**Splunk Introduction**

**Module 1 – Intro to Splunk**

**Splunk Components**

Splunk is often described as a search engine for machine data. It ingests, indexes, and makes sense of large volumes of raw, unstructured data generated by systems, applications, and devices. Examples include login attempts, system errors, security events, or user activities.

Key components in Splunk deployments:

* **Indexer**: Collects incoming data, processes it, and stores it in an organized, searchable format.
* **Search Head**: Provides the interface for running searches, generating reports, and building dashboards.
* **Forwarder**: Lightweight agents installed on source systems to send data into Splunk.

In small environments, a single Splunk instance may perform all roles. In larger setups, these roles are separated across multiple instances for scalability.

**Basic Splunk Functions**

Splunk provides core functionality to work with machine data:

* **Data Ingestion**: Forwarders, network listeners (TCP/UDP), HTTP Event Collector (HEC), APIs, and connectors bring data into Splunk.
* **Indexing**: Raw data is parsed, enriched with metadata, and stored in a searchable format.
* **Search and Analysis**: Users can query data with Splunk’s Search Processing Language (SPL).
* **Dashboards and Reports**: Searches and visualizations can be saved and shared for monitoring and analysis.

Splunk operates across on-premises servers, cloud environments, and hybrid infrastructures, making it highly adaptable.

**Module 2 – Using Splunk**

**Define Splunk Apps**

A Splunk app is a collection of dashboards, reports, knowledge objects, and configurations packaged together for a specific use case. Examples include Splunk Enterprise Security and IT Service Intelligence.

**Understand Splunk User Roles**

Splunk uses role-based access control:

* **Admin**: Full privileges to manage users, apps, and system settings.
* **Power User**: Can create and share dashboards, reports, and alerts.
* **User**: Can search data, create private knowledge objects, and view shared content.

**Search & Reporting App**

The Search & Reporting app is the default interface for running searches, saving reports, and building dashboards. It is typically the starting point for most Splunk users.

**Splunk Web Interface**

The web interface provides access to:

* Search bar for running SPL queries.
* Tools for saving searches, creating alerts, and visualizations.
* Navigation to apps, reports, dashboards, and knowledge objects.

**Module 3 – Using Search**

**Run Basic Searches**

Basic searches begin with specifying an index or sourcetype:

index=security sourcetype=linux\_secure "failed password"

**Set the Time Range of a Search**

Searches can be scoped to a specific time range (last 15 minutes, last 24 hours, custom time ranges). This improves relevance and performance.

**Save Search Results**

Searches can be saved as reports for later use. Saved searches can also be scheduled.

**Identify the Contents of Search Results**

Search results are made up of **events** (raw log entries with fields). Each event has metadata such as timestamp, host, source, and sourcetype.

**Work with Events**

Events can be filtered, highlighted, or refined by adding/removing search terms.

**Share Search Jobs**

By default, a search job remains active for 10 minutes. Shared searches can remain active for 7 days.

**Export Search Results**

Results can be exported in CSV, JSON, XML, or raw text formats.

**Select Search Modes**

* **Fast Mode**: Prioritizes speed, returns essential fields only.
* **Verbose Mode**: Returns all fields, suitable for troubleshooting.
* **Smart Mode**: Balances speed and completeness by adjusting automatically.

**Control a Search Job**

Users can pause, stop, or extend the time-to-live of a search job.

**Module 4 – Exploring Events**

**Refine Searches**

Refining searches helps reduce noise and improve relevance. SPL commands and filters can narrow down results.

**Understand Timestamps**

Splunk assigns timestamps to events during ingestion. Accurate timestamps are essential for time-based searches and visualizations.

**Use the Events Tab**

The Events tab allows users to interactively add or remove search terms based on what appears in results.

**Module 5 – Search Processing Language (SPL)**

**Use Wildcards**

Wildcards make searches flexible:

* error\* → matches error, errors, error\_code
* \*fail\* → matches failed, failure, login\_fail

**Understand Case Sensitivity**

By default, searches are case-insensitive. Specific field values may be case-sensitive depending on configuration.

**Use Booleans**

Boolean operators refine searches:

* **AND**: Finds events containing all terms.
* **OR**: Finds events containing at least one term.
* **NOT**: Excludes terms.

Parentheses () group conditions, quotation marks "" search exact phrases.

**Use Special Characters**

Quotation marks, parentheses, and operators help structure more complex searches.

**Module 6 – What are Commands?**

**Anatomy of Splunk’s Search Language**

SPL searches are composed of:

* **Search terms**: Keywords or field-value pairs.
* **Commands**: Instructions to process results (e.g., stats, timechart).
* **Functions**: Applied inside commands (e.g., count(), avg()).
* **Arguments**: Options provided to functions/commands.
* **Clauses**: Define filters or groupings.

**Best Practices for Writing Searches**

* Start simple and refine incrementally.
* Use index and sourcetype early for efficiency.
* Use transforming commands (stats, timechart) for summarization.
* Avoid unnecessary wildcards for better performance.

**Module 7 – What are Knowledge Objects?**

**Categories of Knowledge Objects**

Knowledge objects enhance the usability of Splunk data.

1. **Data Interpretation** – Field extractions, event types.
2. **Data Classification** – Tags, event categorization.
3. **Data Enrichment** – Lookups that add external context.
4. **Data Normalization** – Data models that standardize fields.
5. **Data Models** – Structures enabling advanced features like Pivot.

**Types of Knowledge Objects**

* **Saved Searches/Reports**
* **Dashboards**
* **Tags**
* **Lookup Tables**
* **Event Types**
* **Data Models**

**Module 8 – Creating Reports and Dashboards**

**Save a Search as a Report**

Any SPL search can be saved as a report. Reports may run on-demand or be scheduled.

**Edit Reports**

Reports can be modified to update queries, scheduling, or sharing permissions.

**Use Transforming Commands**

Commands such as stats, chart, and timechart turn raw events into meaningful summaries and visualizations.

**Create a Dashboard**

Dashboards are collections of visualizations and reports.

* **Panels** represent individual visualizations or saved searches.
* **Classic Dashboards** are simple to configure.
* **Dashboard Studio** offers modern, customizable designs.

**Add a Report to a Dashboard**

Saved reports can be added to dashboards as panels. Drilldowns can link panels to deeper searches.

**Edit a Dashboard**

Dashboards can be customized by rearranging panels, updating queries, or modifying visualizations.

**Example Use Case**

As a security analyst monitoring login failures:

1. **Ingest Logs**: Linux authentication logs are ingested into Splunk.
2. **Run Search**:
3. index=auth "failed password"
4. **Save Report**: Store this search as *Failed Logins Report*.
5. **Create Dashboard**: Add panels showing:
   * Failed logins over 24 hours.
   * Top 5 usernames with failed logins.
6. **Share Dashboard**: Provide visibility to the team for real-time monitoring.