**King Fahad University of Petroleum and Minerals**

**ICS344 Information security**

Term Project

**Visual Analysis with a SIEM Dashboard**

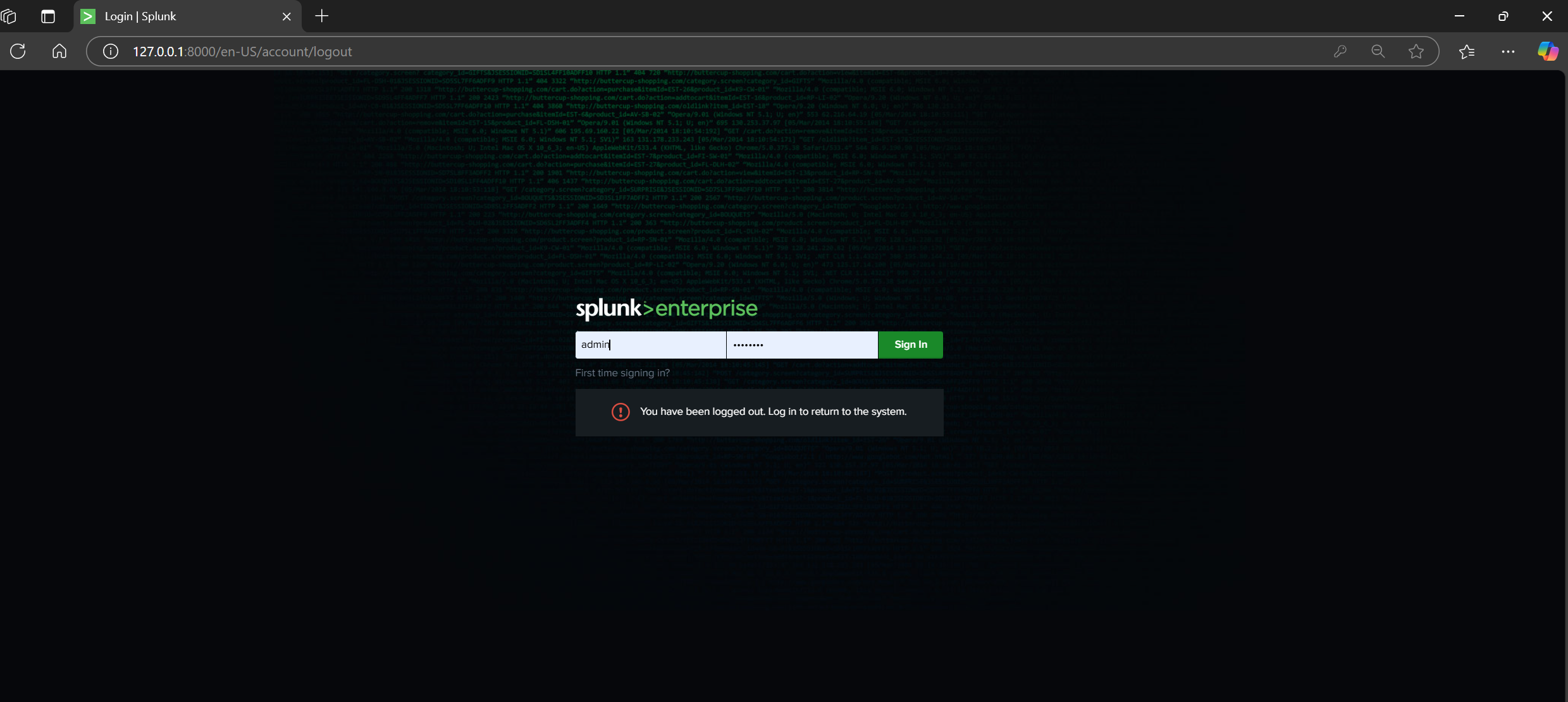
Phase#2

Team

|  |  |
| --- | --- |
| Name | ID |
| Ismael Arqsosi | 202182150 |
| Taha Ali | 202045620 |
| Saad Alharbi | 201935590 |

