Linux Log Intrusion Detection

Using `/var/log/auth.log`

Technical Report (Student Project)

Student: Saurabh Chikte
Branch: Computer Engineering
Date: 5 December 2025

Abstract: This report documents a practical method for detecting failed SSH login attempts by analyzing the Linux authentication log (`/var/log/auth.log`). A small C++ test generator (`./loop`) produced controlled failed SSH attempts. I extracted relevant log entries, parsed timestamps and IP addresses, stored them in a CSV file, and generated an alert report summarizing login failures per IP.

Contents

Chapter 1

Introduction

This project demonstrates a simple workflow for detecting failed SSH login attempts using the Linux authentication log. The approach includes:

- Generating controlled failed SSH attempts using a C++ script.
- Extracting failed authentication log entries from `/var/log/auth.log`.
- Parsing timestamps and IP addresses into a structured CSV.
- Summarizing repeated login failures by IP to identify brute-force patterns.

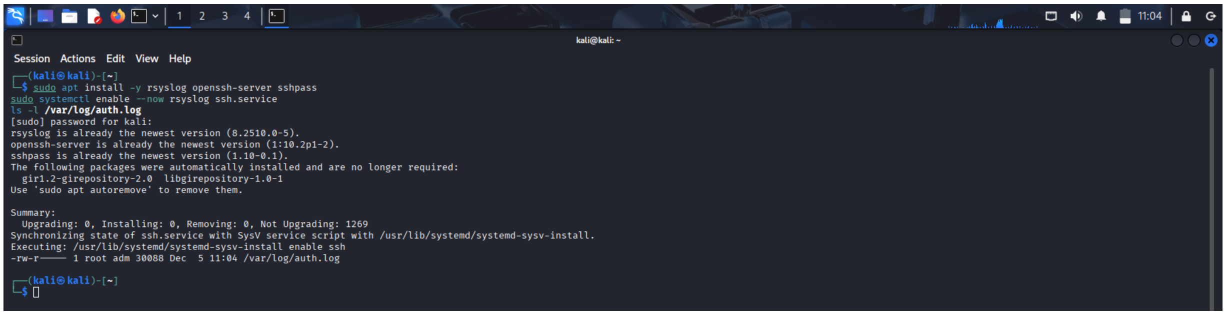
Chapter 2

Methodology

2.1 System and Services

I verified that both `rsyslog` and `ssh` services were enabled so that authentication events were logged correctly.

System setup screenshot

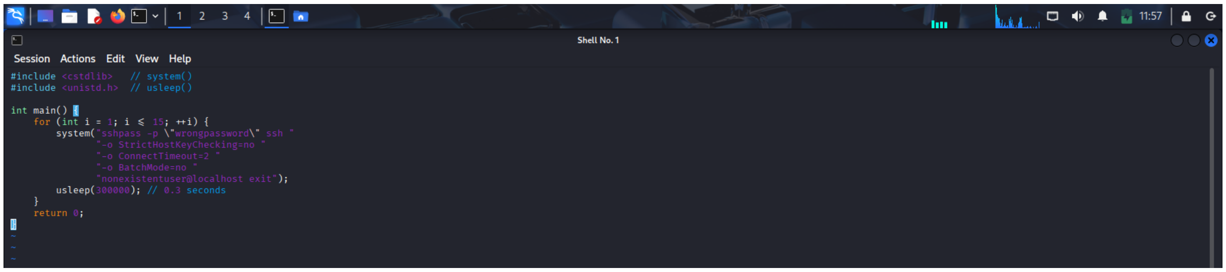


```
┌──(kali㉿kali)-[~]
└─$ sudo apt install -y rsyslog openssh-server sshpass
sudo systemctl enable --now rsyslog ssh.service
ls -l /var/log/auth.log
[sudo] password for kali:
rsyslog is already the newest version (8.2510.0-5).
openssh-server is already the newest version (1:10.2p1-2).
sshpass is already the newest version (1.10-0.1).
The following packages were automatically installed and are no longer required:
  gir1.2-girepository-2.0  libgirepository-1.0-1
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1269
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
-rw-r----- 1 root adm 30088 Dec  5 11:04 /var/log/auth.log

┌──(kali㉿kali)-[~]
└─$ 
```

