SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with ‘A’ Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : 19SB402 NETWORKING AND CYBERSECURITY

II YEAR / IV SEMESTER

Unit IV **SECURITY ELEMENTS**
Topic :Log Files

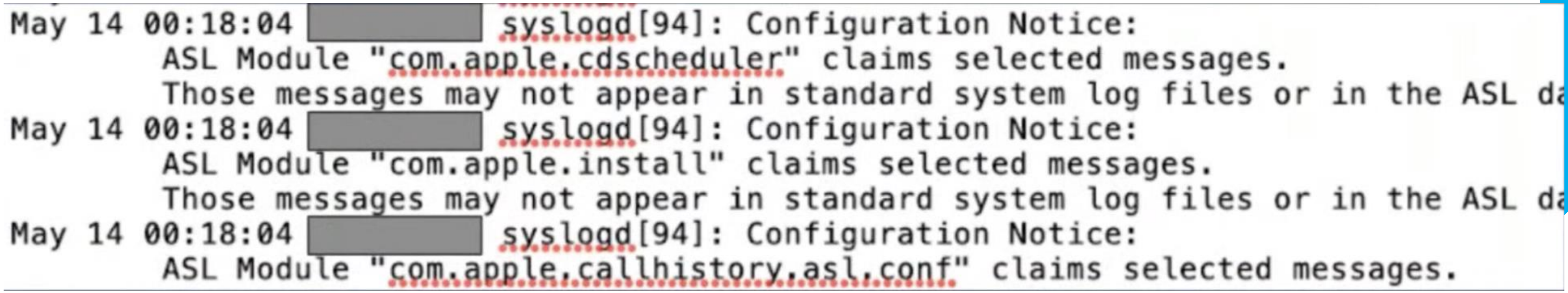
Log files

- Log files are the **primary data source** for network observability.

- A log file is a **computer-generated data file** that **contains information about usage patterns, activities, and operations within an operating system, application, server or another device**.

- Log files are a **historical record of everything** and anything that happens **within a system**, including events such **as transactions, errors and intrusions.**

- That data can be **transmitted in different ways** and can be in **both structured, semi-structured and unstructured format.**



```
May 14 00:18:04 [redacted] syslogd[94]: Configuration Notice:
        ASL Module "com.apple.cdscheduler" claims selected messages.
        Those messages may not appear in standard system log files or in the ASL da
May 14 00:18:04 [redacted] syslogd[94]: Configuration Notice:
        ASL Module "com.apple.install" claims selected messages.
        Those messages may not appear in standard system log files or in the ASL da
May 14 00:18:04 [redacted] syslogd[94]: Configuration Notice:
        ASL Module "com.apple.callhistory.asl.conf" claims selected messages.
```

The basic anatomy of a log file includes:

- **The timestamp** – the **exact time at which the event logged occurred**
- **User information**
- **Event information** – what was the **action taken**
- However, depending on the type of log source, the file will also contain a wealth of relevant data.
- For example, server logs will also include the referred webpage, http status code, bytes served, user agents, and more.

Where do Log Files Come From?

Just about everything produces some version of a log, including:

- Apps
- Containers
- Databases
- Firewalls
- Endpoints
- IoT devices
- Networks
- Servers
- Web Services

Types of Logs

- Nearly **every component in a network generates a different type of data** and **each component collects that data in its own log**. Because of that, **many types of logs** exist, including:

- **Event Log**: **a high-level log** that **records information about network traffic and usage**, such as login attempts, failed password attempts, and application events.
- **Server Log**: **a text document** containing a **record of activities** related to a specific server in a specific period of time.
- **System Log (syslog)**: **a record of operating system events**. It includes **startup messages, system changes, unexpected shutdowns, errors and warnings, and other important processes. Windows, Linux, and macOS all generate syslogs.**

- **Authorization Logs and Access Logs**: include a **list of people or bots accessing certain applications or files.**

- **Change Logs**: include a **chronological** list of changes made to an application or file.

- **Availability Logs**: **track system performance, uptime, and availability.**

- **Resource Logs**: provide information about **connectivity issues** and capacity limits.

- **Threat Logs**: **contain information about system, file, or application traffic** that matches a predefined security profile within a firewall.

Who Uses Log Files?

Log files can provide almost every role at an organization with valuable insights. Below are some of the most common use cases by job function:

ITOps(operations)

- It refers to the **process of managing an organization's IT operations**. ITOps is **responsible for the smooth running of an organization's IT infrastructure** and **supports it to meet the business needs of internal and external users**.
- identify infrastructure balance
- Manage workloads
- Maintain Uptime/Outages
- Ensure business continuity
- Reduce cost and risk

DevOps

- It mean development” and “operations”, **it is the combination of practices and tools designed to increase an organization's** ability to deliver applications and services faster than traditional software development processes.

- Managing CI/CD

- Maintain application uptime

- Detect critical application errors

- Identify areas to optimize application performance

DevSecOps

- DevSecOps stands for development, **security, and operations**. It's an approach to **culture, automation, and platform design that integrates security as a shared responsibility throughout** the entire IT lifecycle.

- Drive a shared ownership on application **development and security**

- Saving time/money and reputational risks by finding potential issues before deployment

SecOps/Security

- Security Operations is a **collaboration between IT security and operations teams that integrates tools, processes, and technology** to keep an enterprise secure while reducing risk. Let's Define SecOps.
- Uncover clues around the ‘who, when, where’ of an attack
- Identify suspicious activity
- See spikes in blocked/allowed traffic
- Implementing the methodologies such as the OODA Loop

IT Analysts

- Compliance management and Reporting

- OpEx (operational expenditure) **is the money a company** or **organization spends on an ongoing, day-to-day basis to run its business**

- CapEx(capital expenditures) major purchases that are usually **capitalized on a company's balance** sheet instead of being expensed.

- Business Insights A **business insight combines data and analysis** to make sense of and deepen your understanding of a situation, giving your company a competitive edge.

Any Query????

Thank you……