LOG ANALYSIS

PART 1

WHAT IS A LOG?

A record of events or activities generated by software, operating systems, or applications

TYPES OF LOG

- Event Log
- Server Log
- Application Log
- Database Log
- Security Log
- System Log
- Audit Log

EVENT LOG

An event log records events and activities on a computer system, such as system events, errors, warnings, and user actions.

Example Log Entry (Security Event):

Logon Type: 3
User: NT AUTHORITY\SYSTEM
Source: Security
Event ID: 4624
Description: An account was successfully logged on.

SYSTEM LOG

System logs track the operation of the operating system and hardware components. They include information about system startups, shutdowns, and hardware issues.

Example:

Log Type: Error
Source: Disk
Event ID: 7
Description: The device, \Device\Harddisk0\DR0, has a bad block.

SECURITY LOGS

Security logs focus on recording security-related events, such as login attempts, account changes, and other activities that may pose a security risk.

Example:

Log Type: Information
Source: Security
Event ID: 4624
Description: An account was successfully logged on.
Logon Type: 3
User: DOMAIN\User

APPLICATION LOGS

Application logs track events and errors related to specific software applications. These logs can help developers and administrators identify issues within an application.

Example:

Log Type: Error
Source: Application Error
Event ID: 1000
Description: Faulting application <Application Name>, version <Version>, faulting module <Module Name>, version <Module Version>, fault address <Memory Address>.

AUDIT LOGS

Audit logs capture information about user activities and changes made to the system configuration. They are crucial for compliance and accountability.

Example:

Log Type: Success Audit
Source: Security
Event ID: 628
Description: User Account Management: User Account Created.
New Account: DOMAIN\NewUser

DEBUG LOGS

Debug logs contain detailed information about the internal workings of a program. These logs are useful for developers when diagnosing and fixing bugs.

Example:

Log Type: Debug
Source: MyApp
Message: Entering function <Function Name>. Variable1=<Value1>, Variable2=<Value2>

TRANSACTION LOGS

Transaction logs track changes made to a database to ensure data integrity and recoverability in case of system failures.

Example:

Log Type: Information
Source: SQL Server
Event ID: 9002
Description: The transaction log for database '<Database Name>' is full due to '<Reason>'.
Transaction log entries: ...

IN **PART 2,** I WILL DISCUSS

HOW TO ANALYZE LOGS??