2.2 Test Data Generation Using C++

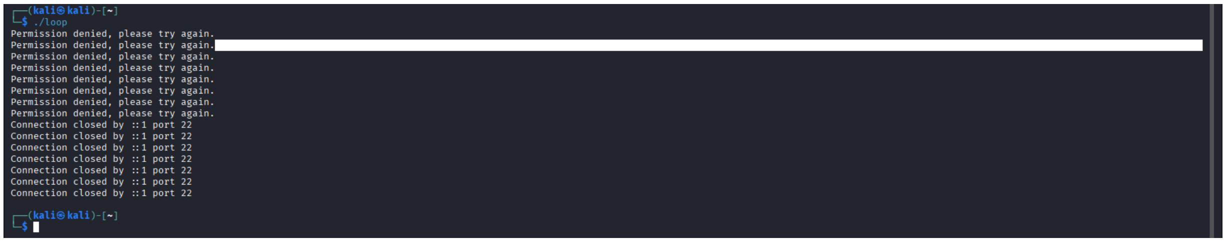
I wrote a C++ program (`loop.cpp`) that repeatedly attempts SSH authentication with an incorrect password. This reliably generates failed login entries for testing.

C++ generator source code (screenshot)



```
#include <cstdlib>   // system()
#include <unistd.h>  // usleep()

int main() {
    for (int i = 1; i <= 15; ++i) {
        system("sshpass -p \"wrongpassword\" ssh "
               "-o StrictHostKeyChecking=no "
               "-o ConnectTimeout=2 "
               "-o BatchMode=no "
               "nonexistentuser@localhost exit");
        usleep(300000); // 0.3 seconds
    }
    return 0;
}
~
~
~
```

Running the generator (./loop)

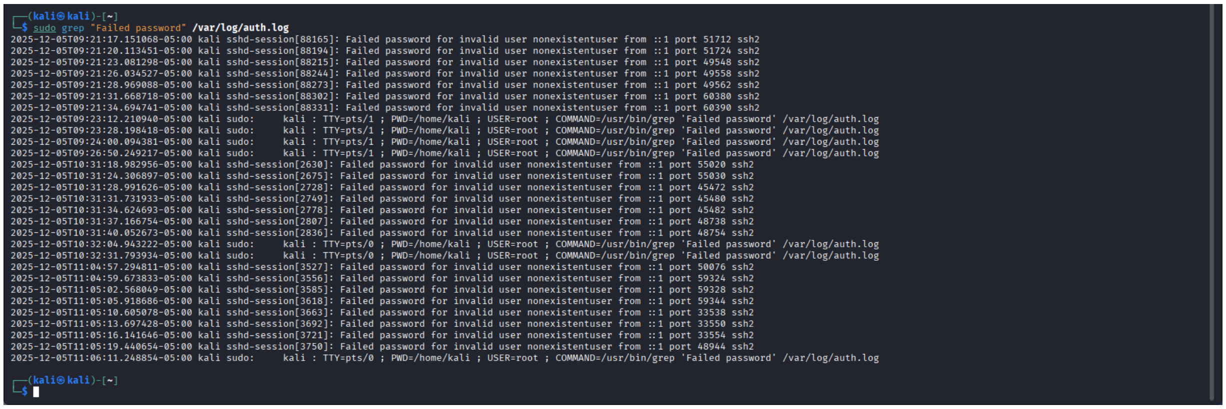


```
┌──(kali㉿kali)-[~]
└─$ ./loop
Permission denied, please try again.
Permission denied, please try again.
Permission denied, please try again.
Permission denied, please try again.
Permission denied, please try again.
Permission denied, please try again.
Permission denied, please try again.
Permission denied, please try again.
Connection closed by ::1 port 22
Connection closed by ::1 port 22
Connection closed by ::1 port 22
Connection closed by ::1 port 22
Connection closed by ::1 port 22
Connection closed by ::1 port 22
Connection closed by ::1 port 22

┌──(kali㉿kali)-[~]
└─$ 
```

2.3 Collecting Failed Authentication Logs

I extracted all lines containing "Failed password" from `/var/log/auth.log` and stored them in `failed_lines.txt`.

