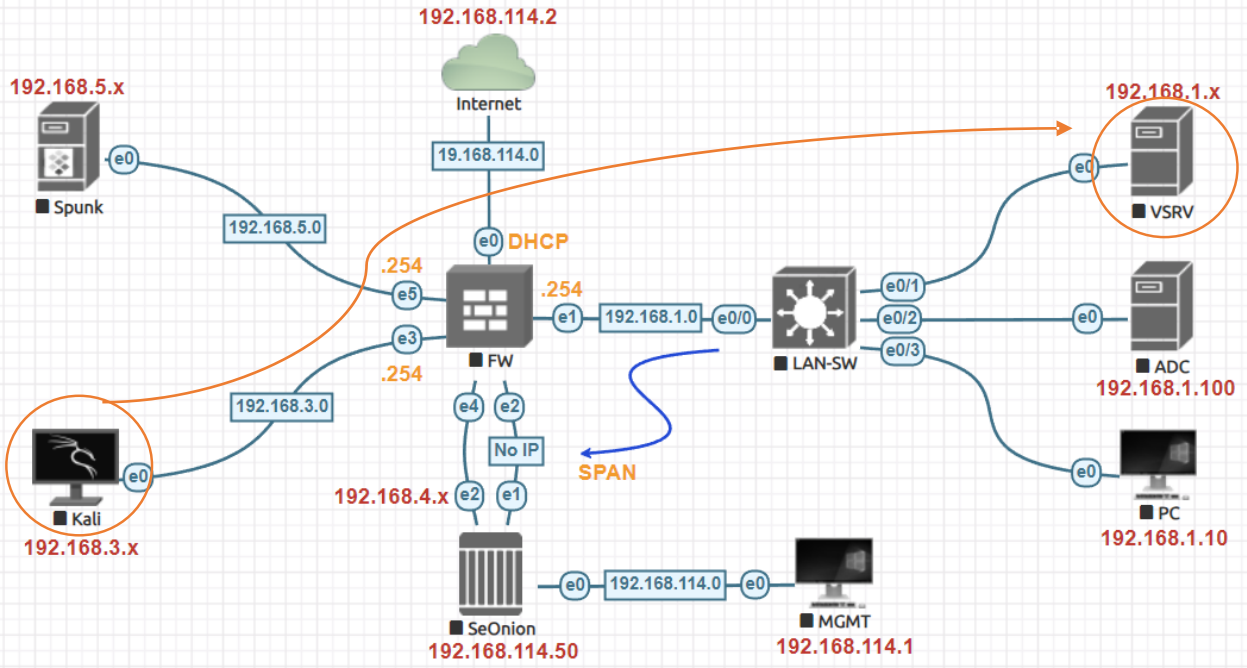
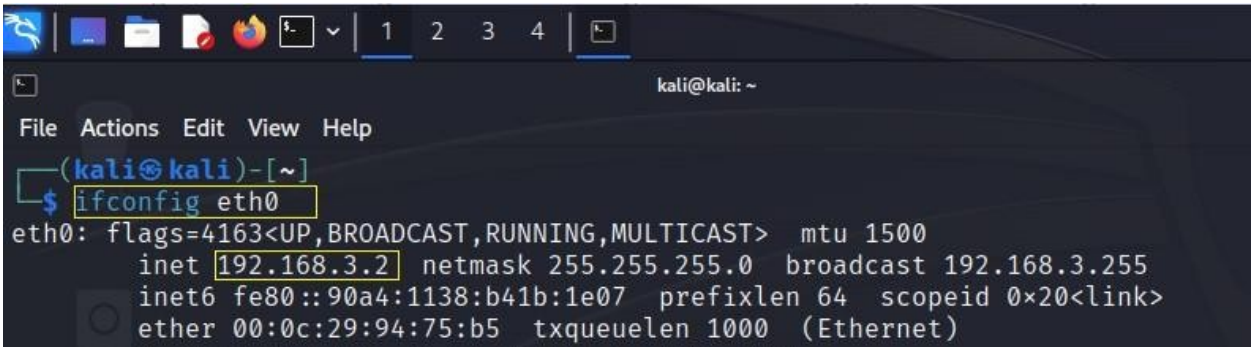
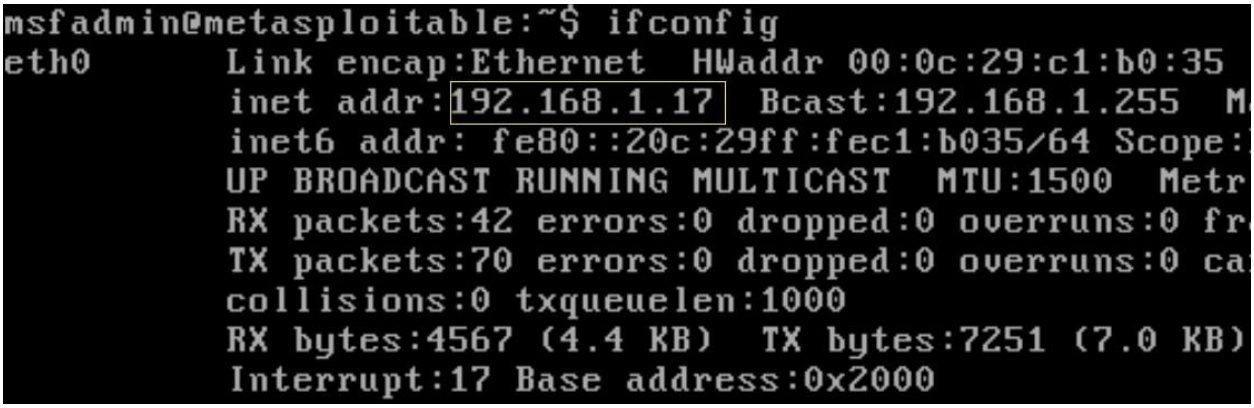
Security Onion Monitoring & Detection:



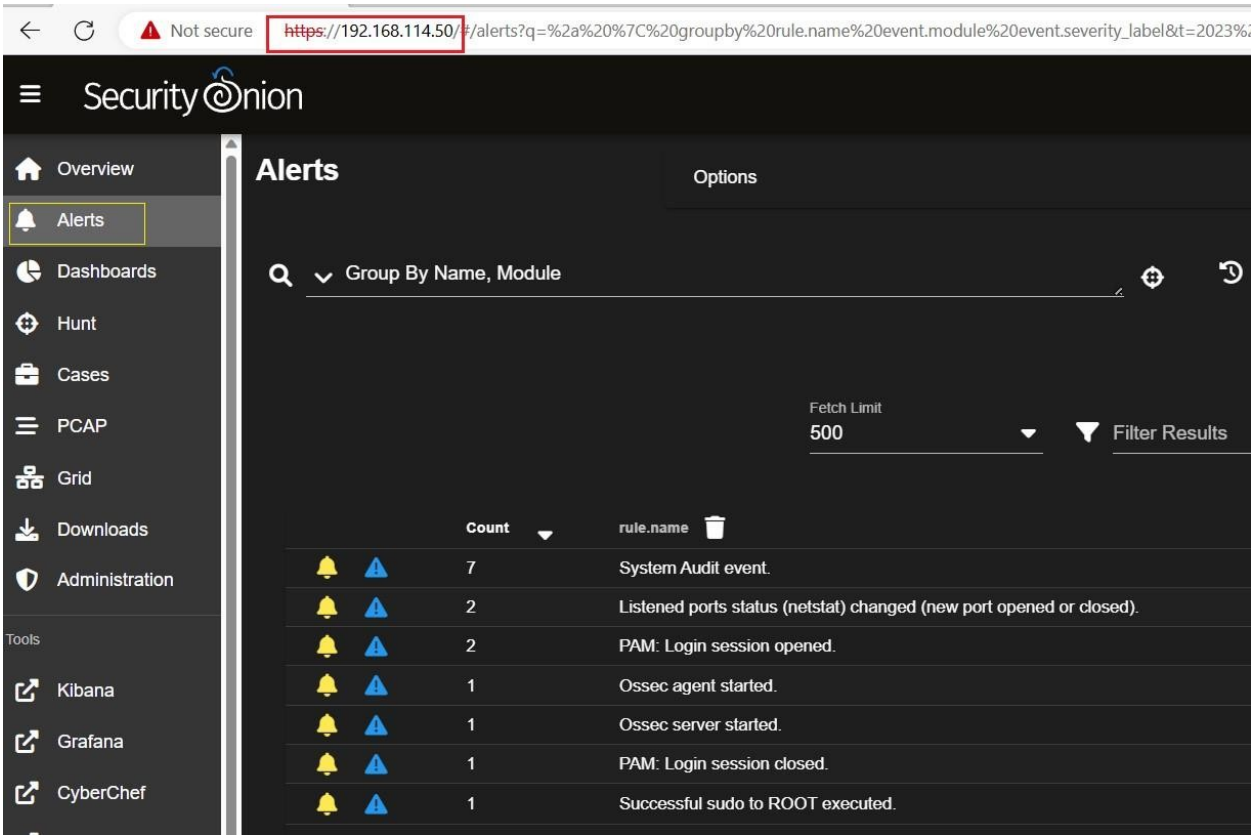
Kali Linux Attacker IP Address in the time of Attack 192.168.3.2.



