# SIEM Lab Setup Documentation - Phase 1

---

## Introduction

**Objective**:
The objective of Phase 1 was to set up a SOC (Security Operations Center) lab, simulate basic cyberattacks, configure log sources from Windows and Linux systems, and detect real-world threats using a SIEM solution.

## What is a SIEM and Why it Matters?

### What is SIEM?

A SIEM (Security Information and Event Management) system aggregates, parses, correlates, and analyzes security-related logs in real time.

**Key Functions**:

- Log Collection and Normalization
- Alerting and Rule-based Correlation
- Dashboards and Incident Response
- Compliance and Reporting

**Popular SIEM Tools**:

1. Splunk
2. Wazuh
3. ELK Stack
4. Security Onion

**Why SIEM is Important**?

SIEMs are essential for early threat detection, compliance, and centralized monitoring of cybersecurity events, such as brute-force attacks, unauthorized access, and log tampering.

# Lab Setup Overview

This lab simulates a basic enterprise network with a Windows host, a Linux VM, and an attacker machine. Log sources are configured to send data to a central SIEM solution.

# Architecture

**Windows Machine**:

- OS: Windows 10
- Tools: Sysmon, Winlogbeat
- Software: Splunk Enterprise

**Linux Machine**:

- OS: Ubuntu/Kali
- Tools: auditd, rsyslog, Filebeat
- Software: Splunk Universal Forwarder

**SIEM Host**:

- Tool: Wazuh / Splunk / ELK Stack
- Receives logs from both Windows and Linux over the network

**Communication**:

- Logs forwarded over TCP (port varies by tool, e.g., 9997 for Splunk)

# Tools Used

- Wazuh / Splunk Free / ELK Stack
- Sysmon for Windows telemetry
- Auditd for Linux auditing
- Winlogbeat, Filebeat  as log forwarders
- Hydra and Netcat for brute force simulation

## Splunk Forwarder Configuration

**1. Install Splunk Forwarder on Linux VM:**

-Download and extract Splunk Forwarder , according to you machine type.

**2. Start Splunk Forwarder:**

sudo /opt/splunkforwarder/bin/splunk start --accept-license

**3. Configure Splunk Forward Server:**

This will forward our defined logs in inputs.conf to splunk enterprise server hosted on
windows machine.

sudo /opt/splunkforwarder/bin/splunk add forward-server <Windows_IP>:9997
**Note** :
This step , might be done again , if machine restarts with new IP_address .

**4. Monitor Logs:**

This step commands forwarder to forward which specific logs to splunk server.

Add the following to /opt/splunkforwarder/etc/system/local/inputs.conf:

[monitor:///var/log/syslog]
disabled = false
index = linux_logs
sourcetype = syslog
[monitor:///var/log/auth.log]
disabled = false
index = linux_logs
sourcetype = linux_secure
[monitor:///var/log/sysmon.log]
disabled = false
index = linux_logs
sourcetype = sysmon_linux

## Splunk Enterprise Configuration

1. **Download Splunk Enterprise for windows from official site .**

2. **Set username and password to login on splunk server later.**

3. **Enable Receiving on Port 9997:**
Settings > Forwarding and Receiving > Configure Receiving > new receiving port > Port 9997

**3. Configure web.conf :**
To allow access to splunk forwarder in linux via actual IP of windows where splunk server
is hosted , edit C:\Program Files\Splunk\etc\system\local\web.conf:

[settings]
enableSplunkWebSSL = false
httpport = 8000
mgmtHostPort = 192.168.1.34:8089

**4. splunk-launch.conf :**

This is necessary , if we are changing IP in above step , to start splunk server with that
actual IP.
Configure environmental variables if needed in splunk-launch.conf , i.e , add bind_ip

**5. Firewall Configuration(this is optional ):**Allow inbound connections on port 9997 (TCP) in Windows Defender Firewall.

**6.** Create new index (namespace or data repository where forwarded logs are
collected and analyzed ) in splunk enterprise , with name as linux_logs.

7. Now restart splunk enterprise and splunk forwarder.

# Detection Use Case 1 - Brute Force Login

**Simulation**:

- Used Hydra to brute-force SSH login to Linux machine
- Also simulated failed RDP attempts on Windows

**Event IDs**:

- `4625`: Failed Windows login
- `4624`: Successful login

**Detection**:

- Alert triggered when ≥5 failed logins occur from same IP within 2 minutes

**Splunk Query Example**:

index=win_logs EventCode=4625 | stats count by src_ip, user | where count > 5

# Detection Use Case 2 - After-Hours Login

**Definition**:

- Business hours: 9:00 AM to 6:00 PM

**Detection**:

- Alert when user login (Event ID `4624` or SSH `Accepted password`) happens outside business hours

**Splunk Example**:

index=linux_logs "Accepted password" | eval hour=strftime(_time, "%H") | where hour<9 OR hour>18

# Detection Use Case 3 - RDP Lateral Movement

**Simulation**:

- RDP session from Admin-PC (A) to Server (B)

**Event IDs**:

- `4624` with `LogonType=10` (RemoteInteractive)

**Detection**:

- Detect logins from internal IPs not normally associated with that system

**MITRE ATT&CK**:

- T1021.001 - Remote Services: RDP

# Detection Use Case 4 - Log Tampering

**Simulation**:

- Commands used:
    - `wevtutil cl Security`
    - `auditpol /set /category:* /success:disable`

**Event IDs**:

- `1102`: Audit log cleared
- `4719`: Audit policy changed

**Detection**:

- Alert when logs are unexpectedly cleared or policies are modified

**MITRE ATT&CK**:

- T1562.002 - Impair Defenses: Disable Windows Event Logging

# Reflection Questions & Answers

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

   SIEM systems enable real-time threat detection, centralized log analysis, and incident response.

2. **Challenges faced while setting up the lab?**

   -> Networking between VMs
   -> Forwarding logs consistently
   -> Tuning detection rules.

3. **Difference between Sysmon logs and Windows Security logs?**

   Sysmon provides detailed process/file/network events, whereas

Security logs focus on access, logon, and audit events.

4. **How does a brute force attack appear in logs?**

   Burst of Event ID `4625` from same IP, possibly followed by `4624` on success.

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

   Analyze timestamps of Event ID `4624` and compare with business hour range.

6. **Tracking RDP lateral movement in logs?**

   Look for LogonType `10` and Event ID `4624` from internal IPs.

7. **Risk of log tampering and detection?**

   Tampering hides evidence. Detected via Event IDs `1102`, `4719`, and file size anomalies.

8. **Improvements if more time was available?**

   Automate log collection, expand attack library, and integrate threat intel feeds.

9. **How does this phase help for interviews/jobs?**

   Hands-on SIEM experience builds real-world blue team skills.

10. **Biggest takeaway from Phase 1?**

    Importance of proper logging and correlation to detect even subtle attacks.