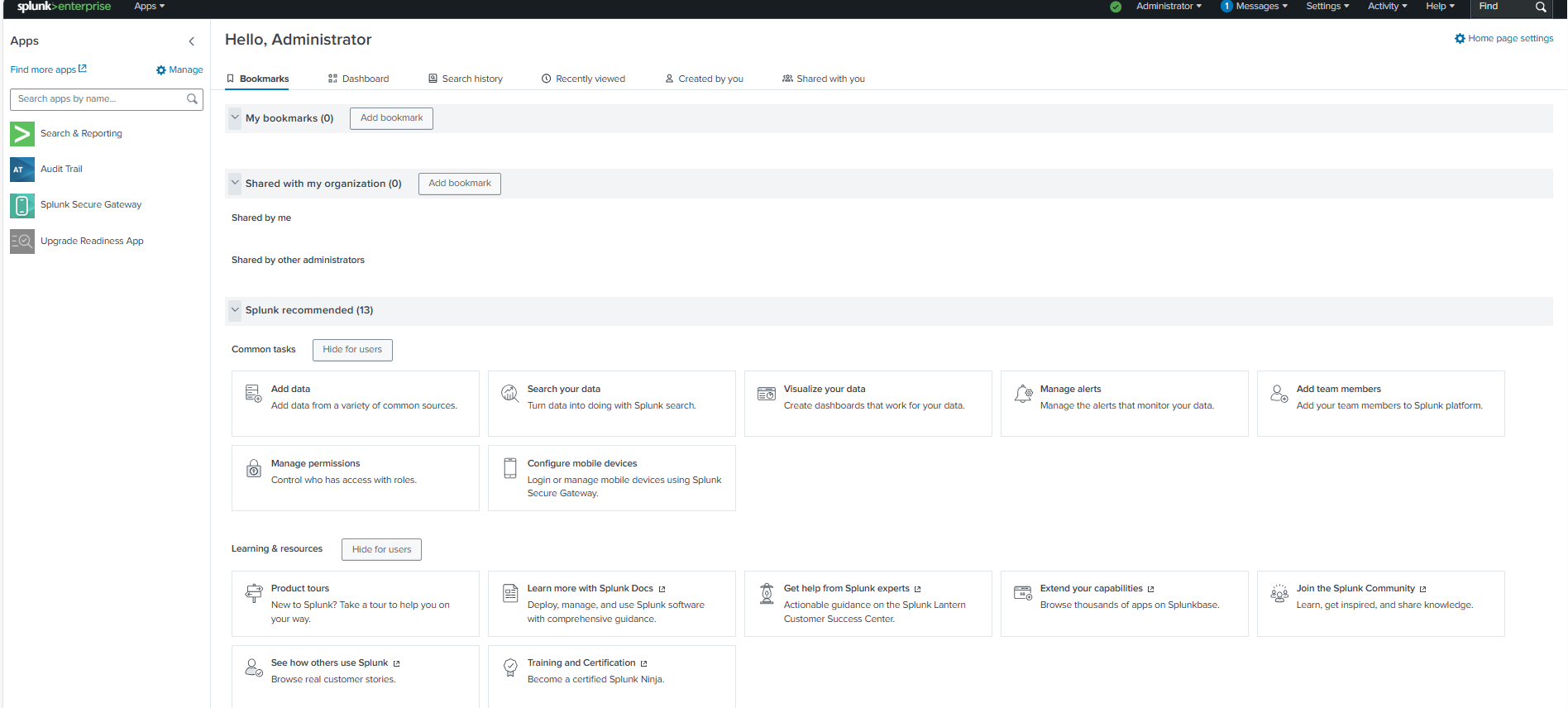
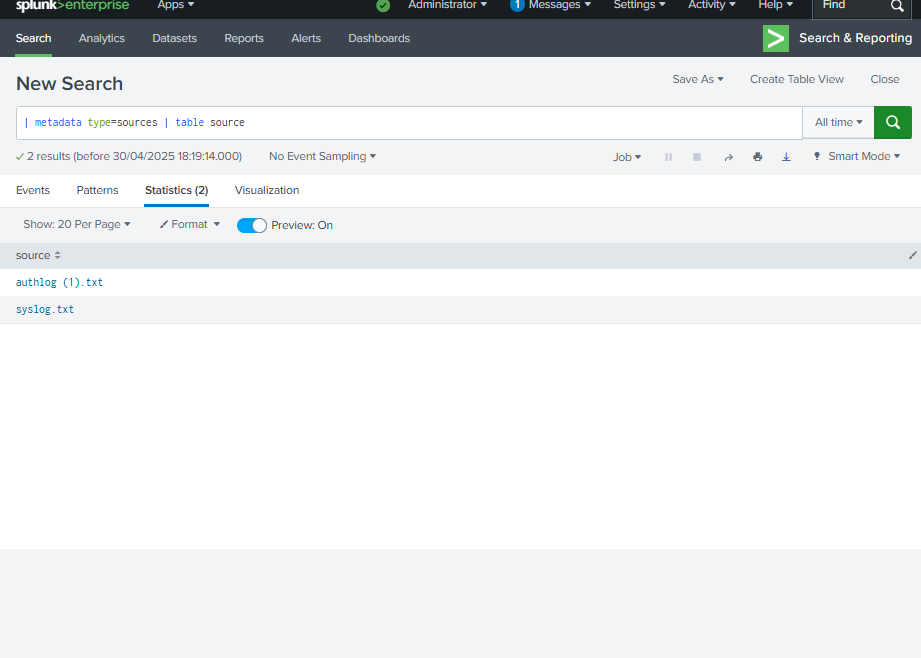
Phase 2:  
  
1- extracting the logs:

2- Download Splunk web and sign in:  


* Add the extracted logs in Splunk to visualize  
    
    
    
  - Apply the search:  
  Search & Reporting => Data Summary => Hosts -Select: metasploitable3 =>Sources= ”authlog(1).txt” ("Failed password" OR "Accepted password"):  
  A screenshot of a computer

  AI-generated content may be incorrect.

Visualization and analysis of the attack:

A screenshot of a computer

AI-generated content may be incorrect.

Analysis Outcomes:  
  
1- Splunk successfully ingested and parsed the log file from the victim machine.  
  
2- SSH authentication activity was clearly visible, showing a large number of Failed password events compared to relatively few Accepted password events.  
  
3- Attack data was effectively classified into two categories (Failed, Accepted) using a command in Splunk.  
  
4- A bar chart visualization provided a clear view of brute-force attack patterns, with 1423 failed login attempts and only 27 successful ones, indicating suspicious login behaviour  
  
5- This visualization enables security teams to quickly detect and respond to brute-force SSH login attempts, highlighting the importance of monitoring failed authentications.