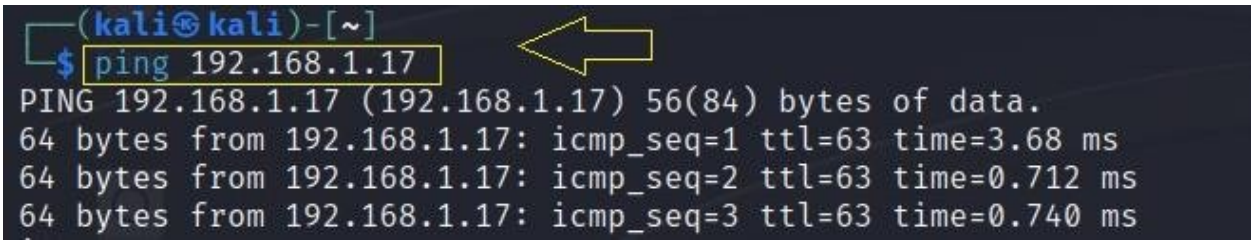
Vulnerable Server in the LAN IP Address in the time of Attack 192.168.1.17.



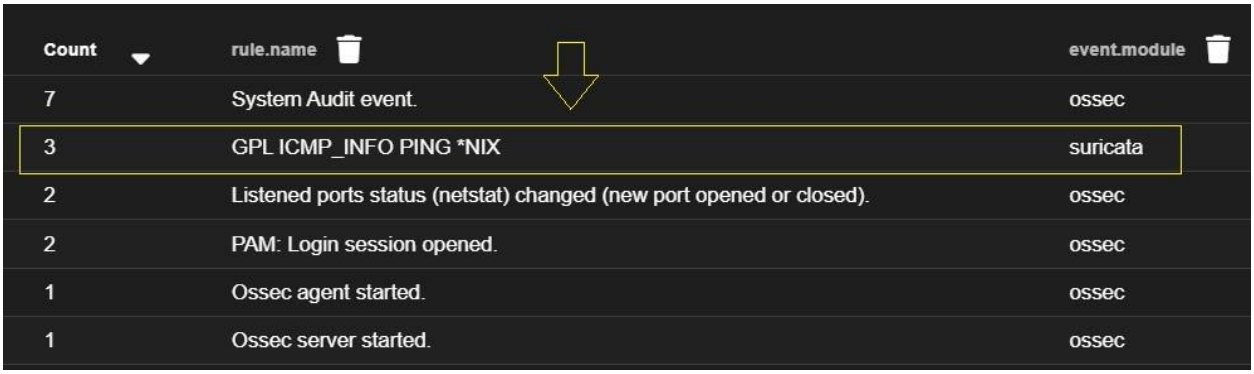
Alerts before attack in Security Onion with Management IP Address 192.168.114.50.



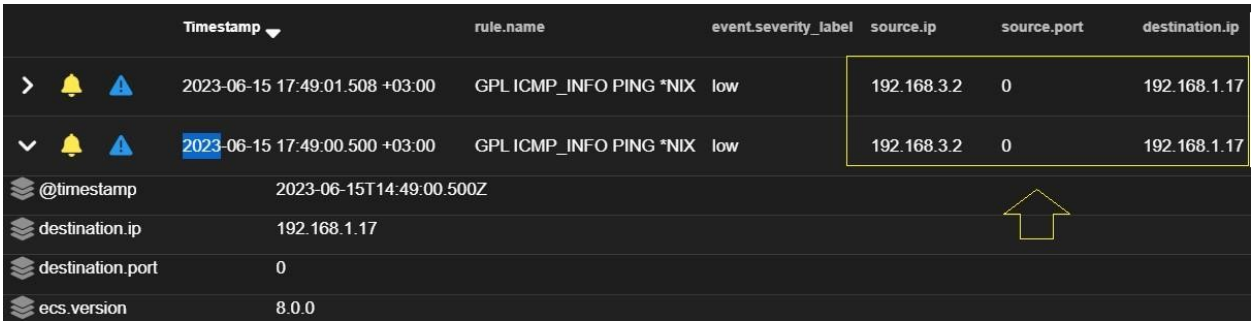
Let's ping Vulnerable Server 192.168.1.17 from Kali Linux attacker system



After attack lets navigate to security onion it shows the alerts.



