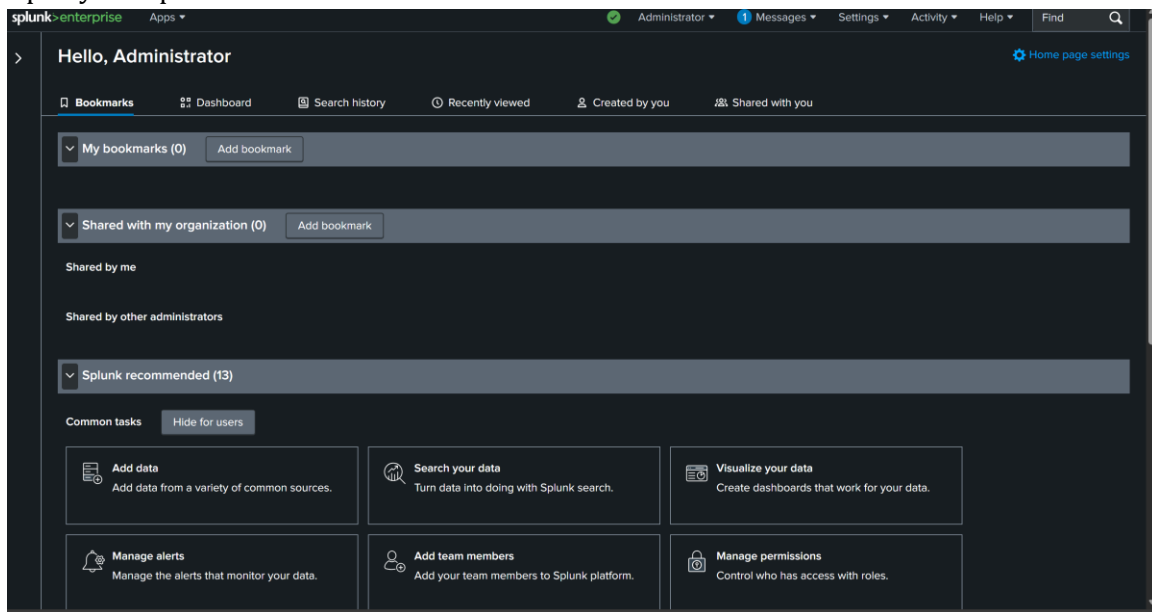


Hands-On Splunk Log Analysis Project

```
source="bns_practice.csv" host="OLALEKAN"  
sourcetype="csv"
```

Step 1: Open Splunk

Open your Splunk instance.



Step 2: Add Data

Navigate to Settings > Add Data.

Upload `bns_practice.csv` with source type set to CSV.

The screenshot shows the Splunk Enterprise web interface. At the top, the navigation bar includes the Splunk logo, 'Apps', and user roles like 'Administrator'. A progress bar indicates the current step is 'Select Source' in the 'Add Data' workflow. The main content area is titled 'Select Source' and instructs the user to choose a file for upload. It shows the 'Selected File' as 'bns_practice.csv' and a 'Select File' button. Below this is a large rectangular drop zone with the text 'Drop your data file here' and 'The maximum file upload size is 500 Mb'. A green checkmark and the text 'File Successfully Uploaded' are visible below the drop zone. At the bottom, there is an 'FAQ' section with three questions: 'What kinds of files can the Splunk platform index?', 'What is a source?', and 'How do I get remote data onto my Splunk platform instance?'.

Add Data

Select Source Set Source Type Input Settings Review Done

< Back Next >

Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. [Learn More](#)

Selected File: `bns_practice.csv`

Select File

Drop your data file here

The maximum file upload size is 500 Mb

File Successfully Uploaded

FAQ

- > What kinds of files can the Splunk platform index?
- > What is a source?
- > How do I get remote data onto my Splunk platform instance?

Step 3: Create Index

Index the data under a new index (e.g., bns_practice).

