



# **TDX ARENA**

## **Certification Report**

**Sebastian Loyacono**

Final Assessment Report Submission

# Case: Pigs Rules

06/22/2025

## Executive Summary

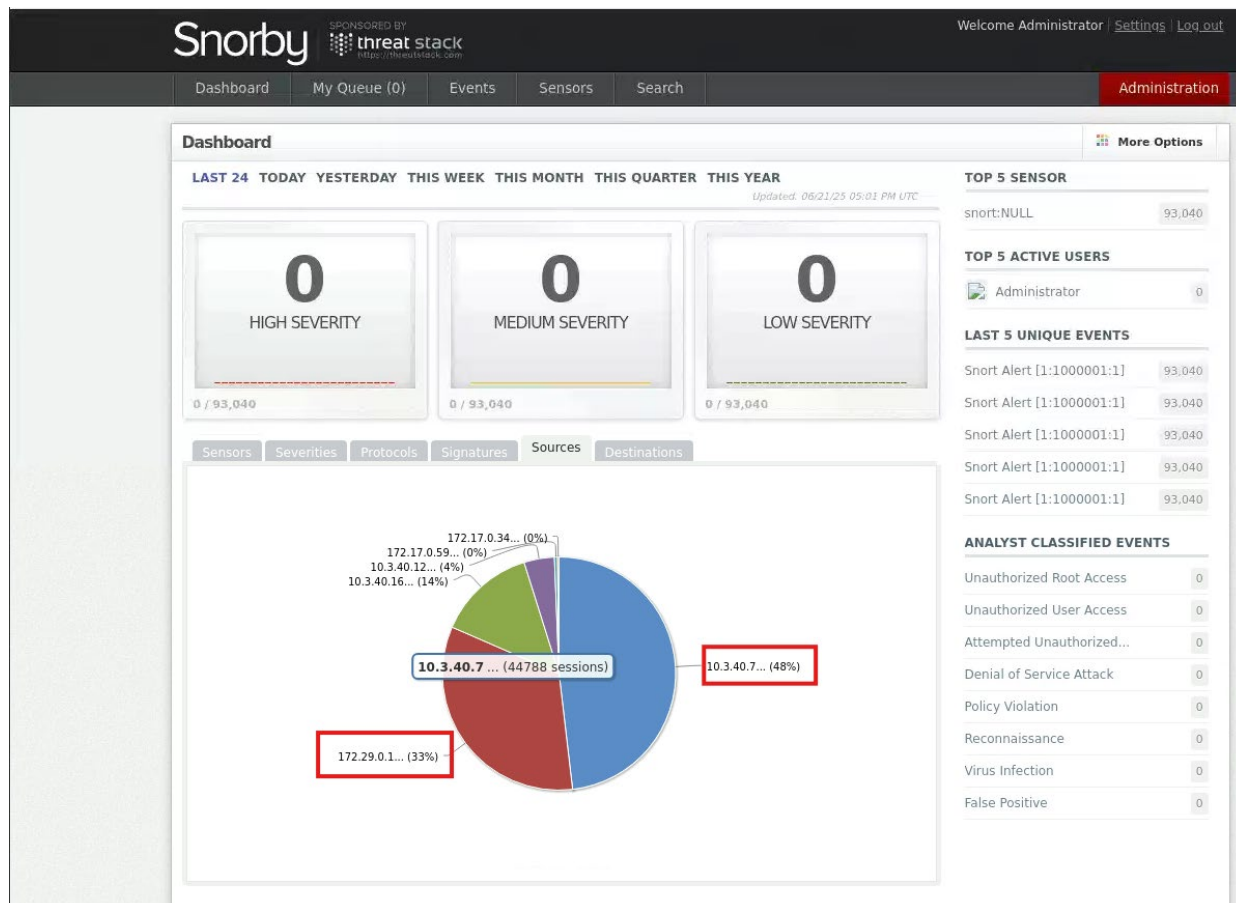
The search started by searching using, snort, and finding 6 different connections. Overall, the connections seemed normal except for two that needed further investigation. Using Snort, it was determined to use a detection rule to facilitate the search for connection request.

This detection rule monitors suspicious network behavior that could indicate a cyberattack is being prepared. Specifically, it looks for a device that sends multiple connection requests across different systems or ports in a short time — a common tactic used by hackers to "scan" for weaknesses in a network before launching an actual attack.

When a device sends at least 20 such connection attempts within 5 seconds, the system flags it as a potential threat. This helps security teams quickly identify and stop attackers who are trying to map out the network to find vulnerable entry points.

