Lab5: Host-based Log Analysis for Intrusion Detection

Instructor: Dr. Maryam R. Aliabadi
Lab Duration: 2 hours
Date: Oct 10^{h}, 2025

Learning Objectives

- Understand system logging and process control.
- Analyze authentication, privilege, and system logs.
- Detect suspicious patterns and possible intrusions.
- Automate log analysis and reporting.

Lab Setup

```
sudo apt udate
sudo apt install rsyslog logwatch logcheck auditd
sudo systemctl enable --now rsyslog
sudo systemctl enable --now auditd
```

Part 1 – Log Discovery and Configuration

1. Explore log files: `ls -lh /var/log`

   Q1. Identify three logs most relevant for detecting intrusions.

2. Inspect `rsyslog` configuration: `cat /etc/rsyslog.conf | grep -v '^#'`

Part 2 – Authentication and Privilege Analysis

1. Extract failed logins:

```
grep "Failed password" /var/log/auth.log
```

2. Extract successful logins:

```
grep "Accepted password" /var/log/auth.log
```

Q2. Which IP address generated the most failed attempts?

3. Identify Brute-Force Patterns (Correlate failed attempts with IP addresses):

```
awk '/Failed password/{print $(NF-3)}' /var/log/auth.log | sort | uniq -c |
sort -nr | head
```

Q3. How many failed login attempts originated from each IP?

4. Detect sudo usage and possible misuse:

```
grep "sudo" /var/log/auth.log | grep "COMMAND"
```

Q4. Were there any unsuccessful sudo attempts?

5. Investigate System Restart and Process Activity: `sudo journalctl -b -1 && sudo tail -n 50 /var/log/syslog`

Q5. Were there unexpected services failing?

Note: By default, your Ubuntu system (or VM) has **no failed logins, no brute-force attempts, and no sudo misuse** logged — so most grep or awk commands will produce **no output**. To generate some results, attempt to SSH into your own system with **wrong credentials** several times. Here is **how to Get Meaningful Results for this lab:**

Log Type	How to Generate
Failed password	Try SSH with wrong password
Successful login	SSH with correct password
sudo misuse	Run sudo with wrong password
Restart logs	Run sudo reboot or restart rsyslog
Denied access	Try reading /etc/shadow as normal user
Audit changes	Modify /etc/passwd after setting watch

Part 3 – Process and System Integrity Analysis

1. Inspect startup/reboot activity: `journalctl --list-boots && journalctl -b -1`

Q5. Were there unexplained restarts?

2. Analyze kernel and system logs for errors: `grep -E "failed|denied" /var/log/syslog`

Q6. Identify any process crash or denied access event.

3. Audit critical file modifications:

```
sudo auditctl -w /etc/passwd -p war -k passwd_changes
sudo ausearch -k passwd_changes
```

Q7. Was /etc/passwd modified during the session?

Part 4 – Automating Log Analysis

1. Create shell script (named auth_summary.sh) to summarize login activity
2. Paste:

```
#!/bin/bash
echo "===== Failed Logins ====="
grep "Failed password" /var/log/auth.log | awk '{print $(NF-3)}' | sort | uniq -c | sort -nr
echo
echo "===== Successful Logins ====="
grep "Accepted password" /var/log/auth.log | awk '{print $(NF-3)}' | sort | uniq -c | sort -nr
echo
echo "===== Sudo Attempts ====="
grep "sudo" /var/log/auth.log | grep "COMMAND"
```

Q8. How can you enhance this script to automatically email a summary report daily?

3. Make it executable: `chmod +x auth_summary.sh && ./auth_summary.sh`
4. Schedule script with cron:

```
crontab -e
# add: 0 9 * * * /home/student/auth_summary.sh >>
/home/student/auth_report.txt
```

Part 5 – Advanced Correlation & Visualization

1. Generate reports with Logwatch: `sudo logwatch --range today --detail high`
2. Extract top event sources:

```
grep "sshd" /var/log/auth.log | awk '{print $1,$2,$3,$(NF-3)}' | sort | uniq
-c | sort -nr | head
```

3. Create I/O Graph using journalctl and awk.

```
journalctl --since "1 hour ago" --output=short-unix | awk '{print $1}' | uniq
-c
```

Q9. At what time were most login attempts observed?

Part 6 – Forensic Interpretation & Report Writing

- Screenshots of key commands & outputs
- Evidence of attack patterns (IP addresses, sudo misuse)
- Incident summary (≤1 page) with indicators of compromise and recommended mitigation steps

Deliverables

- Auth summary script output
- Question answers

- Screenshots of analyzed logs
- Incident report with findings and recommendations
- submit your report with the following name format through the Learning Hub.

Filename: Lab5-FirstName-Lastname-StdNo.PDF

Good luck!