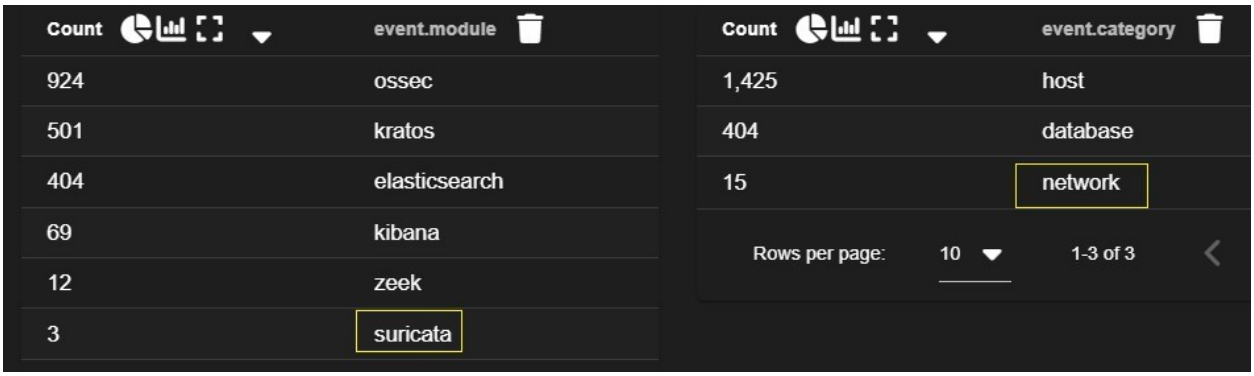
Right click in Alerts on the rule.name and click on Drilldown to see more details.



	Timestamp	rule.name	event.severity_label	source.ip	source.port	destination.ip
	2023-06-15 17:49:01.508 +03:00	GPL ICMP_INFO PING *NIX	low	192.168.3.2	0	192.168.1.17
	2023-06-15 17:49:00.500 +03:00	GPL ICMP_INFO PING *NIX	low	192.168.3.2	0	192.168.1.17

@timestamp	2023-06-15T14:49:00.500Z
destination.ip	192.168.1.17
destination.port	0
ecs.version	8.0.0

Let's check in Dashboards our interest is in Suricata right click choose include.



Count	event.module
924	ossec
501	kratos
404	elasticsearch
69	kibana
12	zeek
3	suricata

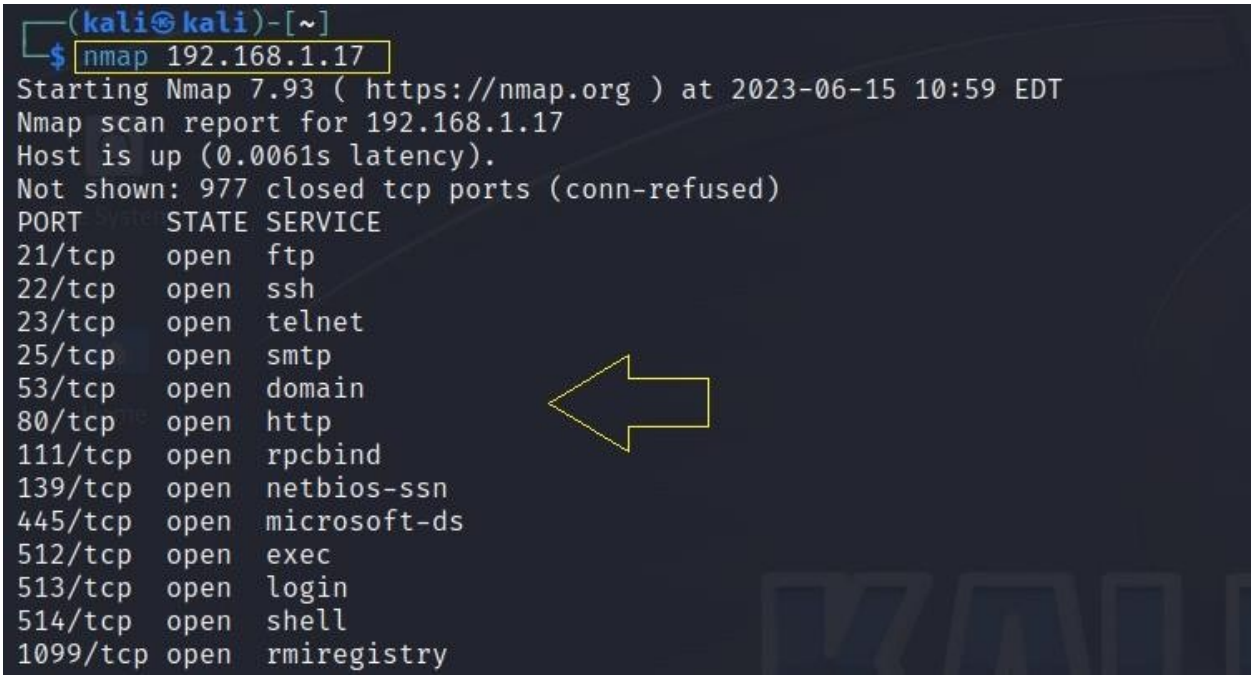
Count	event.category
1,425	host
404	database
15	network

Rows per page: 10 1-3 of 3

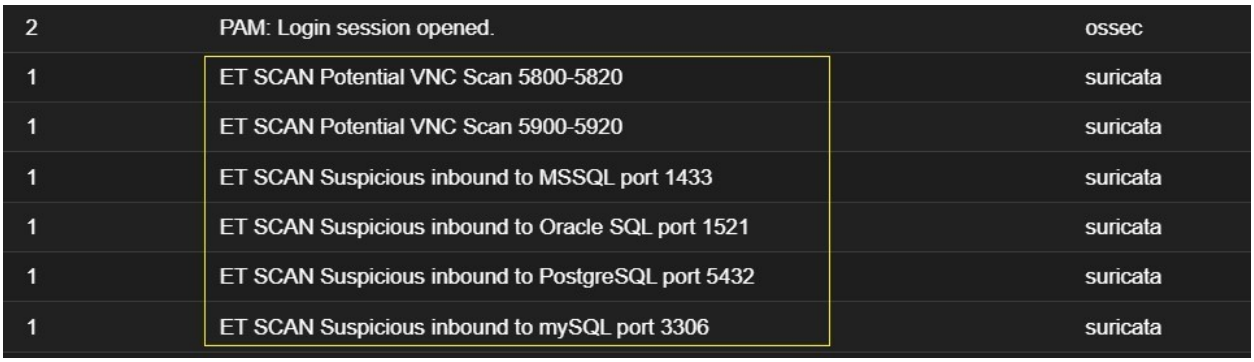
Go down to see more details about source destination and category in Dashboards.

source.ip	source.port	destination.ip	destination.port	rule.name	rule.category
192.168.3.2	0	192.168.1.17	0	GPL ICMP_INFO PING *NIX	Misc activity
192.168.3.2	0	192.168.1.17	0	GPL ICMP_INFO PING *NIX	Misc activity
192.168.3.2	0	192.168.1.17	0	GPL ICMP_INFO PING *NIX	Misc activity

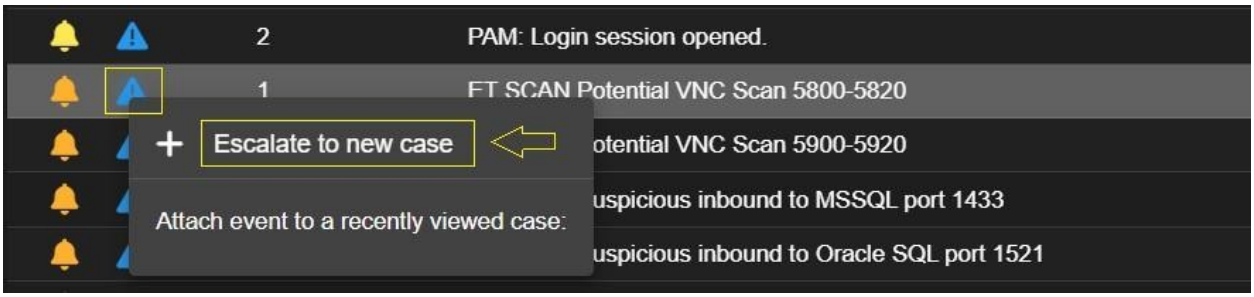
Let’s perform another attack from Kali Linux on vulnerable server 192.168.1.17.



Let’s navigate back to Security Onion Alerts to see the attack.



Right click on Alerts to Escalate to new case.