## Findings and Analysis

IP	Src Port	Dst Port	Flags	Ack
10.3.40.7	42292	22	16	1867494313
172.29.0.1	36730	1720	2	0



It was found that Ip's 10.3.40.7 and 172.29.0.1 had the most sessions suspecting suspicious activity

---

## Methodology


In this investigation, the primary tools and technologies utilized were Snort and Snorby.

Snort is an open-source network intrusion detection and prevention system (IDS/IPS) used to monitor and analyze network traffic in real time. It was employed to detect potentially malicious TCP traffic using custom and predefined rule sets. Snort enabled the capture and filtering of suspicious network packets, allowing for detailed traffic inspection and alert generation.

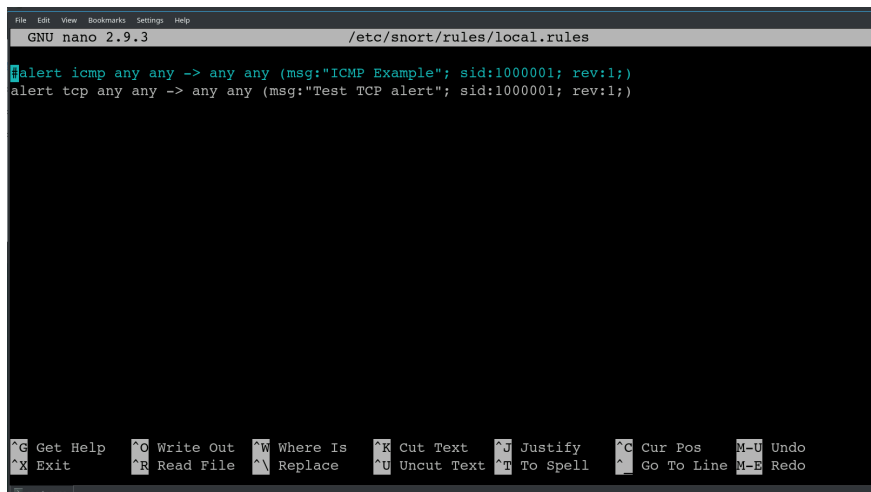
Snorby served as the front-end interface for visualizing the alerts generated by Snort. It provided a user-friendly dashboard that categorized events by priority and type, enabling efficient analysis and interpretation of the data collected. By using Snorby, it was possible to track incidents over time and gain insights into the nature and frequency of potential threats.

Together, these tools offered a comprehensive approach to network monitoring, detection, and visualization, essential for understanding and responding to cybersecurity threats.

## Investigation Process



```
snort: bash — Konsole
File Edit View Bookmarks Settings Help
snort@snort:~$ nano /etc/snort/rules/local.rules
```



```
File Edit View Bookmarks Settings Help
GNU nano 2.9.3 /etc/snort/rules/local.rules
alert icmp any any -> any any (msg:"ICMP Example"; sid:1000001; rev:1;)
alert tcp any any -> any any (msg:"Test TCP alert"; sid:1000001; rev:1;)

^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line  M-B Redo
```

The first step was to add a simple rule to inspect the TCP traffic in general

```

File Edit View Bookmarks Settings Help
snort@snort:~$ nano /etc/snort/rules/local.rules
snort@snort:~$ sudo snort -c /etc/snort/snort.conf -A console
Running in IDS mode

==== Initializing Snort ====
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037
3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088
8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 3444
3:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 23
81 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 80
80 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 99
99 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 3386 ]
Detection:
  Search-Method = AC-Full-Q
  Split Any/Any group = enabled
  Search-Method-Optimizations = enabled
  Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine /usr/local/lib/snort_dynamicengine/libsfe_engine.so... done
Loading all dynamic detection libs from /usr/local/lib/snort_dynamicrules...
WARNING: No dynamic libraries found in directory /usr/local/lib/snort_dynamicrules.
  Finished Loading all dynamic detection libs from /usr/local/lib/snort_dynamicrules
Loading all dynamic preprocessor libs from /usr/local/lib/snort_dynamicpreprocessor/...
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsfe_appid_preproc
.so... done
  Loading dynamic preprocessor library /usr/local/lib/snort_dynamicpreprocessor//libsfe_dce2_preproc.

```

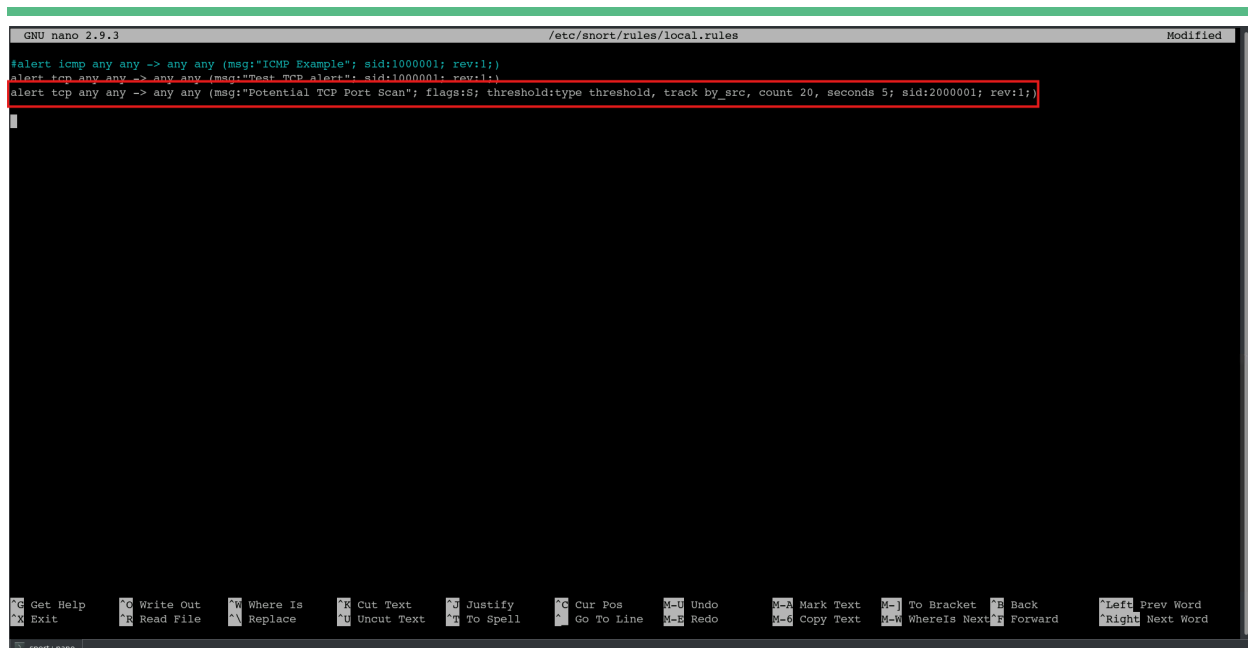
```

snort: bash
==== Initializing Snort ====
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 71
44:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443
9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988
7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9
090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 3386 ]
Detection:
  Search-Method = AC-Full-Q
  Split Any/Any group = enabled
  Search-Method-Optimizations = enabled
  Maximum pattern length = 20

```

As shown in the pictures above, the traffic was inspected in the CLI first with the command *sudo snort -c /etc/snort/snort.conf -A console*

the command *sudo snort -c /etc/snort/snort.conf* was placed to send the filtered information in the snorby front-end interface.



```
GNU nano 2.9.3 /etc/snort/rules/local.rules Modified
#alert icmp any any -> any any (msg:"ICMP Example"; sid:1000001; rev:1;)
#alert tcp any any -> any any (msg:"Test TCP alert"; sid:1000001; rev:1;)
alert tcp any any -> any any (msg:"Potential TCP Port Scan"; flags:S; threshold:type threshold, track by_src, count 20, seconds 5; sid:2000001; rev:1;)
```

Later a new rule was added to the *nano /etc/snort/rules/local.rules*

*alert tcp any any -> any any (msg:"Potential TCP Port Scan"; flags:S; threshold:type threshold, track by\_src, count 20, seconds 5; sid:2000001; rev:1;)* This rule is designed to **detect a TCP SYN port scan**, which is a common **reconnaissance technique** used by attackers to identify open ports.

Snorby - Reconnaissance - Chromium

Not secure | [https://pigs-rule-snorby/results?match\\_all=true&search%5Bsensor%5D%5Bcolumn%5D=cl...](https://pigs-rule-snorby/results?match_all=true&search%5Bsensor%5D%5Bcolumn%5D=cl...)

