7.8.2 Log Facts

Logs, or audit trails, are a record of events on a system. Logging capabilities are built into operating systems, services, and applications. Log entries are generated in response to configuration changes, changes in system state, or in response to network conditions.

Be aware of the following facts about logs:

- Logs must be analyzed to be useful; only by looking at the logs will you be able to discover problems. Depending on the log type, additional tools might be available to analyze logs for patterns.
- By default, some logging is enabled and performed automatically. To gather additional information, you can usually enable more extensive logging.
- Logging requires system resources (processor, memory, and disk). Carefully assess the amount of logging you need for system security.
- The three classic Windows logs are:
  - Application
  - System
  - Security
- You should always promptly resolve or report any suspicious or unauthorized activity revealed in the logs.
- Logging can be a preventative method of security. For example, if someone knows they are being monitored by the system automatically, they are less likely to perform unauthorized or illegal activities. A banner message immediately before login reminds users that the system is being audited.
- Violation logging uses defined threshold for specific events or counters. When activity exceeds the threshold, an action is logged.
- Some forms of auditing might be a violation of user privacy. To avoid privacy conflicts, make sure that auditing applies to all users and is clearly communicated.
- There is no standard log file format between systems.

On most operating systems, you can track and log a wide range of different event types; however, logging everything is not practical from either a logging or analysis perspective. For this reason, you should log only those types of events that are of most interest to your security operations. The following table identifies the types of events the log should include:

Event	Data to Capture
Internet Connection	Internet connection log data should include the: - Name of the user accessing the internet - Name of the host being accessed - IP addresses of the source and destination - Port numbers of the source and destination - Time the connection was made
System Level	System level log data should include: - Successful and unsuccessful login attempts - The user name logging in - Beginning and ending times of access - Activities performed on the system
Application Level	Application/service logs can include virus logs and DNS logs. Log data should include: - Names of files accessed - Actions performed - Database records modified - Any access attempts that were denied - Failed startup attempts
User Level	User level log data should include: - The commands used - Successful and unsuccessful attempts to access resources
Access	An *access log*, or a *security log*, should record information-related system access, such as: - Each time a user attempts to log in - Incorrect password usage - Use of user rights
Performance	A *performance log* should record information about the use of system resources such as printers and servers. With performance logging, system activity is recorded at regular intervals.
Firewall	A firewall log identifies: - Allowed traffic

	▪ Blocked traffic ▪ Ports that are used. For example, you can identify servers that are running a specific service or see computers that are communicating using ports that might indicate malicious software

A system audit uses automated tools to gather and analyze data about a system. The operating system audit subsystem provides the mechanism whereby system events are monitored and logged. The following table defines these mechanisms:

Subsystem	Description
Kernel	The *kernel audit mechanism* is the mechanism that generates log records based on the user process and activities through kernel system calls and is central to the audit subsystem. Each kernel system call has a corresponding entry in a subsystem table that indicates whether or not the call is relevant to security and to which type of events the system will respond.
Device Driver	The *audit device* driver is responsible for accepting log records from the audit kernel. It is used to create and write the intermediate log file and log records.
Daemon	The *audit daemon* is the trusted utility that runs a background process whenever a log is enabled. It is the sole reader of the audit device, which in turn provides the daemon with blocks of records from the log collection file.
Manager Interface	The audit manager interface allows the administrator to handle, set up, initialize, and modify subsystem parameters.
Data Analysis and Reduction	The data analysis and reduction examines log files from current or previous log sessions and reduces or compresses them for archival.

Understanding the concept of SIEM is important for system administrators. The following table identifies SIEM concepts:

SIEM Concept	Description
Aggregation	Data must be collected so that it can be pulled from. Data is pulled from all sorts of locations that provide logs, like workstations and servers. After the data is stored and collected, it is ready for translation or normalization.
Correlation	The data is in a collected but unsorted state. In this stage, rules are created to pull the data desired for reviewing certain events.
Automated Alerts & Triggering	An administrator can make preconfigured settings that trigger automated alerts and send them to to system administrators. These alerts can be customized to show an administrator the most important logs that concern her organization.
Time Synchronization	This policy ensures that alerts are showing at the correct time across an organization. Time zones need to be taken into account. There could be an effort to force correct time settings via a GPO as well.
Event Deduplication	The practice in SIEM that tries to narrow events down by eliminating duplicate events.
WORM	WORM stands for "write once, read many" and refers to the storage method that allows the writing of data only once, but then allows users to read the data as many times as they want. This way, logs cannot be easily modified or destroyed.