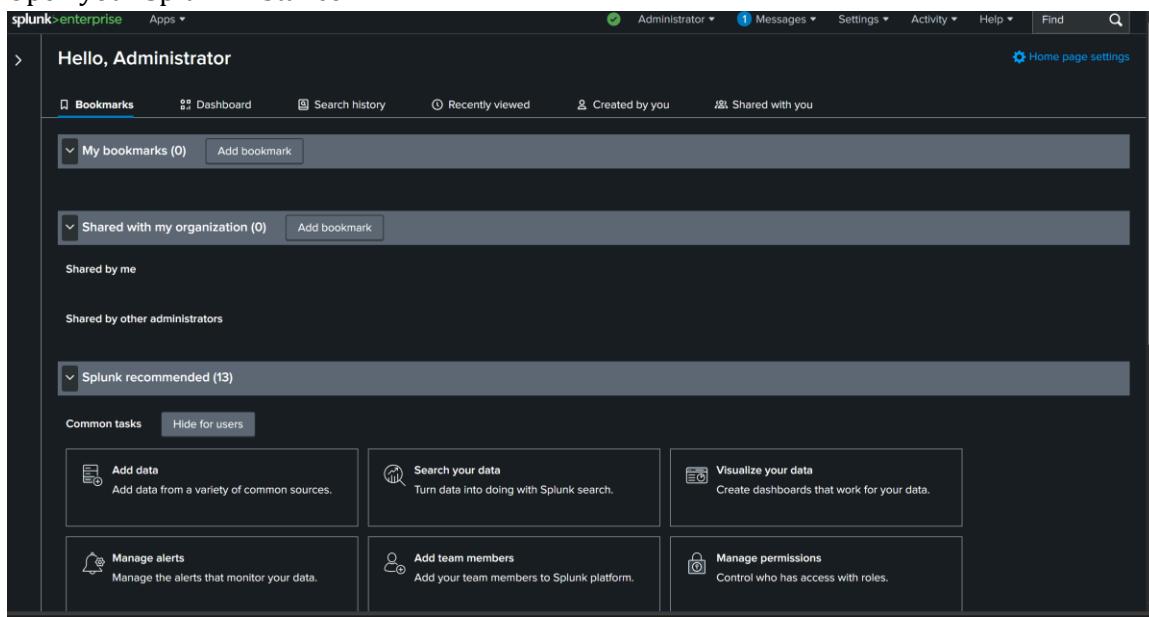


Hands-On Splunk Log Analysis Project

**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 Add Data interface. At the top, there is a navigation bar with links for 'splunk enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', 'Find', and a search icon. Below the navigation bar, a progress bar indicates the current step: 'Add Data' (green dot), 'Select Source' (white circle), 'Set Source Type' (white circle), 'Input Settings' (white circle), 'Review' (white circle), and 'Done' (white circle). A 'Next >' button is located at the end of the progress bar. To the left of the progress bar, the text 'Add Data' is displayed. The main content area has a title 'Select Source' and instructions: 'Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below.' A link 'Learn More' is provided. Below this, it says 'Selected File: bns_practice.csv' and has a 'Select File' button. There is a large rectangular area for file upload with the placeholder text 'Drop your data file here'. Below this area, it states 'The maximum file upload size is 500 Mb'. A green checkmark icon followed by the text 'File Successfully Uploaded' is shown. At the bottom of the content area, there is a 'FAQ' section with three expandable items: '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?'. The entire interface is presented in a light gray background with white and light blue UI elements.

Step 3: Create Index

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

The screenshot shows the Splunk Add Data interface with the title "Review". It displays the configuration details for indexing a CSV file:

- Input Type: Uploaded File
- File Name: bns_practice.csv
- Source Type: csv
- Host: OLALEKAN
- Index: BNS_PRATICE_CSV1

At the bottom right of the review section is a "Submit" button.

