M. Kaan Arici 16.12.2024
Mandatory 2.3 - SOF-ELK

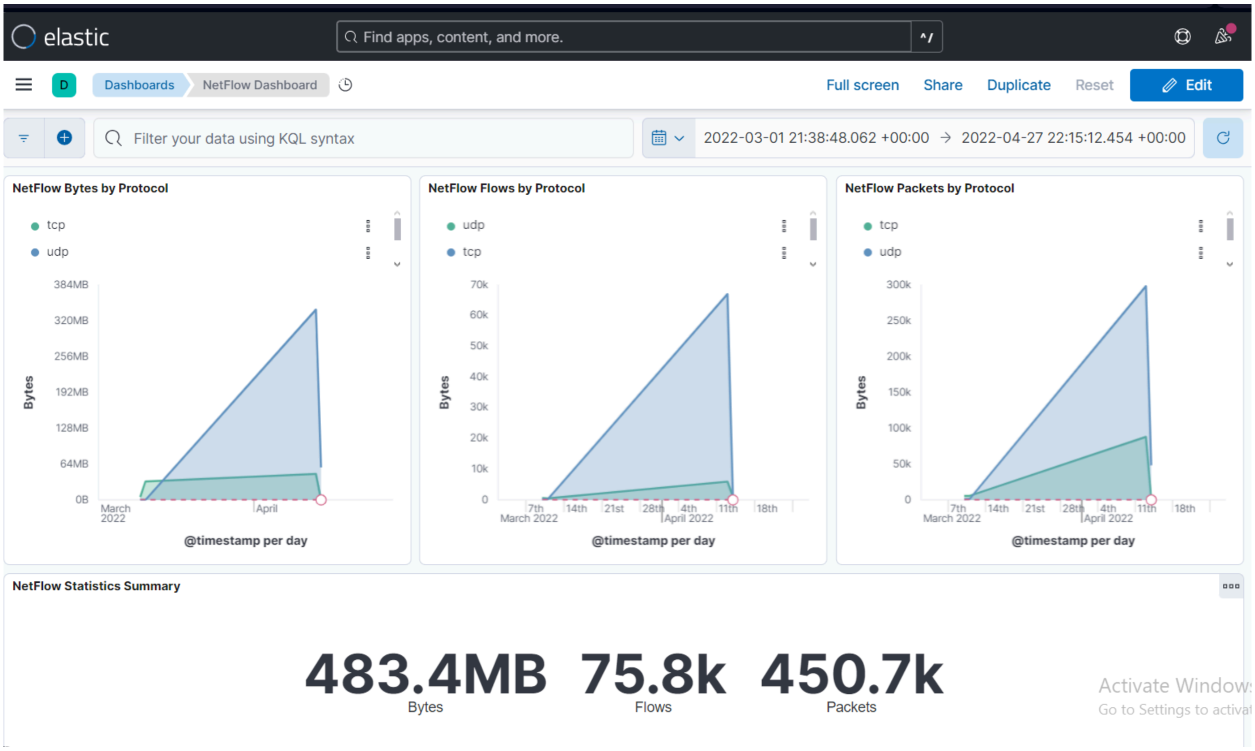
Overview

This exercise involved analyzing NetFlow data using SOF-ELK to identify suspicious traffic, such as port scans and SYN flood attacks. The goal was to filter out normal traffic, focus on anomalies, and determine what might have occurred.

Steps to Analyze Network Traffic and Findings

1. Importing and Setting Up the NetFlow Data

- Imported netflow-lab-v14042022.zip into SOF-ELK.
- Set the time frame to **March 1, 2022 – April 27, 2022**, where most data was present.



