

Day 21 of Learning Cyber Security

Platform: Kali Linux

Name: Ayesha Nadeem

Topic: Splunk



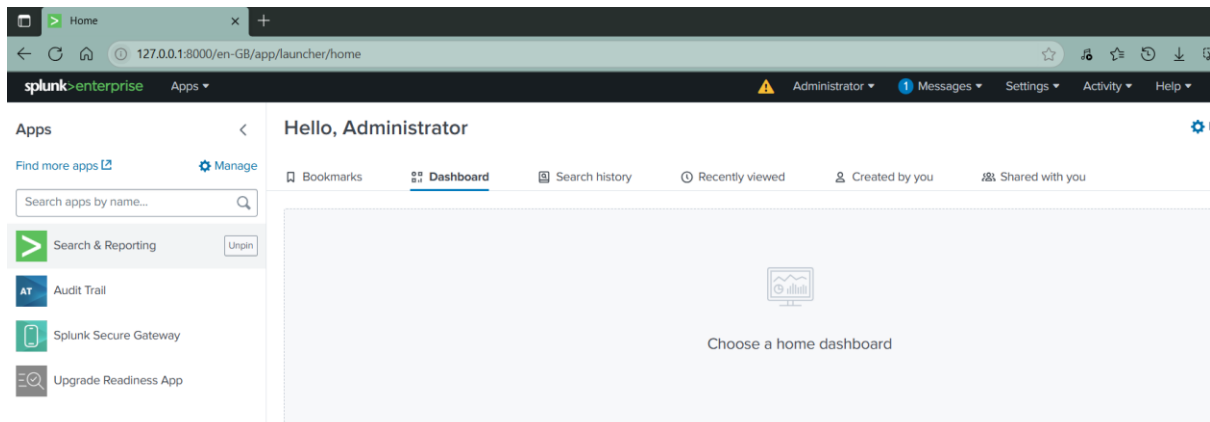
splunk

Contact Me: ayeshanm8@gmail.com

Date: 21th July, 2025

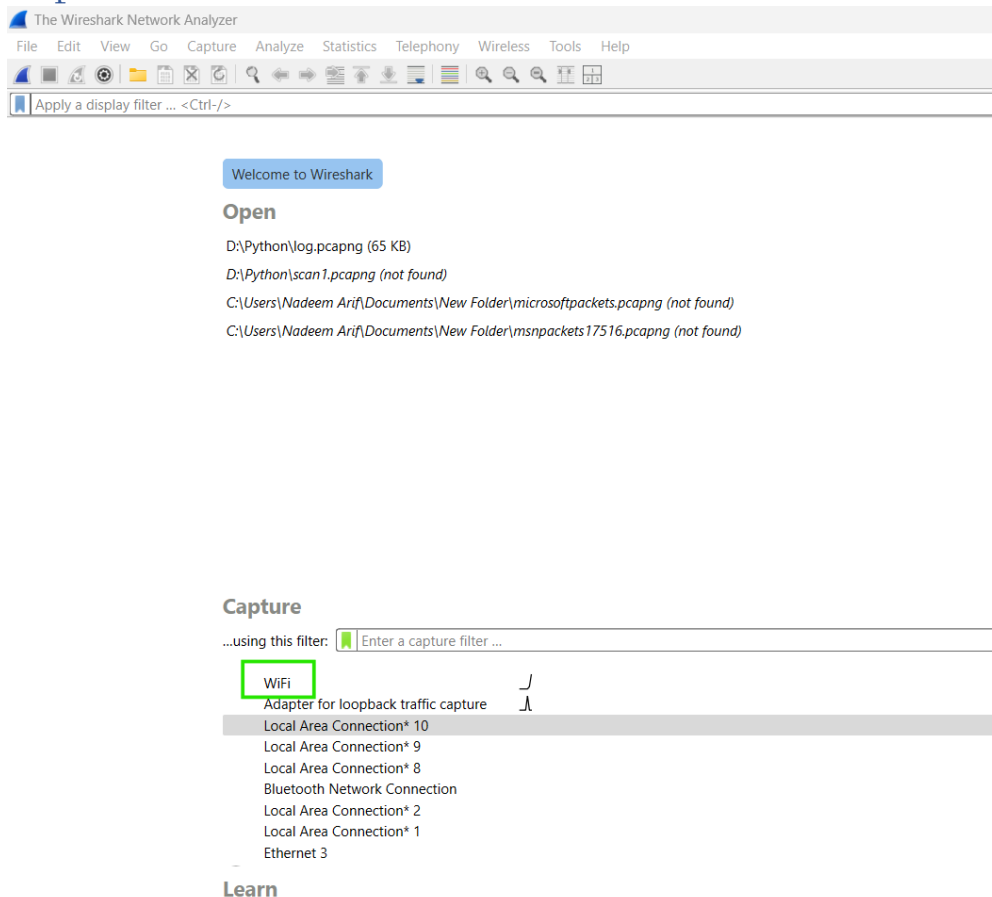
Splunk Enterprise

Welcome to Splunk dashboard



