

Simple Log Analyzer for Failed Logins

Author: Daniel Chisasura

Version: 1.0






License: MIT

Platform: Linux (Debian/Ubuntu-based systems)

Overview

This Bash script helps system administrators detect potential brute-force attacks by analyzing failed login attempts in the system's authentication log. It identifies IP addresses with repeated failures and flags those exceeding a configurable threshold.

Features

-  Reads from `/var/log/auth.log` (default)
-  Filters for "Failed password" entries
-  Counts failed login attempts per IP
-  Alerts for IPs exceeding a defined threshold
-  Validates log file readability before execution

Usage

1. Save the Script

Save the script as `log_analyzer.sh` and make it executable:

```
chmod +x log_analyzer.sh
```

2. Run the Script with Root Privileges

```
sudo ./log_analyzer.sh
```


Configuration

You can modify the following variables in the script to suit your environment:

`LOG_FILE="/var/log/auth.log" # Path to the log file`

`FAILED_LOGIN_THRESHOLD=5 # Alert threshold for failed attempts`

Sample Output

 Analyzing log file: /var/log/auth.log

Threshold for alerts is set to 5 failed attempts.

```
-----  
🚨 ALERT: IP Address 203.0.113.45    failed login 12 times.  
🚨 ALERT: IP Address 192.168.1.100  failed login 8 times.  
-----
```

✅ Analysis complete.

Lessons Learned

- **Root access is required** to read system logs.
- **Thresholds help reduce noise** and focus on real threats.
- **Automation improves visibility** into login activity.
- **Regular monitoring** can help detect and prevent brute-force attacks.

Disclaimer

This script is intended for educational and administrative use. Always verify flagged IPs before taking action to avoid blocking legitimate users.