King Fahad University of Petroleum and Minerals

ICS344 Information security

Term Project

Visual Analysis with a SIEM Dashboard

Phase#2

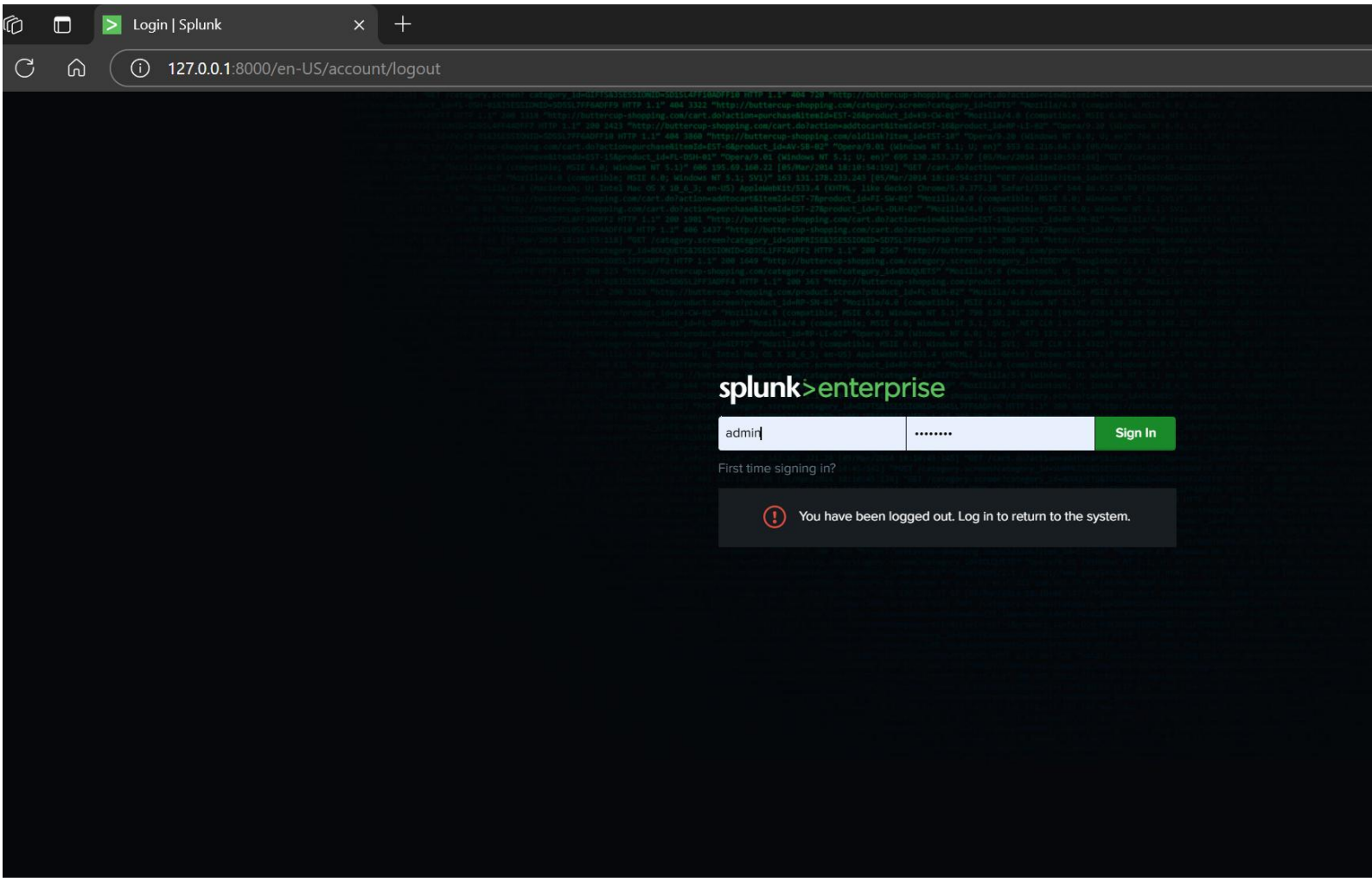
Team

Name	ID
Ismael Arqsosi	202182150
Taha Ali	202045620