Snorby SPONSORED BY threatstack <https://threatstack.com> Welcome Administrator | [Settings](#) | [Log out](#)

Dashboard My Queue (0) Events Sensors Search Administration

Reconnaissance 85 events found Hotkeys Classify Event(s) More Options

Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp
0	snort:NULL	172.29.0.1	172.29.0.3	Snort-Alert[1:2000001:1]	5:15 PM

**IP Header Information** Perform Mass Classification Event Export Options Permalink

Source	Destination	Ver	Hlen	Tos	Len	ID	Flags	Off	TTL	Proto	Csum
172.29.0.1	172.29.0.3	4	5	0	44	29366	0	0	45	6	49879

**Signature Information**

Generator ID	Sig. ID	Sig. Revision	Activity (0/7961)	Category	Sig Info
1	2000001	1	0.00%	N/A	<a href="#">Query Signature Database</a> <a href="#">View Rule</a>

**TCP Header Information**

Src Port	Dst Port	Seq	Ack	Off	Res	Flags	Win	Csum	URP
36730	50576	3169496642	0	6	0	2	1024	31663	0

**Payload**

No Payload Data Available

**Notes**

This event currently has zero notes - You can add a note by clicking the button below.

[Add A Note To This Event](#)

0	snort:NULL	172.29.0.1	172.29.0.3	Snort-Alert[1:2000001:1]	5:15 PM
0	snort:NULL	172.29.0.1	172.29.0.3	Snort-Alert[1:2000001:1]	5:15 PM
0	snort:NULL	172.29.0.1	172.29.0.3	Snort-Alert[1:2000001:1]	5:15 PM
0	snort:NULL	172.29.0.1	172.29.0.3	Snort-Alert[1:2000001:1]	5:15 PM
0	snort:NULL	172.29.0.1	172.29.0.3	Snort-Alert[1:2000001:1]	5:15 PM
0	snort:NULL	172.29.0.1	172.29.0.3	Snort-Alert[1:2000001:1]	5:15 PM
0	snort:NULL	172.29.0.1	172.29.0.3	Snort-Alert[1:2000001:1]	5:15 PM
0	snort:NULL	172.29.0.1	172.29.0.3	Snort-Alert[1:2000001:1]	5:15 PM
0	snort:NULL	172.29.0.1	172.29.0.3	Snort-Alert[1:2000001:1]	5:15 PM
0	snort:NULL	172.29.0.1	172.29.0.3	Snort-Alert[1:2000001:1]	5:15 PM
0	snort:NULL	172.29.0.1	172.29.0.3	Snort-Alert[1:2000001:1]	5:15 PM
0	snort:NULL	172.29.0.1	172.29.0.3	Snort-Alert[1:2000001:1]	5:15 PM
0	snort:NULL	172.29.0.1	172.29.0.3	Snort-Alert[1:2000001:1]	5:15 PM
0	snort:NULL	172.29.0.1	172.29.0.3	Snort-Alert[1:2000001:1]	5:15 PM
0	snort:NULL	172.29.0.1	172.29.0.3	Snort-Alert[1:2000001:1]	5:15 PM

Lastly, the traffic shown in snorby is filtered to show only the threat were showing the information of the TCP traffic that is searching for open ports.



## Recommendations

The source IP 172.29.0.1 was observed performing TCP SYN scans across multiple ports, indicating possible reconnaissance activity. The behavior is consistent with pre-attack scanning tactics used by threat actors. We recommend blocking this IP at the perimeter firewall, reviewing associated host activity, and performing a full investigation to assess exposure. Future incidents can be mitigated by enabling stricter egress rules and segmenting sensitive assets.

**Reconnaissance** 85 events found Hotkeys Classify Event(s) More Options

Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp
0	snort:NULL	172.29.0.1	172.29.0.3	Snort-Aler1-1-2000001-1	5:15 PM

**IP Header Information** Perform Mass Classification Event Export Options Permalink

Source	Destination	Ver	Hlen	Tos	Len	ID	Flags	Off	TTL	Proto	Csum
172.29.0.1	172.29.0.3	4	5	0	44	29366	0	0	45	6	49879

**Signature Information**

Generator ID	Sig. ID	Sig. Revision	Activity (0/7961)	Category	Sig Info
1	2000001	1	0.00%	N/A	<span>Query Signature Database</span> <span>View Rule</span>

**TCP Header Information**

Src Port	Dst Port	Seq	Ack	Off	Res	Flags	Win	Csum	URP
36730	50576	3169496642	0	6	0	2	1024	31663	0

**Payload**

No Payload Data Available

**Notes**

This event currently has zero notes - You can add a note by clicking the button below.

Add A Note To This Event