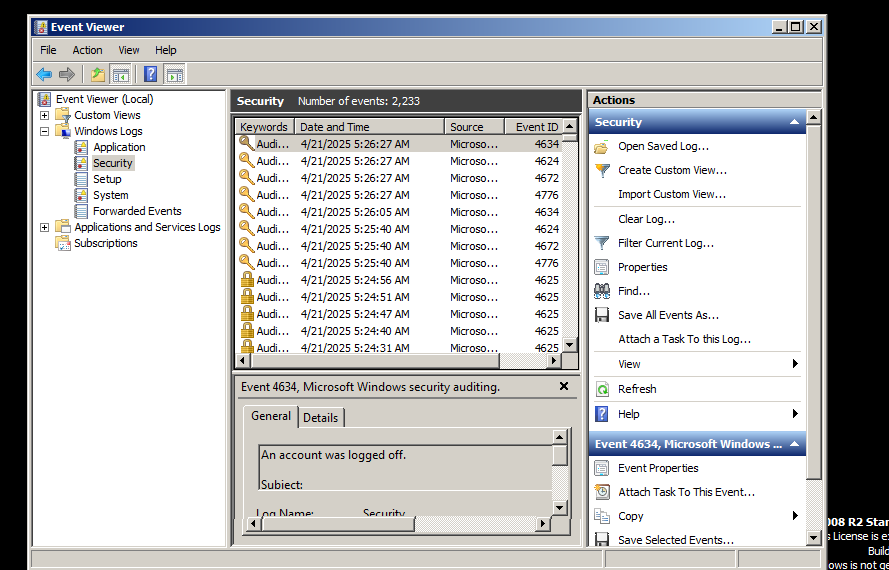
**Phase 2: SIEM Dashboard & Analysis**

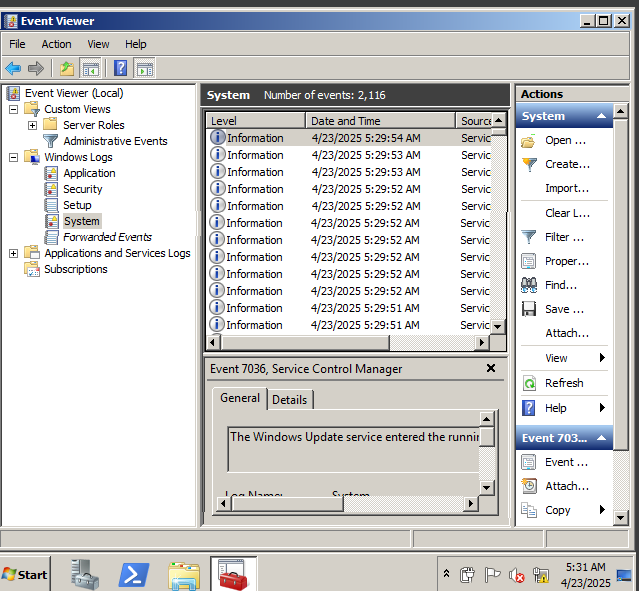
**2.1 Splunk Setup**

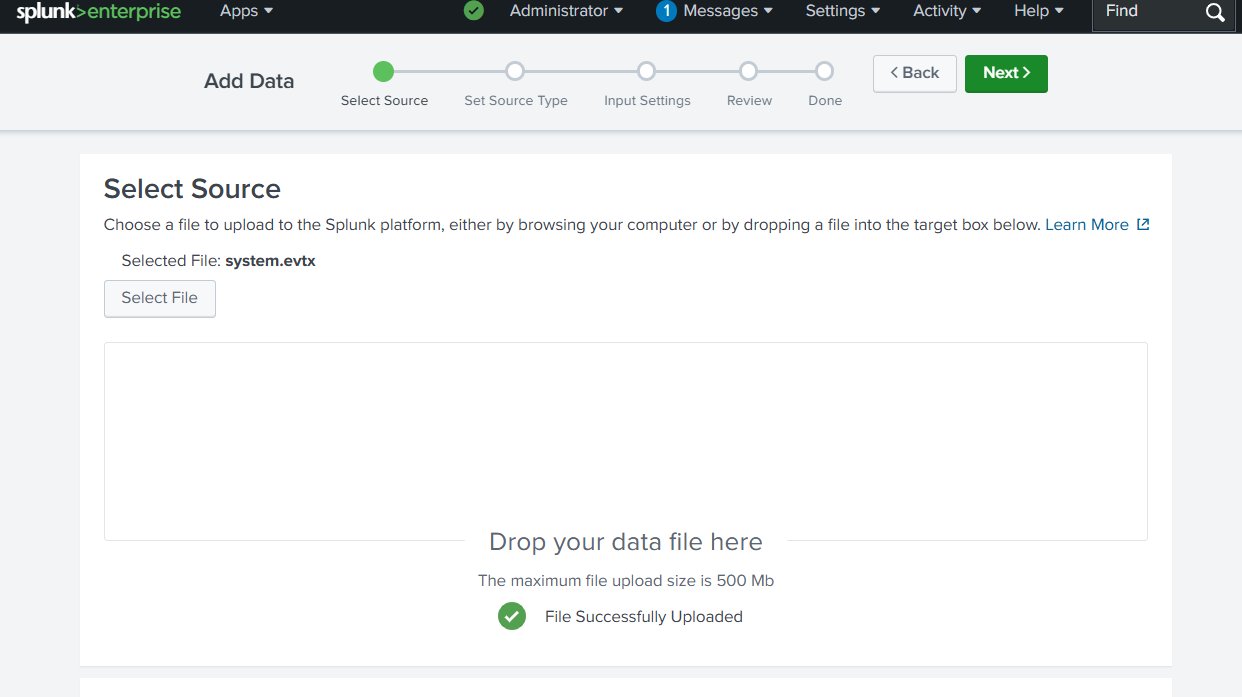
* Installed Splunk Enterprise on Windows host machine (instead of Kali, due to stability issues on Kali)
* Accessed via http://localhost:8000