Grep output — failed SSH entries



```
┌──(kali㉿kali)-[~]
└─$ sudo grep "Failed password" /var/log/auth.log
2025-12-05T09:21:17.151068-05:00 kali sshd-session[88165]: Failed password for invalid user nonexistentuser from ::1 port 51712 ssh2
2025-12-05T09:21:20.113451-05:00 kali sshd-session[88194]: Failed password for invalid user nonexistentuser from ::1 port 51724 ssh2
2025-12-05T09:21:23.081298-05:00 kali sshd-session[88215]: Failed password for invalid user nonexistentuser from ::1 port 49548 ssh2
2025-12-05T09:21:26.034527-05:00 kali sshd-session[88244]: Failed password for invalid user nonexistentuser from ::1 port 49558 ssh2
2025-12-05T09:21:28.969088-05:00 kali sshd-session[88273]: Failed password for invalid user nonexistentuser from ::1 port 49562 ssh2
2025-12-05T09:21:31.668718-05:00 kali sshd-session[88302]: Failed password for invalid user nonexistentuser from ::1 port 60380 ssh2
2025-12-05T09:21:34.694741-05:00 kali sshd-session[88331]: Failed password for invalid user nonexistentuser from ::1 port 60390 ssh2
2025-12-05T09:23:12.210940-05:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-12-05T09:23:28.198418-05:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-12-05T09:24:00.094381-05:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-12-05T09:26:50.249217-05:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-12-05T10:31:18.982956-05:00 kali sshd-session[2630]: Failed password for invalid user nonexistentuser from ::1 port 55020 ssh2
2025-12-05T10:31:24.306897-05:00 kali sshd-session[2675]: Failed password for invalid user nonexistentuser from ::1 port 55030 ssh2
2025-12-05T10:31:28.991626-05:00 kali sshd-session[2728]: Failed password for invalid user nonexistentuser from ::1 port 45472 ssh2
2025-12-05T10:31:31.731933-05:00 kali sshd-session[2749]: Failed password for invalid user nonexistentuser from ::1 port 45480 ssh2
2025-12-05T10:31:34.624693-05:00 kali sshd-session[2778]: Failed password for invalid user nonexistentuser from ::1 port 45482 ssh2
2025-12-05T10:31:37.166754-05:00 kali sshd-session[2807]: Failed password for invalid user nonexistentuser from ::1 port 48738 ssh2
2025-12-05T10:31:40.052673-05:00 kali sshd-session[2836]: Failed password for invalid user nonexistentuser from ::1 port 48754 ssh2
2025-12-05T10:32:04.943222-05:00 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-12-05T10:32:31.793934-05:00 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-12-05T11:04:57.294811-05:00 kali sshd-session[3527]: Failed password for invalid user nonexistentuser from ::1 port 50076 ssh2
2025-12-05T11:04:59.673833-05:00 kali sshd-session[3556]: Failed password for invalid user nonexistentuser from ::1 port 59324 ssh2
2025-12-05T11:05:02.568049-05:00 kali sshd-session[3585]: Failed password for invalid user nonexistentuser from ::1 port 59328 ssh2
2025-12-05T11:05:05.918686-05:00 kali sshd-session[3618]: Failed password for invalid user nonexistentuser from ::1 port 59344 ssh2
2025-12-05T11:05:10.605078-05:00 kali sshd-session[3663]: Failed password for invalid user nonexistentuser from ::1 port 33538 ssh2
2025-12-05T11:05:13.697428-05:00 kali sshd-session[3692]: Failed password for invalid user nonexistentuser from ::1 port 33550 ssh2
2025-12-05T11:05:16.141646-05:00 kali sshd-session[3721]: Failed password for invalid user nonexistentuser from ::1 port 33554 ssh2
2025-12-05T11:05:19.440654-05:00 kali sshd-session[3750]: Failed password for invalid user nonexistentuser from ::1 port 48944 ssh2
2025-12-05T11:06:11.248854-05:00 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log

┌──(kali㉿kali)-[~]
└─$ 
```