Saad Alharbi	201935590

Phase 2: SIEM Dashboard & Analysis

2.1 Splunk Setup

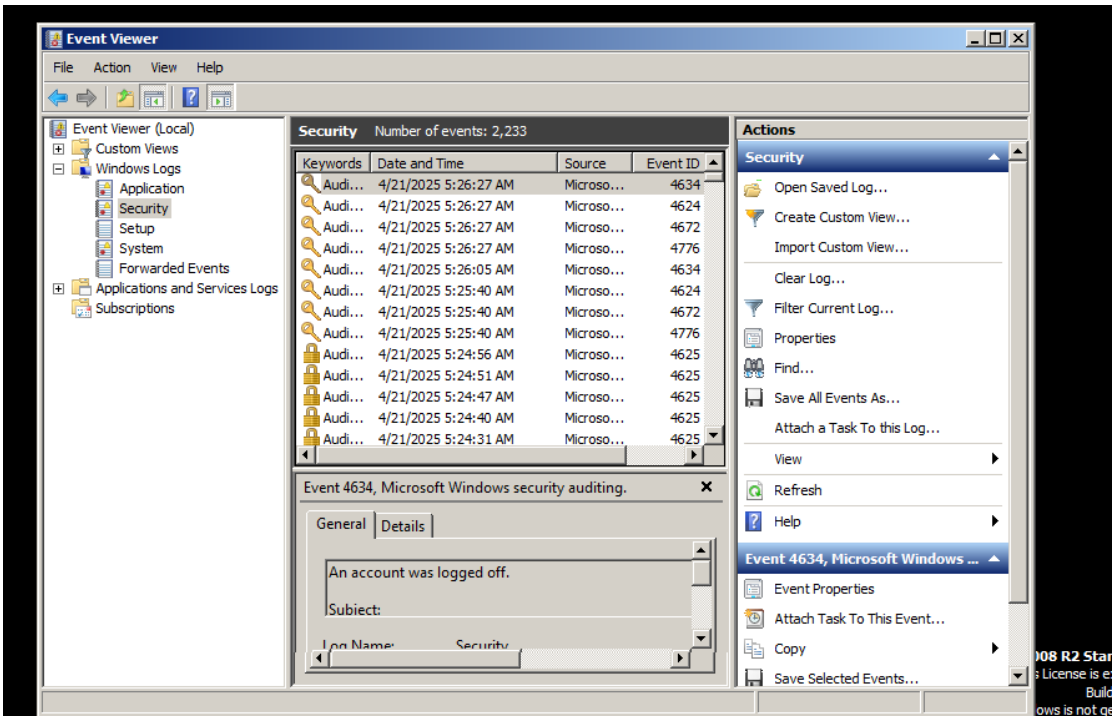
- Installed Splunk Enterprise on Windows host machine (instead of Kali, due to stability issues on Kali)
- Accessed via http://localhost:8000

