Reconnaissance Phase

- attempt to discover and collect information about a target
- it could be knowledge about the system in use, the web application, employees or location

- start by examining any reconnaissance attempt against the webserver; imreallynotbatman.com
- look at the available log sources, we will find some log sources covering the network traffic, which means all the inbound traffic towards our web server will be logged into the log source that contains the web traffic

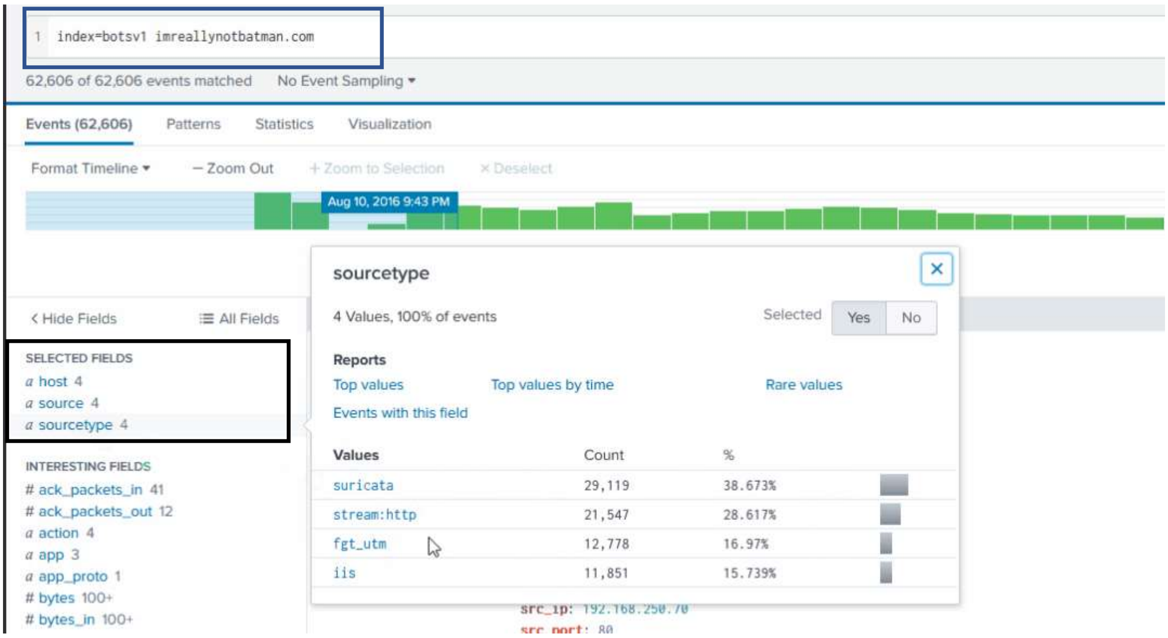
All the event logs that we are going to investigate are present in index=botsv1

Domain Name + Log Sources

Start by searching for the domain in the search head and see which log source includes traces of domain.

Search Query: index=botsv1 imreallynotbatman.com

Search Query explanation: look for the event logs in the index > "botsv1" which contains "imreallynotbatman"



```
index=botsv1 imreallynotbatman.com
```

62,606 of 62,606 events matched   No Event Sampling ▾

SELECTED FIELDS
a host 4
a source 4
a sourcetype 4

INTERESTING FIELDS
# ack_packets_in 41
# ack_packets_out 12
a action 4
a app 3
a app_proto 1
# bytes 100+
# bytes_in 100+

sourcetype

4 Values, 100% of events

Selected Yes No

Reports
Top values   Top values by time   Rare values
Events with this field

Values	Count	%
suricata	29,119	38.673%
stream:http	21,547	28.617%
fgt_utm	12,778	16.97%
iis	11,851	15.739%

src_ip: 192.168.250.70
src_port: 80

sourcetype field, following log sources contain the traces for the term "imreallynotbatman.com"

- Suricata

[contains the details of the alerts from the Suricata IDS]

- stream:http

[network flow related to http traffic]

- fortigate_utm

[contains Fortinet Firewall logs]

- iis

[contains web server logs]

Attackers IP Address

Identify the IP address attempting to perform reconnaissance activity on our web server.