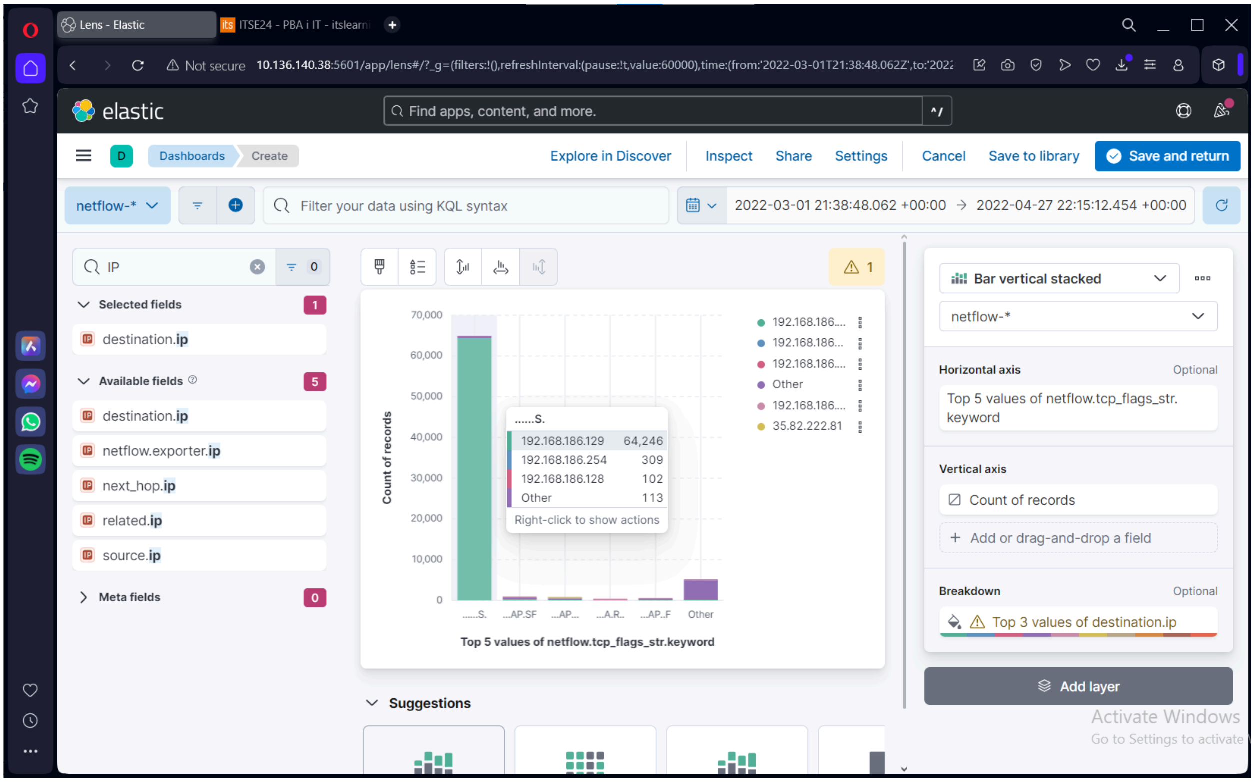
2022-03-01 21:38:48.062 +00:00 → 2022-04-27 22:15:12.454 +00:00

NetFlow Statistics Summary

483.4MB Bytes
75.8k Flows
450.7k Packets

2. Initial Filtering and Observations

- The destination IP 192.168.186.129 had **over 64,000 records**, far higher than typical traffic (100–300 records for other IPs).



2022-03-01 21:38:48.062 +00:00 → 2022-04-27 22:15:12.454 +00:00

Selected fields: 1
- destination.ip

Available fields: 5
- destination.ip
- netflow.exporter.ip
- next_hop.ip
- related.ip
- source.ip

Meta fields: 0

......S.

