TDX ARENA

Certification Report

Brett Reich
Final Assessment Report Submission

Case: Pigs Rule

8/9/24

Executive Summary

As the SOC analyst at Flying Piglet post office, intel was gained about Hactivists attempting to launch a campaign to gain unauthorized access into our network. To counter this potential threat and identify the malicious traffic we needed to sniff the incoming traffic.

To sniff the traffic the Snort utility was used. In conjunction with Snorby, this helped determine the IP address of the Hactivist's attack. An IP address that was not related to our network was found to be constantly sending packets to the network. Once this was found, the configuration for Snort could be altered to make sure not to capture any legitimate traffic.

Findings and Analysis

Finding	Finding Details	Description
IP Address	142.250.31.106	An IP address from outside the network that was sending packets continuously.

This IP address outside of the network was constantly sending packets into the network.

Finding	Finding Details	Description
Attack	Potential DoS attack.	A potential Denial of Service attack, as it only seems to come from one IP address.

This attempt to slow down the Flying Piglet servers only seemed to be coming from one IP address, making it seem to be a DoS attack.

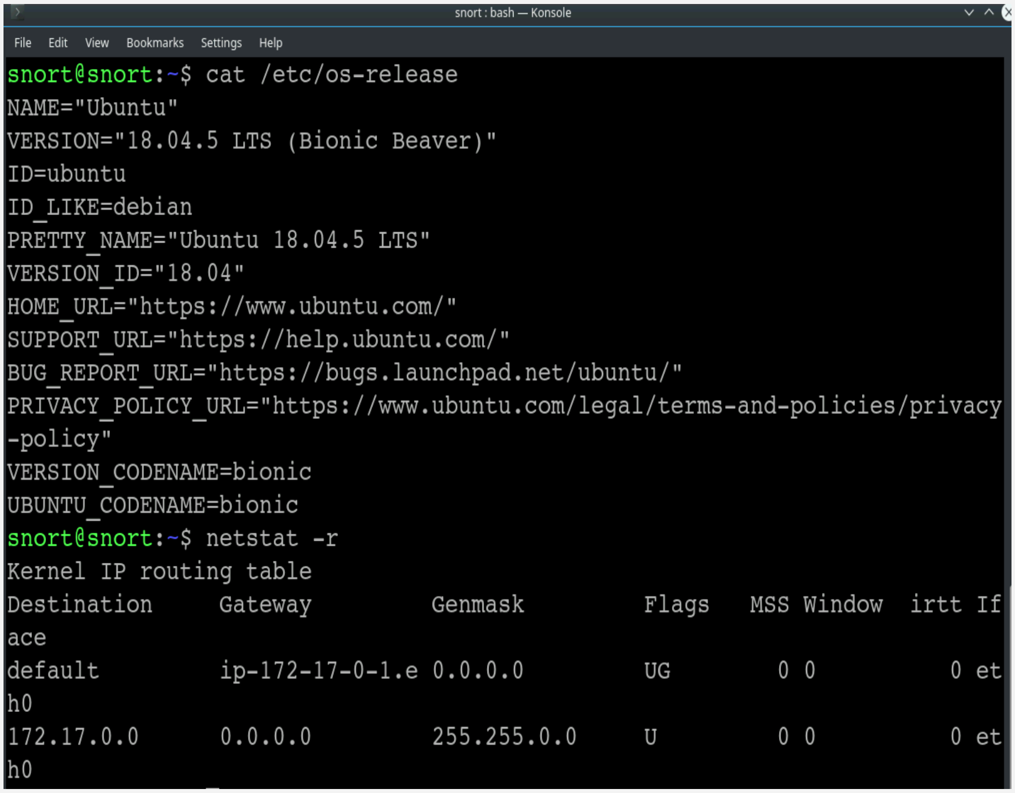
Methodology

Tools and Technologies Used

- **Snort**: Snort is a network intrusion detection system that allows for real-time traffic analysis and packet logging. I used Snort to sniff the incoming traffic on the network and configure the rules to help narrow the packets down to the malicious source..
- **Snorby:** Snorby is a web-based interface that allows a user-friendly and visual breakdown of the alerts that were configured on Snort. I used Snorby to identify the IP address of the attacks.