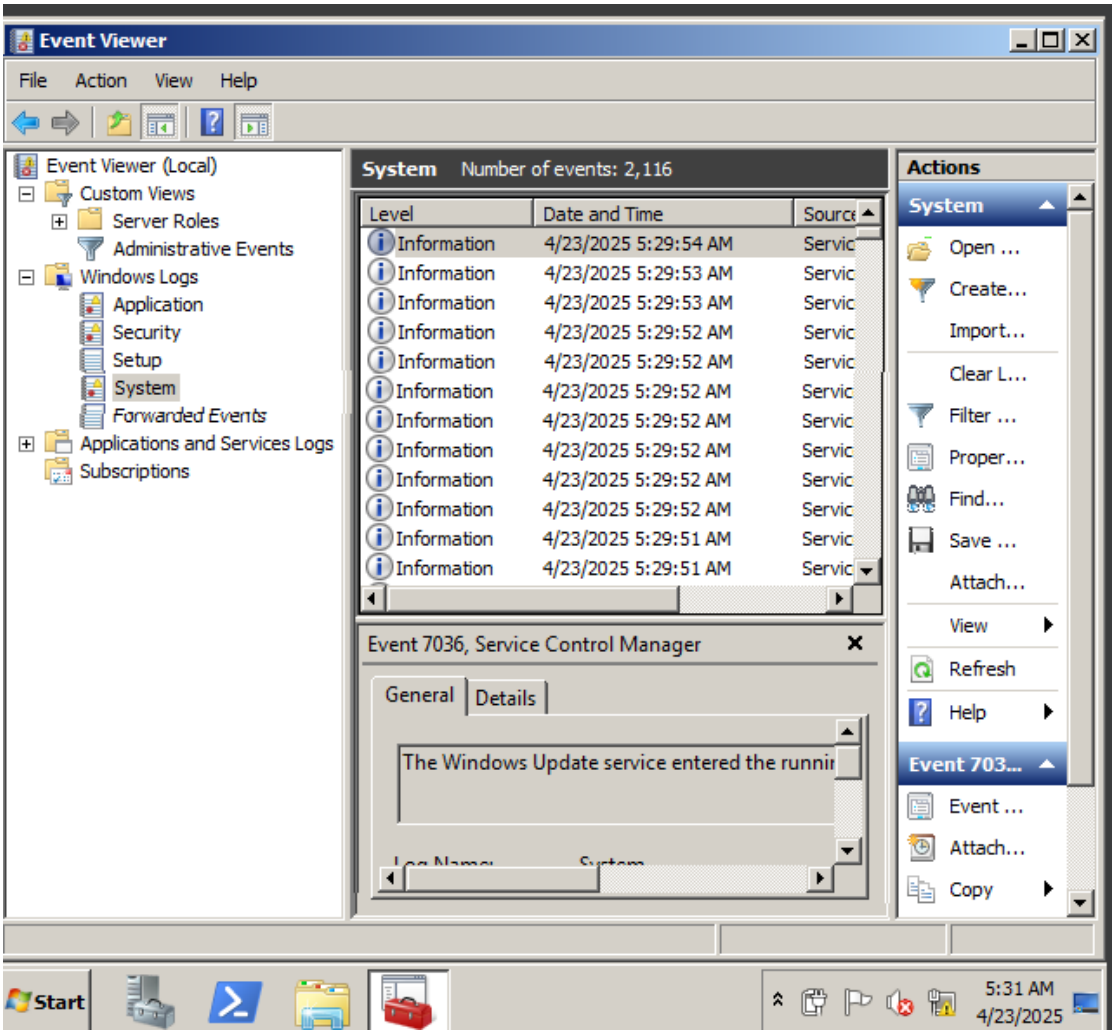


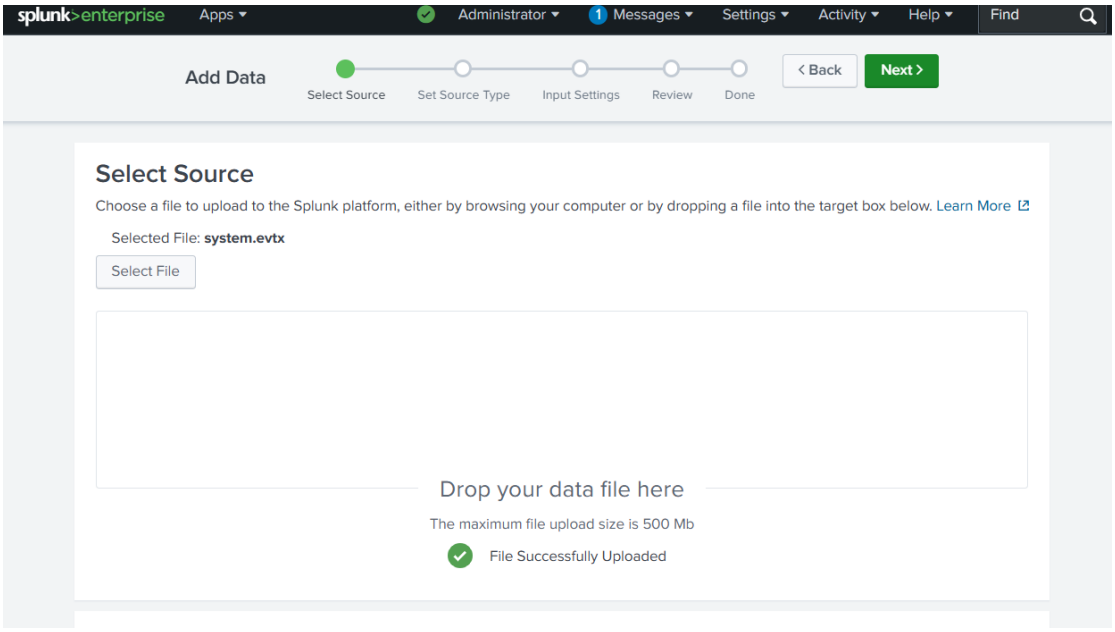
2.2 Log Collection from Victim