192.168.186.129	64,246
192.168.186.254	309
192.168.186.128	102
Other	113

Bar vertical stacked

netflow-*

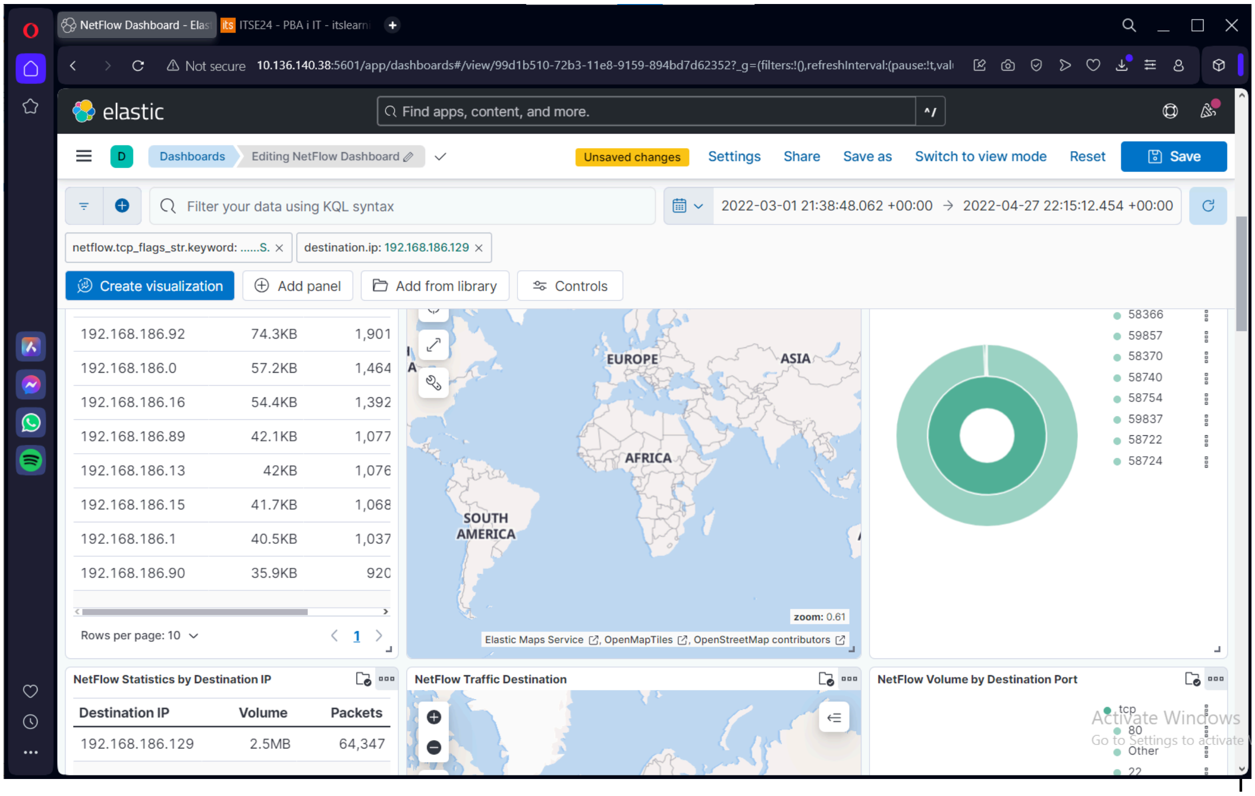
Horizontal axis: Top 5 values of netflow.tcp_flags_str.keyword

Vertical axis: Count of records

Breakdown: Top 3 values of destination.ip

3. Filtering Suspicious Traffic

- Applied filters to focus on **TCP SYN packets** (.....S) and small network byte sizes (≤80 bytes - typical to SYN packets).


NetFlow Dashboard - Elas
ITSE24 - PBA i IT - itslearn
Not secure
10.136.140.38:5601/app/dashboards#/view/99d1b510-72b3-11e8-9159-894bd7d62352?_g=(filters:!(),refreshInterval:(pause:!t,val
elastic
Find apps, content, and more.
Dashboards
Editing NetFlow Dashboard
Unsaved changes
Settings
Share
Save as
Switch to view mode
Reset
Save
Filter your data using KQL syntax
Create visualization
Add panel
Add from library
Controls
EUROPE
ASIA
AFRICA
SOUTH AMERICA
zoom: 0.61
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors
58366
59857
58370
58740
58754
59837
58722
58724
Rows per page: 10
1
NetFlow Traffic Destination
NetFlow Volume by Destination Port
tcp
80
Other
22
Activate Windows
Go to Settings to activate

2022-03-01 21:38:48.062 +00:00 → 2022-04-27 22:15:12.454 +00:00

netflow.tcp_flags_str.keyword: ......S.

