DIGITAL FORENSIC REPORT (STAR METHODOLOGY)

Case Title: *Framework for Syslog Analysis – Brute-Force Attack Investigation*
Case ID: 1
Date: 12 Jan 2025

- A **syslog analysis framework** defines how forensic investigators collect, preserve, correlate, and analyse log evidence after a cyberattack.This framework is designed specifically for **post-attack digital forensics**, not detection systems.

Executive Summary

- This case investigates malicious activity on an Ubuntu system that reported abnormal SSH activity.
- A forensic examination was conducted on syslog and auth.log obtained from a logical evidence file (.L01). ‘
- Analysis confirmed a **port-scan reconnaissance phase**, followed by a **high-volume brute-force attack** from **192.168.1.50**, resulting in a **successful compromise of the root account at 02:15:08**.
- Timeline reconstruction clearly maps attacker behavior from initial scanning to final intrusion.

S — Situation

Initial Request

The goal was to confirm whether an unauthorized login occurred and reconstruct the attacker’s activity timeline.

Scene & Evidence

The investigation involved **remote log extraction** from a Linux victim machine.
Evidence collected:

Evidence ID	Description	File	Date/Time Collected
E01-SYSLOG	Ubuntu System Log	syslog	12 Jan 2025, 03:00
E01-AUTHLOG	SSH Authentication Log	auth.log	12 Jan 2025, 03:00
L01-LOGSET	Logical Evidence Container	logs.l01	Created 12 Jan

Chain of Custody

- **12 Jan, 03:00** – Logs exported by victim.
- **12 Jan, 03:05** – Logs hashed using SHA-256.
- **12 Jan, 03:15** – Logs packaged into .L01 file using FTK Imager.
- **12 Jan, 03:20** – .L01 loaded into Autopsy for analysis.
- Integrity verified at every transfer.

T — Task

Objectives

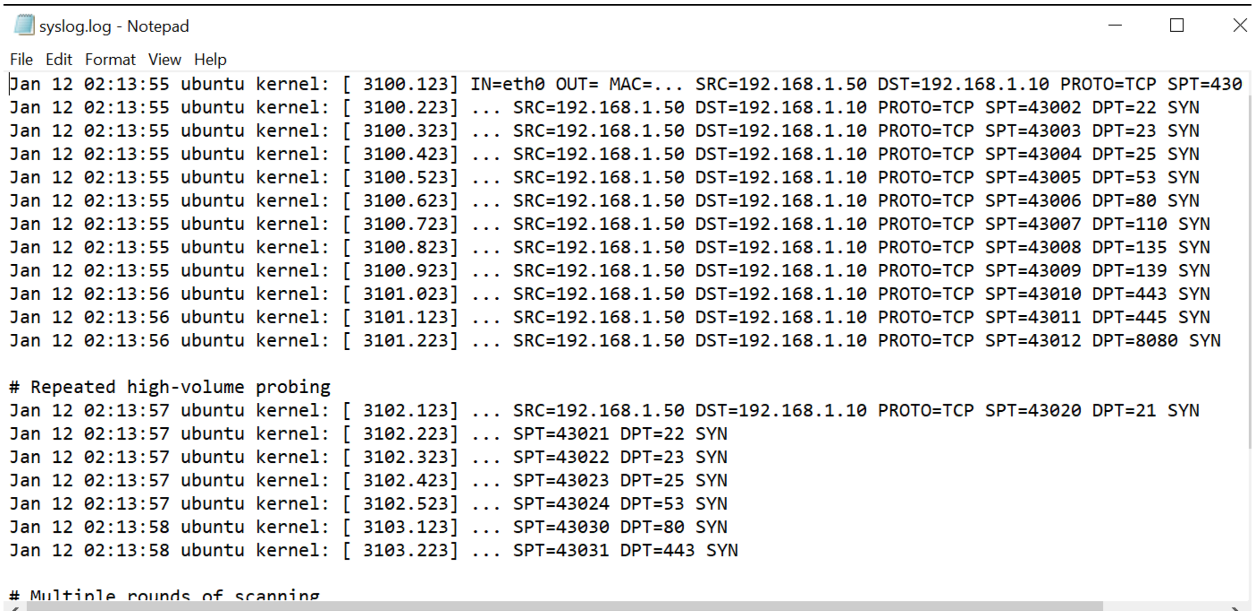
The examination focused on:

1. Detecting malicious patterns inside syslog and auth.log.
2. Confirming whether brute-force attempts occurred.

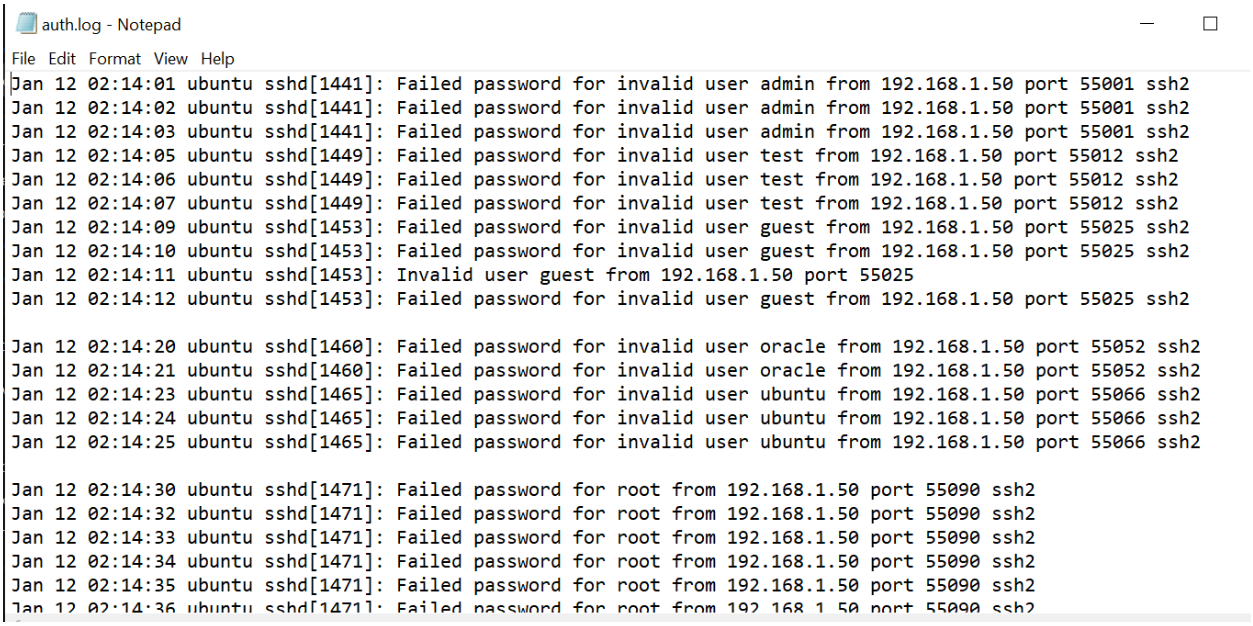
3. Identifying the attacker’s IP, accounts targeted, and attack sequence.
4. Verifying if any account compromise occurred.
5. Reconstructing a forensic timeline for reporting.

