**Splunk**

**EC2 Instance Requirements:**

AMI: Ubuntu 22.04 (Lightweight OS)

Instance Type: t3.medium (2 vCPU, 4GB RAM)

Storage: 20GB gp3 SSD

Security Group:

22 (SSH)

8000 (Splunk Web UI)

9997 (Forwarder Log Port)

**Commands:**

sudo apt update && sudo apt upgrade -y

wget -O splunk-9.4.1.deb "https://download.splunk.com/products/splunk/releases/9.4.1/linux/splunk-9.4.1-e3bdab203ac8-linux-amd64.deb"

ls -lh splunk-9.4.1.deb

sudo dpkg -i splunk-9.4.1.deb

sudo mkdir -p /opt/splunk/etc/system/local

echo -e "[user\_info]\nUSERNAME = admin\nPASSWORD = YourStrongPassword" | sudo tee /opt/splunk/etc/system/local/user-seed.conf

#Note:

USERNAME = admin

PASSWORD = YourStrongPassword

sudo chown -R splunk:splunk /opt/splunk/etc/system/local/user-seed.conf

sudo chmod 600 /opt/splunk/etc/system/local/user-seed.conf

sudo /opt/splunk/bin/splunk restart

open http://<EC2-Public-IP>:8000

Task: Visualizing SSH Login Attempts from Logs:

Go to the "Apps" dropdown (Top-left corner)

Click on "Manage Apps"

Find "Search & Reporting"

If it's disabled, click "Enable"

Visit:-

http://<Your-EC2-Public-IP>:8000/en-US/app/search/search

* 1️. Open Data Summary
* 2️. Choose Host, Source, or SourceType (Choose any one)
* 3️. Run a Search Query
* 4️. Select Visualization
* 5️. Click on Pivot
* 6️. Select Line Chart, Area Chart, or Pie Chart (Choose according to your choice)
* 7️. Filter by Time Period