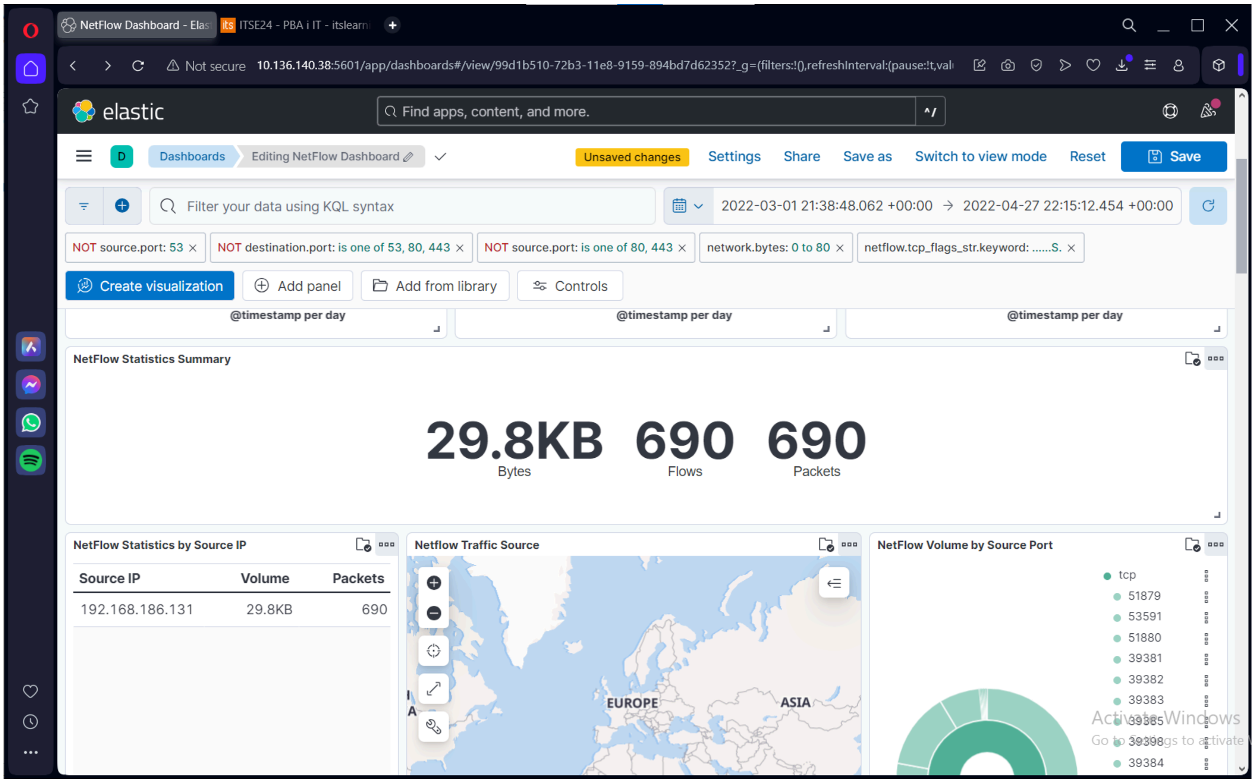
destination.ip: 192.168.186.129

192.168.186.92	74.3KB	1,901
192.168.186.0	57.2KB	1,464
192.168.186.16	54.4KB	1,392
192.168.186.89	42.1KB	1,077
192.168.186.13	42KB	1,076
192.168.186.15	41.7KB	1,068
192.168.186.1	40.5KB	1,037
192.168.186.90	35.9KB	920

NetFlow Statistics by Destination IP

Destination IP	Volume	Packets
192.168.186.129	2.5MB	64,347

- Excluded normal traffic by filtering out common ports like 53 (DNS), 80 (HTTP), and 443 (HTTPS).



10.136.140.38:5601/app/dashboards#/view/99d1b510-72b3-11e8-9159-894bd7d62352?_g=(filters:!(),refreshInterval:(pause:!t,val

2022-03-01 21:38:48.062 +00:00 → 2022-04-27 22:15:12.454 +00:00

NOT source.port: 53 × | NOT destination.port: is one of 53, 80, 443 × | NOT source.port: is one of 80, 443 × | network.bytes: 0 to 80 × | netflow.tcp_flags_str.keyword: ......S. ×