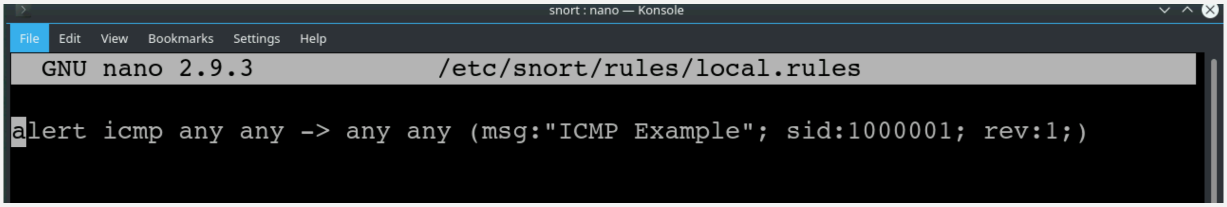
Investigation Process

1. I started by figuring out the OS and network settings for the machine that was running.



```
snort@snort:~$ cat /etc/os-release
NAME="Ubuntu"
VERSION="18.04.5 LTS (Bionic Beaver)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 18.04.5 LTS"
VERSION_ID="18.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy
-policy"
VERSION_CODENAME=bionic
UBUNTU_CODENAME=bionic
snort@snort:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt If
ace
default         ip-172-17-0-1.e 0.0.0.0         UG        0 0          0 et
h0
172.17.0.0      0.0.0.0         255.255.0.0     U         0 0          0 et
h0
```

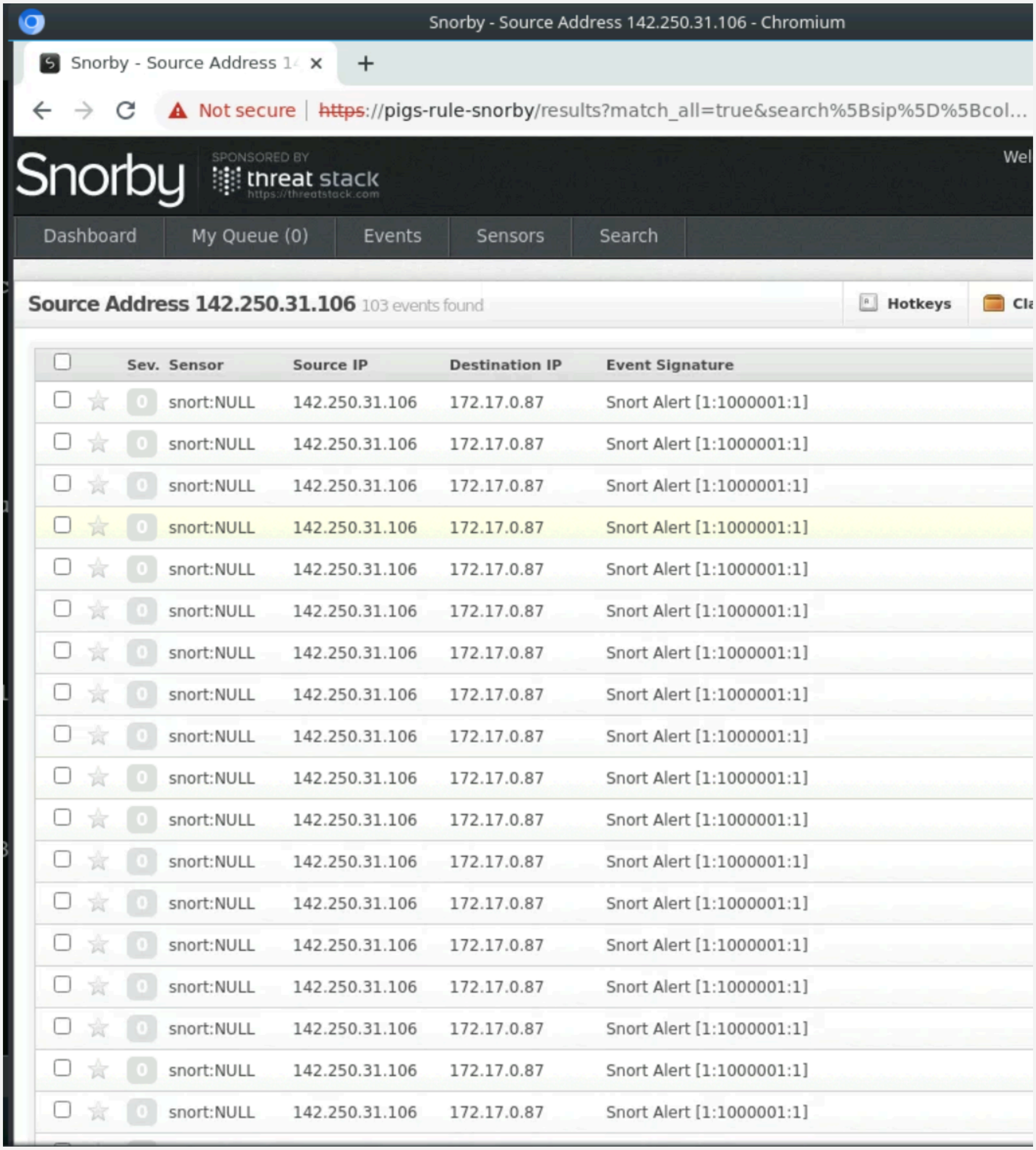
2. Next, I configured Snort through the CLI to pick up any ICMP traffic.



```
 GNU nano 2.9.3              /etc/snort/rules/local.rules

alert icmp any any -> any any (msg:"ICMP Example"; sid:1000001; rev:1;)
```

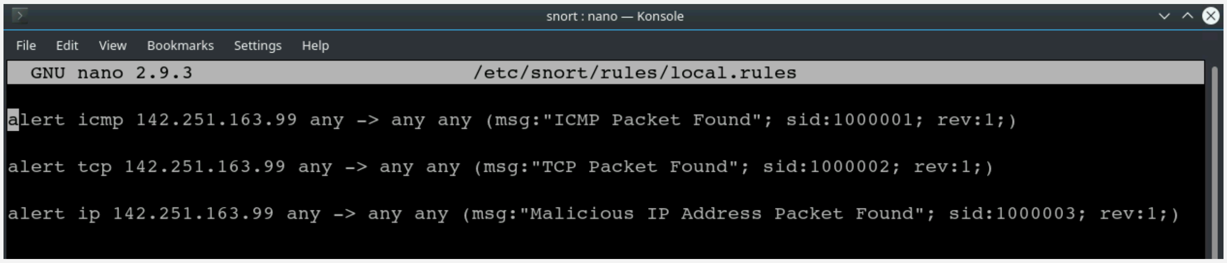
3. Then, I used Snorby to find an IP address that was constantly hitting the network that was not part of it.


Snorby - Source Address 142.250.31.106 - Chromium
Snorby - Source Address 1
Not secure
~~https~~://pigs-rule-snorby/results?match_all=true&search%5Bsip%5D%5Bcol...
Snorby
SPONSORED BY
threat stack
https://threatstack.com
Wel
Dashboard
My Queue (0)
Events
Sensors
Search
Hotkeys
Cla

Source Address 142.250.31.106 103 events found

□		Sev.	Sensor	Source IP	Destination IP	Event Signature
□	☆	0	snort:NULL	142.250.31.106	172.17.0.87	Snort Alert [1:1000001:1]
□	☆	0	snort:NULL	142.250.31.106	172.17.0.87	Snort Alert [1:1000001:1]
□	☆	0	snort:NULL	142.250.31.106	172.17.0.87	Snort Alert [1:1000001:1]
□	☆	0	snort:NULL	142.250.31.106	172.17.0.87	Snort Alert [1:1000001:1]
□	☆	0	snort:NULL	142.250.31.106	172.17.0.87	Snort Alert [1:1000001:1]
□	☆	0	snort:NULL	142.250.31.106	172.17.0.87	Snort Alert [1:1000001:1]
□	☆	0	snort:NULL	142.250.31.106	172.17.0.87	Snort Alert [1:1000001:1]
□	☆	0	snort:NULL	142.250.31.106	172.17.0.87	Snort Alert [1:1000001:1]
□	☆	0	snort:NULL	142.250.31.106	172.17.0.87	Snort Alert [1:1000001:1]
□	☆	0	snort:NULL	142.250.31.106	172.17.0.87	Snort Alert [1:1000001:1]
□	☆	0	snort:NULL	142.250.31.106	172.17.0.87	Snort Alert [1:1000001:1]
□	☆	0	snort:NULL	142.250.31.106	172.17.0.87	Snort Alert [1:1000001:1]
□	☆	0	snort:NULL	142.250.31.106	172.17.0.87	Snort Alert [1:1000001:1]
□	☆	0	snort:NULL	142.250.31.106	172.17.0.87	Snort Alert [1:1000001:1]
□	☆	0	snort:NULL	142.250.31.106	172.17.0.87	Snort Alert [1:1000001:1]
□	☆	0	snort:NULL	142.250.31.106	172.17.0.87	Snort Alert [1:1000001:1]
□	☆	0	snort:NULL	142.250.31.106	172.17.0.87	Snort Alert [1:1000001:1]
□	☆	0	snort:NULL	142.250.31.106	172.17.0.87	Snort Alert [1:1000001:1]

4. After finding the anomaly of an IP address, I reconfigured Snort to focus directly on this address specifically.



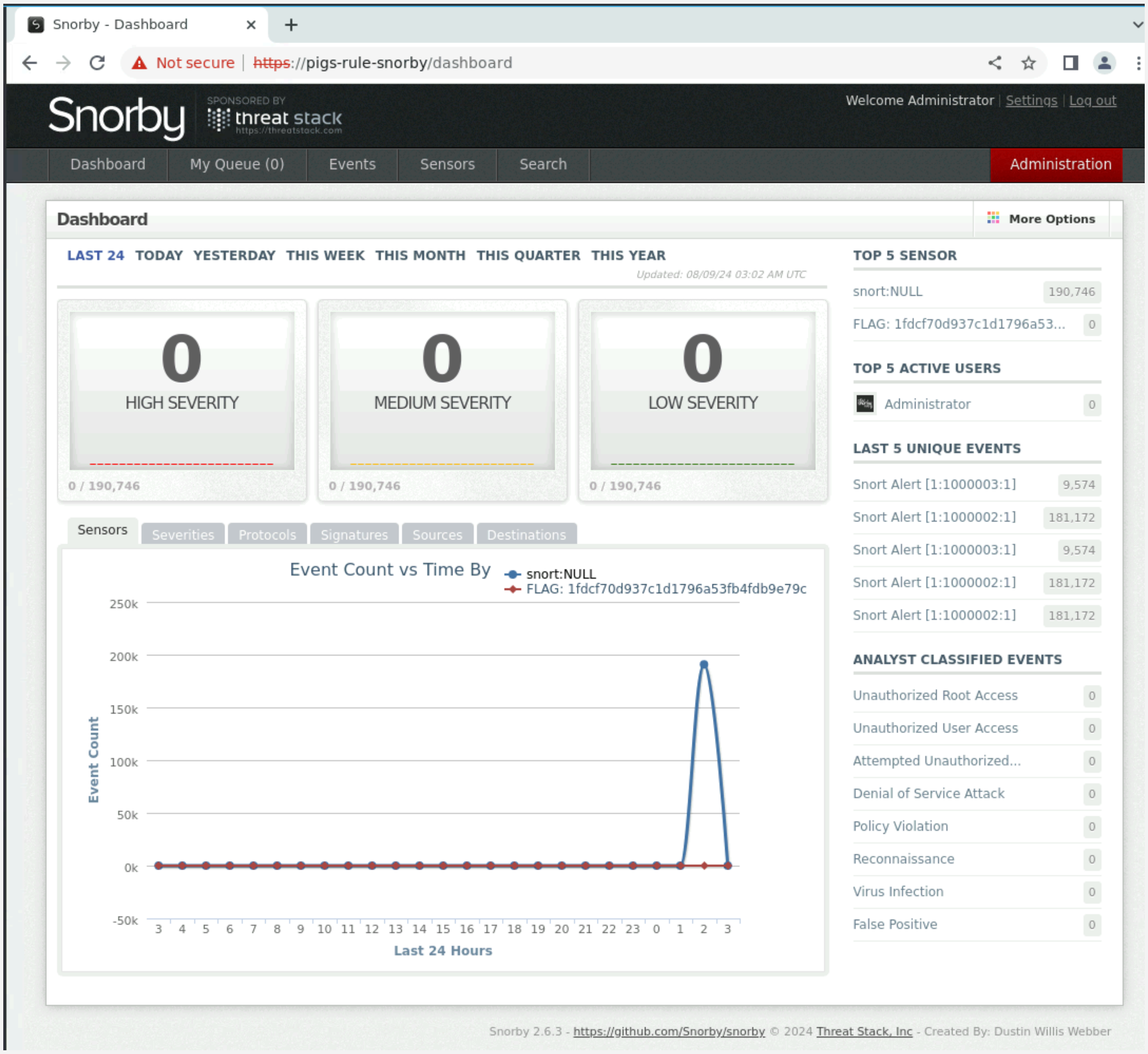
```
  GNU nano 2.9.3                         /etc/snort/rules/local.rules

alert icmp 142.251.163.99 any -> any any (msg:"ICMP Packet Found"; sid:1000001; rev:1;)

alert tcp 142.251.163.99 any -> any any (msg:"TCP Packet Found"; sid:1000002; rev:1;)

alert ip 142.251.163.99 any -> any any (msg:"Malicious IP Address Packet Found"; sid:1000003; rev:1;)
```

