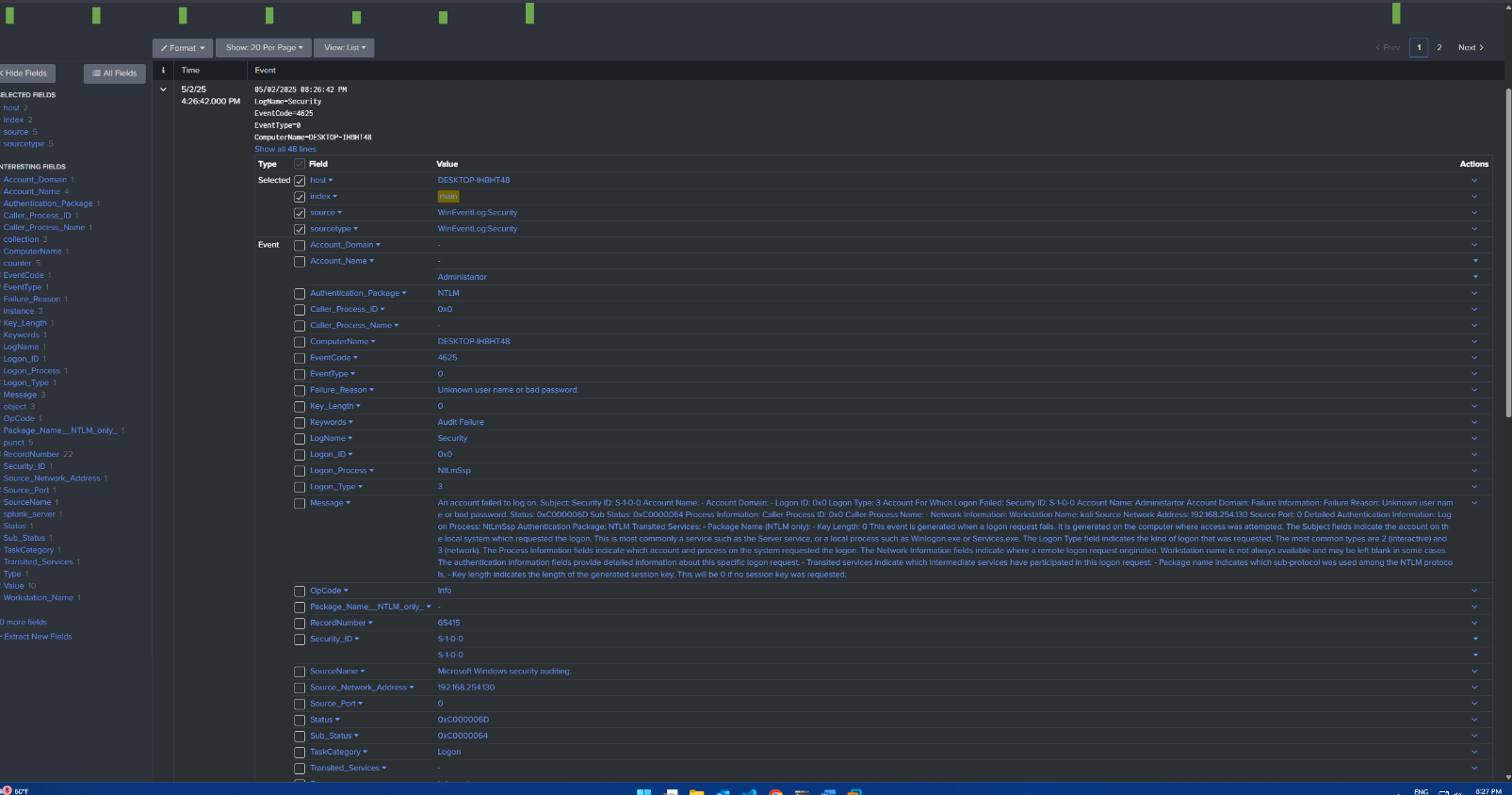
Attacks were conducted from a Kali Linux attacker machine (192.168.254.130) targeting the vulnerable services on the Windows 10 and Kali Linux targets, with logs captured by both Splunk and Wazuh.

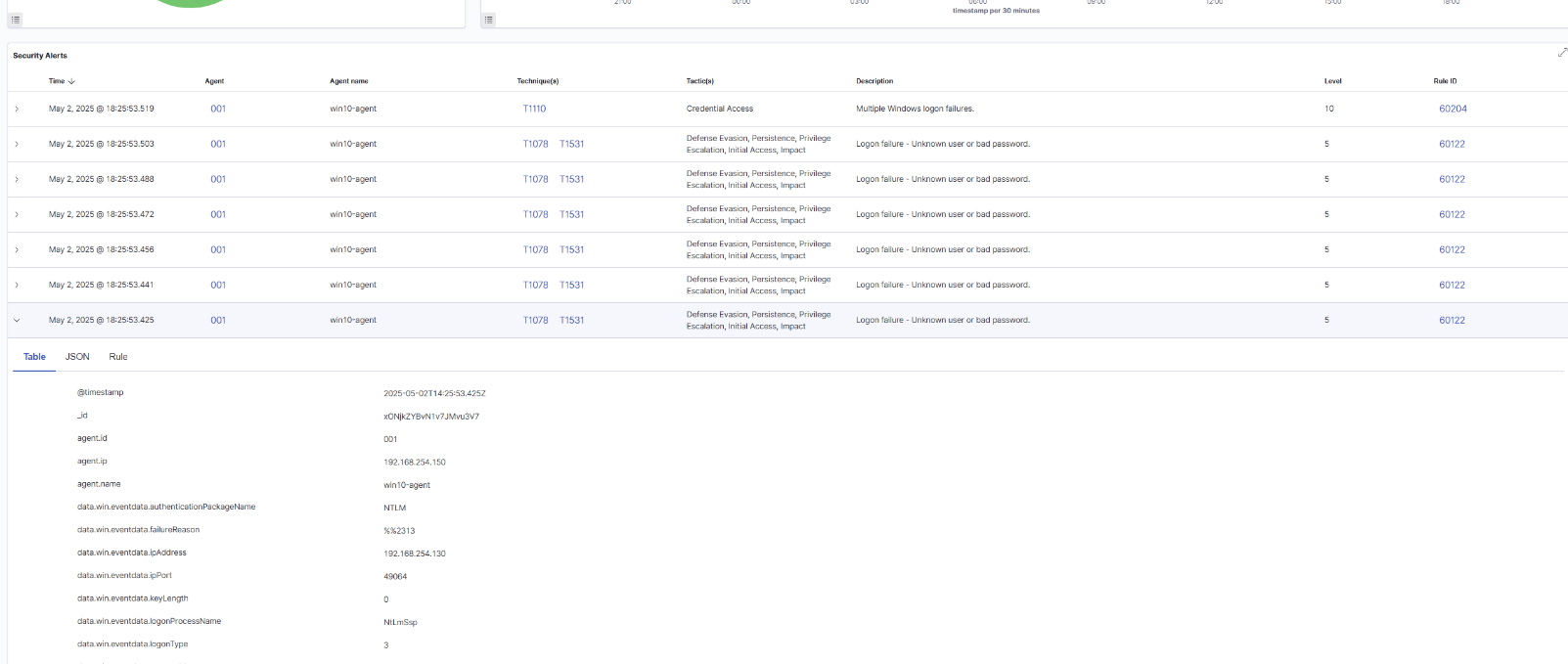
## Windows 10 Target (192.168.254.150)

* Launched a brute-force attack on the SMB service using Hydra with the rockyou.txt

wordlist:

hydra -l Administrator -P /usr/share/wordlists/rockyou.txt smb://192.168.254.150

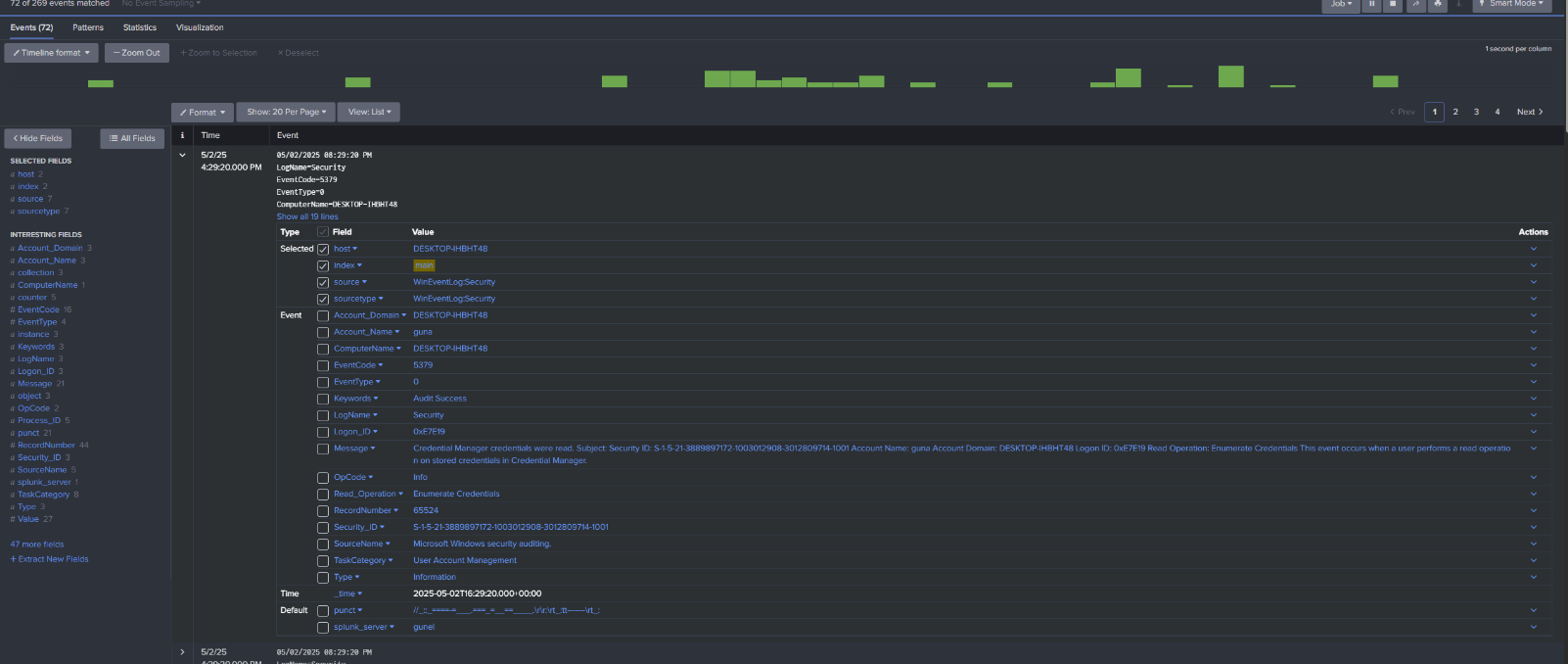




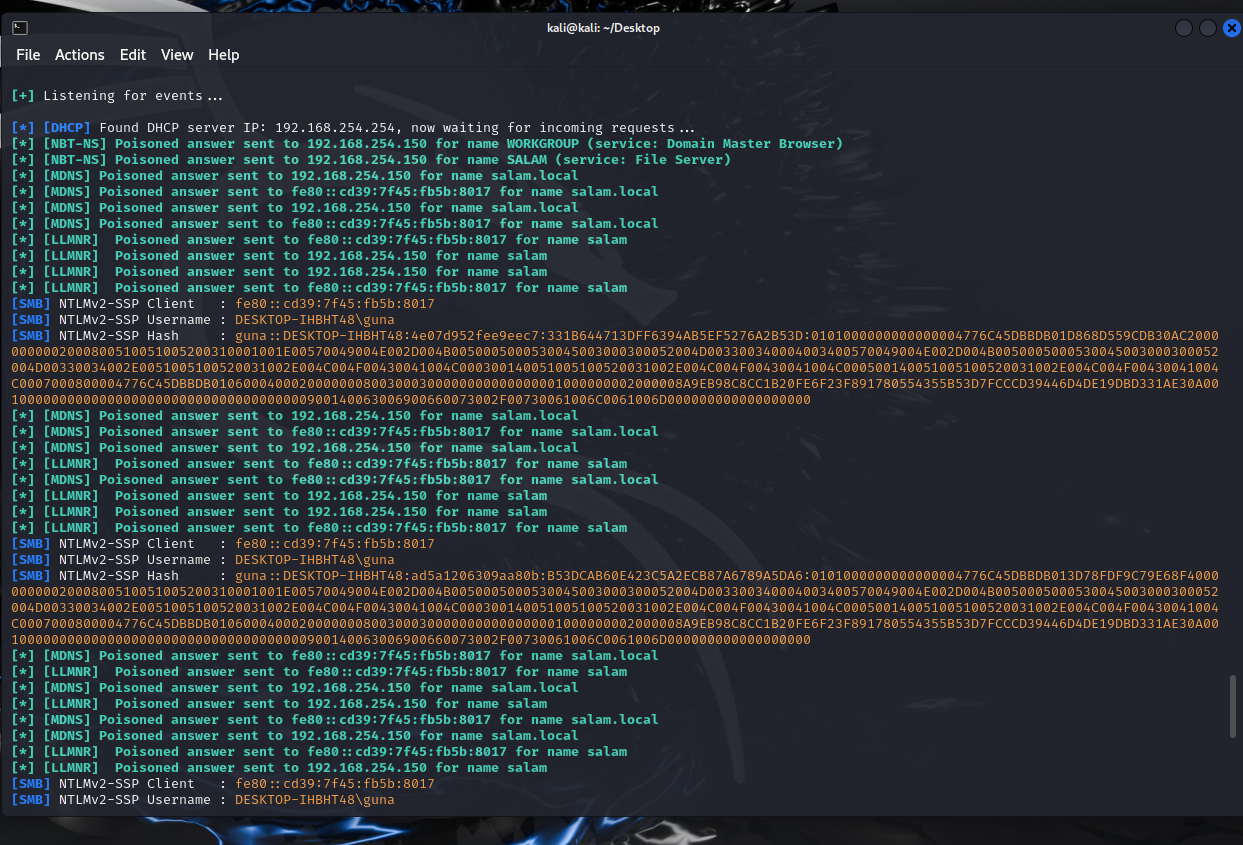
* Performed a brute-force attack on the RDP service using the same wordlist:

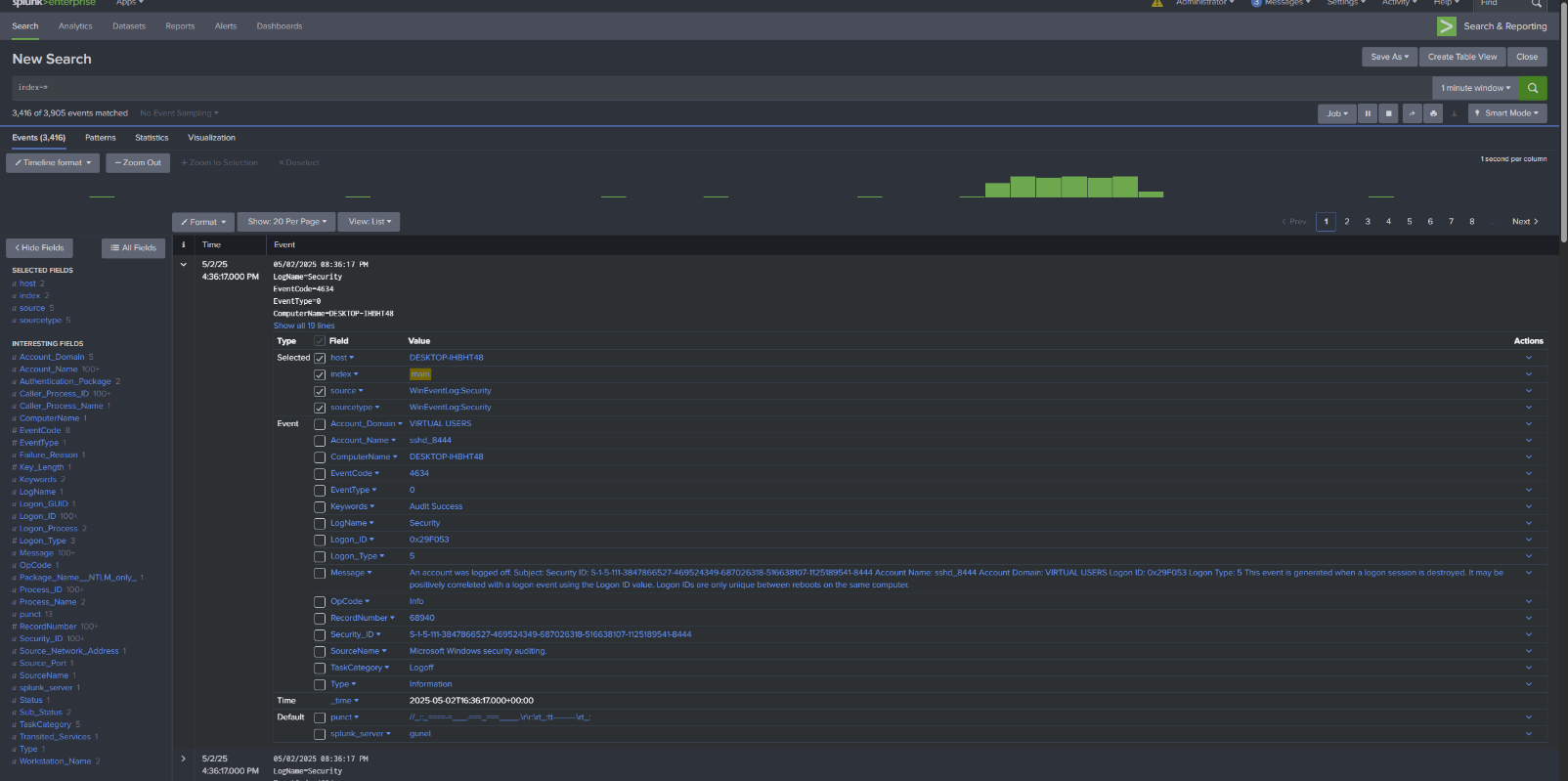
hydra -l Administrator -P /usr/share/wordlists/rockyou.txt rdp://192.168.254.150