- 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

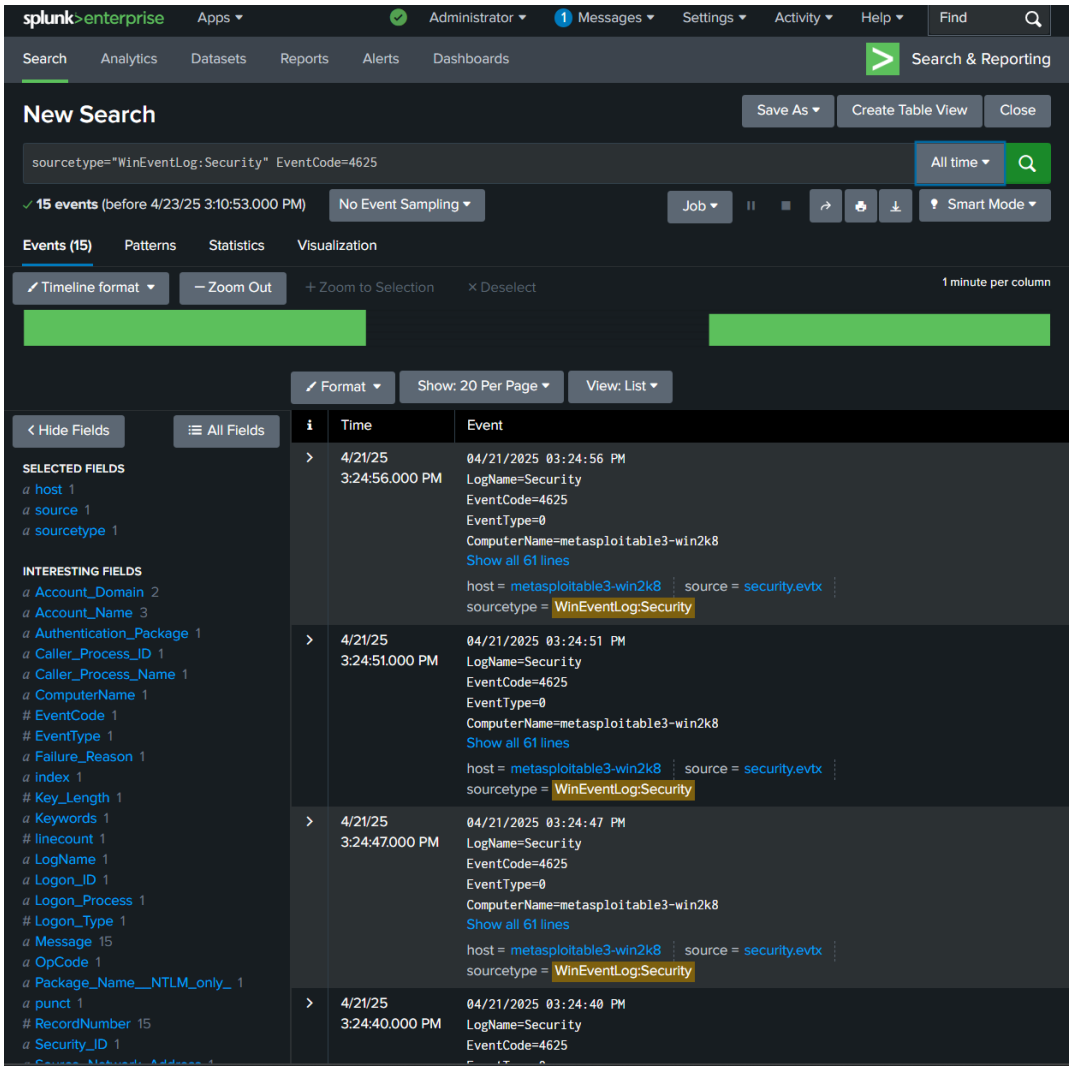
- Screenshots:

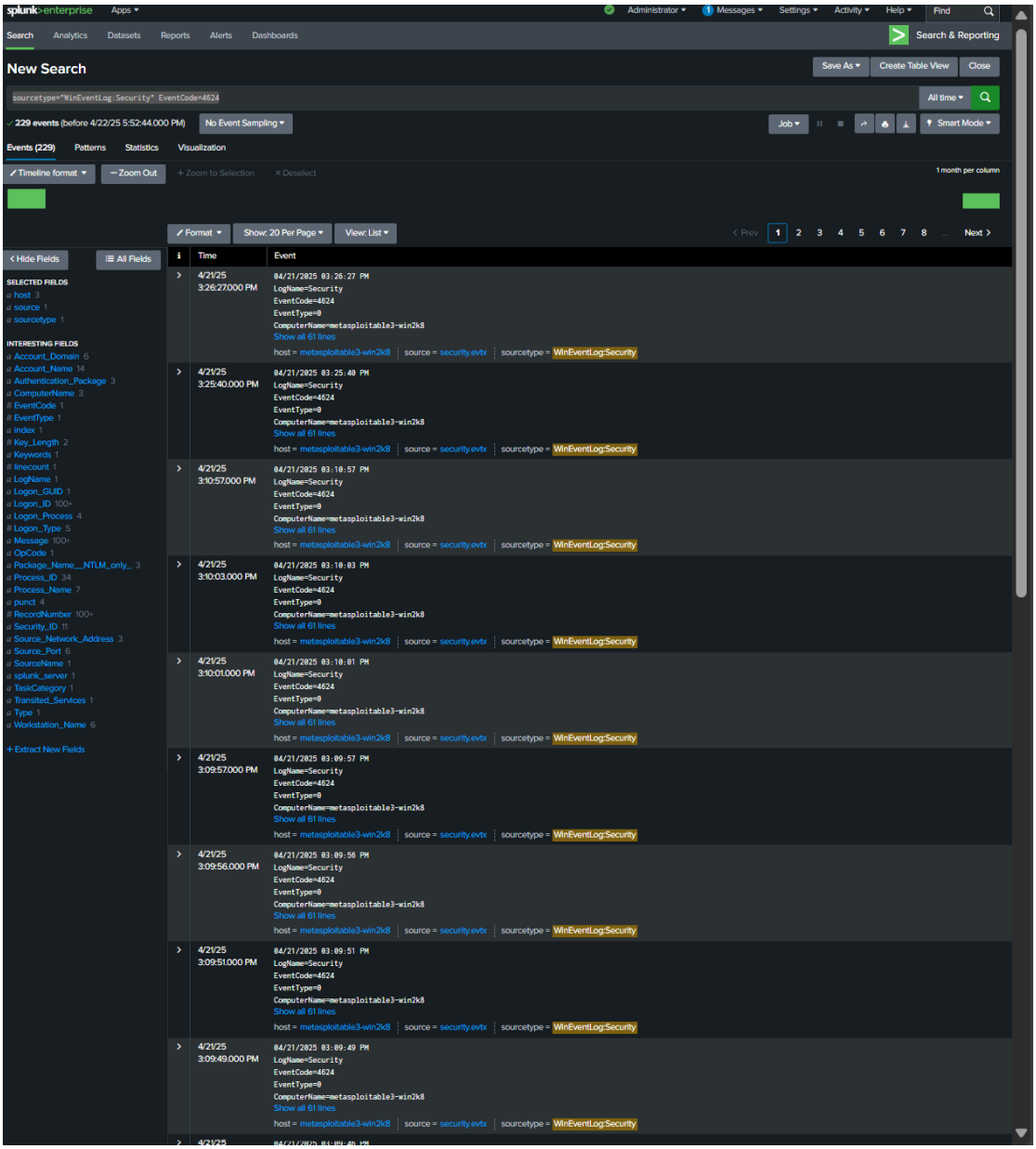


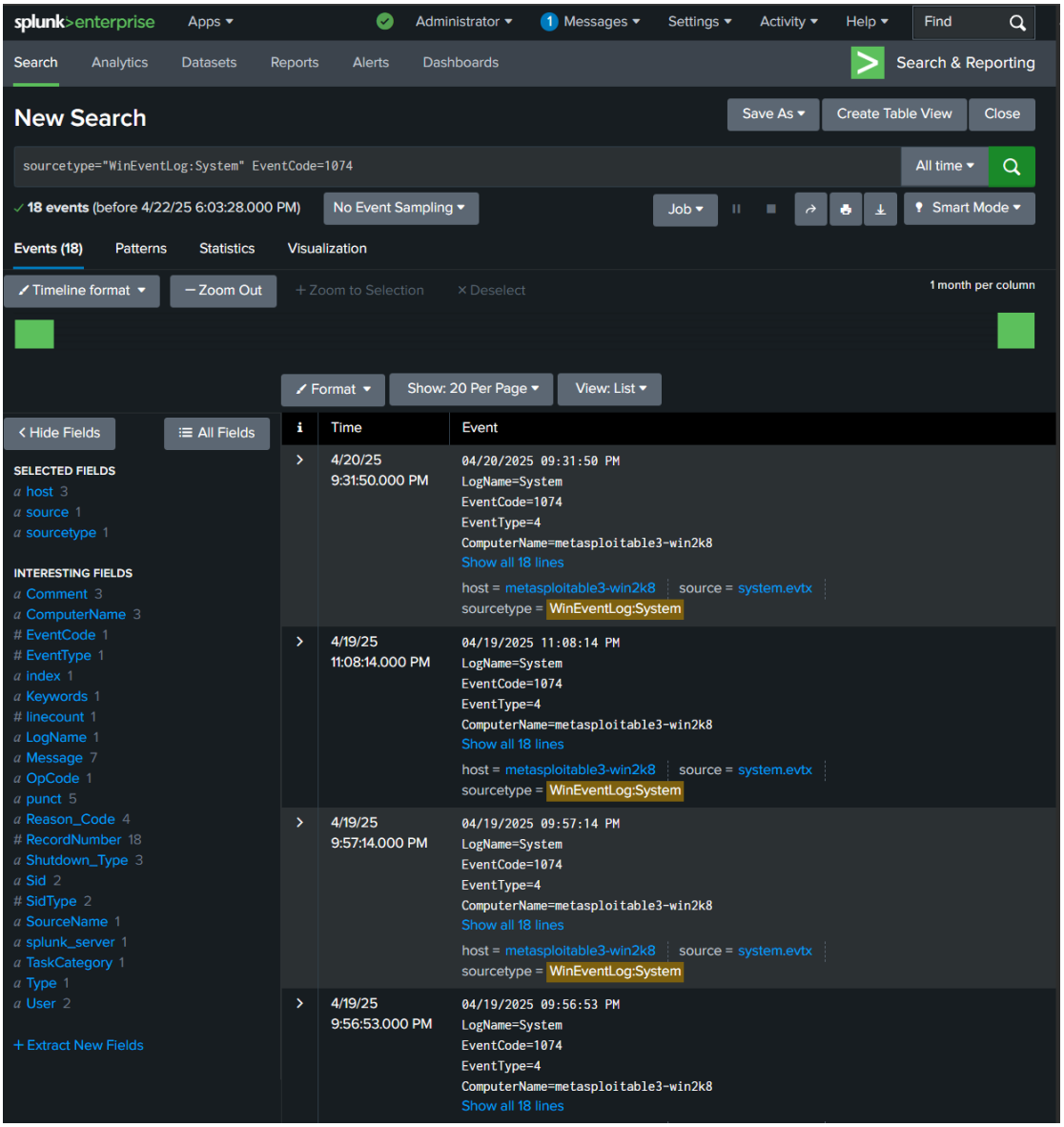


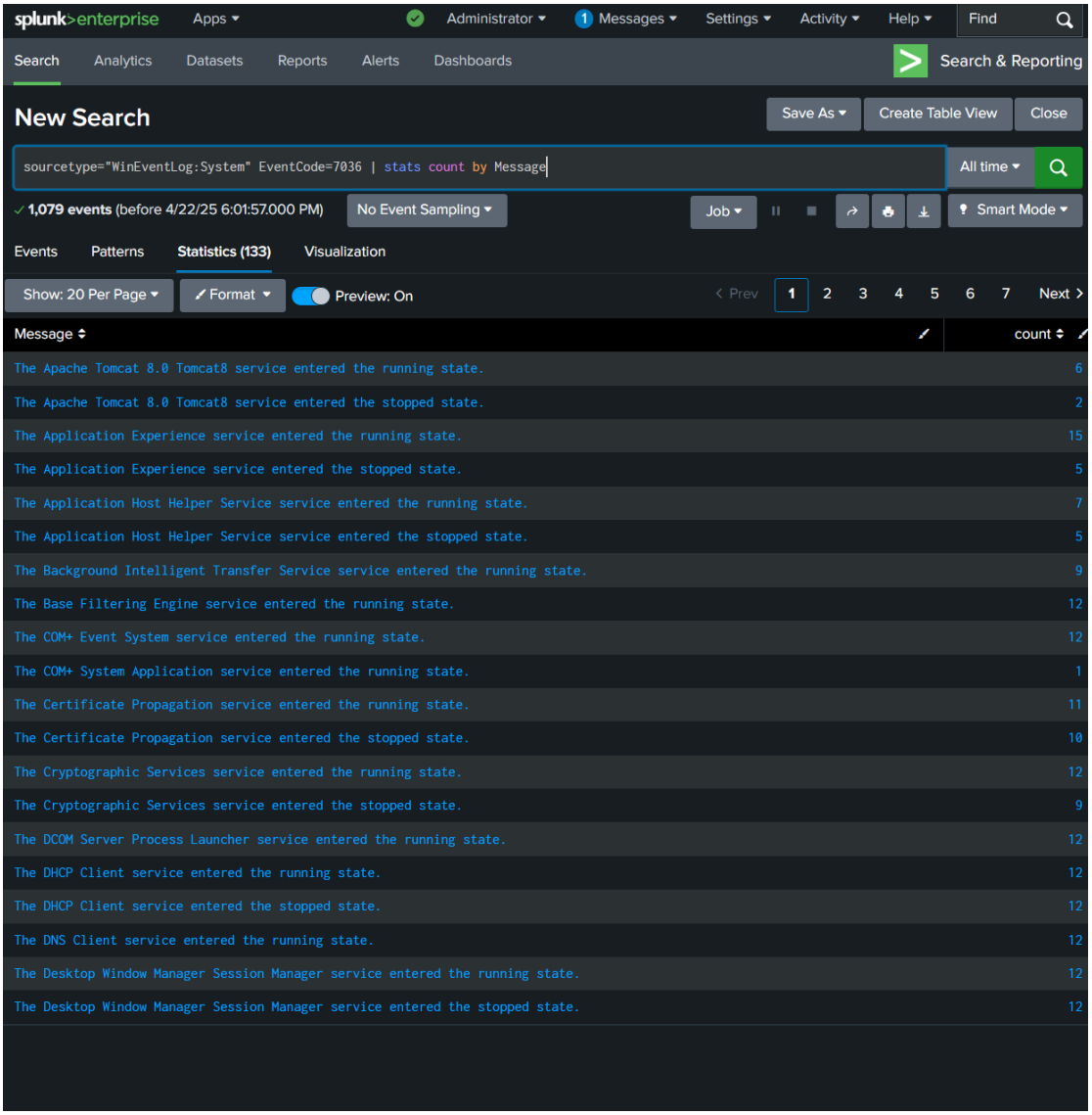


- Searched for Event ID 4624 (successful logins) and 4625 (failed logins):
- sourcetype="WinEventLog:Security" EventCode=4624
- sourcetype="WinEventLog:Security" EventCode=4625
- Searched system logs for Event ID 7036 (service start):