Limitations & Scope

- Logs provided are logical files, not full disk images.
- No browser, filesystem, or memory artifacts available.
- Analysis limited strictly to SSH and firewall/kernel log activity.



```
Jan 12 02:13:55 ubuntu kernel: [ 3100.123] IN=eth0 OUT= MAC=... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=430
Jan 12 02:13:55 ubuntu kernel: [ 3100.223] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43002 DPT=22 SYN
Jan 12 02:13:55 ubuntu kernel: [ 3100.323] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43003 DPT=23 SYN
Jan 12 02:13:55 ubuntu kernel: [ 3100.423] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43004 DPT=25 SYN
Jan 12 02:13:55 ubuntu kernel: [ 3100.523] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43005 DPT=53 SYN
Jan 12 02:13:55 ubuntu kernel: [ 3100.623] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43006 DPT=80 SYN
Jan 12 02:13:55 ubuntu kernel: [ 3100.723] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43007 DPT=110 SYN
Jan 12 02:13:55 ubuntu kernel: [ 3100.823] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43008 DPT=135 SYN
Jan 12 02:13:55 ubuntu kernel: [ 3100.923] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43009 DPT=139 SYN
Jan 12 02:13:56 ubuntu kernel: [ 3101.023] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43010 DPT=443 SYN
Jan 12 02:13:56 ubuntu kernel: [ 3101.123] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43011 DPT=445 SYN
Jan 12 02:13:56 ubuntu kernel: [ 3101.223] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43012 DPT=8080 SYN

# Repeated high-volume probing
Jan 12 02:13:57 ubuntu kernel: [ 3102.123] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43020 DPT=21 SYN
Jan 12 02:13:57 ubuntu kernel: [ 3102.223] ... SPT=43021 DPT=22 SYN
Jan 12 02:13:57 ubuntu kernel: [ 3102.323] ... SPT=43022 DPT=23 SYN
Jan 12 02:13:57 ubuntu kernel: [ 3102.423] ... SPT=43023 DPT=25 SYN
Jan 12 02:13:57 ubuntu kernel: [ 3102.523] ... SPT=43024 DPT=53 SYN
Jan 12 02:13:58 ubuntu kernel: [ 3103.123] ... SPT=43030 DPT=80 SYN
Jan 12 02:13:58 ubuntu kernel: [ 3103.223] ... SPT=43031 DPT=443 SYN

# Multiple rounds of scanning
```

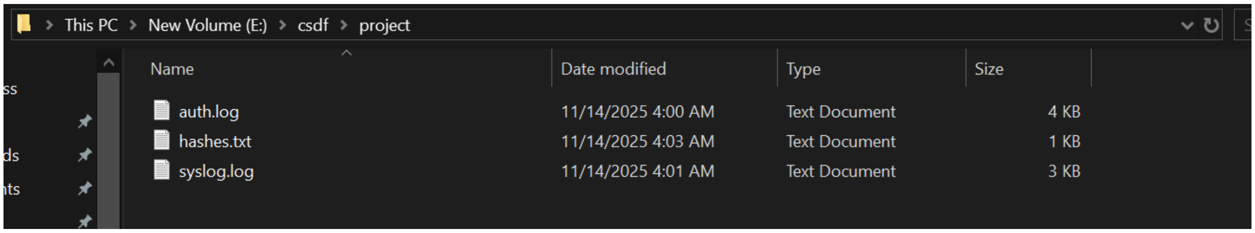


```
Jan 12 02:14:01 ubuntu sshd[1441]: Failed password for invalid user admin from 192.168.1.50 port 55001 ssh2
Jan 12 02:14:02 ubuntu sshd[1441]: Failed password for invalid user admin from 192.168.1.50 port 55001 ssh2
Jan 12 02:14:03 ubuntu sshd[1441]: Failed password for invalid user admin from 192.168.1.50 port 55001 ssh2
Jan 12 02:14:05 ubuntu sshd[1449]: Failed password for invalid user test from 192.168.1.50 port 55012 ssh2
Jan 12 02:14:06 ubuntu sshd[1449]: Failed password for invalid user test from 192.168.1.50 port 55012 ssh2
Jan 12 02:14:07 ubuntu sshd[1449]: Failed password for invalid user test from 192.168.1.50 port 55012 ssh2
Jan 12 02:14:09 ubuntu sshd[1453]: Failed password for invalid user guest from 192.168.1.50 port 55025 ssh2
Jan 12 02:14:10 ubuntu sshd[1453]: Failed password for invalid user guest from 192.168.1.50 port 55025 ssh2
Jan 12 02:14:11 ubuntu sshd[1453]: Invalid user guest from 192.168.1.50 port 55025
Jan 12 02:14:12 ubuntu sshd[1453]: Failed password for invalid user guest from 192.168.1.50 port 55025 ssh2

Jan 12 02:14:20 ubuntu sshd[1460]: Failed password for invalid user oracle from 192.168.1.50 port 55052 ssh2
Jan 12 02:14:21 ubuntu sshd[1460]: Failed password for invalid user oracle from 192.168.1.50 port 55052 ssh2
Jan 12 02:14:23 ubuntu sshd[1465]: Failed password for invalid user ubuntu from 192.168.1.50 port 55066 ssh2
Jan 12 02:14:24 ubuntu sshd[1465]: Failed password for invalid user ubuntu from 192.168.1.50 port 55066 ssh2
Jan 12 02:14:25 ubuntu sshd[1465]: Failed password for invalid user ubuntu from 192.168.1.50 port 55066 ssh2

Jan 12 02:14:30 ubuntu sshd[1471]: Failed password for root from 192.168.1.50 port 55090 ssh2
Jan 12 02:14:32 ubuntu sshd[1471]: Failed password for root from 192.168.1.50 port 55090 ssh2
Jan 12 02:14:33 ubuntu sshd[1471]: Failed password for root from 192.168.1.50 port 55090 ssh2
Jan 12 02:14:34 ubuntu sshd[1471]: Failed password for root from 192.168.1.50 port 55090 ssh2
Jan 12 02:14:35 ubuntu sshd[1471]: Failed password for root from 192.168.1.50 port 55090 ssh2
Jan 12 02:14:36 ubuntu sshd[1471]: Failed password for root from 192.168.1.50 port 55090 ssh2
```