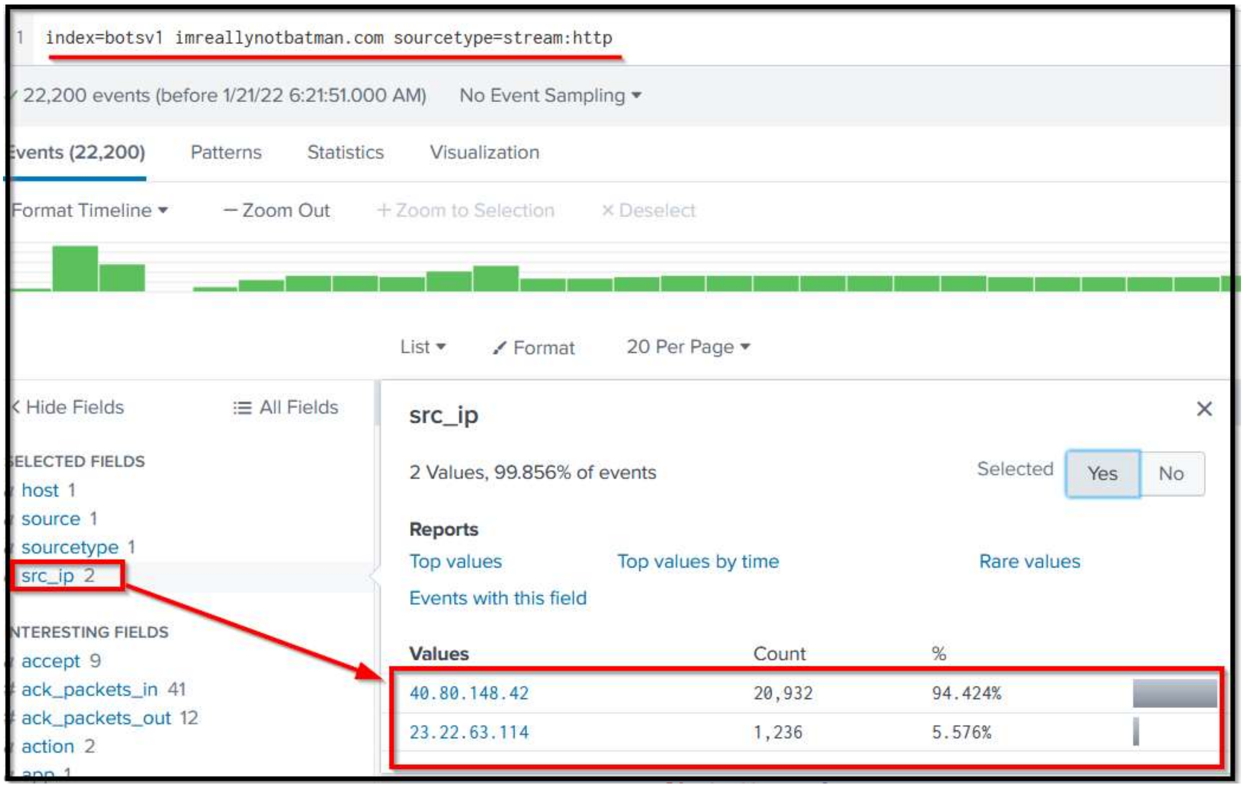
- look at the web traffic coming into the network
- look at the above log sources

stream:http

- contains http traffic logs [webserver]
- examine the src_ip field [contains the source IP address it finds in the logs]

Search Query: index=botsv1 imreallynotbatman.com sourcetype=stream:http

Search Query explanation: look for the term “imreallynotbatman.com” in the stream.http log source



```
index=botsv1 imreallynotbatman.com sourcetype=stream:http
```

22,200 events (before 1/21/22 6:21:51.000 AM)   No Event Sampling

src_ip

2 Values, 99.856% of events

Values	Count	%
40.80.148.42	20,932	94.424%
23.22.63.114	1,236	5.576%

Found 2 IPs in the src_ip field: 40.80.148.42 and 23.22.148.42

- 40.80.148.42 [higher percentage of the logs] 94.42%
- 23.22.63.114 [lower percentage of the logs] 5.576%

dest_ip > 192.168.250.70 [webserver address]

To confirm our suspicion about the IP address 40.80.148.42, click the IP and examine the logs. Analyse the below fields to see what kind of traffic is coming from 40.80.148.42:

- User-Agent
- Server
- Post requests
- URIs