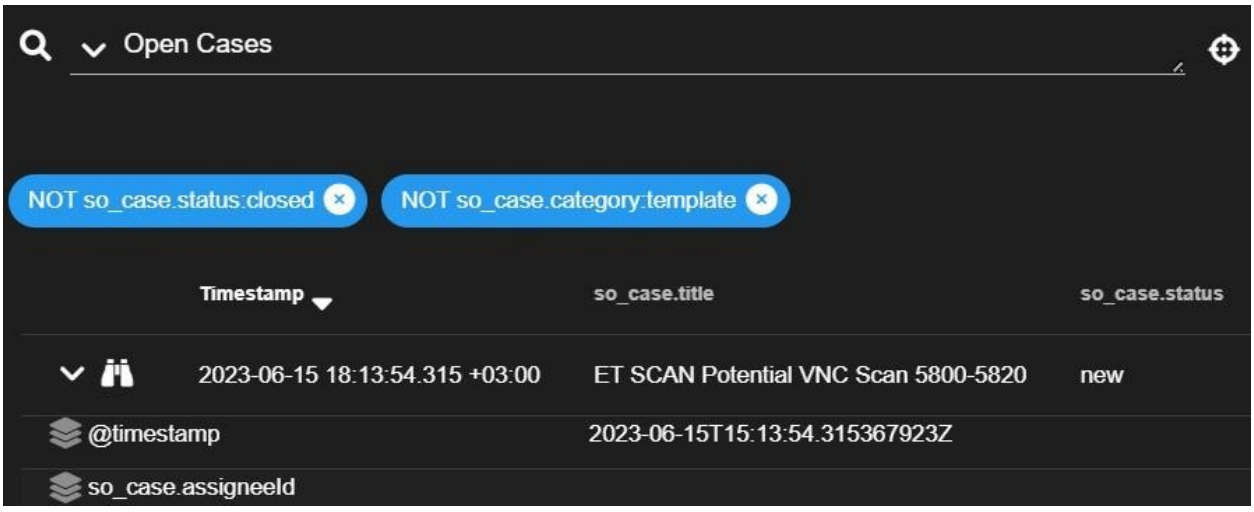


Let’s go to Hunt on the top Search make it NIDS Alerts.

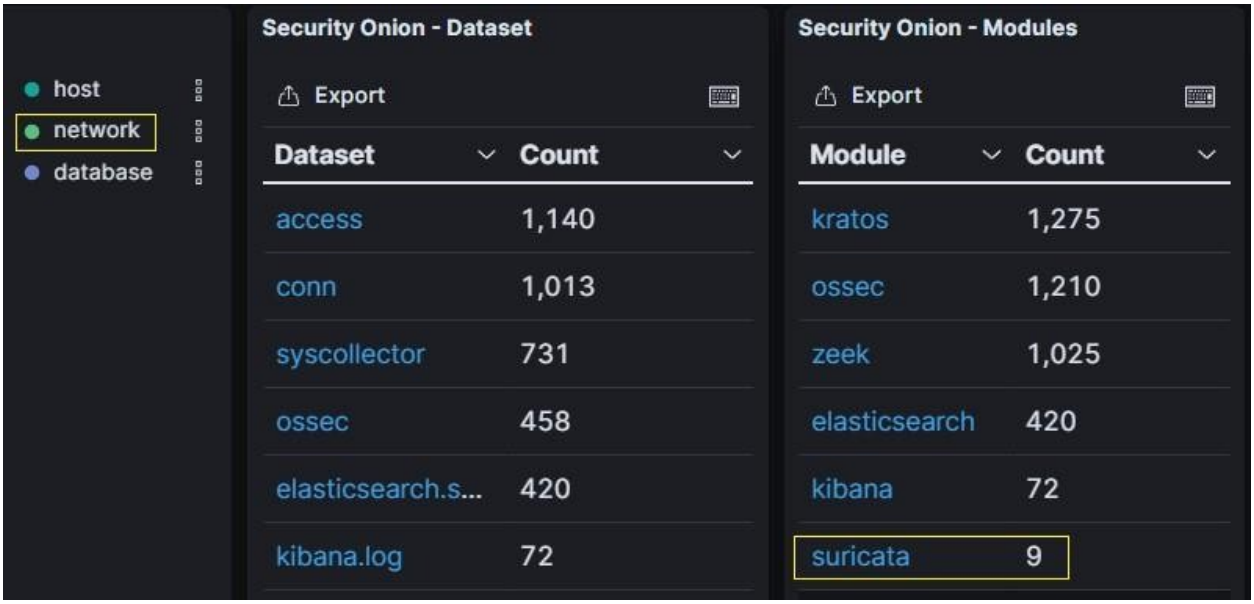
rule.category	rule.gid	rule.uuid	rule.name
Misc activity	1	2100366	GPL ICMP_INFO PING *NIX
Potentially Bad Traffic	1	2010935	ET SCAN Suspicious inbound to MSSQL port 1433
Potentially Bad Traffic	1	2010936	ET SCAN Suspicious inbound to Oracle SQL port 1521
Potentially Bad Traffic	1	2010937	ET SCAN Suspicious inbound to mySQL port 3306
Potentially Bad Traffic	1	2010939	ET SCAN Suspicious inbound to PostgreSQL port 5432
Attempted Information Leak	1	2002910	ET SCAN Potential VNC Scan 5800-5820
Attempted Information Leak	1	2002911	ET SCAN Potential VNC Scan 5900-5920