The screenshot shows the 'Add Data' wizard in Splunk Enterprise, specifically the 'Review' step. The progress bar at the top indicates the steps: Select Source, Set Source Type, Input Settings, Review, and Done. The 'Review' step is currently active. Below the progress bar, there is a 'Review' section with the following details:

- Input Type: Uploaded File
- File Name: bns_practice.csv
- Source Type: csv
- Host: OLALEKAN
- Index: BNS_PRATICE_CSVI

At the top right of the wizard, there are buttons for '< Back' and 'Submit >'. The 'Submit >' button is highlighted in green.

Step 4: Search Events by User

index=bns_practice user="Mbua"

The screenshot shows the Splunk Search interface. The search bar at the top contains the query `index=bns_practice user="Mbua"`. The search results are displayed in a table format. The table has columns for Time, Event, and Source. The search results show 38 events. The first event is from 7/25/25 at 19:21:57, with the event description `2025-07-25 19:21:57,79.244.64:180,Mbua,news.threatpost.com,DELETE,/index,503,2572,Mozilla/5.0,783,api_request,,Ghana,clean,session-78357`. The second event is from 7/25/25 at 7:18:19, with the event description `2025-07-25 19:18:19,207.186.104.88,Mbua,www.darkreading.com,DELETE,/config,200,4318,PostmanRuntime/7.26.8,467,api_request,,Germany,unknown,session-78691`. The third event is from 7/25/25 at 7:14:07, with the event description `2025-07-25 19:14:07,116.251.190.230,Mbua,api.infosecinstitute.com,DELETE,/admin,401,626,dirbuster,217,login_attempt,failure,SSO,Nigeria,malicious,session-28726`. The fourth event is from 7/25/25 at 7:12:02, with the event description `2025-07-25 19:12:02,16.169.110.16,Mbua,api.infosecinstitute.com,POST,/q=script>alert(1)</script>,400,1273,Mozilla/5.0,766,vpn_log,,Germany,suspicious,session-87596`. The search results are displayed in a table format with columns for Time, Event, and Source. The search results show 38 events. The first event is from 7/25/25 at 19:21:57, with the event description `2025-07-25 19:21:57,79.244.64:180,Mbua,news.threatpost.com,DELETE,/index,503,2572,Mozilla/5.0,783,api_request,,Ghana,clean,session-78357`. The second event is from 7/25/25 at 7:18:19, with the event description `2025-07-25 19:18:19,207.186.104.88,Mbua,www.darkreading.com,DELETE,/config,200,4318,PostmanRuntime/7.26.8,467,api_request,,Germany,unknown,session-78691`. The third event is from 7/25/25 at 7:14:07, with the event description `2025-07-25 19:14:07,116.251.190.230,Mbua,api.infosecinstitute.com,DELETE,/admin,401,626,dirbuster,217,login_attempt,failure,SSO,Nigeria,malicious,session-28726`. The fourth event is from 7/25/25 at 7:12:02, with the event description `2025-07-25 19:12:02,16.169.110.16,Mbua,api.infosecinstitute.com,POST,/q=script>alert(1)</script>,400,1273,Mozilla/5.0,766,vpn_log,,Germany,suspicious,session-87596`.

Step 5: Failed Logins per User

index=bns_practice event_type="login_attempt" login_status="failure" | stats count by user, src_ip

The screenshot shows the Splunk Enterprise interface with a search query: `index=bns_practice event_type="login_attempt" login_status="failure" | stats count by user, src_ip`. The results are displayed in a table with columns: user, src_ip, and count. The table shows 38 events, with 20 per page displayed. The users listed are Dennis, Mbua, Mutwiri, and Olalekan, each with multiple failed login attempts from various IP addresses.

user	src_ip	count
Dennis	194.182.122.134	1
Dennis	238.254.61.1	1
Dennis	254.78.64.162	1
Dennis	38.45.25.84	1
Mbua	116.251.198.238	1
Mbua	128.194.94.254	1
Mbua	28.112.70.110	1
Mbua	58.195.71.157	1
Mutwiri	141.14.198.192	1
Mutwiri	221.121.73.233	1
Mutwiri	38.54.11.78	1
Mutwiri	6.131.27.35	1
Mutwiri	68.156.102.69	1