A — Action (Methodology & Analysis)

Forensic Methodology

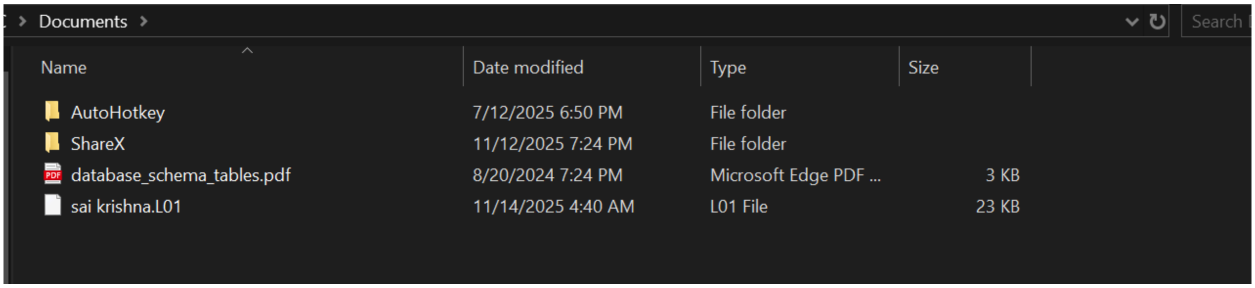
1. Preservation

- Received syslog and auth.log.
- Hashing performed:
  - `sha256sum syslog`
  - `sha256sum auth.log`
- Logs preserved in original state; investigation performed on copies.
- 

Name	Date modified	Type	Size
auth.log	11/14/2025 4:00 AM	Text Document	4 KB
hashes.txt	11/14/2025 4:03 AM	Text Document	1 KB
syslog.log	11/14/2025 4:01 AM	Text Document	3 KB

2. Evidence Imaging

- Created `.L01` logical image using Encase Imager.
- Loaded L01 into Autopsy (v4.21) under *Logical Files*.
- Extracted files for separate timeline reconstruction.

- 

Name	Date modified	Type	Size
AutoHotkey	7/12/2025 6:50 PM	File folder	
ShareX	11/12/2025 7:24 PM	File folder	
database_schema_tables.pdf	8/20/2024 7:24 PM	Microsoft Edge PDF ...	3 KB
sai krishna.L01	11/14/2025 4:40 AM	L01 File	23 KB

3. Tools Used

- **Encase Imager** — Logical evidence creation
- **Autopsy v4.21** — Timeline & log artifact parsing
- **Ubuntu Syslog Parser (manual analysis)**
- **Regex-based log extraction**