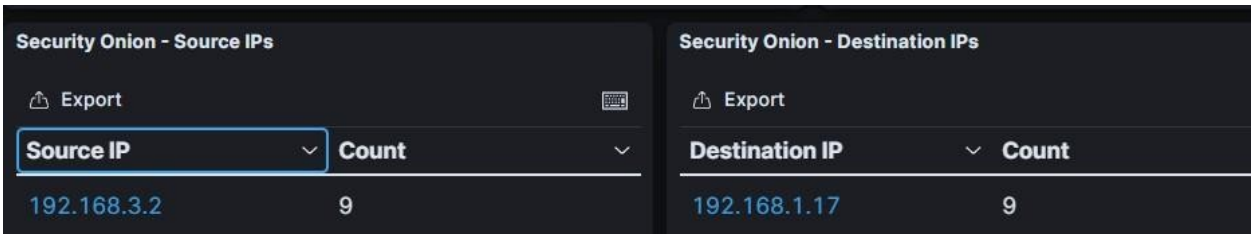
source.ip	source.port	destination.ip	destination.port	rule.name
192.168.3.2	56630	192.168.1.17	5815	ET SCAN Potential VNC Scan 5800-5820
192.168.3.2	41128	192.168.1.17	1521	ET SCAN Suspicious inbound to Oracle SQL port 1521
192.168.3.2	33262	192.168.1.17	5903	ET SCAN Potential VNC Scan 5900-5920
192.168.3.2	49660	192.168.1.17	1433	ET SCAN Suspicious inbound to MSSQL port 1433
192.168.3.2	54542	192.168.1.17	5432	ET SCAN Suspicious inbound to PostgreSQL port 5432
192.168.3.2	36018	192.168.1.17	3306	ET SCAN Suspicious inbound to mySQL port 3306

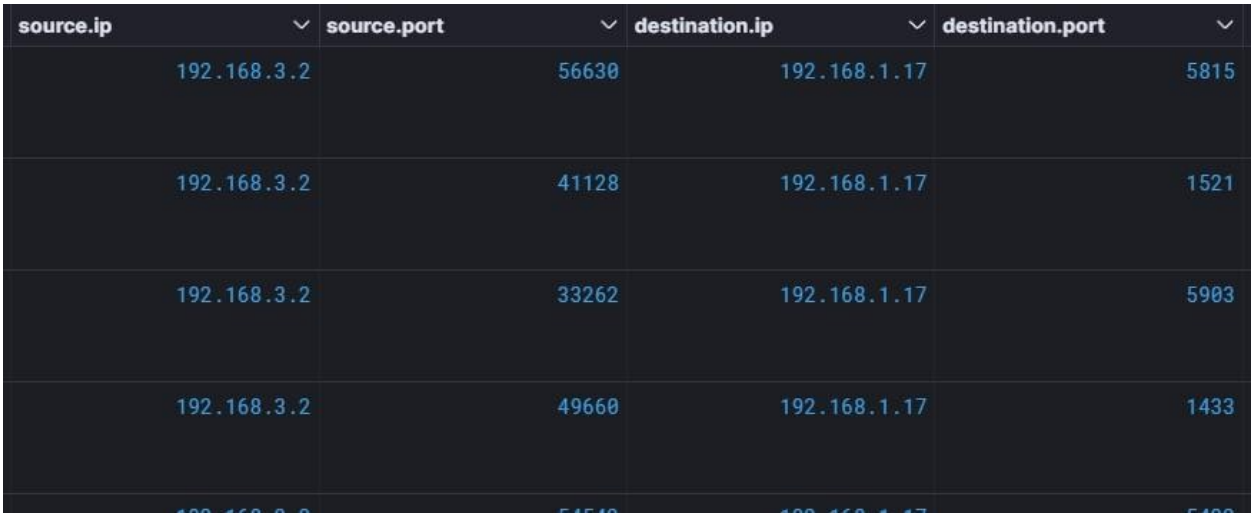
Navigate to Cases to find out the open cases.