Step 6: Detect Known Bad Tools

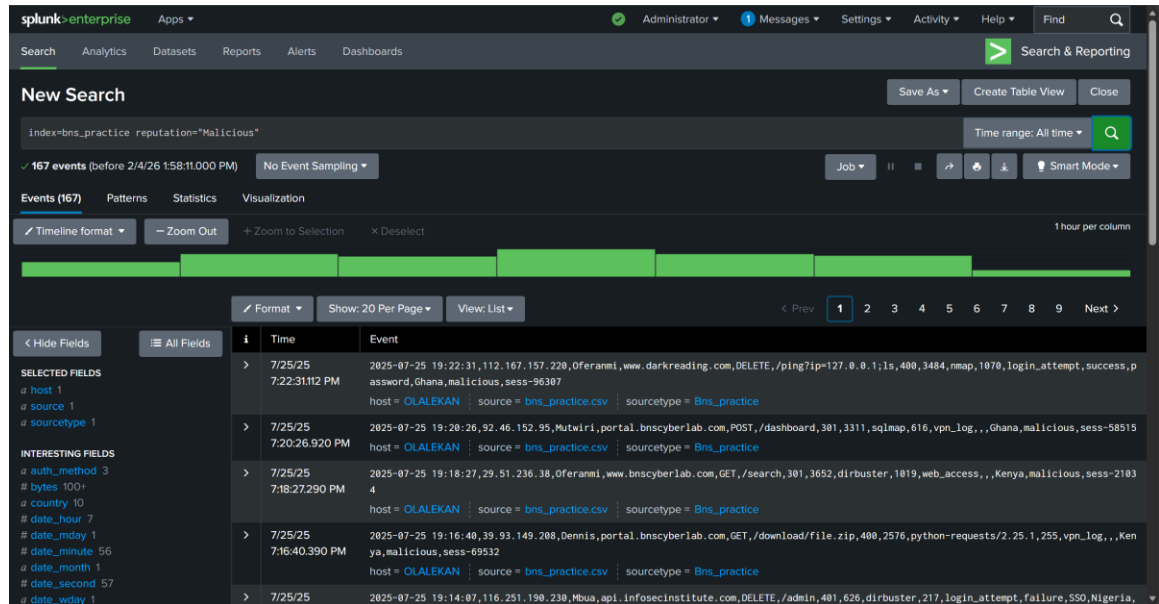
index=bns_practice user_agent IN ("sqlmap", "Nikito", "nmap", "dirbuster")

The screenshot shows the Splunk Enterprise interface with a search query: `index=bns_practice user_agent IN ("sqlmap", "Nikito", "nmap", "dirbuster")`. The results are displayed in a table with columns: Time, Event, and Source. The table shows 101 events, with 20 per page displayed. The events are filtered by the user agent, showing various tools like sqlmap, Nikito, nmap, and dirbuster. The table also includes a sidebar with fields like host, source, and sourcetype.

Time	Event	Source
7/25/25 7:22:31.112 PM	2025-07-25 19:22:31.112.167.157.220,Offeranmi, www.darkreading.com,DELETE,/ping?ip=127.0.0.1;1s,480,3484,nmap,1070,login_attempt,success,p	host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice
7/25/25 7:20:26.920 PM	2025-07-25 19:20:26.92.46.152.95,Mutwiri,portal.bns cyberlab.com,POST,/dashboard,301,3311,sqlmap,616,vpn_log,,Ghana,malicious, sess-38515	host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice
7/25/25 7:18:27.290 PM	2025-07-25 19:18:27.29.51.236.38,Offeranmi, www.bns cyberlab.com,GET,/search,301,3652,dirbuster,1019,web_access,,Kenya,malicious, sess-2183	host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice
7/25/25 7:14:07.116 PM	2025-07-25 19:14:07.116.251.190.230,Mbua,api.infosecinstitute.com,DELETE,/admin,401,626,dirbuster,217,login_attempt,failure,550,Nigeria,malicious, sess-28726	host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice

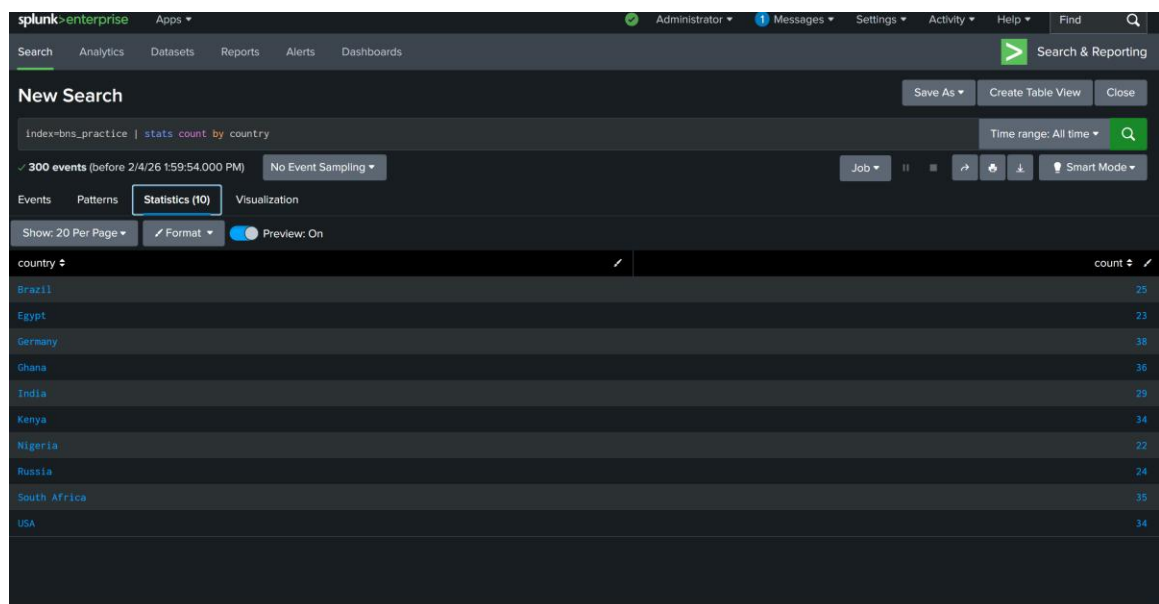
Step 7: Malicious Reputation Events

index=bns_practice reputation="Malicious"



Step 8: Top Countries by Event Count

index=bns_practice | stats count by country



Step 9: Access from Unusual Countries

index=bns_practice country IN ("Russia", "Brazil", "India")

New Search

index=bns_practice country IN ("Russia", "Brazil", "India")

Time range: All time

78 events (before 2/4/26 2:01:39.000 PM) No Event Sampling

Events (78) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect

Format Show: 20 Per Page View: List

#	Time	Event
>	7/25/25 7:10:53.125 PM	2025-07-25 19:18:53, 125.76.42.182, Samuel.portal.bns cyberlab.com, GET, /dashboard, 500, 3023, python-requests/2.25.1, 1084, login_attempt, failure, MFA, Brazil, clean, sess-19879 host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice
>	7/25/25 6:50:57.221 PM	2025-07-25 18:58:57, 221.213.232.58, Mbua.cdn.bns cyberlab.com, POST, /dashboard, 500, 3772, Java/1.8.0_191, 584, login_attempt, success, MFA, India, malicious, sess-61962 host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice
>	7/25/25 6:48:14.320 PM	2025-07-25 18:48:14, 32.225.12.238, Mbua.mail.cybernews.com, DELETE, /index, 302, 2740, sqlmap, 332, api_request, , India, malicious, sess-90226 host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice
>	7/25/25 6:45:27.170 PM	2025-07-25 18:45:27, 170.204.180.16, Oferanmi.portal.bns cyberlab.com, GET, /index, 403, 3446, Mozilla/5.0, 575, api_request, , India, unknown, sess-46163 host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice
>	7/25/25	2025-07-25 18:36:55, 58.195.71.157, Mbua.api.infosecinstitute.com, GET, /?q=<script>alert(1)</script>, 401, 4715, dirbuster, 220, login_attempt,