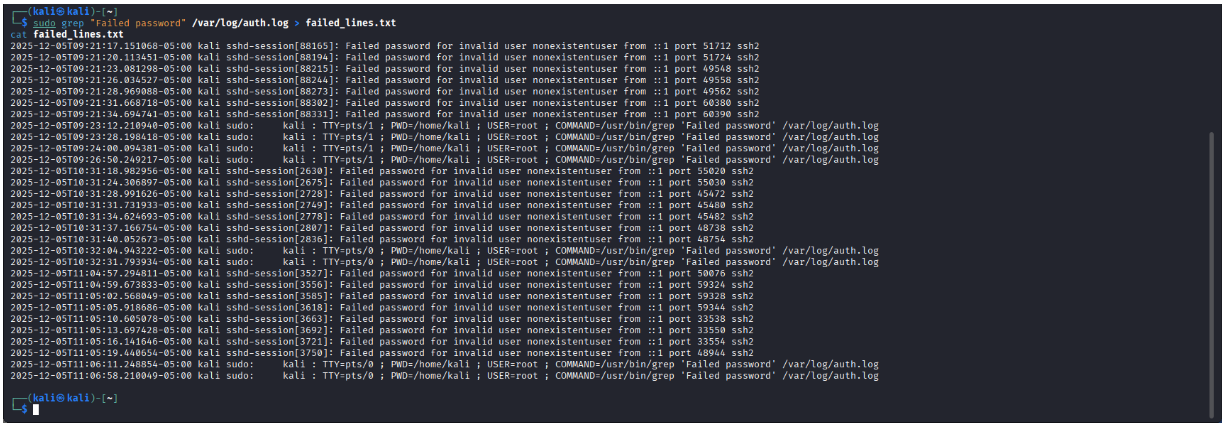
2.4 Creating the CSV (Timestamp and IP)

From each log entry, I extracted:

- Timestamp (first token)
- IP address (token after the word “from”)

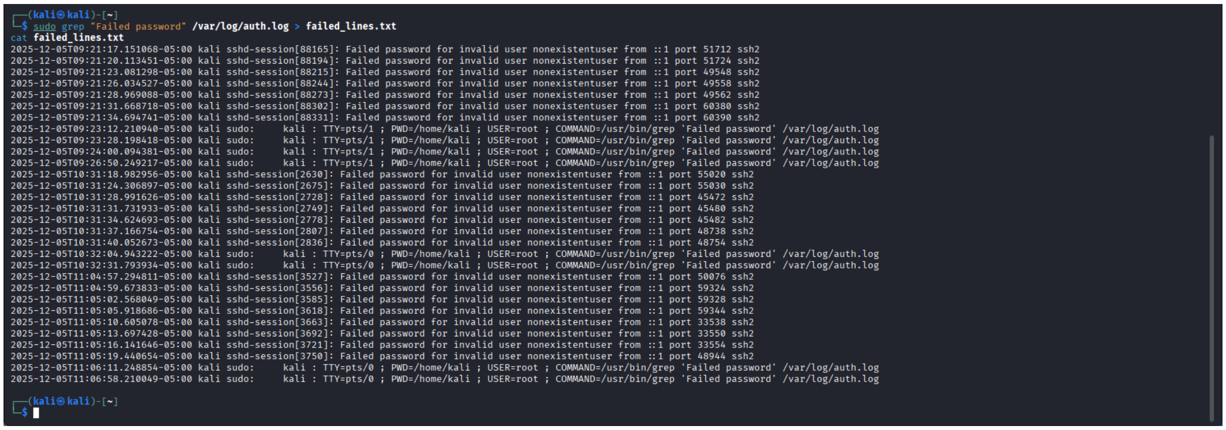
IPv6 loopback (`::1`) was normalized to `127.0.0.1`.

Saved failed lines



```
┌──(kali㉿kali)-[~]
└─$ sudo grep "Failed password" /var/log/auth.log > failed_lines.txt
cat failed_lines.txt
2025-12-05T09:21:17.151068-05:00 kali sshd-session[88165]: Failed password for invalid user nonexistentuser from ::1 port 51712 ssh2
2025-12-05T09:21:20.113451-05:00 kali sshd-session[88194]: Failed password for invalid user nonexistentuser from ::1 port 51724 ssh2
2025-12-05T09:21:23.081298-05:00 kali sshd-session[88215]: Failed password for invalid user nonexistentuser from ::1 port 49548 ssh2
2025-12-05T09:21:26.034527-05:00 kali sshd-session[88244]: Failed password for invalid user nonexistentuser from ::1 port 49558 ssh2
2025-12-05T09:21:28.969088-05:00 kali sshd-session[88273]: Failed password for invalid user nonexistentuser from ::1 port 49562 ssh2
2025-12-05T09:21:31.668718-05:00 kali sshd-session[88302]: Failed password for invalid user nonexistentuser from ::1 port 60380 ssh2
2025-12-05T09:21:34.694741-05:00 kali sshd-session[88331]: Failed password for invalid user nonexistentuser from ::1 port 60390 ssh2
2025-12-05T09:23:12.210940-05:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-12-05T09:23:28.198418-05:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-12-05T09:24:00.094381-05:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-12-05T09:26:50.249217-05:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-12-05T10:31:18.982956-05:00 kali sshd-session[2630]: Failed password for invalid user nonexistentuser from ::1 port 55020 ssh2
2025-12-05T10:31:24.306897-05:00 kali sshd-session[2675]: Failed password for invalid user nonexistentuser from ::1 port 55030 ssh2
2025-12-05T10:31:28.991626-05:00 kali sshd-session[2728]: Failed password for invalid user nonexistentuser from ::1 port 45472 ssh2
2025-12-05T10:31:31.731933-05:00 kali sshd-session[2749]: Failed password for invalid user nonexistentuser from ::1 port 45480 ssh2
2025-12-05T10:31:34.624693-05:00 kali sshd-session[2778]: Failed password for invalid user nonexistentuser from ::1 port 45482 ssh2
2025-12-05T10:31:37.166754-05:00 kali sshd-session[2807]: Failed password for invalid user nonexistentuser from ::1 port 48738 ssh2
2025-12-05T10:31:40.052673-05:00 kali sshd-session[2836]: Failed password for invalid user nonexistentuser from ::1 port 48754 ssh2
2025-12-05T10:32:04.943222-05:00 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-12-05T10:32:31.793934-05:00 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-12-05T11:04:57.294811-05:00 kali sshd-session[3527]: Failed password for invalid user nonexistentuser from ::1 port 50076 ssh2
2025-12-05T11:04:59.673833-05:00 kali sshd-session[3556]: Failed password for invalid user nonexistentuser from ::1 port 59324 ssh2
2025-12-05T11:05:02.568049-05:00 kali sshd-session[3585]: Failed password for invalid user nonexistentuser from ::1 port 59328 ssh2
2025-12-05T11:05:05.918686-05:00 kali sshd-session[3618]: Failed password for invalid user nonexistentuser from ::1 port 59344 ssh2
2025-12-05T11:05:10.605078-05:00 kali sshd-session[3663]: Failed password for invalid user nonexistentuser from ::1 port 33538 ssh2
2025-12-05T11:05:13.697428-05:00 kali sshd-session[3692]: Failed password for invalid user nonexistentuser from ::1 port 33550 ssh2
2025-12-05T11:05:16.141646-05:00 kali sshd-session[3721]: Failed password for invalid user nonexistentuser from ::1 port 33554 ssh2
2025-12-05T11:05:19.440654-05:00 kali sshd-session[3750]: Failed password for invalid user nonexistentuser from ::1 port 48944 ssh2
2025-12-05T11:06:11.248854-05:00 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-12-05T11:06:58.210049-05:00 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log

┌──(kali㉿kali)-[~]
└─$ 
```

CSV output (timestamp, IP)

