System Logs and Monitoring - Learning Summary

Overview

System logs on Linux are files containing information about system and user activities. They are crucial for:

- Monitoring system behavior
- Troubleshooting issues
- Identifying security breaches
- Assessing penetration testing effectiveness

Proper log configuration and regular analysis enhance system security.

Key Types of Logs

1. Kernel Logs

- **Location:** `/var/log/kern.log`
- **Contents:** Kernel activity, driver status, system calls
- **Uses:** Identify hardware issues, crashes, malware behavior

2. System Logs

- **Location:** `/var/log/syslog`
- **Contents:** Service starts/stops, login attempts, reboots
- **Uses:** Detect access patterns, diagnose availability issues

Example Entry:

```
Feb 28 2023 15:04:22 server sshd[3010]: Failed password for htb-student
from 10.14.15.2 port 50223 ssh2
```

3. Authentication Logs

- **Location:** `/var/log/auth.log`
- **Contents:** Successful/failed authentication attempts
- **Uses:** Track unauthorized access, validate security settings

Example Entry:

```
Feb 28 2023 18:15:01 sshd[5678]: Accepted publickey for admin from
10.14.15.2 port 43210 ssh2
```

4. Application Logs

- **Location:** Varies (e.g., `/var/log/apache2/error.log`, `/var/log/mysql/error.log`)
- **Contents:** Application-specific events and errors
- **Uses:** Find vulnerabilities or misconfigurations

Example Access Log Entry:

```
2023-03-07T10:15:23+00:00 servername privileged.sh: htb-student accessed
/root/hidden/api-keys.txt
```

Common Log Locations for Services

Service	Log File Location
Apache	`/var/log/apache2/access.log`
Nginx	`/var/log/nginx/access.log`
OpenSSH	`/var/log/auth.log` (Ubuntu) / `/var/log/secure` (CentOS)
MySQL	`/var/log/mysql/mysql.log`
PostgreSQL	`/var/log/postgresql/postgresql-version-main.log`
Systemd	`/var/log/journal/`

5. Security Logs

- **Locations:** Varies (e.g., `/var/log/fail2ban.log`, `/var/log/ufw.log`)
- **Uses:** Identify failed login attempts, firewall activities, config changes

---

Tools for Log Analysis

- **tail** – View end of log files in real-time
- **grep** – Search for patterns in logs
- **sed** – Stream editing for filtering and formatting
- GUI log viewers (in Linux desktops)

Best Practices:

- Set appropriate log levels
- Configure log rotation
- Secure log files from unauthorized access
- Review logs regularly

Learning Tip: Regularly practice analyzing logs from a Linux virtual machine using tools like `grep`, `tail`, and check `/var/log/` structure.