Splunk: Basics

## **Splunk: Basics – Notes**

### **1. Introduction**

* Splunk = **Log management & analysis platform**.
* Used for **searching, monitoring, and visualizing machine-generated data** from websites, apps, servers, and security tools.
* Core benefit: turn raw log data into **actionable intelligence**.

### **2. Splunk Components**

1. **Forwarder** – Collects and sends log data to Splunk indexer.
   * **Universal Forwarder**: lightweight agent for data forwarding.
2. **Indexer** – Stores incoming data, creates indexes, makes it searchable.
3. **Search Head** – User interface for searching, analyzing, and visualizing data.
4. **Deployment Server** – Manages configurations and apps across multiple Splunk instances.

### **3. Navigating Splunk**

* **Search & Reporting App** – Main interface for running searches and creating reports/dashboards.
* **Search Processing Language (SPL)** – Used to query and analyze indexed data.
* **Time Picker** – Filter events by time range.
* **Data Preview & Field Extraction** – Identify relevant fields from raw data.
* **Dashboards** – Visual representations of search results.

### **4. Adding Data**

* Methods to add data:
  + **Upload** (e.g., log file from local system).
  + **Monitor** (real-time directory/file monitoring).
  + **Forwarder** (collect from remote machines).
* Data is parsed, indexed, and ready for search.

### **5. Conclusion**

* Splunk provides **real-time and historical log analysis**.
* Understanding components, navigation, and ingestion methods is essential before moving into advanced search and correlation.
* Useful for **SIEM tasks**, threat hunting, and operational monitoring.

