1. **What kind of information would be saved into following types of log files**

   Operating system, app, and service log files contain event information. They are critical for detecting security threats, addressing faults, and maintaining system functionality. The primary log file types, their contents, storage locations, possible threats, and how to monitor them on Windows, Mac, and Ubuntu Linux are covered here.

1- Application Logs

Records of application-specific events such as errors, warnings, performance issues, and user activity (e.g., failed login attempts, crashes).

Storage Locations:

Windows: C:\ProgramData\YourApplication\Logs\

MacOS: /Library/Logs/YourApplication/

Linux (Ubuntu): /var/log/application-name.log

Threats Detected: Unusual application behavior, errors, or unauthorized access attempts. Attackers may exploit vulnerabilities in applications, and their activity can appear in these logs.

Monitoring: In Windows, use Event Viewer; in MacOS, use the Console app; and in Ubuntu, use commands like tail or grep to view specific logs.

2- Event Logs

Information Saved: System-wide logs detailing events like application installations, system boot times, user logins/logouts, and hardware changes.

Storage Locations:

Windows: C:\Windows\System32\winevt\Logs\

MacOS: /var/log/system.log

Linux (Ubuntu): /var/log/syslog

Threats Detected: Unauthorized logins, hardware tampering, and system misuse. Failed login attempts or privilege escalations are red flags for potential attacks.

Monitoring: Event Viewer in Windows provides detailed event filtering; Console in MacOS offers system-wide log views; in Ubuntu, use journalctl to filter specific events.

3- Service Logs

Information Saved: Logs related to specific services running in the background, such as web servers, networking services, or databases. They record start/stop times, status messages, and errors.

Storage Locations:

Windows: Depends on the service, e.g., C:\Program Files\ServiceName\Logs\

MacOS: /Library/Logs/ServiceName/

Linux (Ubuntu): /var/log/service-name.log

Threats Detected: Denial-of-service attacks, unauthorized access to services, service crashes, or failures may indicate external attacks or configuration errors.

Monitoring: In Windows, monitor services through Task Manager and Event Viewer. On MacOS, use Console to track service logs. In Linux, monitor services using systemctl status or journalctl.

4. System Logs

Information Saved: Records related to core system operations like kernel messages, driver activity, boot sequences, and system crashes. These logs help diagnose hardware and operating system issues.

Storage Locations:

Windows: C:\Windows\System32\LogFiles\

MacOS: /var/log/system.log

Linux (Ubuntu): /var/log/kern.log

Threats Detected: System crashes, kernel panics, or malicious attempts to compromise hardware drivers. Unauthorized changes or malfunctioning hardware can appear in these logs.

Monitoring: In Windows, use Event Viewer to track system issues. On MacOS, the Console app is used, while in Ubuntu, tools like dmesg and journalctl help track system-level events.

2. **Where in each of the common Operating Systems those logs would be stored (Windows, Mac, Linux(changes per distro so provide in answer which you are using)**

Windows: Use Event Viewer to review system, application, and security logs. You can also set up alerts via Windows Task Scheduler for specific event triggers.
MacOS: The Console app provides access to all system logs. It also allows filtering and searching for specific log events.

Ubuntu Linux: Use command-line tools like tail, journalctl, or grep to view logs in real-time or search for specific issues. Tools like logwatch can be set up for automated monitoring.

3. **What kind of threats could you notice by monitoring each log file?**
4. **How would you go about monitoring logs on your personal computer?**

Application Logs: Identify application crashes, unauthorized access attempts, and vulnerability exploitation.
Event Logs: Track system-wide issues such as failed logins, system changes, or unusual user activities.
Service Logs: Detect service failures, unauthorized access, or denial-of-service attacks.

System Logs: Identify system malfunctions, hardware issues, or security breaches involving core system components.

Sources

1. Microsoft. “View and Understand Event Logs.” Microsoft Support, 2023.
2. Apple Support. “Use Console to View Logs on Your Mac.” Apple, 2024.
3. Ubuntu Documentation. "Log Files - Where They Are and How to Read Them." Ubuntu Wiki, 2023.
4. Red Hat. "Linux Log Files Explained." Red Hat, 2023.
5. Cybersecurity & Infrastructure Security Agency (CISA). “Log Management and Monitoring for Security,” 2023.