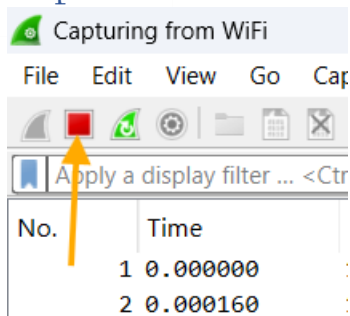
Save log file form wireshark:

Step 1:



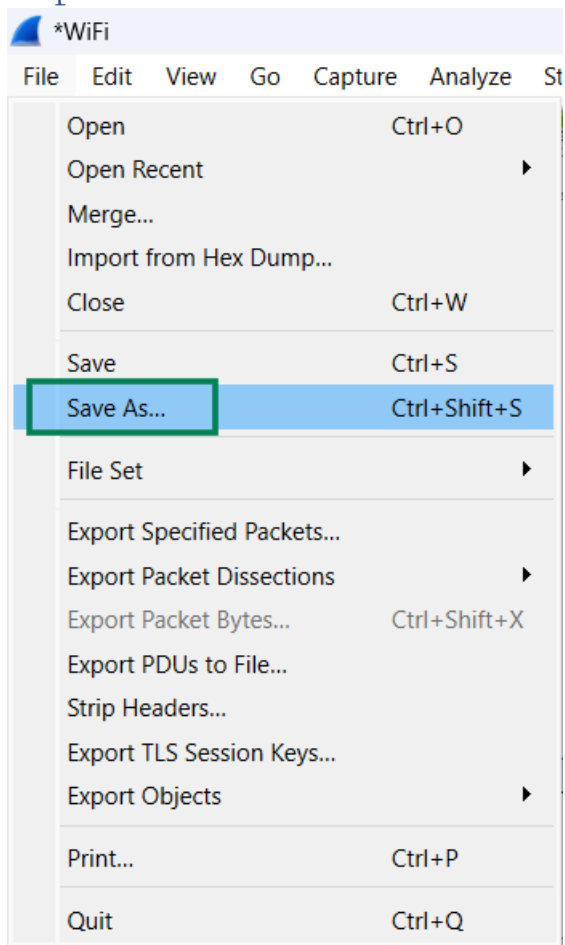
Double click on WiFi/eth0 to start capturing packet.

Step 2:

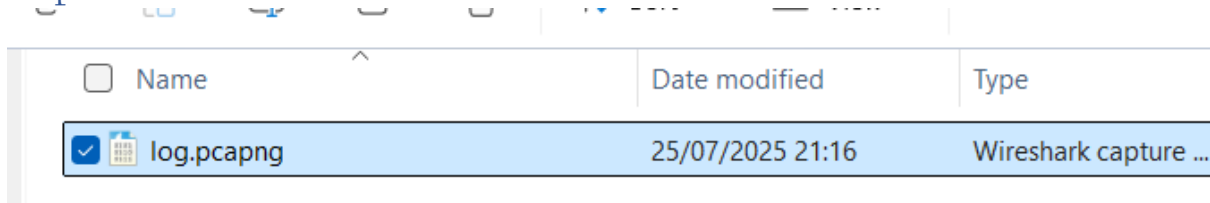


Click on red button to stop capturing packet.