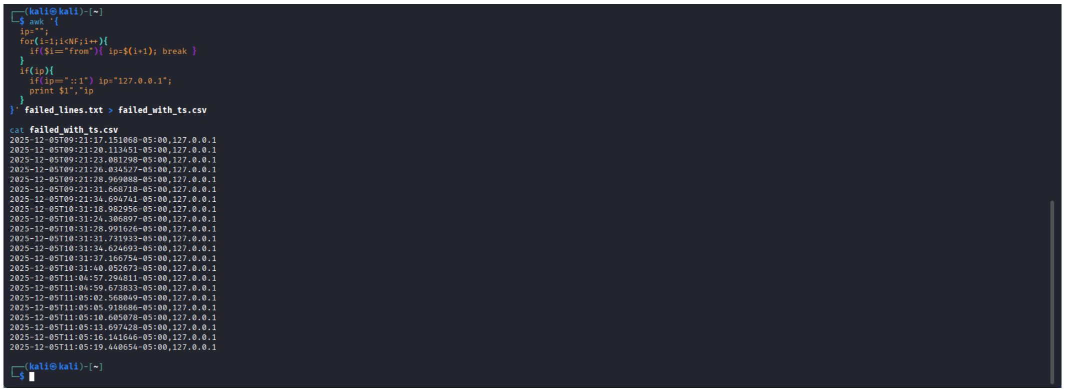


```
┌──(kali㉿kali)-[~]
└─$ sudo grep "Failed password" /var/log/auth.log > failed_lines.txt
cat failed_lines.txt
2025-12-05T09:21:17.151068-05:00 kali sshd-session[88165]: Failed password for invalid user nonexistentuser from ::1 port 51712 ssh2
2025-12-05T09:21:20.113451-05:00 kali sshd-session[88194]: Failed password for invalid user nonexistentuser from ::1 port 51724 ssh2
2025-12-05T09:21:23.081298-05:00 kali sshd-session[88215]: Failed password for invalid user nonexistentuser from ::1 port 49548 ssh2
2025-12-05T09:21:26.034527-05:00 kali sshd-session[88244]: Failed password for invalid user nonexistentuser from ::1 port 49558 ssh2
2025-12-05T09:21:28.969088-05:00 kali sshd-session[88273]: Failed password for invalid user nonexistentuser from ::1 port 49562 ssh2
2025-12-05T09:21:31.668718-05:00 kali sshd-session[88302]: Failed password for invalid user nonexistentuser from ::1 port 60380 ssh2
2025-12-05T09:21:34.694741-05:00 kali sshd-session[88331]: Failed password for invalid user nonexistentuser from ::1 port 60390 ssh2
2025-12-05T09:23:12.210940-05:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-12-05T09:23:28.198418-05:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-12-05T09:24:00.094381-05:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-12-05T09:26:50.249217-05:00 kali sudo:     kali : TTY=pts/1 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-12-05T10:31:18.982956-05:00 kali sshd-session[2630]: Failed password for invalid user nonexistentuser from ::1 port 55020 ssh2
2025-12-05T10:31:24.306897-05:00 kali sshd-session[2675]: Failed password for invalid user nonexistentuser from ::1 port 55030 ssh2
2025-12-05T10:31:28.991626-05:00 kali sshd-session[2728]: Failed password for invalid user nonexistentuser from ::1 port 45472 ssh2
2025-12-05T10:31:31.731933-05:00 kali sshd-session[2749]: Failed password for invalid user nonexistentuser from ::1 port 45480 ssh2
2025-12-05T10:31:34.624693-05:00 kali sshd-session[2778]: Failed password for invalid user nonexistentuser from ::1 port 45482 ssh2
2025-12-05T10:31:37.166754-05:00 kali sshd-session[2807]: Failed password for invalid user nonexistentuser from ::1 port 48738 ssh2
2025-12-05T10:31:40.052673-05:00 kali sshd-session[2836]: Failed password for invalid user nonexistentuser from ::1 port 48754 ssh2
2025-12-05T10:32:04.943222-05:00 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-12-05T10:32:31.793934-05:00 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-12-05T11:04:57.294811-05:00 kali sshd-session[3527]: Failed password for invalid user nonexistentuser from ::1 port 50076 ssh2
2025-12-05T11:04:59.673833-05:00 kali sshd-session[3556]: Failed password for invalid user nonexistentuser from ::1 port 59324 ssh2
2025-12-05T11:05:02.568049-05:00 kali sshd-session[3585]: Failed password for invalid user nonexistentuser from ::1 port 59328 ssh2
2025-12-05T11:05:05.918686-05:00 kali sshd-session[3618]: Failed password for invalid user nonexistentuser from ::1 port 59344 ssh2
2025-12-05T11:05:10.605078-05:00 kali sshd-session[3663]: Failed password for invalid user nonexistentuser from ::1 port 33538 ssh2
2025-12-05T11:05:13.697428-05:00 kali sshd-session[3692]: Failed password for invalid user nonexistentuser from ::1 port 33550 ssh2
2025-12-05T11:05:16.141646-05:00 kali sshd-session[3721]: Failed password for invalid user nonexistentuser from ::1 port 33554 ssh2
2025-12-05T11:05:19.440654-05:00 kali sshd-session[3750]: Failed password for invalid user nonexistentuser from ::1 port 48944 ssh2
2025-12-05T11:06:11.248854-05:00 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log
2025-12-05T11:06:58.210049-05:00 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log

┌──(kali㉿kali)-[~]
└─$ 
```

2.5 Generating the Alert Report

The CSV file was grouped by IP to produce `alert_report.txt`, highlighting repeated failed logins.