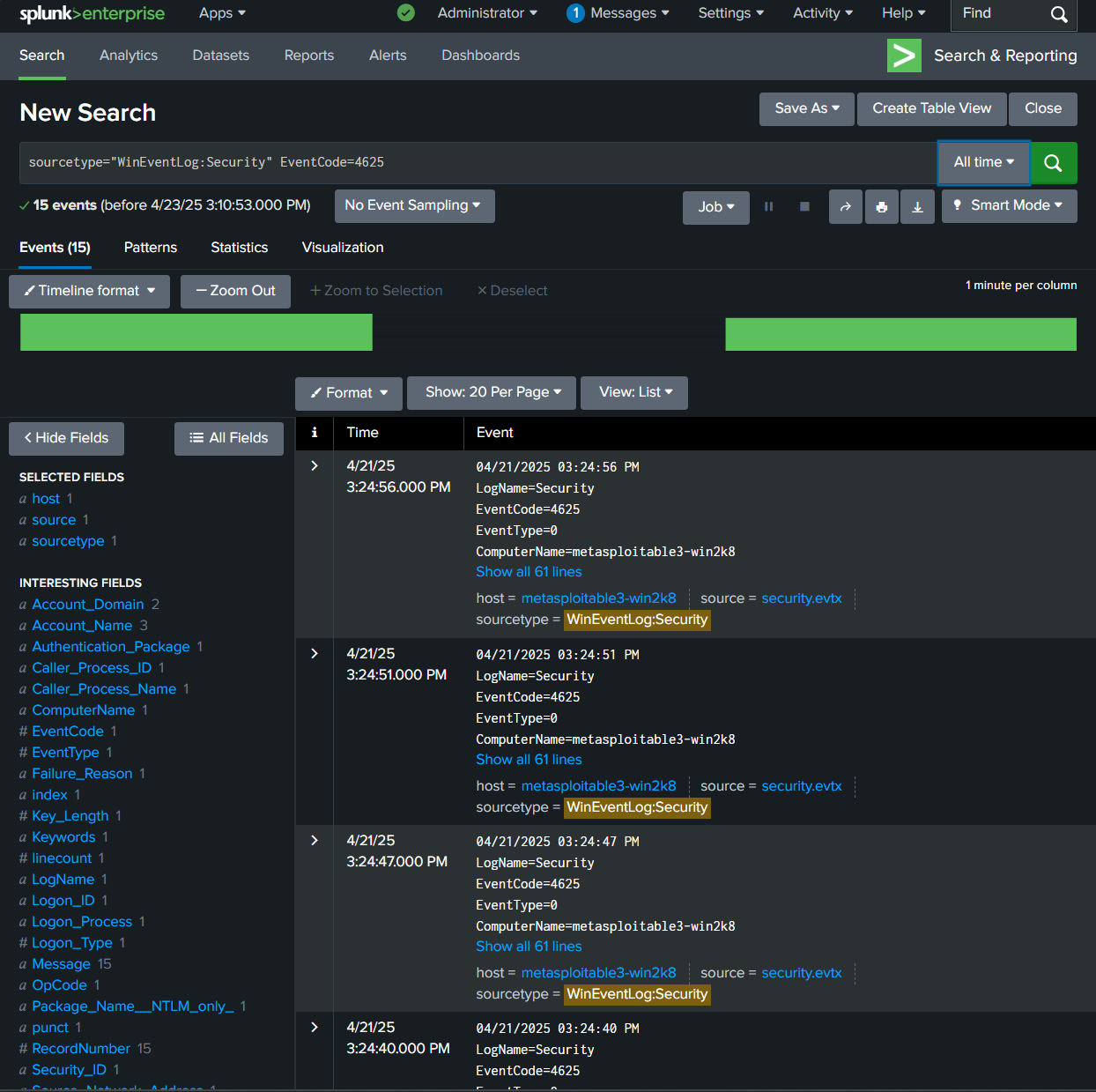
**2.2 Log Collection from Victim**

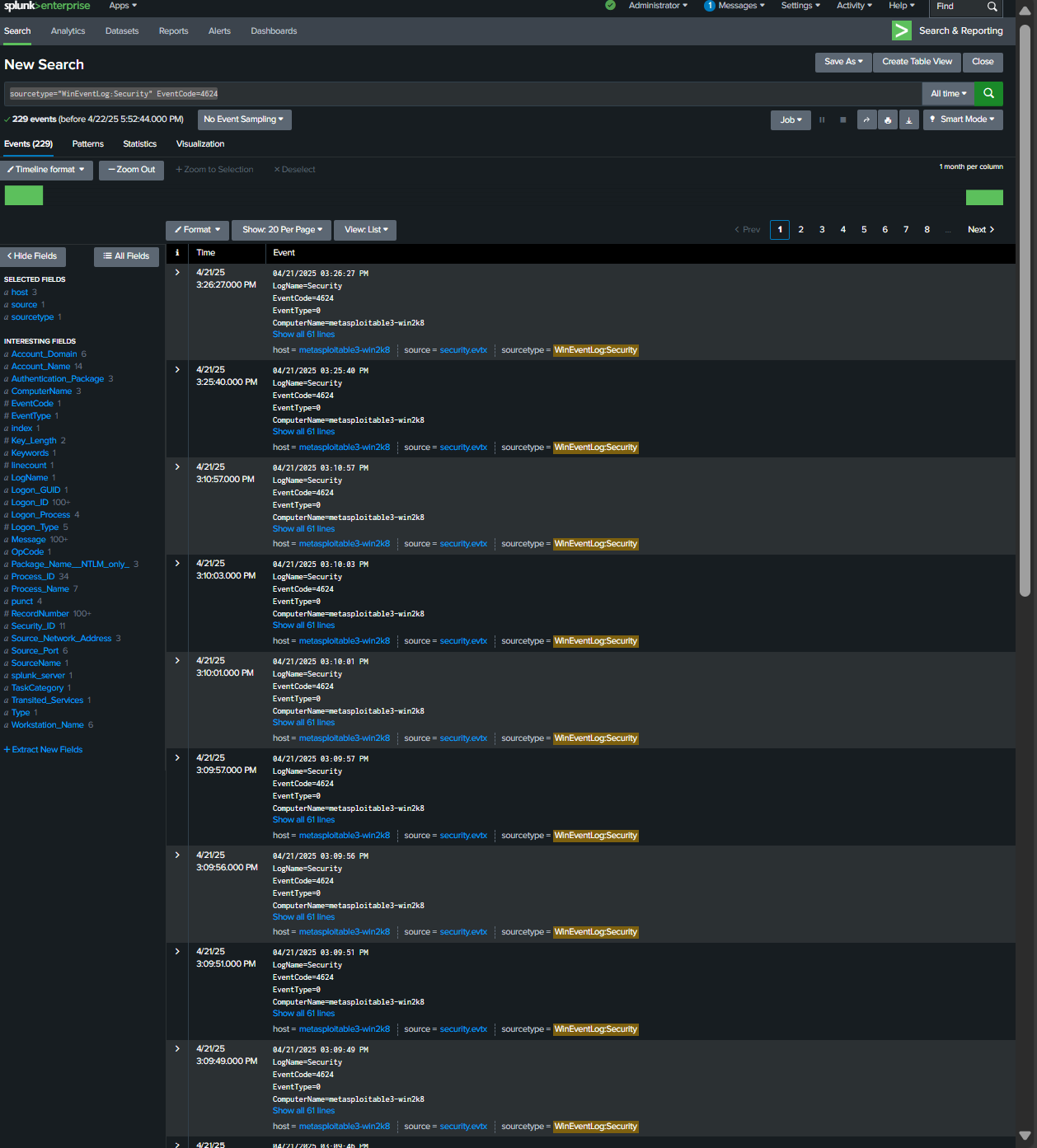
* Exported the following .evtx logs from Metasploitable3:
  + security.evtx
  + system.evtx
* Imported both logs into Splunk using the Add Data wizard
* Assigned host as Metasploitable3, sourcetype as WinEventLog:Security or WinEventLog:System
* Screenshots:

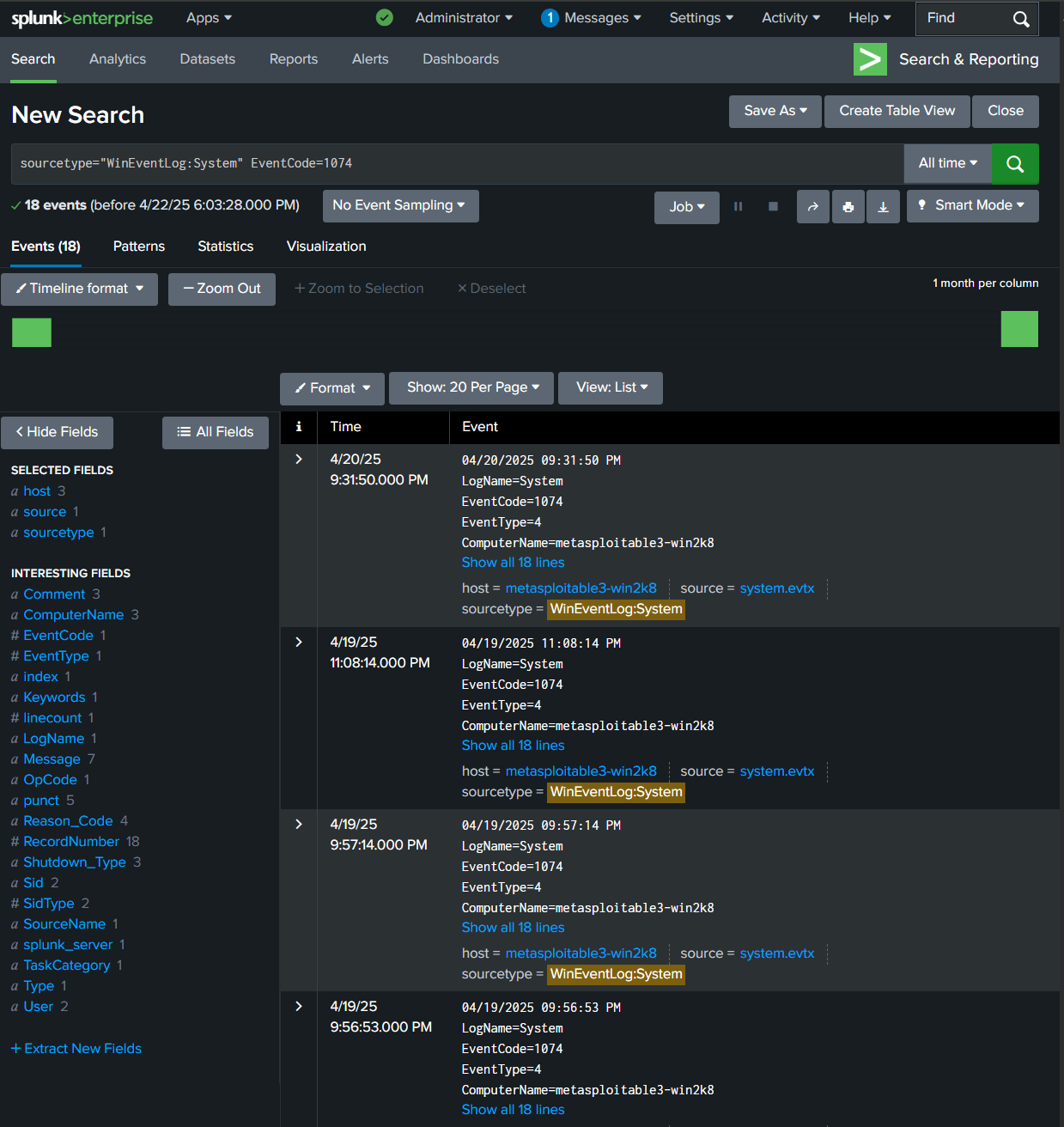


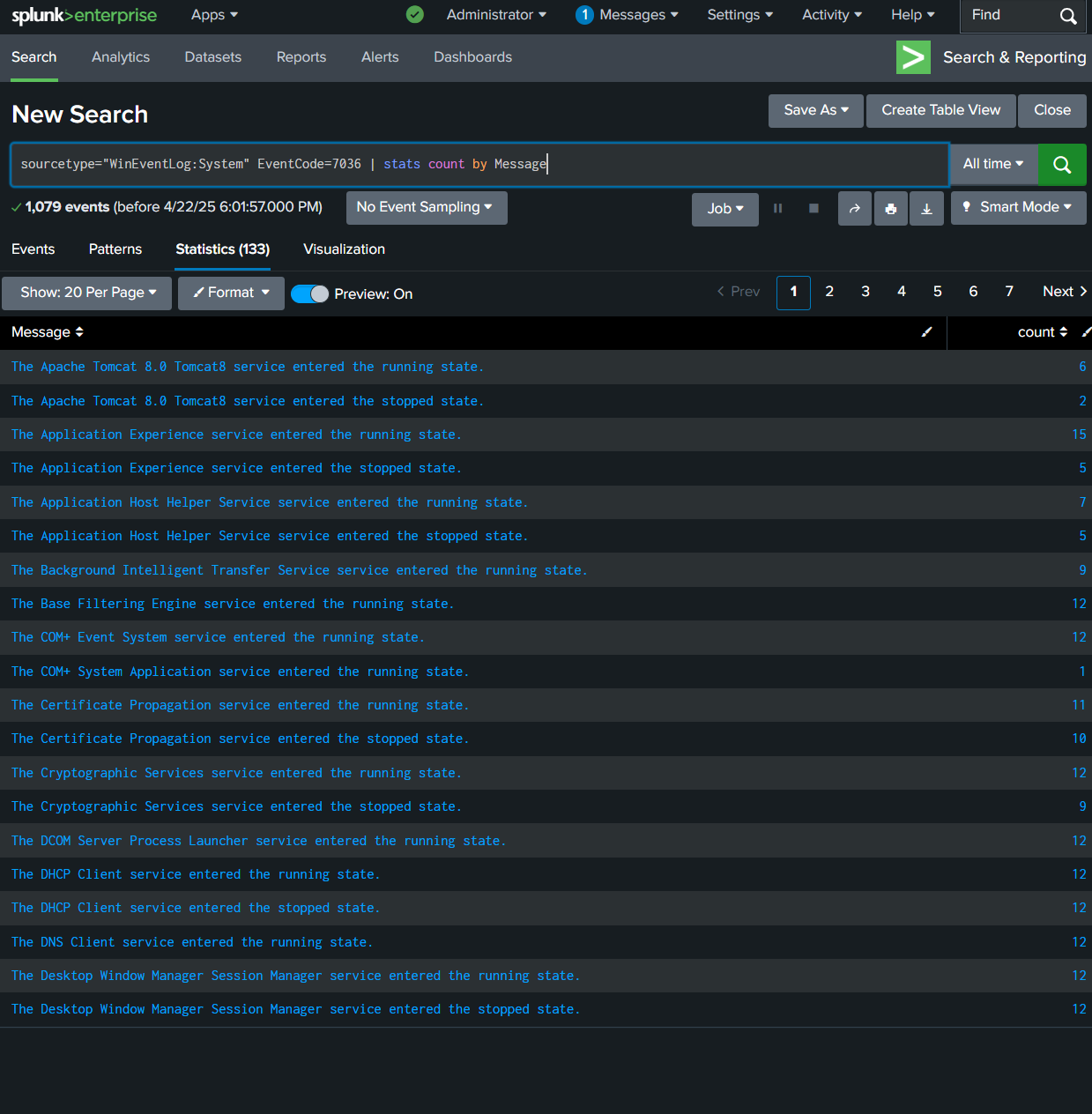




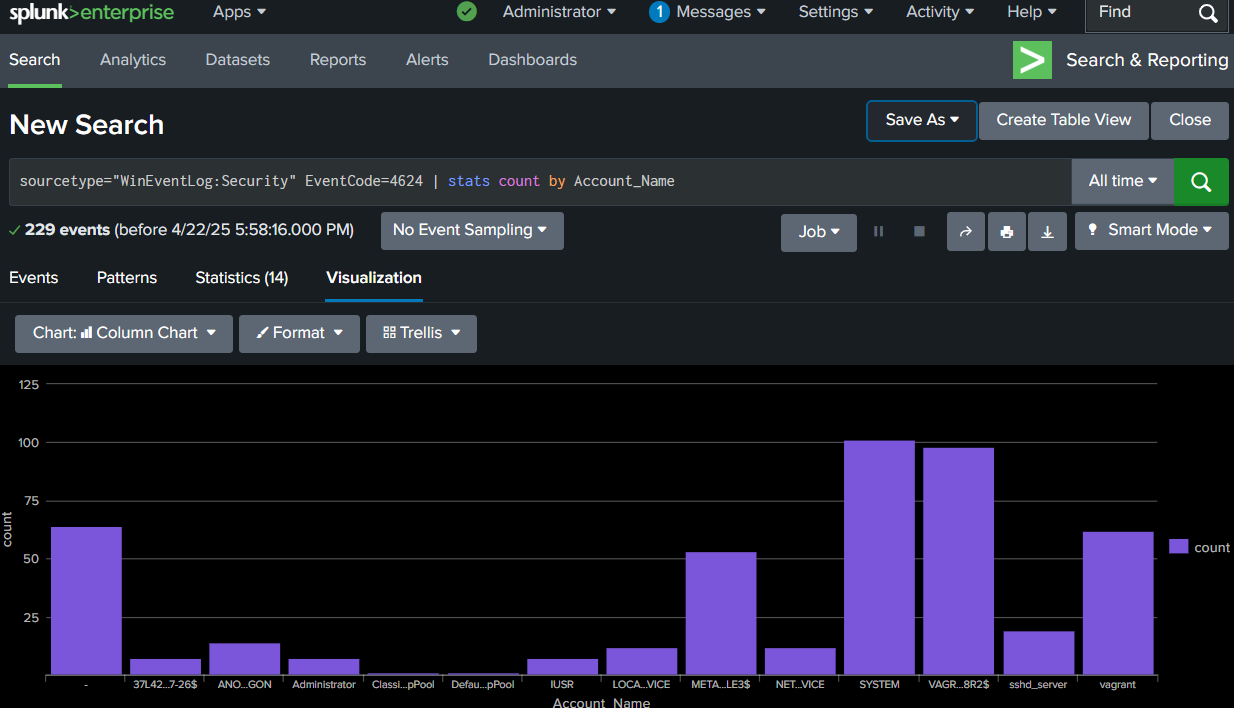
* Searched for Event ID 4624 (successful logins) and 4625 (failed logins):
* sourcetype="WinEventLog:Security" EventCode=4624
* sourcetype="WinEventLog:Security" EventCode=4625
* Searched system logs for Event ID 7036 (service start):

