**Chapter 15 – Log Analysis**

* **Logs:** records of events within a system
* **Examples of Logs:** user logins, system errors, network connections, changes to data, or system configuration
* **Why are they important?**

|  |  |
| --- | --- |
| **System Troubleshooting** | Analyzing system errors helps in responding to failures and minimizing system downtime. |
| **Cyber Security Incidents** | Crucial in detecting and responding to security incidents. Ex: Firewall logs and IDS logs |
| **Threat Hunting** | Use collected logs to search for possible threats  Look for anomalies or unusual patterns. |
| **Compliance** | Organization must maintain detailed activity of their system and network |

* **Give examples of security incidents**

Unauthorized access attempts, malware, data breaches

* **What are the components of logs?**

1. Timestamp of the event
2. Name of the system/ application that generated the log entry
3. Type of event
4. User who initiated the event
5. The IP address of the device

* Log collection

|  |  |
| --- | --- |
| **Identify Sources** | Where can the logs come from? Server, database, application, network devices |
| **Choose Log Collector** | A tool or software that is compatible with your infrastructure |
| **Configure Collection Parameters** | Time synchronization is enabled.  Determine intervals of logging  Prioritization of certain events. |
| **Test Collection** | Run a test to ensure the logging of all events from all resources |
| **NTP** | This protocol is crucial to maintain the integrity of the timeline when logging events |

* **What is Log Management?**

|  |  |
| --- | --- |
| Storage | Secure plan for storage |
| Organization | Classify logs based on types, sources, or other criteria |
| Backup | Backup logs to prevent data loss. |
| Review | Periodically Review Logs |

* **What is Log Centralization?**

1. **Choose a centralized system:** like Splunk or Elastic Stack
2. **Integrate Sources:** Collect all source sin one place
3. **Set up Monitoring:** like alerts for specified events
4. **Integration with incident management**

* What is Log Storage

|  |  |
| --- | --- |
| Security Requirements | Logs stored with secure protocols |
| Accessibility needs | Can be accessed quickly and easily |
| Storage Capacity | Should be large enough to sustain all logs |
| Cost Considerations | It’s either local or cloud-based storage budget |
| Retention Time | Ease of retrieval and speed |
| Disaster Recovery Plan | If the system fails, you should be able to retrieve logs |

* What are good practices when it comes to logs?

1. Encrypt sensitive logs
2. Regular backups
3. Automate retention, deletion, and storage processes to avoid human errros

* What are the types of logs?

Application logs, audit logs, security logs, server logs, system logs, network logs, database logs, and web server logs

* What are **application logs**?

Messages from applications that might provide errors, status or warnings.

* What are **audit logs**?

Events, actions and changes occurring within a system or application

* What are **security logs**?

Logins, permission alterations, or firewall activities

* What are **server logs**?

Event logs, error logs, and access logs regarding server operations

* What are **system logs**?

Kernel activities, system errors, boot sequences, hardware status

* **Network Logs**?

Communication an activity within a network: data transfers, capturing information about events

* **Database Logs**?

Queries performed, actions, updates in a database

* **Webserver logs?**

Requests processed by web servers: URLS, source Ip addresses, response codes, etc..

* **Give an example of a logging tool.**

Splunk

* What are the **three components of Splunk**?

|  |  |
| --- | --- |
| Forwarder | Collects data and sends it to Splunk instance. It doesn’t affect the performance of the end point as it requires a few resources. Examples of data sources include windows machine, web server, database |
| Indexer | Processes the data it receives from the forwarder.  It normalizes the data into field-value pairs, determining the data type of the data and saving them as events. |
| Search Head | This is where the user can look for logs or any related term . |

* What does the **incident handling lifecycle consist of**?

1. **Preparation:** defining policies, incorporating security controls
2. **Detection Analysis:** getting alerts from security controls and investigating the incident to get the root cause
3. **Post Incident Activities:** The actions needed to be done to prevent the incident from spreading throughout the network or system and gaining back the control from the attacker.
4. **Containment eradication and discovery:** Identifying weakness that lead to the attack and improving the system to avoid that incident from happening again

|  |  |
| --- | --- |
| Elasticsearch | Full-text search and analytics engine used to store JSON-formatted documents  Performs correlation on data, analyzing data and storing it. |
| Logstash | Data processing engine that takes data from different sources and sends it to destination which can be Kibanna or a listening port. |
| Beats | Data shippers, host-based agent (data collection) agent  Sends data from end points to Elastic Search. |