NetFlow Statistics Summary

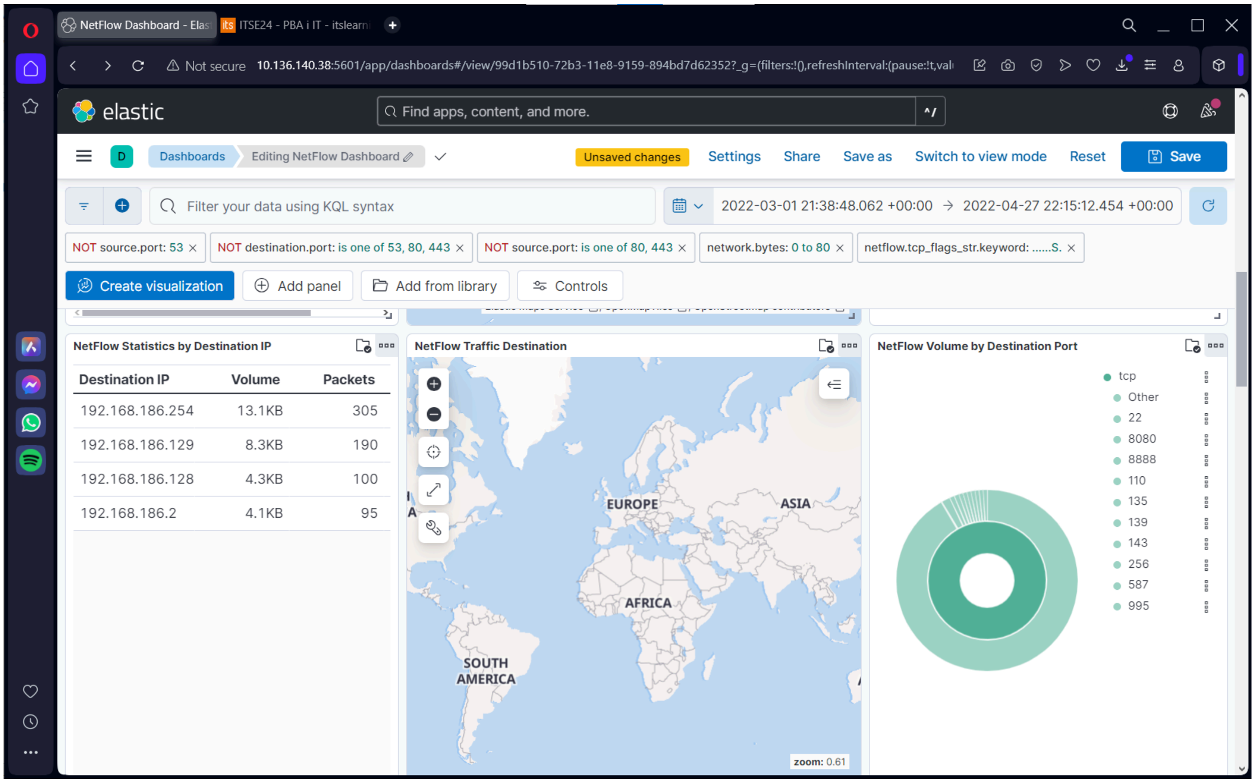
29.8KB Bytes | 690 Flows | 690 Packets

NetFlow Statistics by Source IP

Source IP	Volume	Packets
192.168.186.131	29.8KB	690

NetFlow Volume by Source Port

- The refined data revealed unusual traffic patterns likely related to scanning or attacks.



10.136.140.38:5601/app/dashboards#/view/99d1b510-72b3-11e8-9159-894bd7d62352?_g=(filters:!(),refreshInterval:(pause:!t,val

2022-03-01 21:38:48.062 +00:00 → 2022-04-27 22:15:12.454 +00:00

NOT source.port: 53 × | NOT destination.port: is one of 53, 80, 443 × | NOT source.port: is one of 80, 443 × | network.bytes: 0 to 80 × | netflow.tcp_flags_str.keyword: ......S. ×

NetFlow Statistics by Destination IP

Destination IP	Volume	Packets
192.168.186.254	13.1KB	305
192.168.186.129	8.3KB	190
192.168.186.128	4.3KB	100
192.168.186.2	4.1KB	95

NetFlow Volume by Destination Port

Conclusion

The analysis revealed that 192.168.186.129 was likely targeted by a **SYN flood attack** and **port scanning activity**.