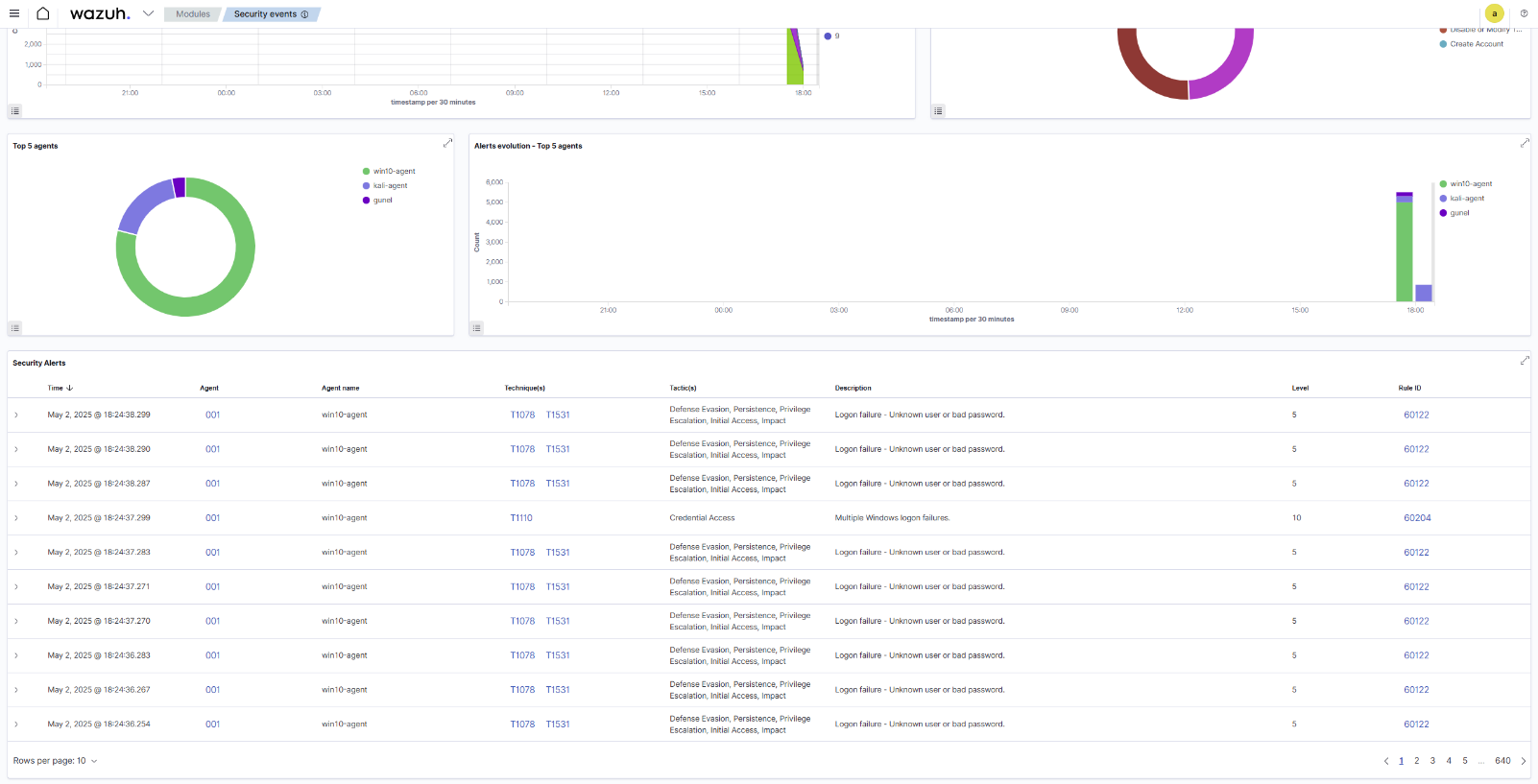


Performed llmnr attack with responder tool





* Performed a brute-force attack on the SSH service using the same wordlist:

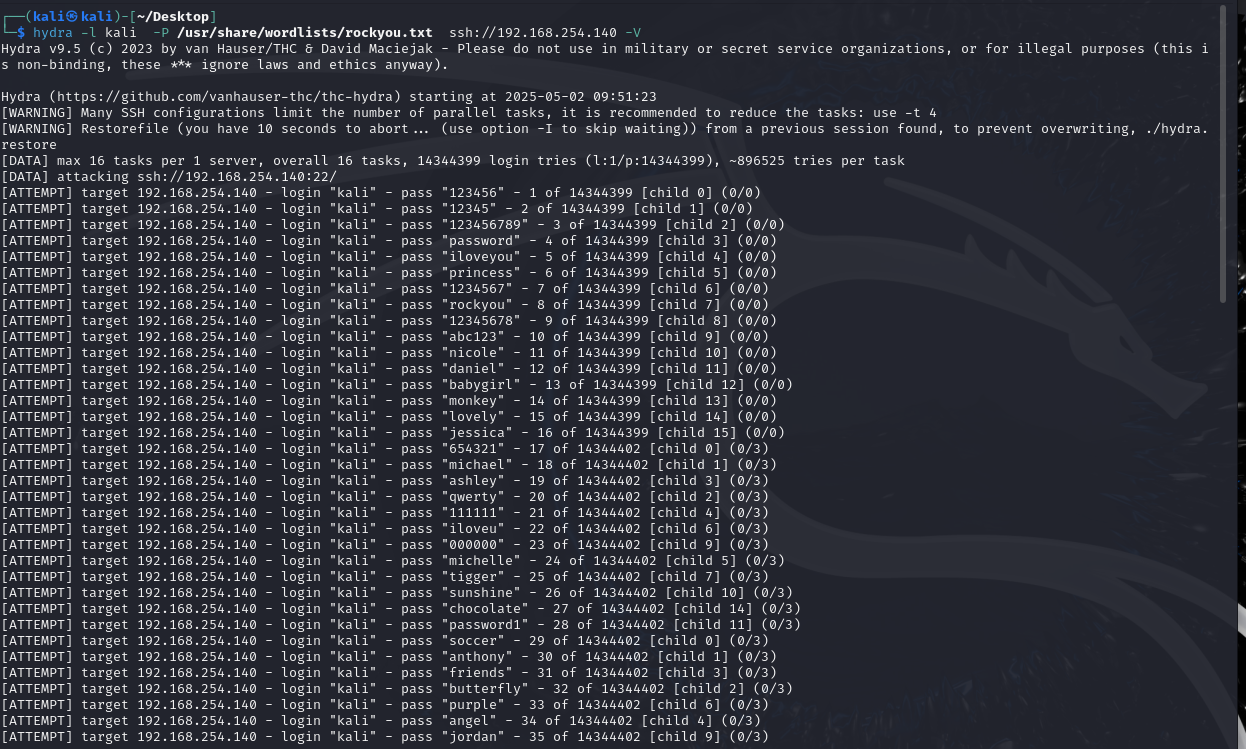
hydra -l Administrator -P /usr/share/wordlists/rockyou.txt ssh://192.168.254.150

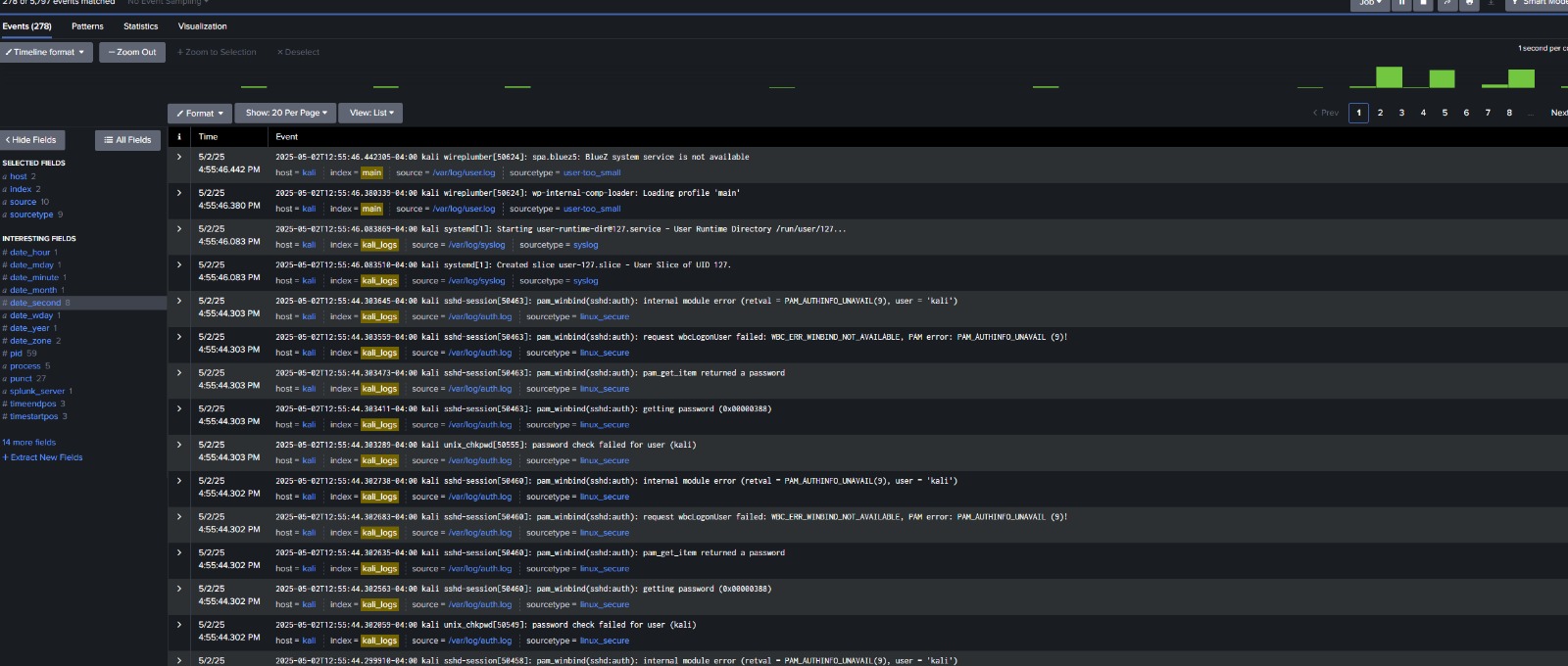
* The attacks generated multiple login attempts, with logs captured by both Splunk and Wazuh.