Step 10: Failed Logins from High-Risk Countries

index=bns_practice event_type="login_attempt" login_status="failure" country IN ("Russia", "Brazil", "India")

New Search

index=bns_practice event_type="login_attempt" login_status="failure" country IN ("Russia", "Brazil", "India")

Time range: All time

7 events (before 2/4/26 2:03:55.000 PM) No Event Sampling

Events (7) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect

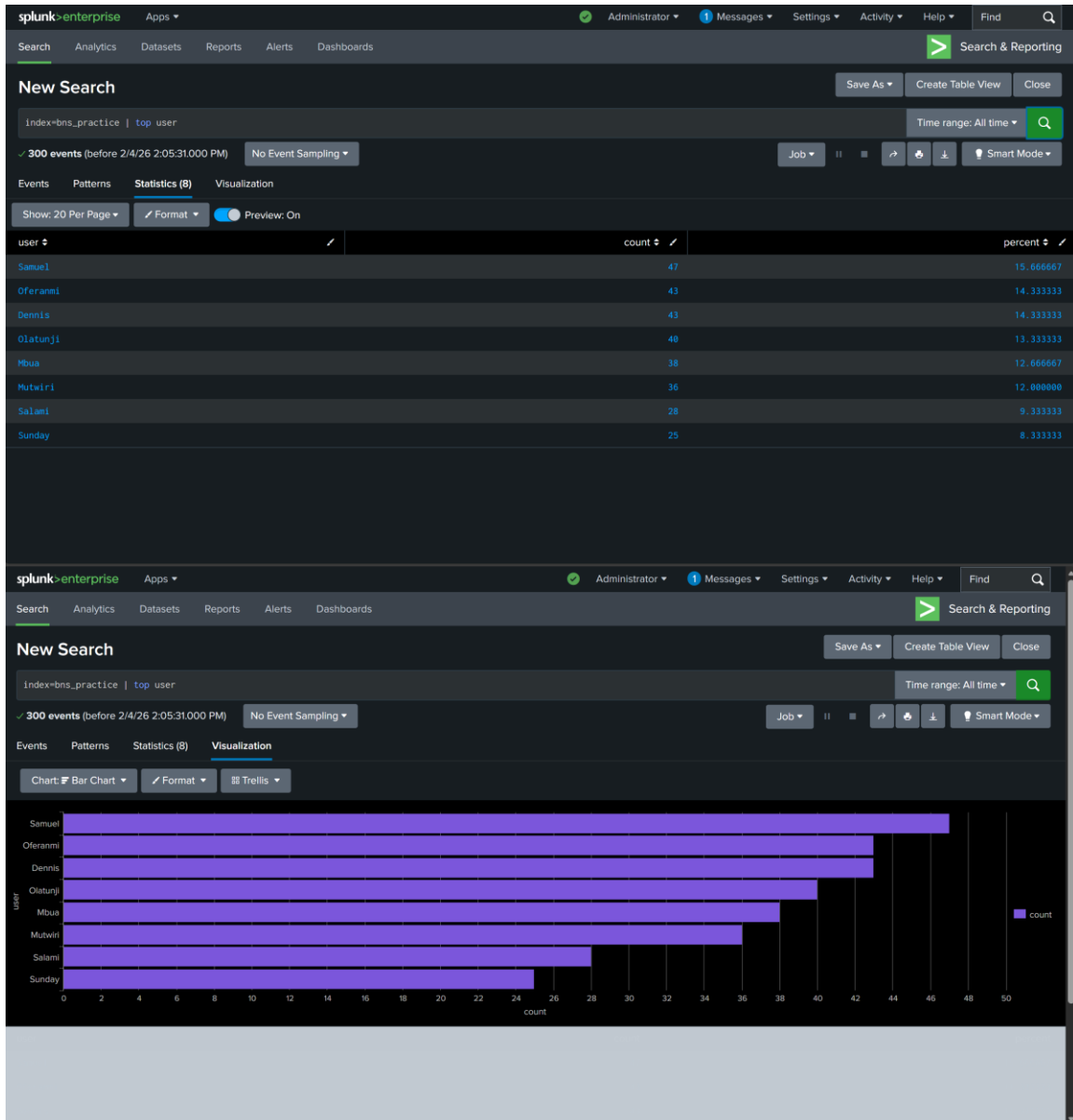
Format Show: 20 Per Page View: List

#	Time	Event
>	7/25/25 7:10:53.125 PM	2025-07-25 19:18:53, 125.76.42.182, Samuel.portal.bns cyberlab.com, GET, /dashboard, 500, 3023, python-requests/2.25.1, 1084, login_attempt, failure, MFA, Brazil, clean, sess-19879 host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice
>	7/25/25 6:36:55.580 PM	2025-07-25 18:36:55, 58.195.71.157, Mbua.api.infosecinstitute.com, GET, /?q=<script>alert(1)</script>, 401, 4715, dirbuster, 220, login_attempt, failure, MFA, Russia, malicious, sess-37374 host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice
>	7/25/25 5:27:25.340 PM	2025-07-25 17:27:25, 34.133.30.10, Oferanmi.portal.bns cyberlab.com, GET, /search, 403, 3670, Nikto, 1145, login_attempt, failure, MFA, Russia, malicious, sess-45174 host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice
>	7/25/25 4:56:17.141 PM	2025-07-25 16:56:17, 141.14.198.192, Mutwiri.forum.hackread.com, PUT, /login, 400, 3633, sqlmap, 374, login_attempt, failure, password, Brazil, malicious, sess-81536 host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice

Step 11: Create User Activity Dashboard

index=bns_practice | top user

Click Visualization > Select Bar Chart.



Step 12: Visualize Automated Tool Activity

index=bns_practice user_agent IN ("dirbuster", "sqlmap", "Nikito", "nmap") | stats count by user_agent