Step 4: Search Events by User

index=bns_practice user="Mbua"

The screenshot shows the Splunk Search & Reporting interface with the search bar containing "index=bns_practice user='Mbua'". The results show 38 events found between July 25, 2025, and July 26, 2025. The results table includes columns for Time, Event, and several source fields. The results are as follows:

Time	Event
7/25/25 7:21:57 PM	host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice
7/25/25 7:18:19.207 PM	host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice
7/25/25 7:14:07!16 PM	host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice
7/25/25 7:12:02!60 PM	host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice

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 interface with a search bar containing the query: index=bns_practice event_type="login_attempt" login_status="failure" | stats count by user, src_ip. Below the search bar, it displays 38 events from before 2/4/26 1:52:49:000 PM. The results are shown in a table with columns: user, src_ip, and count. The data shows multiple users (Dennis, Mbua, Mutwiri) attempting to log in from various IP addresses, with each attempt counted as 1.

user	src_ip	count
Dennis	194.182.122.134	1
Dennis	238.254.61.1	1
Dennis	254.76.64.162	1
Dennis	38.45.25.84	1
Mbua	116.251.190.230	1
Mbua	128.194.94.254	1
Mbua	28.112.70.119	1
Mbua	58.195.71.157	1
Mutwiri	141.14.198.192	1
Mutwiri	221.121.73.233	1
Mutwiri	38.54.11.70	1
Mutwiri	6.131.27.35	1
Mutwiri	60.156.102.69	1

Step 6: Detect Known Bad Tools

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

The screenshot shows the Splunk interface with a search bar containing the query: index=bns_practice user_agent IN ("sqlmap", "Nikito", "nmap", "dirbuster"). Below the search bar, it displays 101 events from before 2/4/26 1:56:38:000 PM. The results are shown in a timeline format with a green bar indicating the duration of the events. The data shows multiple instances of known bad tools being used, such as sqlmap, Nikito, nmap, and dirbuster, across different hosts and times.

Time	Event
7/25/25 7:22:31:112 PM	2025-07-25 19:22:31,112.167.157.220,Oferammi,www.darkreading.com,DELETE,/ping?ip=127.0.0.1;ls,400,3484,nmap,1070,login_attempt,success,p password,Ghana,malicious,ses-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.bnscyberlab.com,POST,/dashboard,301,3311,sqlmap,616,vpn_log,,,Ghana,malicious,ses-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,Oferammi,www.bnscyberlab.com,GET,/search,301,3652,dirbuster,1019,web_access,,Kenya,malicious,ses-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,SSO,Nigeria, malicious,ses-28726 host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice

Step 7: Malicious Reputation Events

index=bns_practice reputation="Malicious"

The screenshot shows the Splunk Enterprise interface with a search bar containing "index=bns_practice reputation='Malicious'". The results section displays 167 events from July 25, 2025, with various log entries. On the left, there's a sidebar with "SELECTED FIELDS" and "INTERESTING FIELDS" lists. The main table has columns for Time and Event.

Time	Event
7/25/25 7:22:31.112 PM	2025-07-25 19:22:31.112.167.157.157.0ferammi,www.darkreading.com,DELETE,/ping?ip=127.0.0.1;ls,400,3484,nmap,1070,login_attempt,success,p password,Ghana,malicious,ses-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.bnscyberlab.com,POST,/dashboard,301,3311,sqlmap,616,vpn_log,,Ghana,malicious,ses-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,Oferammi,www.bnscyberlab.com,GET,/search,301,3652,dirbuster,1019,web_access,,,Kenya,malicious,ses-2103 4 host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice
7/25/25 7:16:40.390 PM	2025-07-25 19:16:40.39.93.149.208,Dennis,portal.bnscyberlab.com,GET,/download/file.zip,400,2576,python-requests/2.25.1,255,vpn_log,,Kenya,ma malicious,ses-69532 host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice
7/25/25	2025-07-25 19:14:07,116.251.198.230,Mbuia,api.infosecinstitute.com,DELETE,/admin,401,626,dirbuster,217,login_attempt,failure,SSO,Nigeria, ses-22000 host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice

Step 8: Top Countries by Event Count

index=bns_practice | stats count by country

The screenshot shows the Splunk Enterprise interface with a search bar containing "index=bns_practice | stats count by country". The results section displays 300 events, with a table showing the top countries and their event counts.

country	count
Brazil	25
Egypt	23
Germany	38
Ghana	36
India	29
Kenya	34
Nigeria	22
Russia	24
South Africa	35
USA	34

Step 9: Access from Unusual Countries

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

The screenshot shows the Splunk Enterprise interface with a search bar containing the query "index=bns_practice country IN [\"Russia\", \"Brazil\", \"India\"]". Below the search bar, it says "78 events (before 2/4/26 2:01:39.000 PM) No Event Sampling". The main area displays a table of event logs with columns for Time and Event. The table includes selected fields like host, source, and sourcetype, and interesting fields such as auth_method, bytes, country, date_hour, date_minute, date_month, date_second, and date_wday. The results show multiple log entries from various hosts, mostly from OLAKEAN, with different timestamps and event details.

	Time	Event
>	7/25/25 7:10:53.125 PM	2025-07-25 19:10:53,125,76.42.182,Samuel,portal.bnscyberlab.com,GET,/dashboard,500,3023,python-requests/2.25.1,1084,login_attempt,failure,MFA,Brazil,clean,sess-19879 host = OLAKEAN source = bns_practice.csv sourcetype = Bns_practice
>	7/25/25 6:50:57.221 PM	2025-07-25 18:50:57,221.213.232.58,Mbua,cdn.bnscyberlab.com,POST,/dashboard,500,3772,Java/1.8.0_191,584,login_attempt,success,MFA,India,malicious,sess-61962 host = OLAKEAN 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 = OLAKEAN source = bns_practice.csv sourcetype = Bns_practice
>	7/25/25 6:45:27.70 PM	2025-07-25 18:45:27,170.204.100.16,Oferammi,portal.bnscyberlab.com,GET,/index,403,3446,Mozilla/5.0,575,api_request,,,India,unknown,sess-46163 host = OLAKEAN 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, host = OLAKEAN source = bns_practice.csv sourcetype = Bns_practice