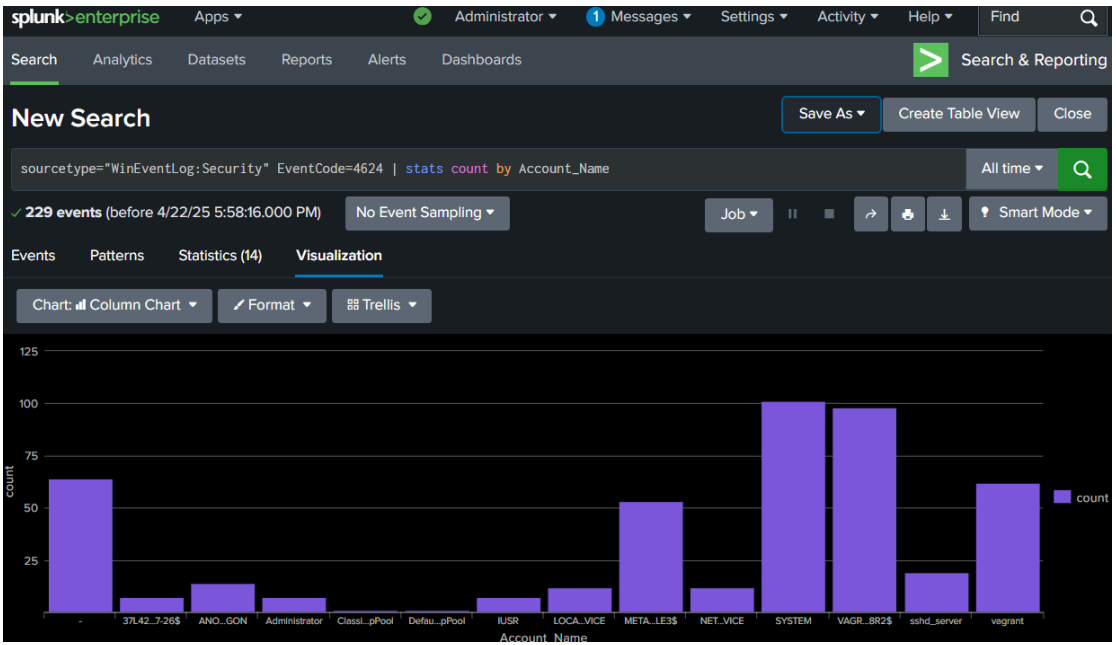

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
sourcetype="WinEventLog:Security" EventCode=4624
All time
229 events (before 4/22/25 5:52:44.000 PM)
No Event Sampling
Job
Smart Mode
Events (229)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 month per column
Format
Show: 20 Per Page
View: List
Prev
1
2
3
4
5
6
7
8
Next
Hide Fields
All Fields
SELECTED FIELDS
host 3
source 1
sourcetype 1
INTERESTING FIELDS
Account_Domain 6
Account_Name 14
Authentication_Package 3
ComputerName 3
EventCode 1
EventType 1
index 1
Key_Length 2
Keywords 1
linecount 1
LogName 1
Logon_GUID 1
Logon_ID 100+
Logon_Process 4
Logon_Type 5
Message 100+
OpCode 1
Package_Name__NTLM_only_ 3
Process_ID 34
Process_Name 7
punct 4
RecordNumber 100+
Security_ID 11
Source_Network_Address 3
Source_Port 6
SourceName 1
splunk_server 1
TaskCategory 1
Transited_Services 1
Type 1
Workstation_Name 6
+ Extract New Fields
Time
Event
4/21/25 3:26:27.000 PM
04/21/2025 03:26:27 PM
LogName=Security
EventCode=4624
EventType=0
ComputerName=metasploitable3-win2k8
Show all 61 lines
host = metasploitable3-win2k8 source = security.evtx sourcetype = WinEventLog:Security
4/21/25 3:25:40.000 PM
04/21/2025 03:25:40 PM
LogName=Security
EventCode=4624
EventType=0
ComputerName=metasploitable3-win2k8
Show all 61 lines
host = metasploitable3-win2k8 source = security.evtx sourcetype = WinEventLog:Security
4/21/25 3:10:57.000 PM
04/21/2025 03:10:57 PM
LogName=Security
EventCode=4624
EventType=0
ComputerName=metasploitable3-win2k8
Show all 61 lines
host = metasploitable3-win2k8 source = security.evtx sourcetype = WinEventLog:Security
4/21/25 3:10:03.000 PM
04/21/2025 03:10:03 PM
LogName=Security
EventCode=4624
EventType=0
ComputerName=metasploitable3-win2k8
Show all 61 lines
host = metasploitable3-win2k8 source = security.evtx sourcetype = WinEventLog:Security
4/21/25 3:10:01.000 PM
04/21/2025 03:10:01 PM
LogName=Security
EventCode=4624
EventType=0
ComputerName=metasploitable3-win2k8
Show all 61 lines
host = metasploitable3-win2k8 source = security.evtx sourcetype = WinEventLog:Security
4/21/25 3:09:57.000 PM
04/21/2025 03:09:57 PM
LogName=Security
EventCode=4624
EventType=0
ComputerName=metasploitable3-win2k8
Show all 61 lines
host = metasploitable3-win2k8 source = security.evtx sourcetype = WinEventLog:Security
4/21/25 3:09:56.000 PM
04/21/2025 03:09:56 PM
LogName=Security
EventCode=4624
EventType=0
ComputerName=metasploitable3-win2k8
Show all 61 lines
host = metasploitable3-win2k8 source = security.evtx sourcetype = WinEventLog:Security
4/21/25 3:09:51.000 PM
04/21/2025 03:09:51 PM
LogName=Security
EventCode=4624
EventType=0
ComputerName=metasploitable3-win2k8
Show all 61 lines
host = metasploitable3-win2k8 source = security.evtx sourcetype = WinEventLog:Security
4/21/25 3:09:49.000 PM
04/21/2025 03:09:49 PM
LogName=Security
EventCode=4624
EventType=0
ComputerName=metasploitable3-win2k8
Show all 61 lines
host = metasploitable3-win2k8 source = security.evtx sourcetype = WinEventLog:Security