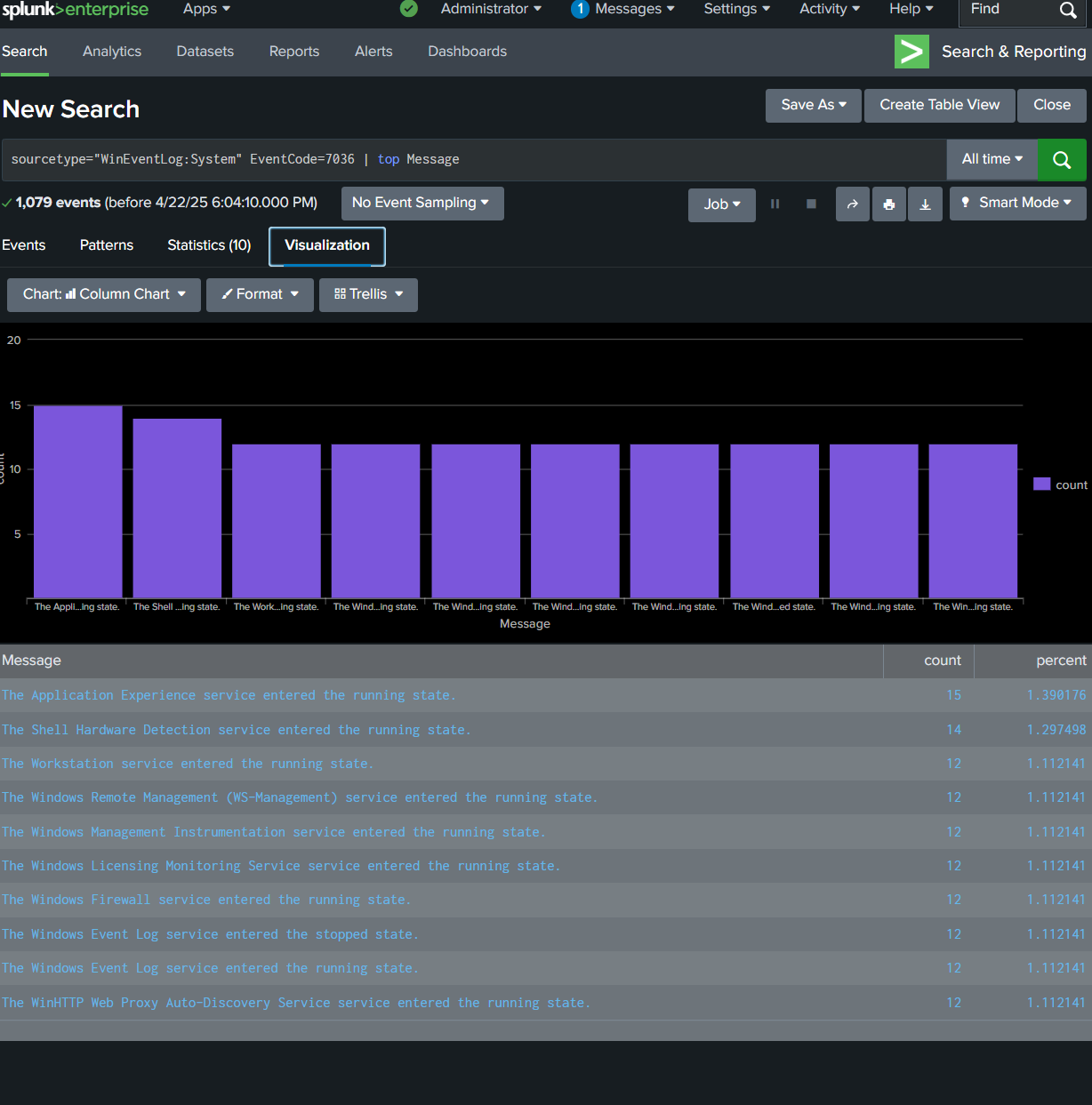






**2.4 Dashboard Creation**

* Created a bar chart
* Visuals:



**I could not collect logs from the Kali attacker machine due to internal issues with Kali's file system and log access.**

Notes:

- Installed and configured Splunk on host machine

- Collected logs from Metasploitable3 (Security and System logs)

- Successfully imported into Splunk using Upload method

- Used Search & Reporting to detect login attempts and system behavior

- Created dashboard panels to show:

- User login activity (Event ID 4624)

- Failed logins (4625)

- Windows service starts (7036)

- Could not include attacker logs due to Kali errors