Step 3:

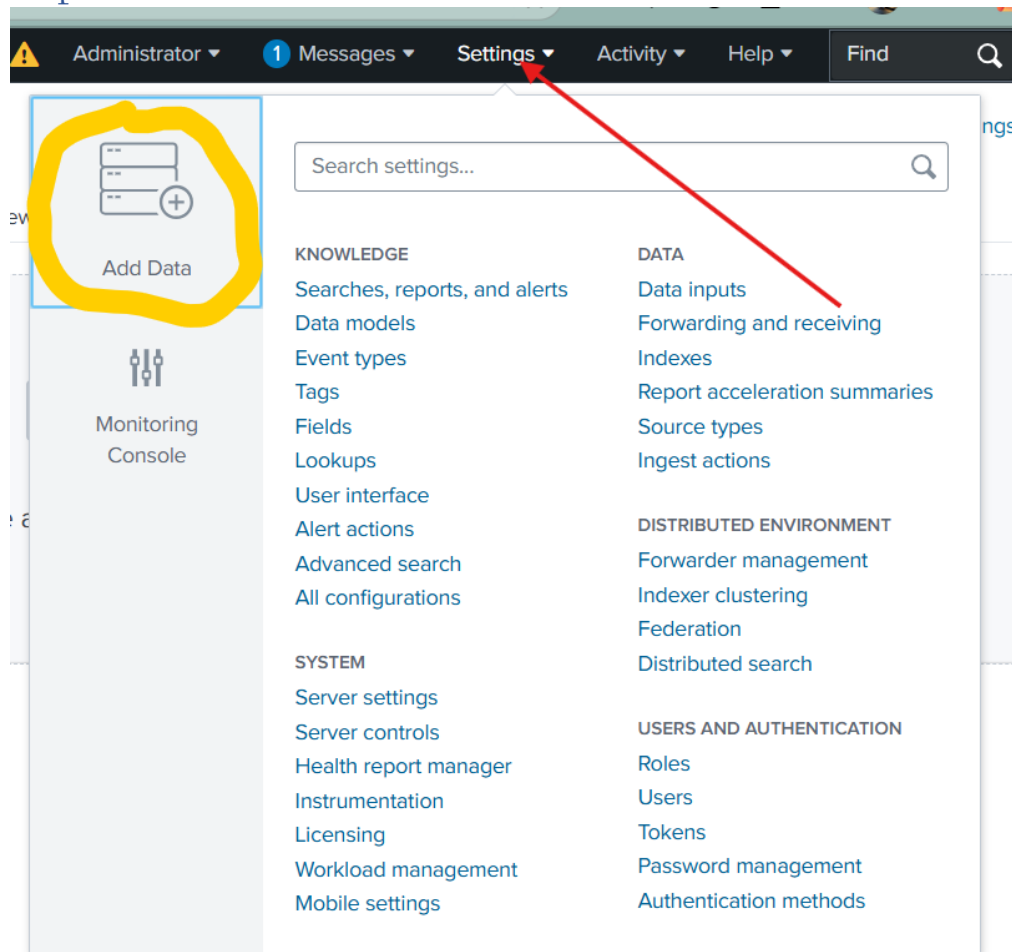


Step 4:



Upload doc in splunk:


Step 1:



Step 2:


4 data sources in total

Or get data in with the following methods



Upload
files from my computer

Local log files
Local structured files (e.g. CSV)
[Tutorial for adding data](#)



Monitor
files and ports on this Splunk platform instance

Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources

Step 3:

Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping

Selected File: **log.pcapng**

Select File

Drop your data file here

The maximum file upload size is 500 Mb



File Successfully Uploaded

Click on next

Step 4:

Save Source Type

Name

My Report

Description

Analysing malicious activity in WiFi network

Category

Custom ▼

App

Search & Reporting ▼

Cancel

Save

Click on save.

Step 5:

Add Data

Select Source Set Source Type **Input Settings** Review Done

< Back **Review >**

Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

☒ Constant value
☐ Regular expression on path
☐ Segment in path

Host field value

Step 6:

Add Data

Select Source Set Source Type Input Settings **Review** Done

< Back **Submit >**

Review

Input Type Uploaded File
File Name log.pcapng
Source Type My Report
Host LAPTOP-A41FU8FM
Index Default

Generate Report:

Step 1:

The screenshot shows the Splunk field selection interface for the field 'linecount'. The left sidebar lists 'SELECTED FIELDS' (host 1, source 1, sourcetype 1) and 'INTERESTING FIELDS' (index 1, linecount 2, punct 100+, splunk_server 1, timestamp 1). The main panel shows 'linecount' with '2 Values, 100% of events'. A green box highlights the 'Reports' section, which includes 'Average over time', 'Maximum value over time', 'Minimum value over time', 'Top values', 'Top values by time' (highlighted with a red arrow), and 'Rare values'. Below this, a table shows the distribution of values:

Values	Count	%
1	205	99.514%
257	1	0.485%

Step 2:

