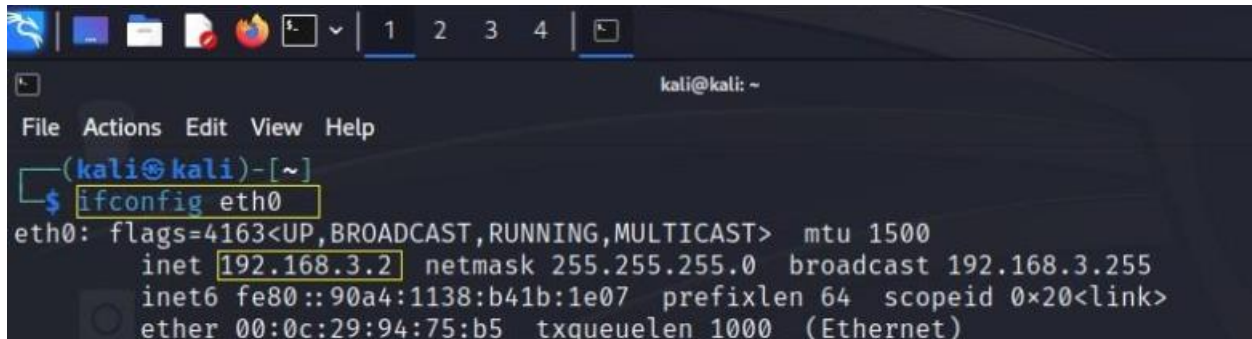



## Security Onion Monitoring & Detection:

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



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ifconfig eth0  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.3.2 netmask 255.255.255.0 broadcast 192.168.3.255  
    inet6 fe80::90a4:1138:b41b:1e07 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:94:75:b5 txqueuelen 1000 (Ethernet)
```

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



```
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c1:b0:35  
          inet addr:192.168.1.17  Bcast:192.168.1.255  M  
          inet6 addr: fe80::20c:29ff:fec1:b035/64 Scope:  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metr  
          RX packets:42 errors:0 dropped:0 overruns:0 fr  
          TX packets:70 errors:0 dropped:0 overruns:0 ca  
          collisions:0 txqueuelen:1000  
          RX bytes:4567 (4.4 KB)  TX bytes:7251 (7.0 KB)  
          Interrupt:17 Base address:0x2000
```

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

The screenshot shows the Security Onion web interface. The left sidebar contains navigation links: Overview, Alerts (highlighted), Dashboards, Hunt, Cases, PCAP, Grid, Downloads, Administration, and Tools. The main area is titled 'Alerts' and includes a search bar, a 'Group By Name, Module' dropdown, a 'Fetch Limit' of 500, and a 'Filter Results' button. Below these controls is a table of alerts.

	Count	rule.name
🔔 🔵	7	System Audit event.
🔔 🔵	2	Listened ports status (netstat) changed (new port opened or closed).
🔔 🔵	2	PAM: Login session opened.
🔔 🔵	1	Ossec agent started.
🔔 🔵	1	Ossec server started.
🔔 🔵	1	PAM: Login session closed.
🔔 🔵	1	Successful sudo to ROOT executed.

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

```
(kali@kali)-[~]  
$ ping 192.168.1.17  
PING 192.168.1.17 (192.168.1.17) 56(84) bytes of data.  
64 bytes from 192.168.1.17: icmp_seq=1 ttl=63 time=3.68 ms  
64 bytes from 192.168.1.17: icmp_seq=2 ttl=63 time=0.712 ms  
64 bytes from 192.168.1.17: icmp_seq=3 ttl=63 time=0.740 ms
```

After attack lets navigate to security onion it shows the alerts

Count	rule.name	event.module
7	System Audit event.	ossec
3	GPL ICMP_INFO PING *NIX	suricata
2	Listened ports status (netstat) changed (new port opened or closed).	ossec
2	PAM: Login session opened.	ossec
1	Ossec agent started.	ossec
1	Ossec server started.	ossec

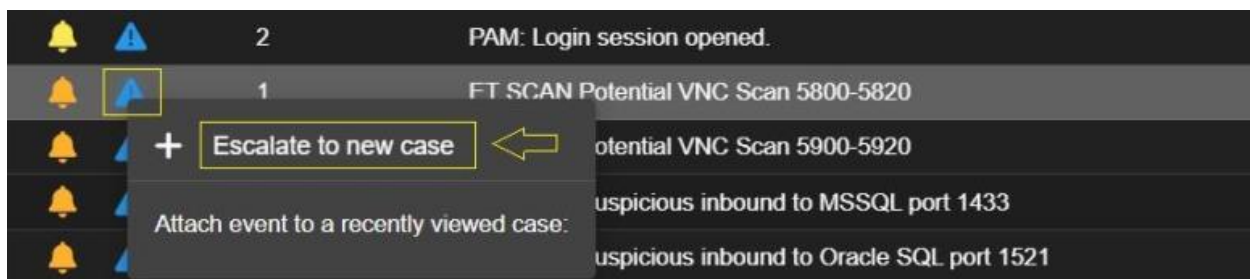
Let's perform another attack from Kali Linux on vulnerable server 192.168.1.17

```
(kali㉿kali)-[~]  
$ nmap 192.168.1.17  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-15 10:59 EDT  
Nmap scan report for 192.168.1.17  
Host is up (0.0061s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry
```





Let's navigate back to Security Onion Alerts to see the attack

2	PAM: Login session opened.	ossec
1	ET SCAN Potential VNC Scan 5800-5820	suricata
1	ET SCAN Potential VNC Scan 5900-5920	suricata
1	ET SCAN Suspicious inbound to MSSQL port 1433	suricata
1	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata
1	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata
1	ET SCAN Suspicious inbound to MySQL port 3306	suricata

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

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

<div><div>● host</div><div>● network</div><div>● database</div></div>	Security Onion - Dataset		Security Onion - Modules	
	Export		Export	
	Dataset	Count	Module	Count
	access	1,140	kratos	1,275
	conn	1,013	ossec	1,210
	syscollector	731	zeek	1,025
	ossec	458	elasticsearch	420
	elasticsearch.s...	420	kibana	72
	kibana.log	72	suricata	9

Security Onion - Source IPs		Security Onion - Destination IPs	
Export		Export	
Source IP	Count	Destination IP	Count
192.168.3.2	9	192.168.1.17	9

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