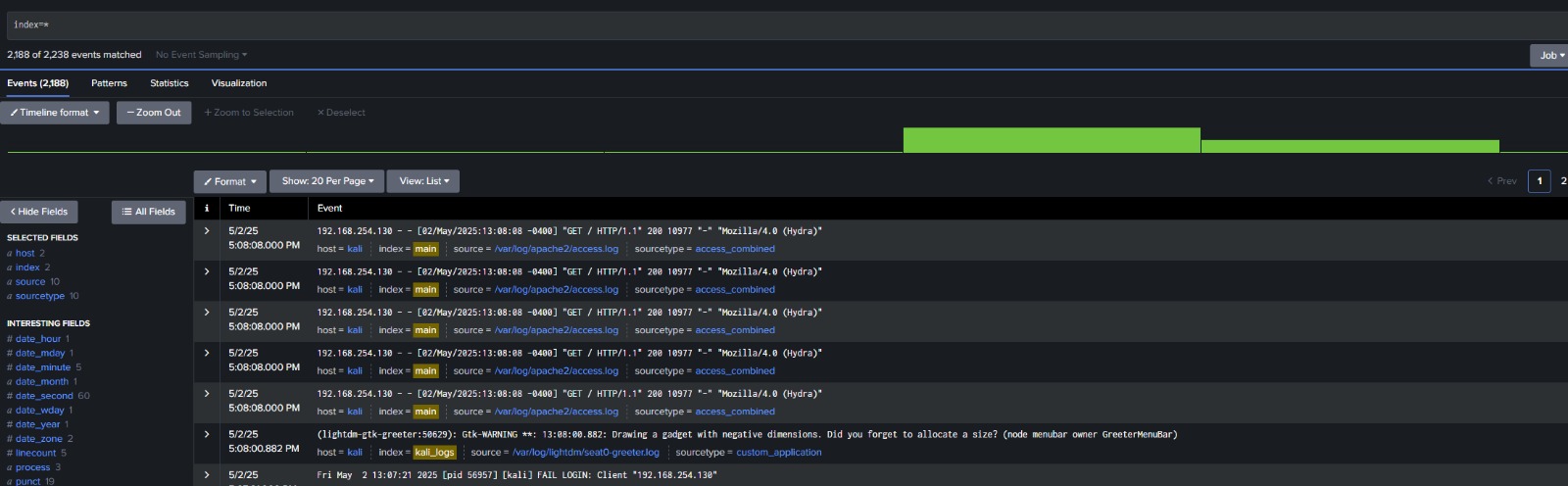
## Kali Linux Target (192.168.254.140)

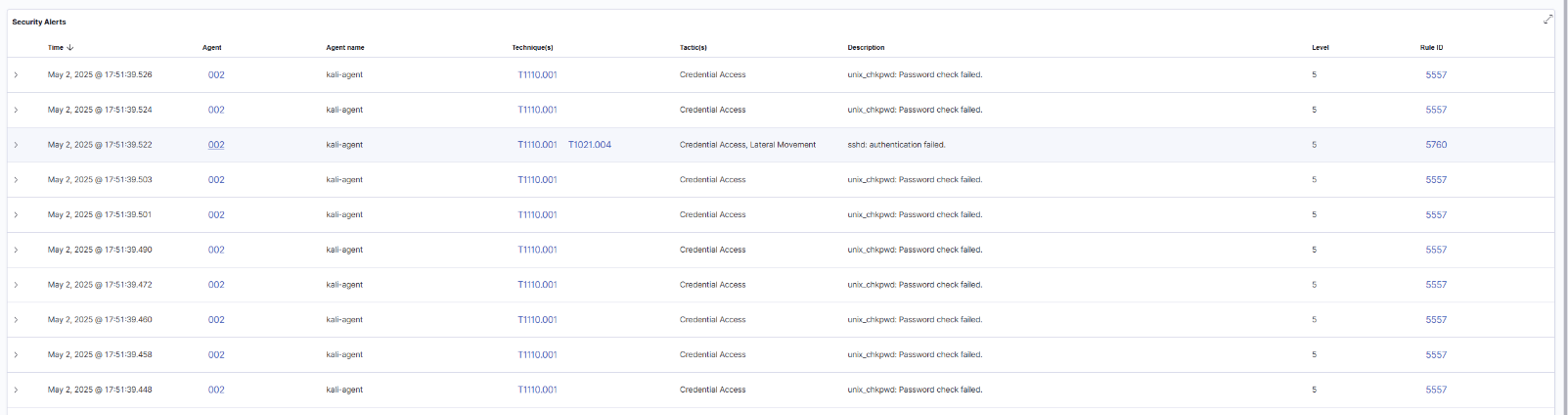
* Conducted a brute-force attack on the SSH service using Hydra:

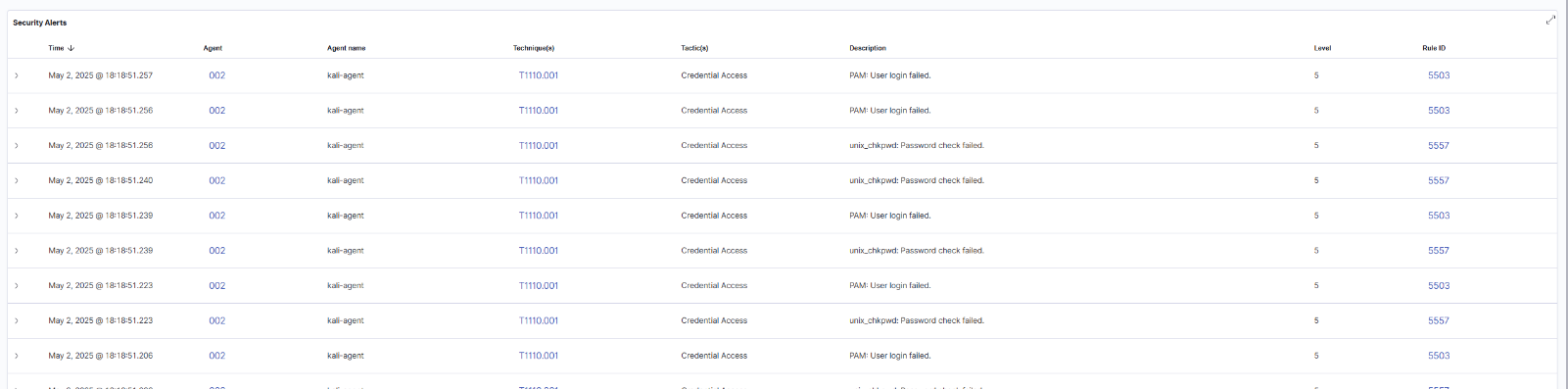
hydra -l kali -P /usr/share/wordlists/rockyou.txt ssh://192.168.254.140





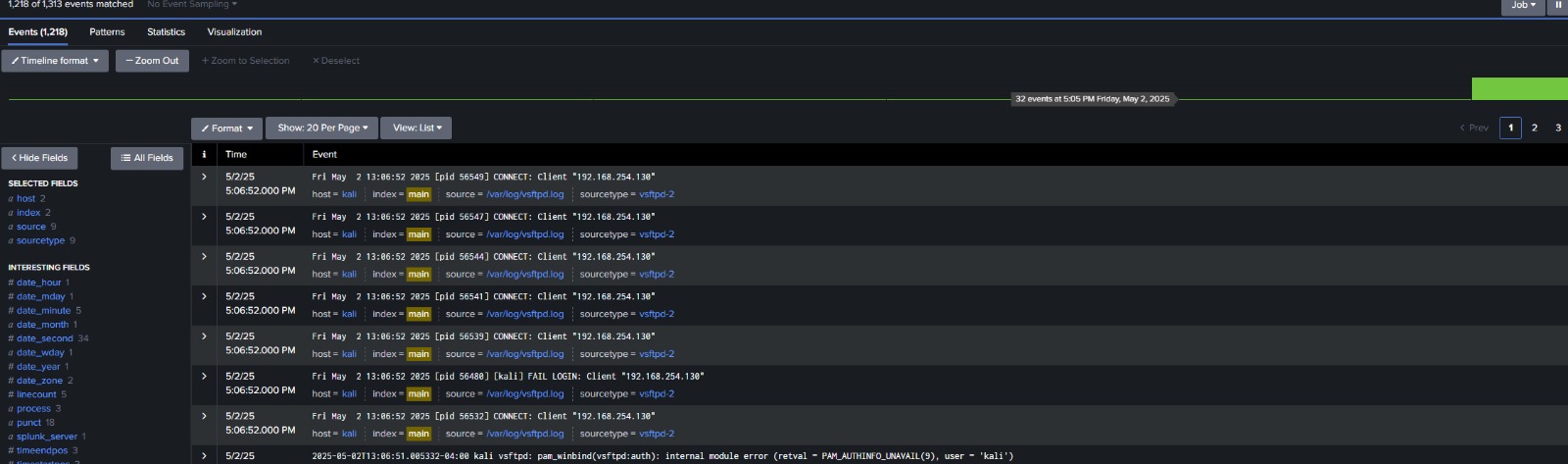


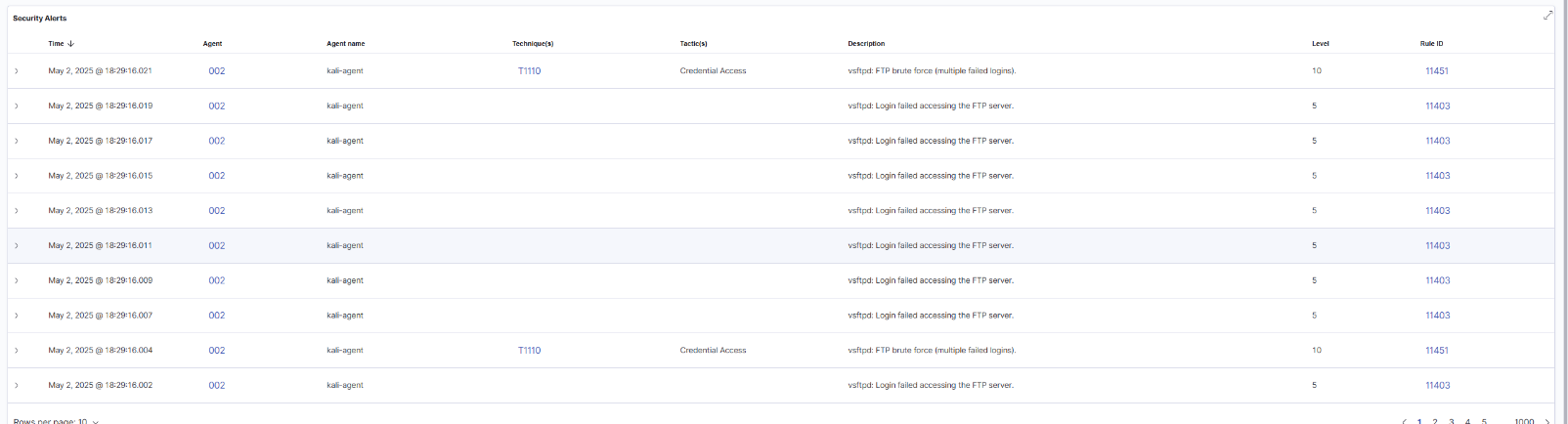


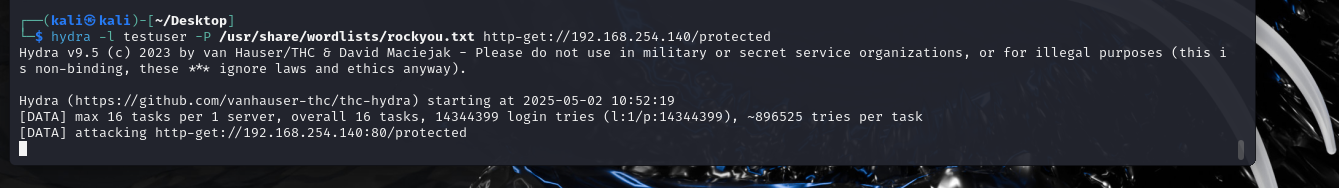


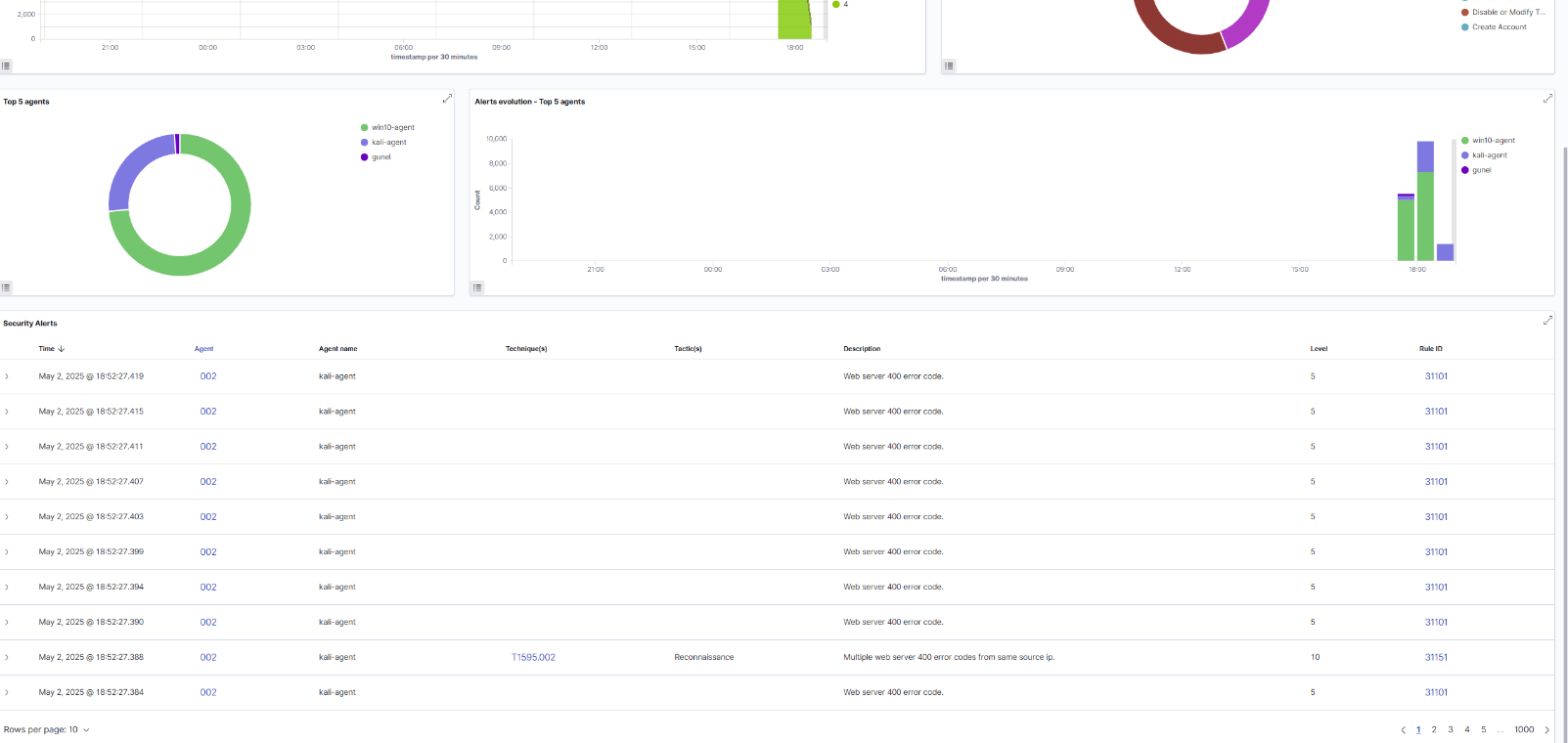
* Performed a brute-force attack on the FTP service (vsftpd):

hydra -l kali -P /usr/share/wordlists/rockyou.txt ftp://192.168.254.140





* Simulated an Apache2-related attack by sending multiple HTTP GET requests
* hydra -l kali -P /usr/share/wordlists/rockyou.txt http-get://192.168.254.140
* 



* These attacks generated authentication and access logs, which were forwarded to both Splunk and Wazuh for analysis.

# Log Analysis and Detection with Splunk

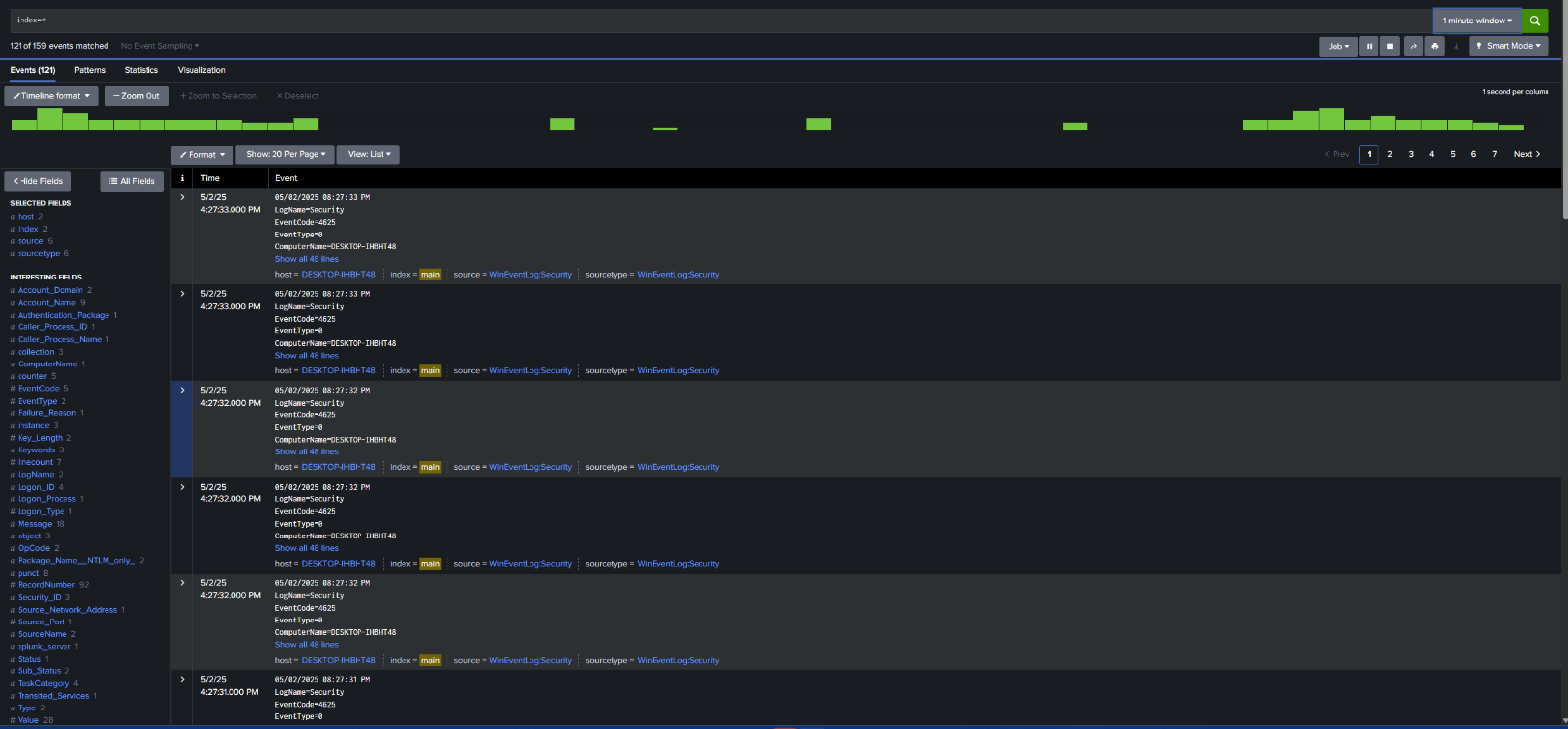
The Splunk SIEM captured and displayed the attack logs from both targets.

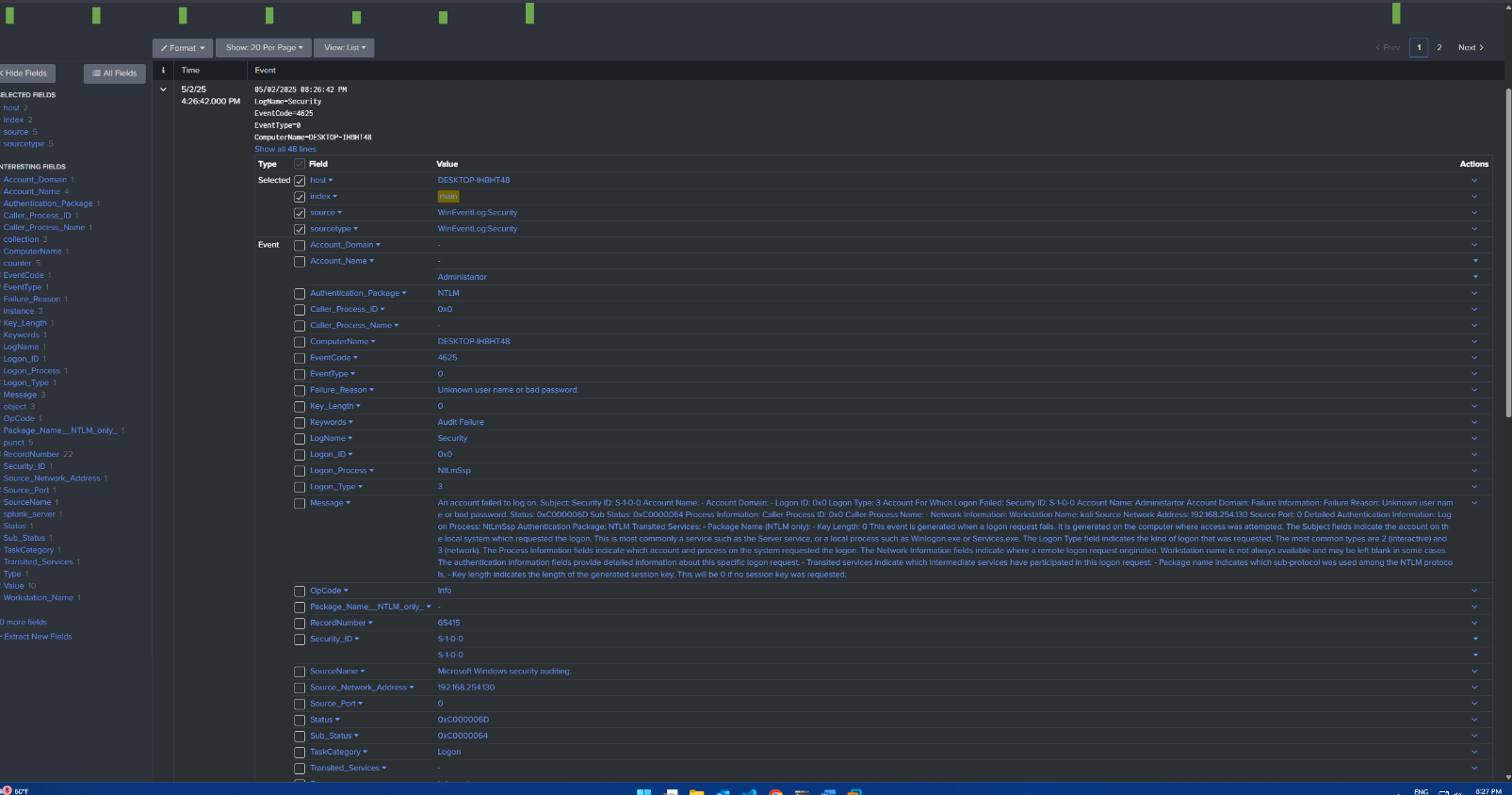
## Windows 10 Logs

* Splunk logs showed EventCode 4625 (failed login attempts) from the Windows Security Event Log. - Timestamp: 05/02/2025 13:25:00 to 13:27:30 PM. - Source IP: 192.168.254.130 (at-

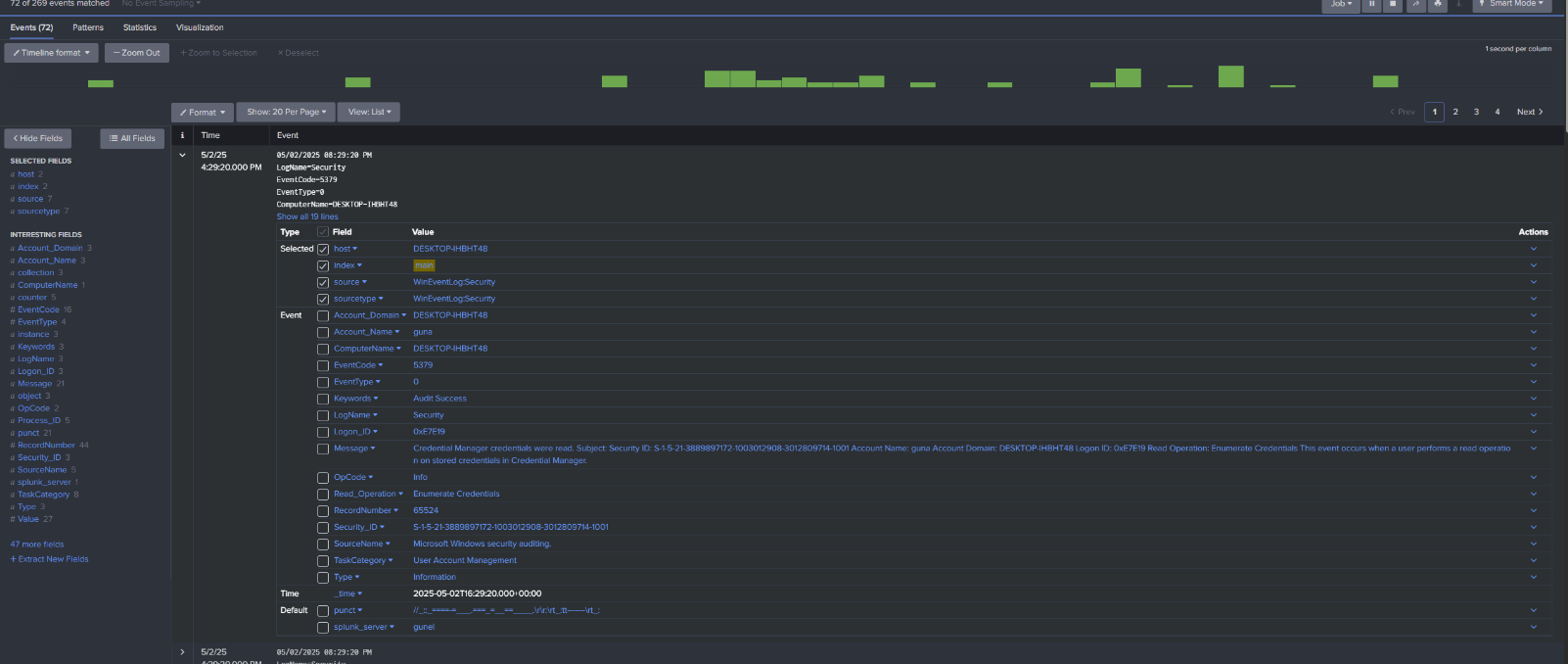
tacker). - Target accounts: "Administrator" and "guest". - Example log entry:

5/25 13:25:00 LogName=Security EventCode=4625 ComputerName=DESKTOP-IH8T Account Name=Administrator Failure Reason=Unknown user name or bad pass

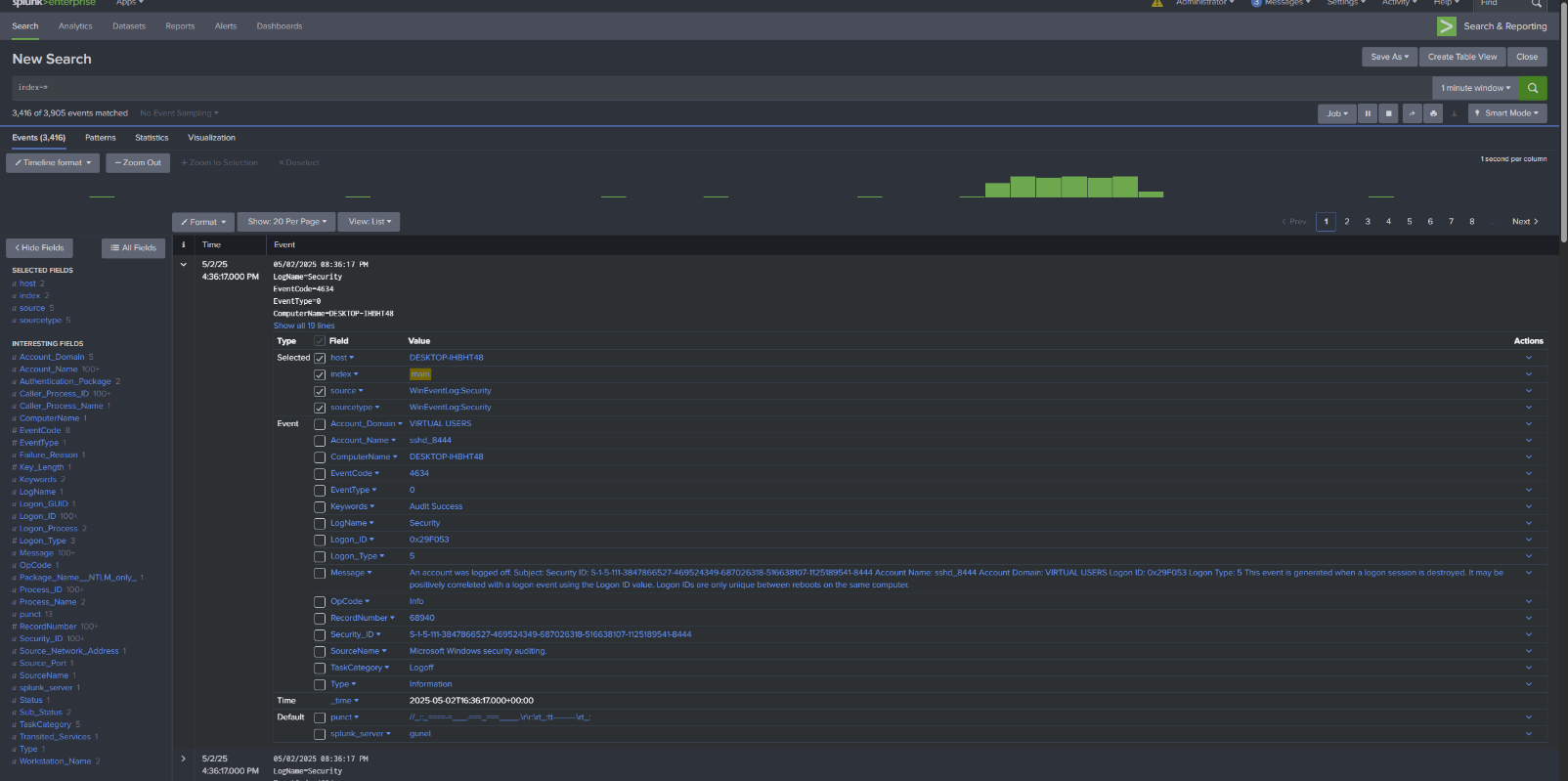
* The timeline graph in Splunk indicated a spike in events around 13:25 PM, correlating with the SMB and RDP attacks.
* **SMB attack**
* 



**RDP ATTACK**



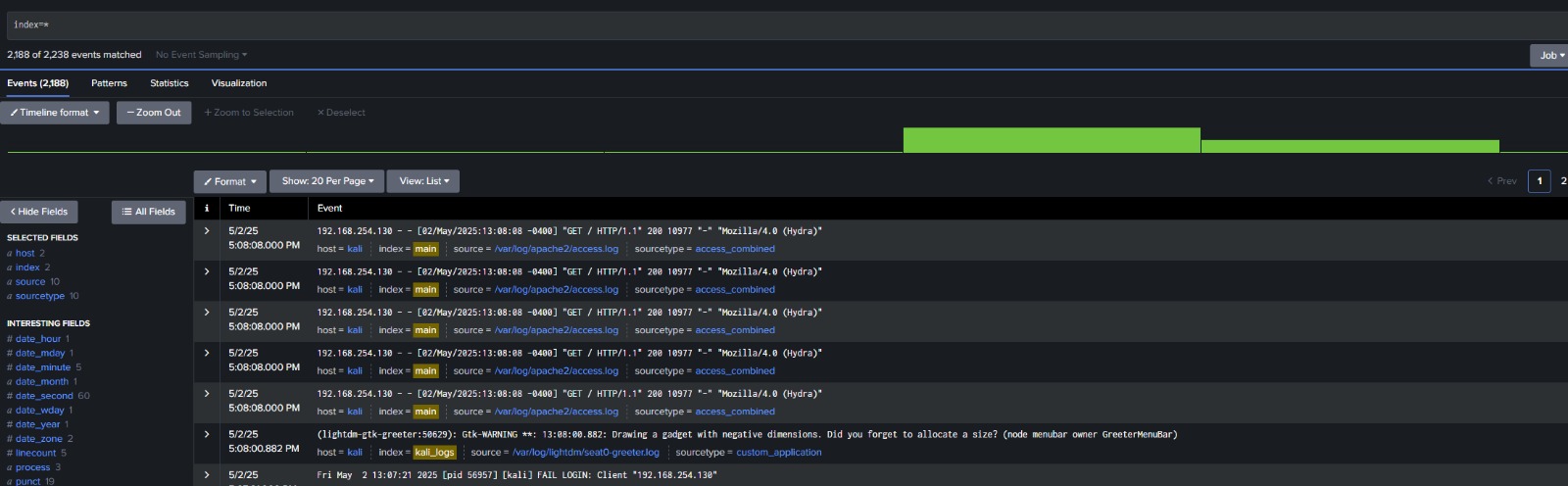
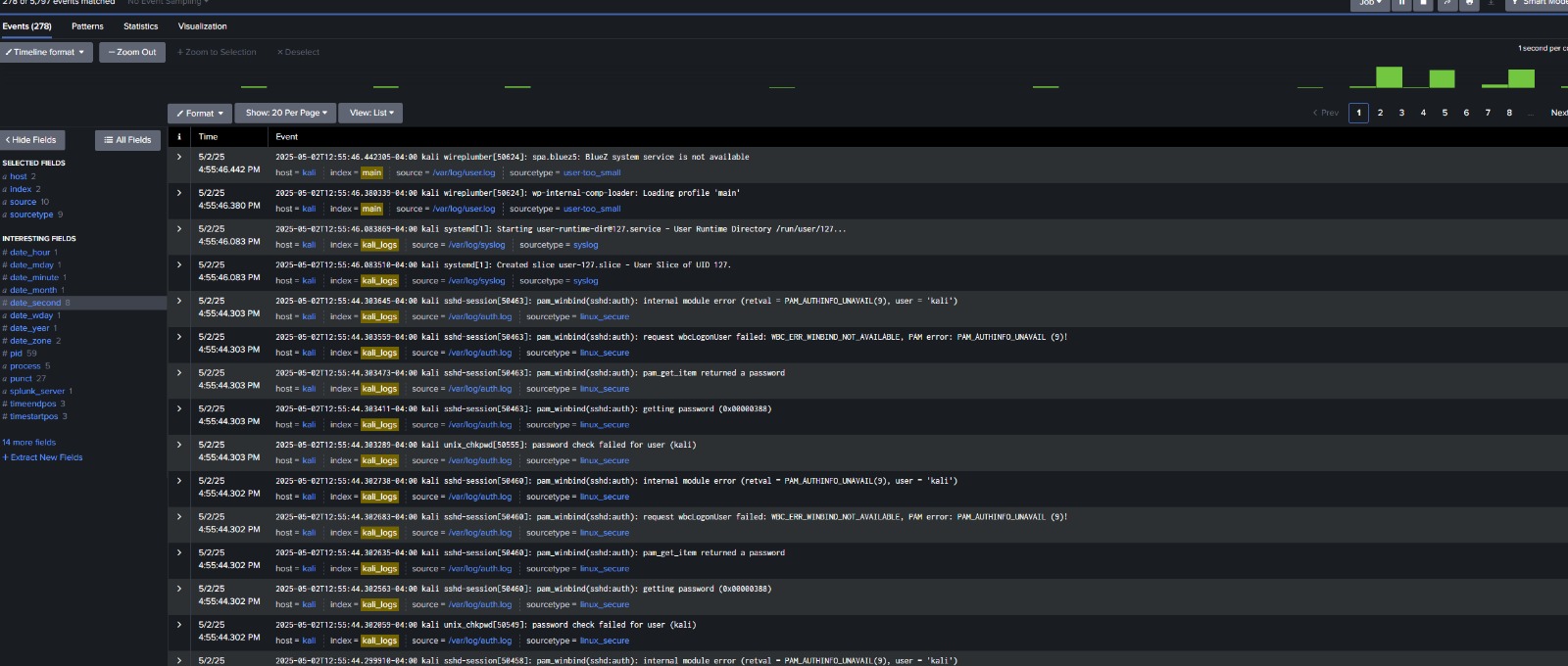
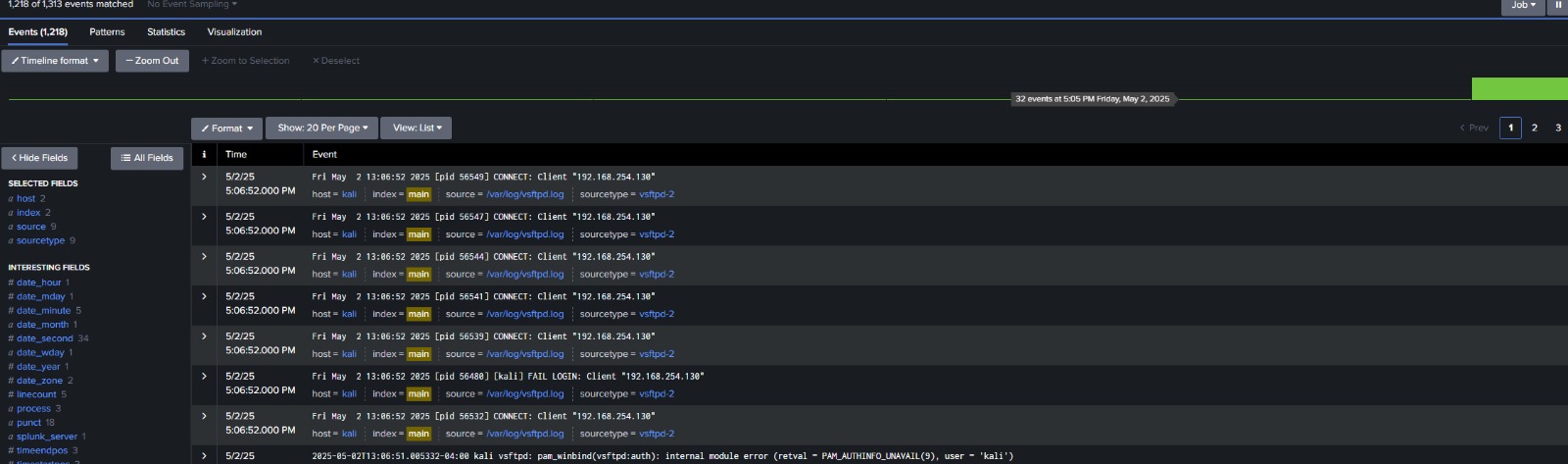
**LLMNR ATTCAK**