4. Analytical Steps

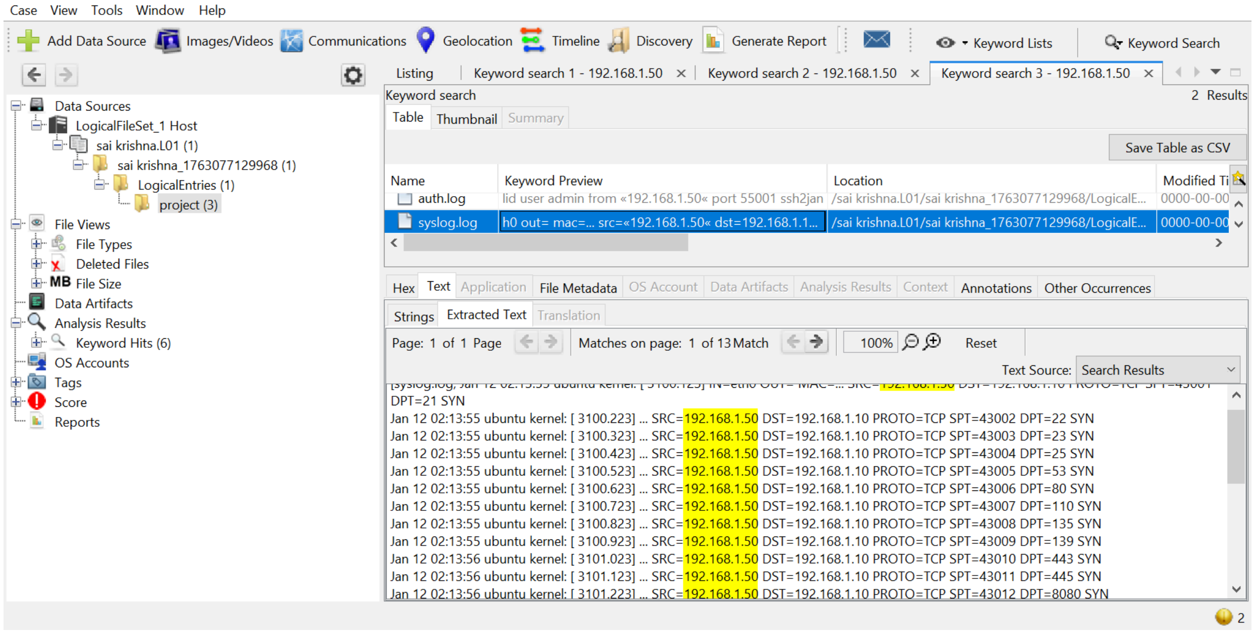
- Identified high-volume SYN packets in syslog → Port scan pattern.
- Correlated timestamps between syslog and auth.log.
- Tracked brute-force attempts user-by-user.
- Verified successful root compromise.

R — Result

Key Findings

Finding 1 — Port Scan Reconnaissance (02:13:55–02:14:00)

Evidence: syslog kernel entries
Details: Attacker scanned critical ports:
21, 22, 23, 25, 53, 80, 110, 135, 139, 443, 445, 8080
Source IP: 192.168.1.50
Purpose: Identifying open remote-access ports.



Name	Keyword Preview	Location	Modified Ti
auth.log	lid user admin from «192.168.1.50« port 55001 ssh2jan	/sai krishna.L01/sai krishna_1763077129968/LogicalE...	0000-00-00
syslog.log	h0 out= mac=... src=«192.168.1.50« dst=192.168.1.1...	/sai krishna.L01/sai krishna_1763077129968/LogicalE...	0000-00-00