Step 10: Failed Logins from High-Risk Countries

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

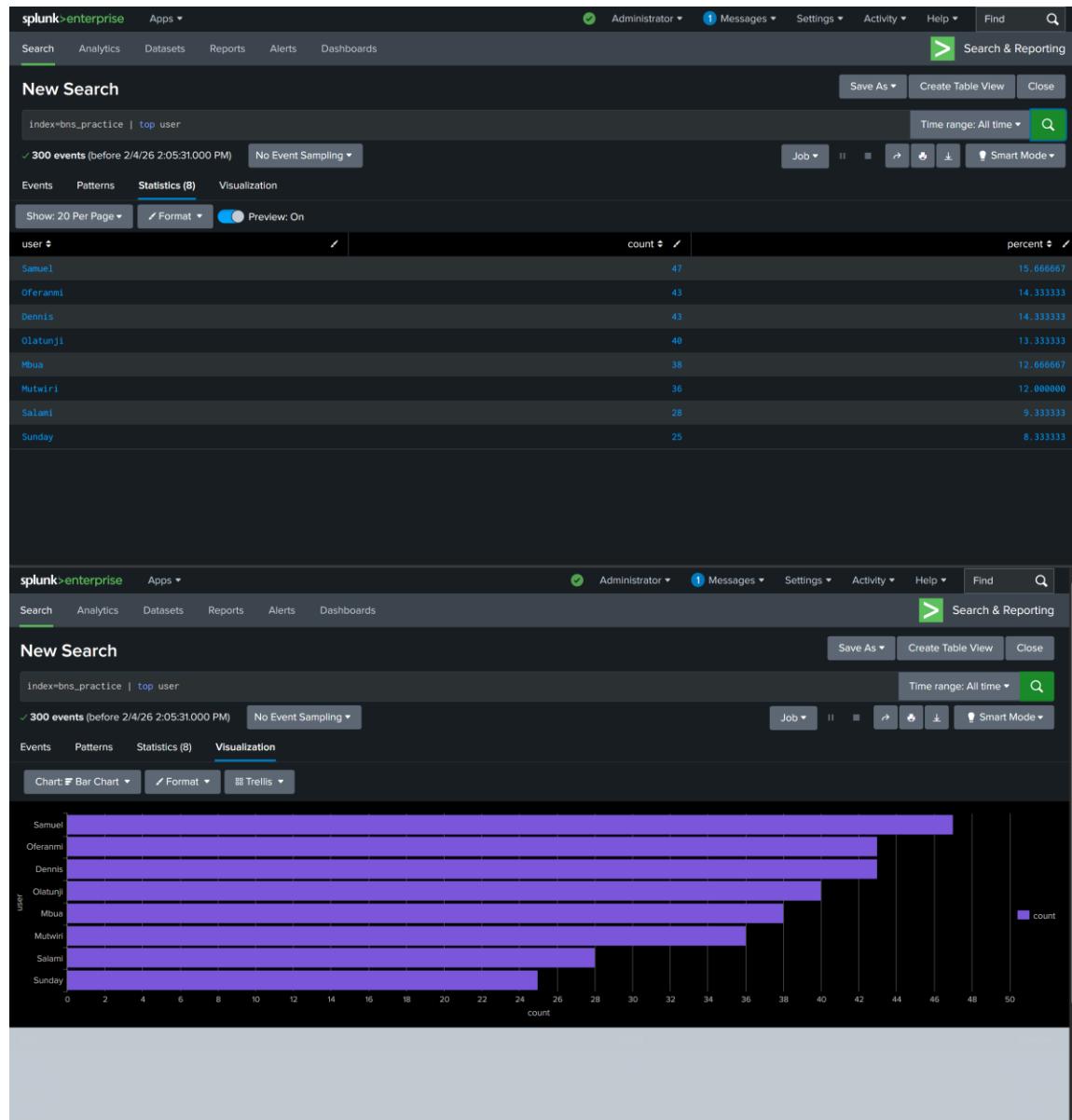
The screenshot shows the Splunk Enterprise interface with a search bar containing the query "index=bns_practice event_type='login_attempt' login_status='failure' country IN [\"Russia\", \"Brazil\", \"India\"]". Below the search bar, it says "7 events (before 2/4/26 2:03:55.000 PM) No Event Sampling". The main area displays a table of event logs with columns for Time and Event. The table includes selected fields like host, source, and sourcetype, and interesting fields such as auth_method, bytes, country, date_hour, date_minute, date_month, date_second, and date_wday. The results show multiple log entries from various hosts, mostly from OLAKEAN, with different timestamps and event details.

	Time	Event
>	7/25/25 7:10:53.125 PM	2025-07-25 19:10:53,125,76.42.182,Samuel,portal.bnscyberlab.com,GET,/dashboard,500,3023,python-requests/2.25.1,1084,login_attempt,failure,MFA,Brazil,clean,sess-19879 host = OLAKEAN 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 = OLAKEAN 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,Oferammi,portal.bnscyberlab.com,GET,/search,403,3670,Nikto,1145,login_attempt,failure,MFA,Russia,malicious,sess-45174 host = OLAKEAN 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 = OLAKEAN 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", "Nikto", "nmap") | stats count by user_agent

The screenshot shows the Splunk Enterprise interface with a search bar containing the query: `index=bns_practice user_agent IN ("dirbuster", "sqlmap", "Nikto", "nmap") | stats count by user_agent`. The search results indicate 101 events found before 2/4/26 2:08:59.00 PM. The Events (101) tab is selected, showing a timeline format with green bars representing event times. Below the timeline is a table of event details:

Time	Event
7/25/25 7:22:31.12 PM	2025-07-25 19:22:31,112.167.157.220,Oferammi,www.darkreading.com,DELETE,/ping?ip=127.0.0.1;ls,400,3484,nmap,1070,login_attempt,success,p password,Ghana,malicious,ses... host = OALEKAN 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.bnscyberlab.com,POST,/dashboard,301,3311,sqlmap,616,vpn_log,,Ghana,malicious,ses... host = OALEKAN 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,Oferammi,www.bnscyberlab.com,GET,/search,301,3652,dirbuster,1019,web_access,,,Kenya,malicious,ses... host = OALEKAN source = bns_practice.csv sourcetype = Bns_practice
7/25/25 7:14:07.116 PM	2025-07-25 19:14:07,116.251.198.238,Mbua,api.infosecinstitute.com,DELETE,/admin,401,626,dirbuster,217,login_attempt,failure,SSO,Nigeria, malicious,ses... host = OALEKAN source = bns_practice.csv sourcetype = Bns_practice

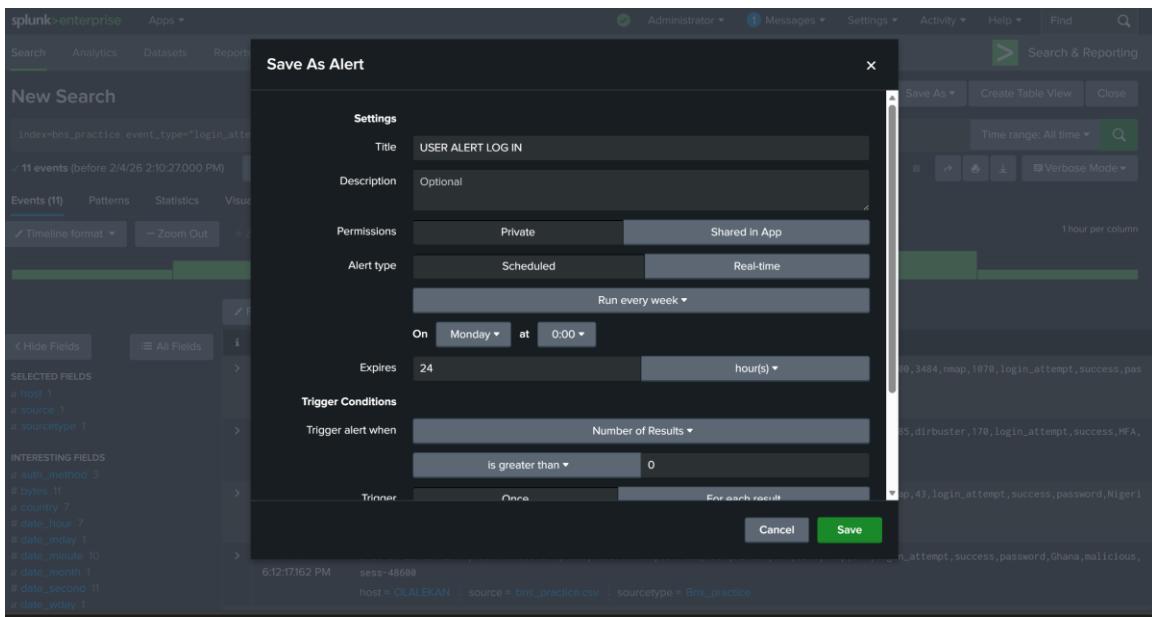
Step 13: Create Alert for Suspicious Successful Login

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 search interface. The search bar contains the query: index=bns_practice event_type="login_attempt" login_status="success" user_agent IN ("sqlmap", "dirbuster", "python-requests", "nmap"). Below the search bar, it says "11 events (before 2/4/26 2:10:27.000 PM) No Event Sampling". The results table has columns for Time and Event. The first few rows of the table are:

Time	Event
7/25/25 7:22:31.12 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,ses-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,cn.bnscyberlab.com,POST,/ping?ip=127.0.0.1;ls,400,1585,dirbuster,170,login_attempt,success,MF A,Nigeria,malicious,ses-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,302,606,nmap,43,login_attempt,success,password,Nigeria,malicious,ses-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,malicious,ses-48680 host = OLALEKAN source = bns_practice.csv sourcetype = Bns_practice



**BY AFOLABI MUHYDEEN OLALEKAN
CYBERSECURITY ANALYST**