## Kali Linux Logs

* Splunk captured syslogs showing failed SSH and FTP login attempts. - Timestamp: 05/02/2025 13:08:52 to 13:10:00 PM. - Source IP: 192.168.254.130. - Example log entry:

5/25 13:08:52 host=kali index=main source=var/log/auth.log sourcetype=l Failed LOGIN attempt for user "kali" from 192.168.254.130

* Additional logs showed HTTP GET requests targeting Apache2, with the source IP as 192.168.254.130.
* 
* Brute-Force to SSH Service
* 
* Brute- force to ftp
* 

# Log Analysis and Detection with Wazuh

The Wazuh SIEM also captured and displayed the attack logs from both targets via the Wazuh dashboard.

## Windows 10 Logs

- Wazuh detected the brute-force attempts on SMB and RDP, generating alerts in the dashboard.

- Timestamp: 05/02/2025 13:25:00 to 13:27:30 PM. - Source IP: 192.168.254.130 (attacker). - Target accounts: "Administrator" and "guest". - Example alert:

Rule: 60103 - Windows Logon Failure Timestamp: 2025-05-02 13:25:00

Source IP: 192.168.254.130

Description: Multiple failed login attempts detected for user "Administ

- The Wazuh dashboard showed a spike in alerts under the "Security Events" tab, with specific rules triggered for brute-force attacks (e.g., Rule ID 60103 for Windows logon failures).

## Kali Linux Logs

- Wazuh captured failed SSH and FTP login attempts, generating corresponding alerts. - Times- tamp: 05/02/2025 13:08:52 to 13:10:00 PM. - Source IP: 192.168.254.130. - Example alert:

Rule: 5710 - SSHD authentication failed Timestamp: 2025-05-02 13:08:52

Source IP: 192.168.254.130

Description: Failed login attempt for user "kali" from 192.168.254.130

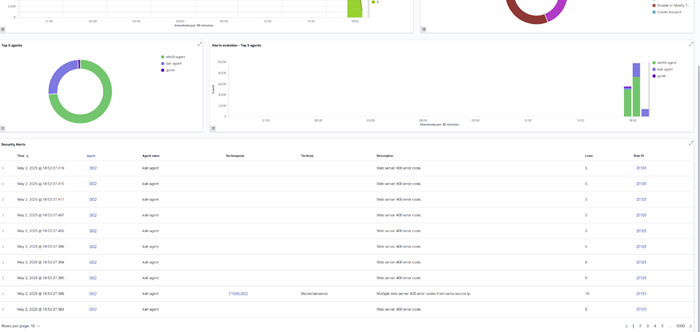
- Additional alerts were generated for the Apache2 HTTP GET requests:

Rule: 31101 - Web server 404 error (possible scanning) Timestamp: 2025-05-02 13:09:00

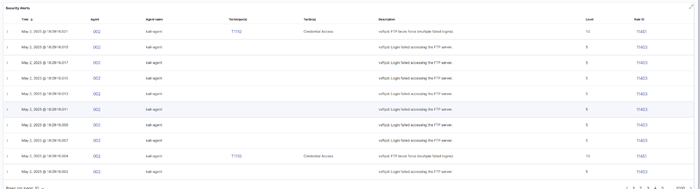
Source IP: 192.168.254.130

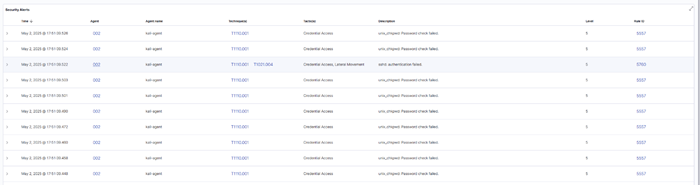
Description: Multiple HTTP requests detected, possible scanning activit





- The Wazuh dashboard visualized these events under the "Security Events" and "Integrity Monitoring" tabs, with a clear timeline of alerts.





# Verification of Log Collection

## Splunk Verification

* In the Splunk web interface, navigated to Search & Reporting. - Ran a search query to confirm logs from both targets:

index=main

* Observed logs from the Windows 10 machine under the sourcetype WinEventLog:Security, showing security events from the attacks. - Observed logs from the Kali Linux machine un-

der the sourcetype linux\_secure (SSH/FTP) and HTTP access logs, confirming successful data ingestion.

## Wazuh Verification

- In the Wazuh dashboard, navigated to the "Security Events" module. - Filtered events by agent (Windows 10 and Kali Linux) and time range (05/02/2025 13:00:00 to 13:30:00). - Confirmed alerts for brute-force attacks on SMB, RDP, SSH, and FTP, as well as HTTP scanning activity on the Kali Linux target. - Used the "Dashboards" tab to visualize the frequency of alerts, confirming successful log collection and analysis.

# Conclusion

Both Splunk and Wazuh SIEMs were successfully set up on separate snapshots of the Ubuntu server, with agents deployed on the Windows 10 and Kali Linux targets. The configurations enabled the collection of Windows Event Logs and Linux syslogs, effectively capturing brute- force attacks on SMB, RDP, SSH, FTP, and HTTP services. The attack simulations from the Kali attacker machine were clearly logged and visualized in both SIEMs, demonstrating their capabilities to monitor and detect security events. Splunk provided detailed log analysis with a user-friendly search interface, while Wazuh offered real-time alerting and compliance-focused dashboards, highlighting their complementary strengths in security monitoring.