Let’s navigate to Tools click on Kibana to open new windows login with same username and password admin@test.local and password Admin@12345

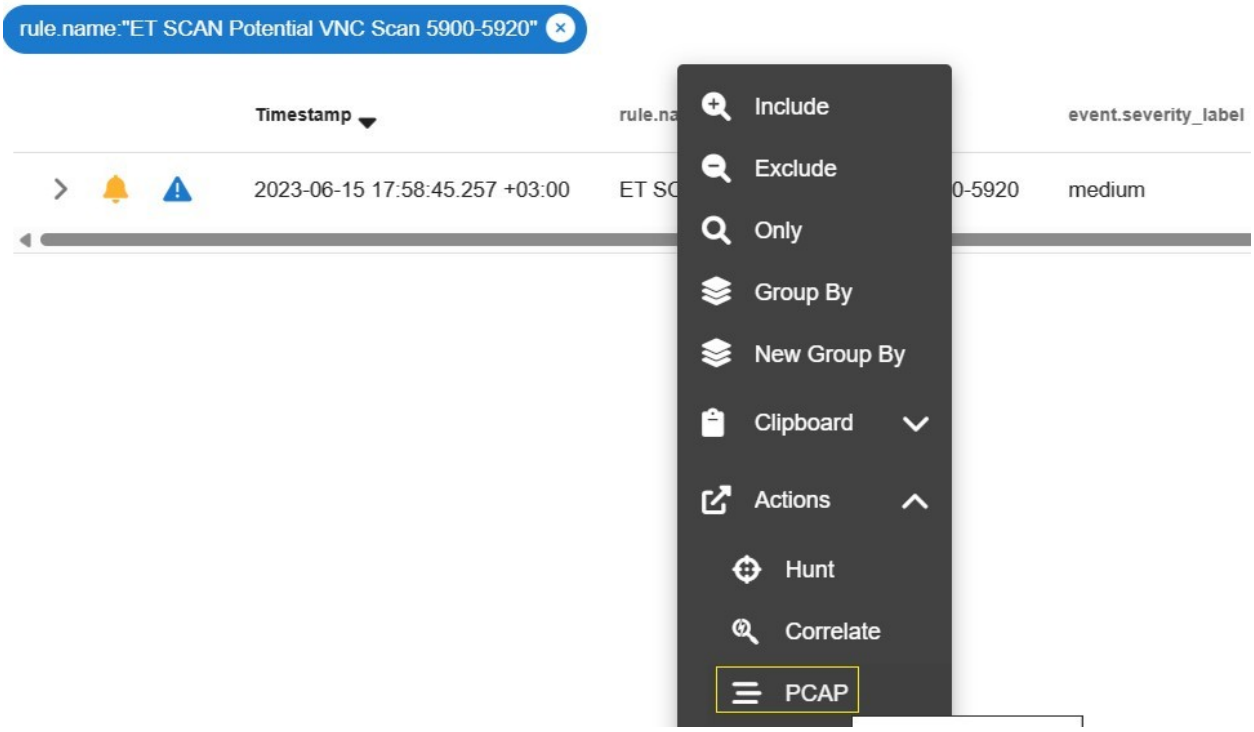






source.ip	source.port	destination.ip	destination.port
192.168.3.2	56630	192.168.1.17	5815
192.168.3.2	41128	192.168.1.17	1521
192.168.3.2	33262	192.168.1.17	5903
192.168.3.2	49660	192.168.1.17	1433

Let’s go back to Alerts right click Drilldown now click on rule.name open in PCAP.



Go to PCAP to investigate the file further for more details.

PCAP

ID	Owner	Date Queued	Date Completed
1003	admin@test.local	2023-06-15 18:40:54.670 +03:00	2023-06-15 18:40:55.682 +03:00

Num	Timestamp	Type	Source IP	Source Port	Destination IP
0	2023-06-15 17:58:45.257 +03:00	TCP	192.168.3.2	33262	192.168.1.17

```
0000  00 0C 29 C1 B0 35 00 0C  29 A2 00 8A 08 00 45 00   ..)..5..).....E.
0016  00 3C AB 36 40 00 3F 06  0B 22 C0 A8 03 02 C0 A8   .<.6@.?.."......
0032  01 11 81 EE 17 0F FD 12  5E 2A 00 00 00 00 A0 02   ........^*......
0048  FA F0 1F B1 00 00 02 04  05 B4 04 02 08 0A 2C 98   ..............,.
0064  87 27 00 00 00 00 01 03  03 07                     .'........
```

Num	Timestamp	Type	Source IP	Source Port	Destination IP
1	2023-06-15 17:58:45.260 +03:00	TCP	192.168.1.17	5903	192.168.3.2