Virtual SOC Attack-Defense Lab

Lab Overview

This report documents the simulation of a security operations center (SOC) environment using a VirtualBox-based home lab. The purpose is to gain hands-on experience with attack detection, log collection, and monitoring using tools like Kali Linux, Ubuntu Server, and Splunk.

Lab Components

Role	System	Description
Attacker	Kali Linux	Used to simulate brute-force SSH attacks
Victim	Ubuntu Server	SSH server target for attacks, log generator
Analyst	Splunk on Ubuntu	Used for collecting and analyzing logs

Setup Summary

1. **Networking:**

   → All VMs configured to use NAT network (custom set).

   → IP addresses:

   • Ubuntu (server): 192.168.X.X
   • Kali (attacker): 192.168.X.X

   → Confirmed communication via ping.

2. **Ubuntu Server Configuration:**

   → Installed OpenSSH:

   • sudo apt update
   • sudo apt install openssh-server
   • sudo systemctl enable --now ssh

   → Verified SSH service is active.

→ Configured rsyslog to forward logs:

- *. * @127.0.0.1:514

3. **Splunk Configuration:**

→ Installed Splunk on Ubuntu

→ Port: 8000 (GUI), 514 (UDP)

→ Created a new data input for syslog

→ Set up Splunk to listen for logs from rsyslog.

Attack Simulation

→ **Tool Used:** Hydra

- Command:
  hydra -L user.txt -P pass.txt ssh://IP Address -t 4

hydra
Hydra is a powerful tool for cracking login credentials across various network services.

-L user.txt
This flag tells Hydra to use a list of usernames from the user.txt file.

-P pass.txt
This flag tells Hydra to use a list of passwords from the pass.txt file.

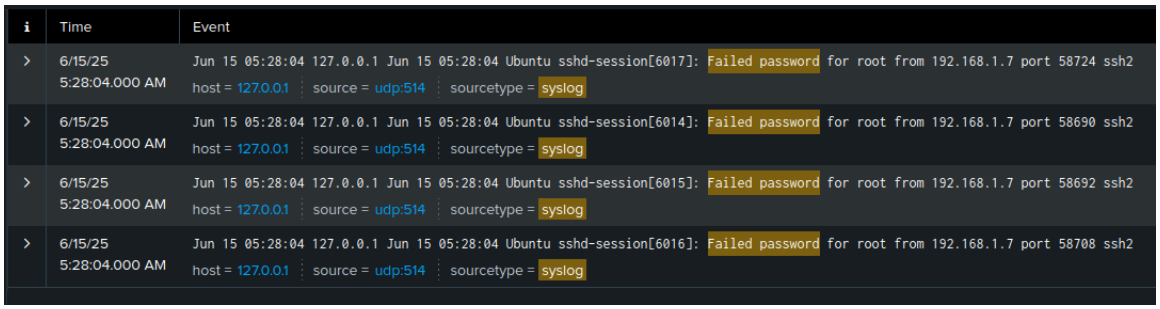
ssh://IP Address
This specifies the target as an SSH service located at a given IP address.

-t 4
This sets 4 concurrent tasks for Hydra to try combinations simultaneously, speeding up the attack.

Objective: Simulate brute-force SSH login attempts from Kali to Ubuntu.
Outcome: Ubuntu logs recorded multiple failed login attempts and forwarded them to Splunk.

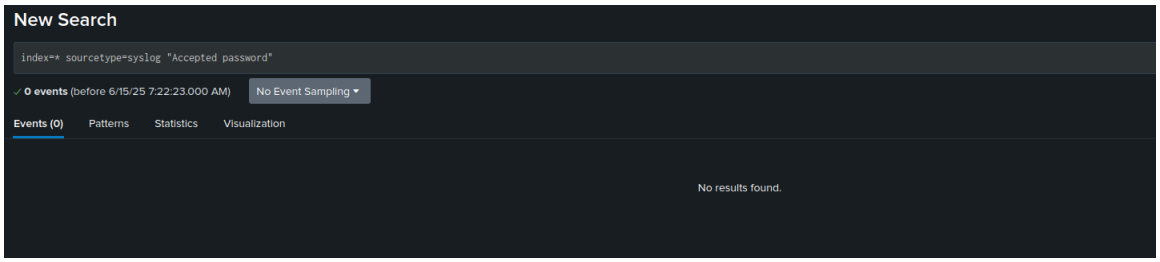
Detection in Splunk

1. **Failed Logins:**
   index=* sourcetype=syslog "Failed password"



2. **Successful Logins:**

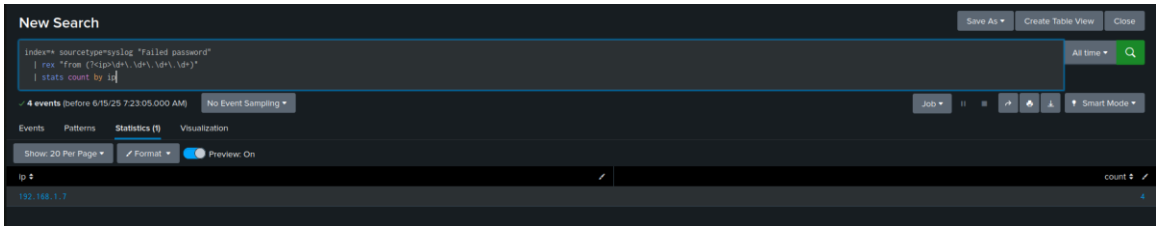
index=* sourcetype=syslog "Accepted password"



No results because there were no successful passwords in the brute force

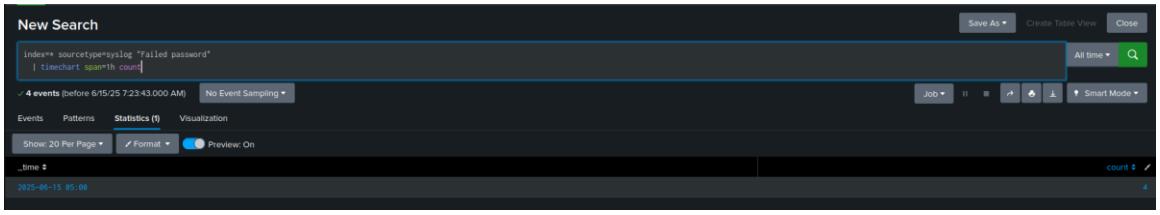
3. **Top Brute-force Sources:**

index=* sourcetype=syslog "Failed password"
| rex "from (?<ip>\d+\.\d+\.\d+\.\d+)"
| stats count by ip



4. **Time-Based Trend:**

index=* sourcetype=syslog "Failed password"
| timechart span=1h count



Lessons Learned

→ Understood basic log flow from system to SIEM (Splunk)

→ Simulated a real-world brute-force scenario

→ Practiced detecting suspicious activity via Splunk queries

→ Learned to forward logs using rsyslog and UDP ports

Conclusion

This simulation was a foundational SOC analyst exercise, proving skills in log collection, attack simulation, detection, and analysis. Future iterations will include:

→ Adding a Windows 10 VM as a victim with Windows Event Forwarding (WEF)

→ Testing detection of malware behavior and privilege escalation.