5. Once this was configured properly, Snorby was able to kick out the flag: 1fdcf70d937c1d1796a53fb4fdb9e79c



Dashboard

Updated: 08/09/24 03:02 AM UTC

0 HIGH SEVERITY 0 / 190,746

0 MEDIUM SEVERITY 0 / 190,746

0 LOW SEVERITY 0 / 190,746

Event Count vs Time By
- snort:NULL
- FLAG: 1fdcf70d937c1d1796a53fb4fdb9e79c

TOP 5 SENSOR

snort:NULL	190,746
FLAG: 1fdcf70d937c1d1796a53...	0

TOP 5 ACTIVE USERS

Administrator	0

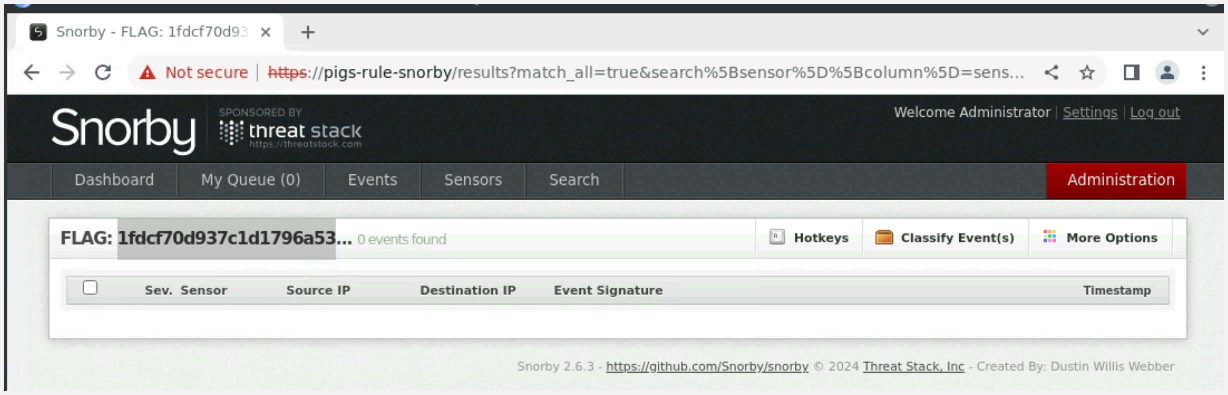
LAST 5 UNIQUE EVENTS

Snort Alert [1:1000003:1]	9,574
Snort Alert [1:1000002:1]	181,172
Snort Alert [1:1000003:1]	9,574
Snort Alert [1:1000002:1]	181,172
Snort Alert [1:1000002:1]	181,172

ANALYST CLASSIFIED EVENTS

Unauthorized Root Access	0
Unauthorized User Access	0
Attempted Unauthorized...	0
Denial of Service Attack	0
Policy Violation	0
Reconnaissance	0
Virus Infection	0
False Positive	0

Snorby 2.6.3 - https://github.com/Snorby/snorby © 2024 Threat Stack, Inc - Created By: Dustin Willis Webber


Snorby - FLAG: 1fdcf70d93
Not secure
https://pigs-rule-snorby/results?match_all=true&search%5Bsensor%5D%5Bcolumn%5D=sens...
Snorby
SPONSORED BY
threat stack
https://threatstack.com
Welcome Administrator | Settings | Log out
Dashboard
My Queue (0)
Events
Sensors
Search
Administration
Hotkeys
Classify Event(s)
More Options

FLAG: 1fdcf70d937c1d1796a53... 0 events found

□	Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp

Snorby 2.6.3 - https://github.com/Snorby/snorby © 2024 Threat Stack, Inc - Created By: Dustin Willis Webber

Recommendations

1. Completely block any traffic from the specified malicious IP address.
2. Make sure the network, through Snort, is configured to detect any anomalies: especially DoS or DDoS attacks, increased traffic from unknown IP addresses, or Nmap scanning.
3. Continue extra vigilant watch on network traffic to make sure malicious actors are not attempting to infiltrate Flying Pigs network through different means.

Appendix A

Network-related Findings	
IP Address	142.250.31.106
Adversary-related Findings	
Attack	Potential DoS attack.