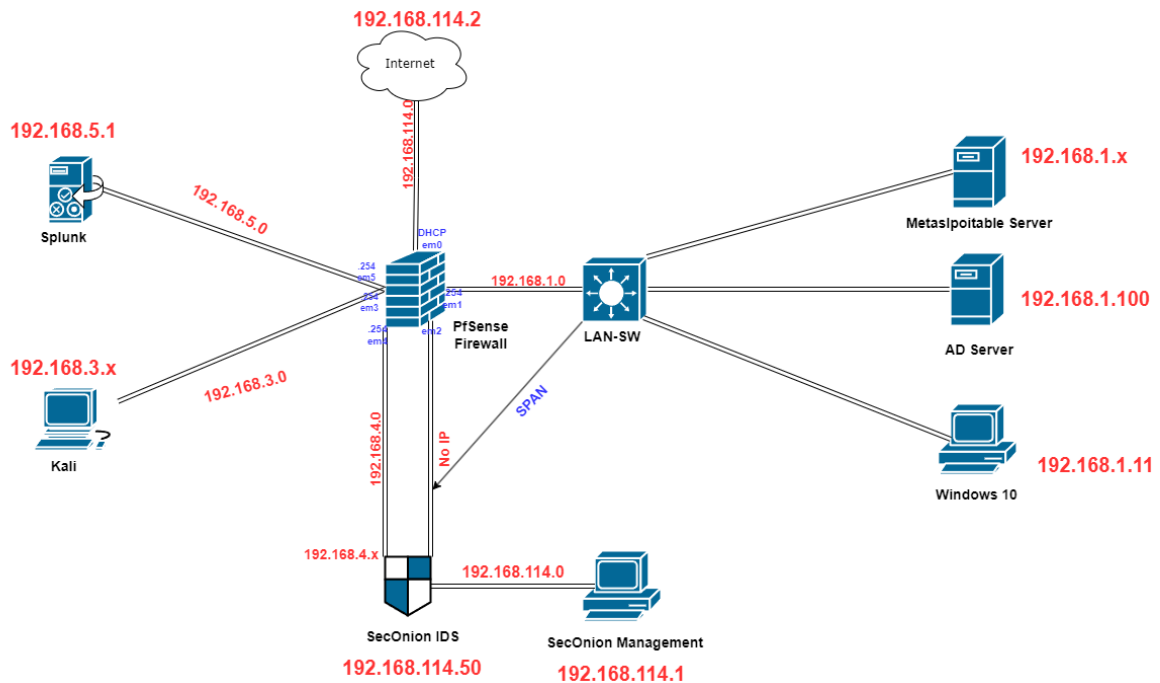


Attacks & Monitoring with Security Onion

1. I will attack my **Metasploitable Server** with **Kali**. And use **Security Onion** as IDS to monitor the relevant logs. Logs are copied to Security Onion via **SPAN** port



Kali IP **192.168.3.2**

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ifconfig  
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::3c80:c618:7ab6:fef prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:ff:b8:78 txqueuelen 1000 (Ethernet)  
    RX packets 16 bytes 2652 (2.5 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 63 bytes 8606 (8.4 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 480 (480.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 480 (480.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$
```

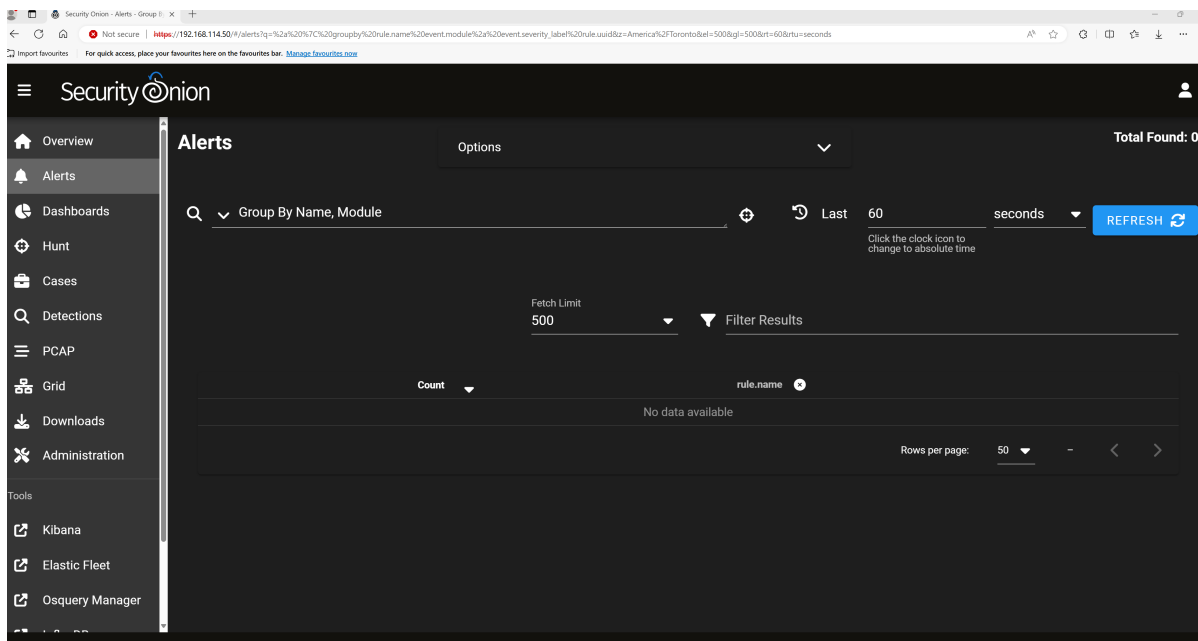
Metasploitable IP in the time of Attack **192.168.1.10**