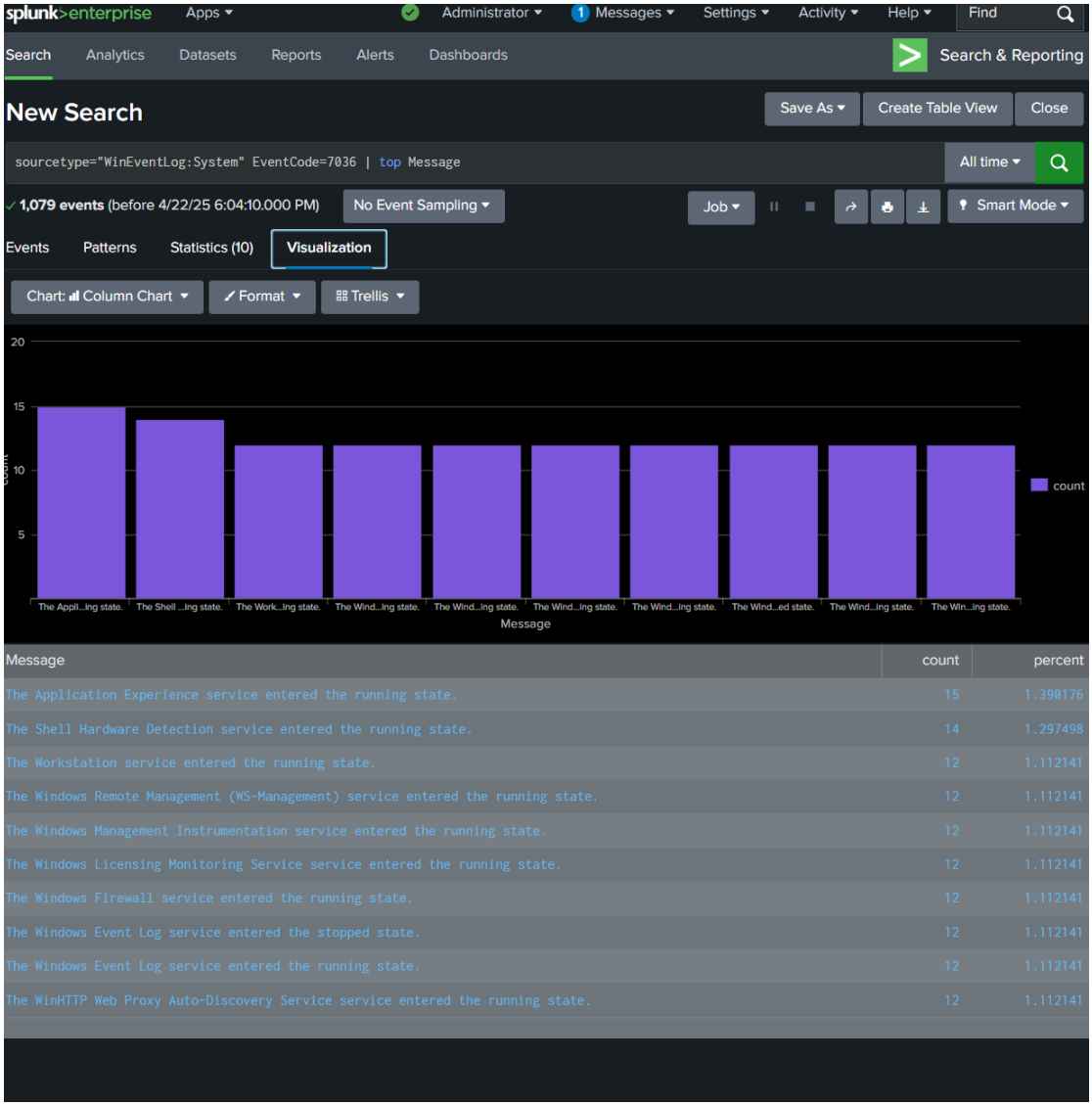

splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
sourcetype="WinEventLog:System" EventCode=1074
All time
18 events (before 4/22/25 6:03:28.000 PM)
No Event Sampling
Job
Smart Mode
Events (18)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 month per column
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
a host 3
a source 1
a sourcetype 1
INTERESTING FIELDS
a Comment 3
a ComputerName 3
EventCode 1
EventType 1
a index 1
a Keywords 1
linecount 1
a LogName 1
a Message 7
a OpCode 1
a punct 5
a Reason_Code 4
RecordNumber 18
a Shutdown_Type 3
a Sid 2
SidType 2
a SourceName 1
a splunk_server 1
a TaskCategory 1
a Type 1
a User 2
+ Extract New Fields
Time
Event
4/20/25 9:31:50.000 PM
04/20/2025 09:31:50 PM
LogName=System
EventCode=1074
EventType=4
ComputerName=metasploitable3-win2k8
Show all 18 lines
host = metasploitable3-win2k8 source = system.evtx
sourcetype = WinEventLog:System
4/19/25 11:08:14.000 PM
04/19/2025 11:08:14 PM
LogName=System
EventCode=1074
EventType=4
ComputerName=metasploitable3-win2k8
Show all 18 lines
host = metasploitable3-win2k8 source = system.evtx
sourcetype = WinEventLog:System
4/19/25 9:57:14.000 PM
04/19/2025 09:57:14 PM
LogName=System
EventCode=1074
EventType=4
ComputerName=metasploitable3-win2k8
Show all 18 lines
host = metasploitable3-win2k8 source = system.evtx
sourcetype = WinEventLog:System
4/19/25 9:56:53.000 PM
04/19/2025 09:56:53 PM
LogName=System
EventCode=1074
EventType=4
ComputerName=metasploitable3-win2k8
Show all 18 lines



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