The screenshot displays the Splunk Enterprise web interface. At the top, the navigation bar includes 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The 'Search & Reporting' section is active, showing a 'New Search' page. The search query is 'index=bns_practice user_agent IN ("dirbuster", "sqlmap", "Nikito", "nmap") | stats count by user_agent'. The results show 101 events. Below the search bar, there are tabs for 'Events (101)', 'Patterns', 'Statistics (3)', and 'Visualization'. The 'Events (101)' tab is selected, and the 'Timeline format' is chosen. A timeline visualization shows four green bars representing event counts over time. Below the timeline, a table lists the events. The table has columns for 'Time' and 'Event'. The events are listed in chronological order, showing the source, host, and user agent for each event.

Time	Event
7/25/25 7:22:31.112 PM	2025-07-25 19:22:31,112.167.157.220,Oferanmi,www.darkreading.com,DELETE,/ping?ip=127.0.0.1;ls,400,3484,nmap,1070,login_attempt,success,password,Ghana,malicious,sess-96307 host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice
7/25/25 7:20:26.920 PM	2025-07-25 19:20:26,92.46.152.95,Mutwiri,portal.bns cyberlab.com,POST,/dashboard,301,3311,sqlmap,616,vpn_log,,Ghana,malicious,sess-58515 host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice
7/25/25 7:18:27.290 PM	2025-07-25 19:18:27,29.51.236.38,Oferanmi,www.bns cyberlab.com,GET,/search,301,3652,dirbuster,1019,web_access,,Kenya,malicious,sess-2103 host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice
7/25/25 7:14:07.116 PM	2025-07-25 19:14:07,116.251.190.230,Mbua,api.infosecinstitute.com,DELETE,/admin,401,626,dirbuster,217,login_attempt,failure,550,Nigeria,malicious,sess-28726 host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice

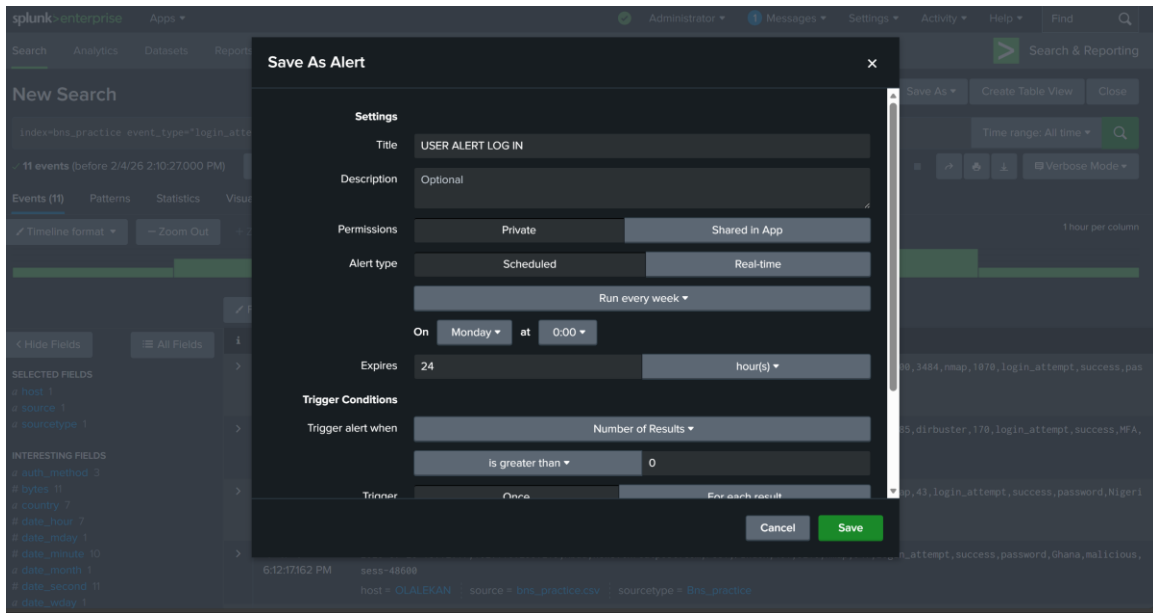
Step 13: Create Alert for Suspicious Successful Login

index=bns_practice event_type="login_attempt" login_status="success" user_agent IN ("sqlmap", "dirbuster", "python-requests", "nmap")

Click Save As > Alert > Configure alert action.

The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. Below this, the 'New Search' section displays a search query: `index=bns_practice event_type="login_attempt" login_status="success" user_agent IN ("sqlmap", "dirbuster", "python-requests", "nmap")`. The search results show 11 events. A dropdown menu is open, showing options: 'Report', 'Alert', 'Existing Dashboard', 'New Dashboard', and 'Event Type'. The 'Alert' option is highlighted. Below the search results, there's a table with columns 'Time' and 'Event'. The table contains four rows of event data, each showing a timestamp and a detailed log entry.

Time	Event
7/25/25 7:22:31.112 PM	2025-07-25 19:22:31.112.167.157.220,0feranmi,ww.darkreading.com,DELETE,/ping?ip=127.0.0.1;ls,480,3484,nmap,1070,login_attempt,success,p assword,Ghana,malicious,sess-96307 host = OLALEKAN : source = bns_practice.csv : sourcetype = Bns_practice
7/25/25 6:40:24.158 PM	2025-07-25 18:40:24.158.33.243.249,Sunday,cdn.bns cyberlab.com,POST,/ping?ip=127.0.0.1;ls,480,1585,dirbuster,170,login_attempt,success,MF A,Nigeria,malicious,sess-48824 host = OLALEKAN : source = bns_practice.csv : sourcetype = Bns_practice
7/25/25 6:36:27.850 PM	2025-07-25 18:36:27.85.30.108.113,Mbua,news.threatpost.com,GET,/ping?ip=127.0.0.1;ls,382,686,nmap,43,login_attempt,success,password,Nige ria,malicious,sess-76490 host = OLALEKAN : source = bns_practice.csv : sourcetype = Bns_practice
7/25/25 6:12:17.162 PM	2025-07-25 18:12:17.162.116.233.219,Mbua,news.threatpost.com,POST,/index,401,3210,nmap,947,login_attempt,success,password,Ghana,maliciou s, sess-48600 host = OLALEKAN : source = bns_practice.csv : sourcetype = Bns_practice



BY AFOLABI MUHYDEEN OLALEKAN
CYBERSECURITY ANALYST