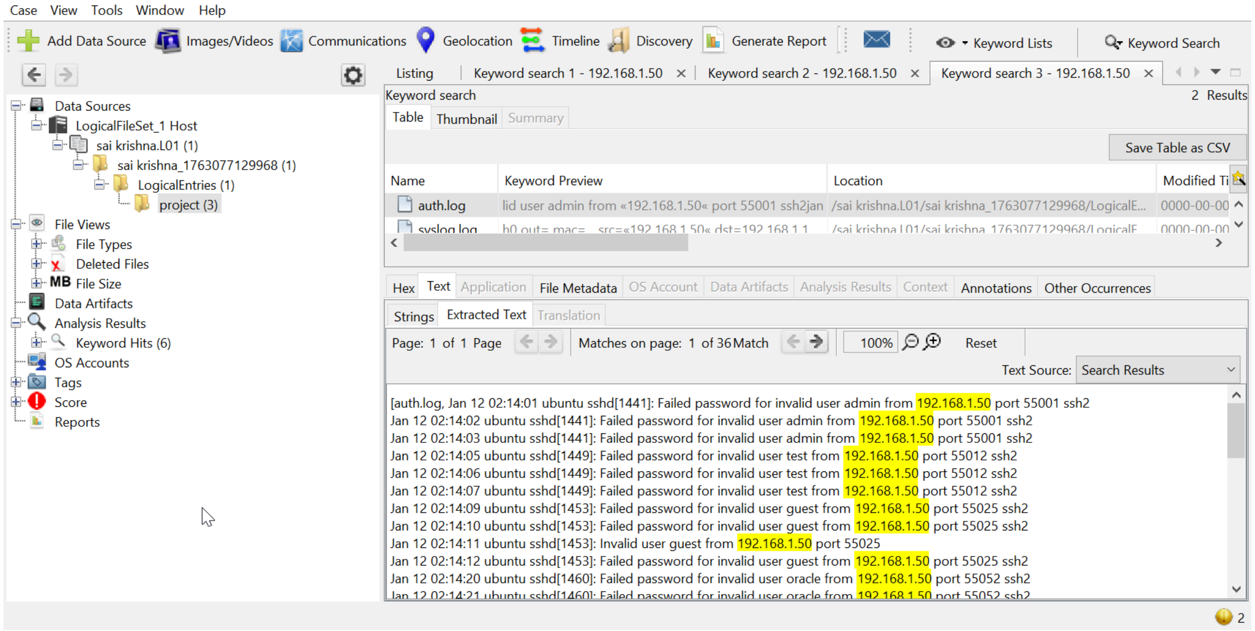
```
[syslog.log, Jan 12 02:13:55 ubuntu kernel: [ 3100.123] IN=eth0 OUT= MAC=... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43001
DPT=21 SYN
Jan 12 02:13:55 ubuntu kernel: [ 3100.223] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43002 DPT=22 SYN
Jan 12 02:13:55 ubuntu kernel: [ 3100.323] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43003 DPT=23 SYN
Jan 12 02:13:55 ubuntu kernel: [ 3100.423] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43004 DPT=25 SYN
Jan 12 02:13:55 ubuntu kernel: [ 3100.523] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43005 DPT=53 SYN
Jan 12 02:13:55 ubuntu kernel: [ 3100.623] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43006 DPT=80 SYN
Jan 12 02:13:55 ubuntu kernel: [ 3100.723] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43007 DPT=110 SYN
Jan 12 02:13:55 ubuntu kernel: [ 3100.823] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43008 DPT=135 SYN
Jan 12 02:13:55 ubuntu kernel: [ 3100.923] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43009 DPT=139 SYN
Jan 12 02:13:56 ubuntu kernel: [ 3101.023] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43010 DPT=443 SYN
Jan 12 02:13:56 ubuntu kernel: [ 3101.123] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43011 DPT=445 SYN
Jan 12 02:13:56 ubuntu kernel: [ 3101.223] ... SRC=192.168.1.50 DST=192.168.1.10 PROTO=TCP SPT=43012 DPT=8080 SYN
```

Finding 2 — Brute-Force Attempts on SSH (02:14:01–02:15:05)

Evidence: auth.log failed SSH entries
Pattern: Attack cycle of 3 attempts per username
Usernames Tried:

- admin
- test
- guest
- oracle
- ubuntu
- root (heavy targeted phase)

Ports used: 55001–55166
Technique: Automated brute-force script.



Name	Keyword Preview	Location	Modified Ti
auth.log	lid user admin from «192.168.1.50« port 55001 ssh2jan	/sai krishna.L01/sai krishna_1763077129968/LogicalE...	0000-00-00
syslog.log	h0 out= mac= src=«192.168.1.50« dst=192.168.1.1	/sai krishna.L01/sai krishna_1763077129968/LogicalE	0000-00-00

```
[auth.log, Jan 12 02:14:01 ubuntu sshd[1441]: Failed password for invalid user admin from 192.168.1.50 port 55001 ssh2
Jan 12 02:14:02 ubuntu sshd[1441]: Failed password for invalid user admin from 192.168.1.50 port 55001 ssh2
Jan 12 02:14:03 ubuntu sshd[1441]: Failed password for invalid user admin from 192.168.1.50 port 55001 ssh2
Jan 12 02:14:05 ubuntu sshd[1449]: Failed password for invalid user test from 192.168.1.50 port 55012 ssh2
Jan 12 02:14:06 ubuntu sshd[1449]: Failed password for invalid user test from 192.168.1.50 port 55012 ssh2
Jan 12 02:14:07 ubuntu sshd[1449]: Failed password for invalid user test from 192.168.1.50 port 55012 ssh2
Jan 12 02:14:09 ubuntu sshd[1453]: Failed password for invalid user guest from 192.168.1.50 port 55025 ssh2
Jan 12 02:14:10 ubuntu sshd[1453]: Failed password for invalid user guest from 192.168.1.50 port 55025 ssh2
Jan 12 02:14:11 ubuntu sshd[1453]: Invalid user guest from 192.168.1.50 port 55025
Jan 12 02:14:12 ubuntu sshd[1453]: Failed password for invalid user guest from 192.168.1.50 port 55025 ssh2
Jan 12 02:14:20 ubuntu sshd[1460]: Failed password for invalid user oracle from 192.168.1.50 port 55052 ssh2
Jan 12 02:14:21 ubuntu sshd[1460]: Failed password for invalid user oracle from 192.168.1.50 port 55052 ssh2
```