Final alert report (counts per IP)



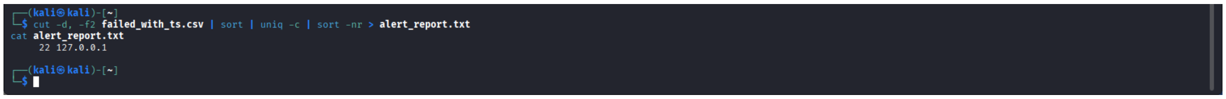
```
┌──(kali㉿kali)-[~]
└─$ awk '{
  ip="";
  for(i=1;i<NF;i++){
    if($i=="from"){ ip=$(i+1); break }
  }
  if(ip){
    if(ip=="::1") ip="127.0.0.1";
    print $1","ip
  }
}' failed_lines.txt > failed_with_ts.csv

cat failed_with_ts.csv
2025-12-05T09:21:17.151068-05:00,127.0.0.1
2025-12-05T09:21:20.113451-05:00,127.0.0.1
2025-12-05T09:21:23.081298-05:00,127.0.0.1
2025-12-05T09:21:26.034527-05:00,127.0.0.1
2025-12-05T09:21:28.969088-05:00,127.0.0.1
2025-12-05T09:21:31.668718-05:00,127.0.0.1
2025-12-05T09:21:34.694741-05:00,127.0.0.1
2025-12-05T10:31:18.982956-05:00,127.0.0.1
2025-12-05T10:31:24.306897-05:00,127.0.0.1
2025-12-05T10:31:28.991626-05:00,127.0.0.1
2025-12-05T10:31:31.731933-05:00,127.0.0.1
2025-12-05T10:31:34.624693-05:00,127.0.0.1
2025-12-05T10:31:37.166754-05:00,127.0.0.1
2025-12-05T10:31:40.052673-05:00,127.0.0.1
2025-12-05T11:04:57.294811-05:00,127.0.0.1
2025-12-05T11:04:59.673833-05:00,127.0.0.1
2025-12-05T11:05:02.568049-05:00,127.0.0.1
2025-12-05T11:05:05.918686-05:00,127.0.0.1
2025-12-05T11:05:10.605078-05:00,127.0.0.1
2025-12-05T11:05:13.697428-05:00,127.0.0.1
2025-12-05T11:05:16.141646-05:00,127.0.0.1
2025-12-05T11:05:19.440654-05:00,127.0.0.1

┌──(kali㉿kali)-[~]
└─$ 
```

Chapter 3

Results

- The authentication log correctly recorded all failed SSH attempts.
- The CSV contained accurate timestamp and IP pairs.
- The alert report showed repeated failures from the local loopback IP (expected during local testing).

Example raw log entries



```
┌──(kali㉿kali)-[~]
└─$ cut -d, -f2 failed_with_ts.csv | sort | uniq -c | sort -nr > alert_report.txt
cat alert_report.txt
     22 127.0.0.1

┌──(kali㉿kali)-[~]
└─$ 
```

Chapter 4

Files Produced

- loop.cpp and ./loop — C++ test generator.
- failed_lines.txt — Raw extracted failed authentication entries.
- failed_with_ts.csv — Parsed dataset (timestamp, IP).
- alert_report.txt — Summary of login failures per IP.
- All screenshots used in this report.

Chapter 5

Conclusion and Next Steps

This project demonstrated a practical workflow for detecting failed SSH logins using native system logs. Standard tools like `grep`, `awk`, and `cut` were sufficient to extract useful information. A C++ script provided repeatable and controlled test data, and basic aggregation helped identify repeated login attempts.

Detecting failed SSH logins is a foundational skill in cybersecurity. SOC analysts and SIEM tools use similar methods to identify brute-force attacks, unauthorized access attempts, and suspicious behaviour on production servers.

- Integrate GeoIP lookup for external attackers.
- Automate alerts if an IP exceeds a threshold of failed attempts.
- Forward logs to a central SIEM (ELK, Splunk, etc.).

Prepared by: **Saurabh Chikte**