```
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:e8:1f:7c
          inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fee8:1f7c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:165 errors:0 dropped:0 overruns:0 frame:0
          TX packets:139 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19292 (18.8 KB)  TX bytes:27332 (26.6 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1362 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1362 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:642385 (627.3 KB)  TX bytes:642385 (627.3 KB)

msfadmin@metasploitable:~$
```


Security Onion managed by my host(SecOnion Management), and before start, there is nothing in Alerts


















2. ping Metasploitable Server **192.168.1.10** from Kali. I stopped after 5 pings.

```
(kali㉿kali)-[~]
$ ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=63 time=1.08 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=63 time=0.671 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=63 time=0.855 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=63 time=1.58 ms
64 bytes from 192.168.1.10: icmp_seq=5 ttl=63 time=0.608 ms
^C
— 192.168.1.10 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4021ms
rtt min/avg/max/mdev = 0.608/0.958/1.578/0.350 ms
```

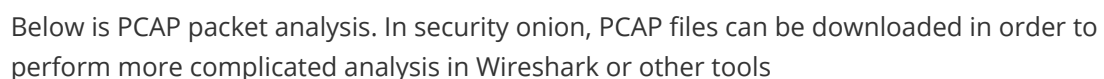
change to absolute time

rule.name:"GPL ICMP PING *NIX" 

	Timestamp 	event.dataset 	rule.name 	event.severity_label 	source.ip 	source.
>  	2024-09-19 16:03:39.700 -04:00	suricata.alert	GPL ICMP PING *NIX	low	192.168.3.2	0
>  	2024-09-19 16:03:38.698 -04:00	suricata.alert	GPL ICMP PING *NIX	low	192.168.3.2	0
>  	2024-09-19 16:03:37.695 -04:00	suricata.alert	GPL ICMP PING *NIX	low	192.168.3.2	0
>  	2024-09-19 16:03:36.681 -04:00	suricata.alert	GPL ICMP PING *NIX	low	192.168.3.2	0
>  	2024-09-19 16:03:35.680 -04:00	suricata.alert	GPL ICMP PING *NIX	low	192.168.3.2	0

3. nmap Metasploitable Server **192.168.1.10** from Kali.

Also, can perform further analysis, like Correlate, PCAP, Google, VirusTotal.



0	2024-09-19 16:32:34.563 -04:00	TCP	192.168.3.2	43522	192.168.1.10	5810	SYN	74
0000	00 0C 29 E8 1F 7C 00 0C 29 68 D6 44 08 00 45 00	...)...)h.D..E.						
0016	00 3C 75 47 40 00 3F 06 41 18 C0 A8 03 02 C0 A8	.<uG@.?.A.....						
0032	01 0A AA 02 16 B2 06 1A 76 87 00 00 00 00 A0 02V.....						
0048	7D 78 DB CF 00 00 02 04 05 B4 04 02 08 0A 85 AE	}X.....						
0064	A6 56 00 00 00 00 01 03 03 07	.V.....						
1	2024-09-19 16:32:34.565 -04:00	TCP	192.168.1.10	5810	192.168.3.2	43522	RST ACK	60
0000	00 0C 29 68 D6 44 00 0C 29 E8 1F 7C 08 00 45 00	...)h.D...)...)E.						
0016	00 28 00 00 40 00 40 06 B5 73 C0 A8 01 0A C0 A8	.(. @. @. .s.....						
0032	03 02 16 B2 AA 02 00 00 00 00 06 1A 76 88 50 14V.P.						
0048	00 00 ED 1C 00 00 00 00 00 00 00 00						

Security Onion includes **Hunt** and **Dashboard** function as well, Navigate to **Hunt**, search by **NIDS Alerts**

rule.category	rule.gid	rule.uuid	rule.name
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

event.dataset	source.ip	source.port	destination.ip	destination.port	rule.name
suricata.alert	192.168.3.2	50510	192.168.1.10	1521	ET SCAN Suspicious I
suricata.alert	192.168.3.2	53892	192.168.1.10	1433	ET SCAN Suspicious I
suricata.alert	192.168.3.2	34634	192.168.1.10	5432	ET SCAN Suspicious I
suricata.alert	192.168.3.2	39832	192.168.1.10	5911	ET SCAN Potential VN
suricata.alert	192.168.3.2	36862	192.168.1.10	5815	ET SCAN Potential VN
suricata.alert	192.168.3.2	59160	192.168.1.10	3306	ET SCAN Suspicious I

In Security Onion, it allows to escalate logs from Alerts, Dashboards and Hunt to **Case**, then assign analysts, add comments and attachments, and track observables.

Overview

Alerts

Dashboards

Hunt

Cases

Detections

PCAP

Grid

Downloads

Administration

Tools

Kibana

Review escalated event details in the Events tab below. Click here to update this description.

COMMENTS

ATTACHMENTS

OBSERVABLES

EVENTS

HISTORY

+

A Add Comment

Provide follow-up information to this case

CANCEL

ADD

Summary

Assignee:
unassigned

Status:
new

Details

Severity:
medium

Priority:
0

TLP:
unknown

4. For a more intuitive visualization, Kibana is integrated into Security Onion