Finding 3 — Successful Intrusion (02:15:08)

Evidence:

```
Accepted password for root from 192.168.1.50 port 55182 ssh2
pam_unix(sshd:session): session opened for user root
```

Conclusion: Attacker gained full root access.

Finding 4 — Attacker Disconnects (02:15:11)

Clear user logout indicating completion of malicious activity.

Conclusions

The logs conclusively prove:

- The attacker (192.168.1.50) initiated a **systematic port scan**, followed by a **high-speed brute-force attack**.
- Despite multiple failed attempts, the attacker successfully logged in as **root** at **02:15:08**.
- This constitutes a full system compromise.

Our Proposed Framework:

A **syslog analysis framework** defines how forensic investigators collect, preserve, correlate, and analyse log evidence after a cyberattack.This framework is designed specifically for **post-attack digital forensics**, not detection systems.

1. Evidence Acquisition Layer

Purpose: Collect logs without altering metadata.

Steps:

- Collect **syslog** and **auth.log** from the victim Linux machine.
- Calculate **SHA-256 hashes** to preserve integrity.
- Store evidence using **FTK Imager** into `.L01` or `.E01` containers.
- Record every transfer in the chain of custody.

2. Evidence Ingestion Layer

Purpose: Introduce logs into a forensic platform.

Steps:

- Import `.L01` into **Autopsy** as “Logical Evidence File”.
- Enable modules: *File Analysis*, *Log Analysis*, *Timeline Analysis*.
- Autopsy extracts timestamps + metadata automatically.

Outcome: Logs appear as structured items with searchable fields.

3. Log Parsing & Normalization Layer

Purpose: Convert raw text logs into structured events.

Parsing operations:

- Extract timestamp, hostname, process, PID.
- Extract SSH event type:
    - Failed password
    - Invalid user
    - Accepted login

    - Disconnect

- Extract network information from syslog:
    - Source IP
    - Destination port
    - Protocol
    - TCP flags

Normalization:

- Standardize fields such as `user`, `event_type`, `source_ip`, `port`.

4. Correlation & Linking Layer

Purpose: Match related events across multiple logs.

Correlation logic:

- **Syslog kernel events** (port scans) correlate with **auth.log SSH failures** within the same minute.
- Repeated failures for multiple usernames → **brute force behavior**.
- Spike in failures followed by a success → **compromise indicator**.
- Connect attacker IP across all entries → **192.168.1.50**.

Outcome: A clear chain from reconnaissance → brute force → intrusion.

5. Pattern Recognition Layer

Purpose: Detect and classify malicious behaviour.

Patterns used:

Pattern Name	Indicators Found
Port Scan Pattern	Rapid SYN packets across many ports

Username Enumeration Pattern	Invalid user attempts: admin/test/guest
Brute-Force Pattern	3 attempts per username, sequential
Privilege Compromise Pattern	Successful root login after failures
Exit Pattern	Disconnect after 3 seconds

6. Timeline Reconstruction Layer

Purpose: Build chronological representation of attacker activity.

7. Reporting & Documentation Layer

Purpose: Convert analysis into a court-ready or academic-ready report.

Deliverables:

- STAR methodology investigation
- Timeline diagram
- Hash verification
- Screenshots from Autopsy
- Findings + recommendations

Outcome: A complete forensic case report.