**🔹 Lab Report: Locating Log Files**

**📌 Objectives**

The objective of this lab was to get familiar with locating and manipulating Linux log files. Specifically, the lab aimed to:

* Understand the purpose and structure of log files.
* Locate log files on both known and unknown systems.
* Differentiate between application, system, and web server log files.
* Monitor log files in real time using Linux commands.

**📌 Required Resources**

* Security Workstation Virtual Machine (VM)
* Linux terminal with root privileges

**📌 Lab Tasks & Procedures**

**Part 1: Log File Overview**

Log files are essential for tracking system and application events. They help in troubleshooting, performance monitoring, and security analysis.

**Step 1: Web Server Log Example**

**Sample Apache log entry:**

[Wed Mar 22 11:23:12.207022 2017] [core:error] [pid 3548:tid 4682351596] [client 209.165.200.230] File does not exist: /var/www/apache/htdocs/favicon.ico

**Breakdown:**

* **Timestamp:** Wed Mar 22 11:23:12.207022 2017
* **Type:** Error
* **PID:** 3548
* **Client IP:** 209.165.200.230
* **Description:** Missing file favicon.ico

📌 **Answer:** On March 22, 2017 at 11:23:12, the client 209.165.200.230 attempted to request the file /var/www/apache/htdocs/favicon.ico, which did not exist. This triggered an error.

**Logstash Example Output:**

83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] 'GET /presentations/... HTTP/1.1' 200 203023

📌 **Answer:** Yes, this is still a web transaction. Although the log format differs, the presence of GET requests, client IPs, and browser headers confirms it is a web server log. The format difference is due to configuration and logging style.

**Step 2: Operating System Log Example**

Linux stores system events under /var/log/messages.

**Sample log entries:**

Mar 20 14:28:29 secOps kernel: [21239.566409] pcnet32 0000:00:03.0 enp0s3: link down

Mar 20 14:28:33 secOps kernel: [21243.404646] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex

📌 **Answer:** On May 19, between 04:19:53 and 04:21:27, the network interface was flapping (going up and down repeatedly), confirming the reported issue of network slowness.

**Part 2: Locating Log Files in Unknown Systems**

For unknown systems, logs must be identified manually. Using **nginx** as an example:

* Documentation was checked using:
* man nginx
* Confirmed nginx was running using:
* ps ax | grep nginx
* Located configuration file under /etc/nginx/nginx.conf.
* Located log files under /var/log/nginx/.

📌 Logs found:

* access.log
* Rotated/compressed logs like access.log.1.gz, access.log.2.gz

These confirm nginx was logging access events.

**Part 3: Monitoring Log Files in Real Time**

Real-time monitoring was done using the tail command:

sudo tail /var/log/nginx/access.log

📌 Output included multiple HTTP requests such as:

127.0.0.1 - - [21/May/2017:15:32:32 -0400] 'GET / HTTP/1.1' 304 0

This confirmed live monitoring of nginx logs.

**📌 Summary**

This lab demonstrated:

* Log files are critical for both applications and operating systems.
* Different services use different formats and store logs in /var/log/.
* For unknown systems, documentation, process status, and config files help locate logs.
* Tools like cat, more, less, and especially tail are essential for working with and monitoring logs in real time.

**📌 Learning Outcomes**

By completing this lab, I learned to:

* Identify and interpret different log formats (Apache, Logstash, kernel logs).
* Use Linux commands to navigate and view log files.
* Locate logs for unfamiliar services (e.g., nginx).
* Monitor live logs using the tail command.
* Understand the role of logs in troubleshooting and security analysis.

**📌 Conclusion**

Logs are a fundamental component of system administration and cybersecurity. Mastering how to locate, interpret, and monitor logs is critical for troubleshooting, detecting security incidents, and ensuring system health. This lab provided hands-on experience that directly applies to real-world scenarios in IT and cybersecurity operations. 







