



**Sebastian Loyacono** 

Final Assessment Report Submission



trying to map out the network to find vulnerable entry points.

## **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

### **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.

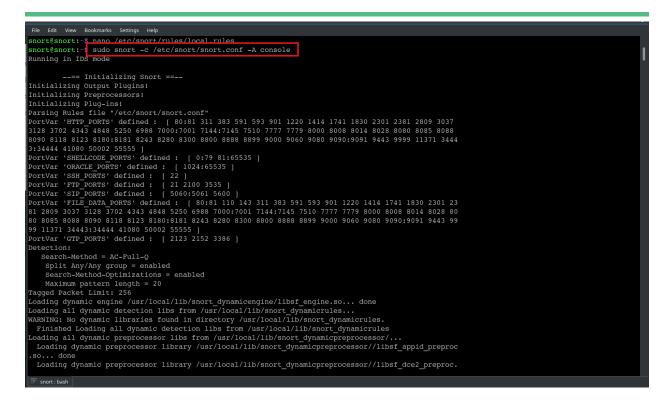
Snorby served as the front-end interface for visualizing the alerts generated by Snort. It provided a user-friendly dashboard that categorized events by priority and type, enabling efficient analysis and interpretation of the data collected. By using Snorby, it was possible to track incidents over time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

• ••	
	$\sim$ $\sim$
File Edit View Bookmarks Settings Help	
<pre>snort@snort:~\$ nano /etc/snort/rules/local.rules</pre>	
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;)	
<sup>^</sup> G Get Help <sup>^</sup> O Write Out <sup>^</sup> W Where Is <sup>^</sup> K Cut Text <sup>^</sup> J Justify <sup>^</sup> C Cur Pos M=U Un <sup>^</sup> X Exit <sup>^</sup> R Read File <sup>^</sup> \ Replace <sup>^</sup> U Uncut Text <sup>^</sup> T To Spell <sup>^</sup> G To Line M=E Re	do do

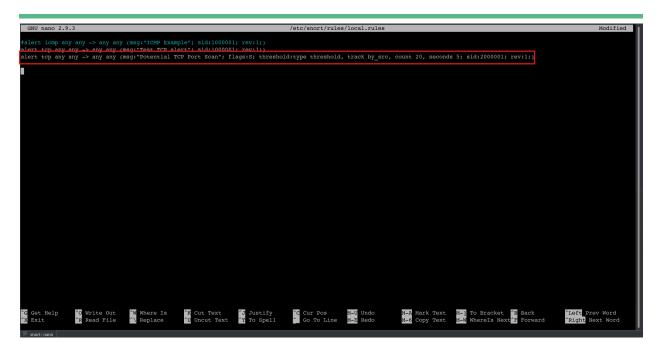
The first step was to add a simple rule to inspect the TCP traffic in general



README - KWrite - KWrite	snort : bash — Konsole	~ ^ 😣
- File Edit View Bookmarks Settings Help		
IMAP Preprocessor Statistics		
Total sessions		
Max concurrent sessions		
POP Preprocessor Statistics		
Total sessions	: 0	
Max concurrent sessions	: 0	
Reputation Preprocessor Statistics		
Total Memory Allocated: 0		
Snort exiting		
snort@snort:~\$ sudo snort _c /etc/snort/snor	rt.conf	
Running in IDS mode		
== Initializing Snort ==		
Initializing Output Plugins!		
Initializing Preprocessors!		
Initializing Plug-ins! Parsing Rules file "/etc/snort/snort.conf"		
	383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:	.7001 71
	303 391 393 901 1220 1414 1/41 1030 2301 2301 2301 303/ 3120 3/02 4343 4048 5230 6988 /0003 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9(	
9999 11371 34443:34444 41080 50002 55555 1		JI J445
PortVar 'SHELLCODE PORTS' defined : [ 0:79	81:65535 1	
PortVar 'ORACLE PORTS' defined : [ 1024:655		
PortVar 'SSH PORTS' defined : [ 22 ]		
PortVar 'FTP PORTS' defined : [ 21 2100 353	35 ]	
PortVar 'SIP PORTS' defined : [ 5060:5061 5		
PortVar 'FILE DATA PORTS' defined : [ 80:81	1 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 52	250 6988
7000:7001 7144:7145 7510 7777 7779 8000 800	08 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060	0 9080 9
090:9091 9443 9999 11371 34443:34444 41080 5	50002 55555 j	
PortVar 'GTP_PORTS' defined : [ 2123 2152 3	3386 ]	
Detection:		
Search-Method = AC-Full-Q		
Split Any/Any group = enabled		
Search-Method-Optimizations = enabled		
Maximum pattern length = 20		
➢ snort ; bash		

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.



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.

sev. Sensor         Source IP         Destination IP         Event Signature         Interchange           *         Snort:NULL         172.29.0.1         172.29.0.3         Snort-Alect Lindococccccccccccccccccccccccccccccccccc			Si	norby - Reconna	aissance - (	Chromium				
Control         Series         Series         Series         Series         Administration           •	norby - Reconnais	sance × +								
Concernation         Search         Administra           2000000000000000000000000000000000000	→ C ▲ Not	secure   https://pigs	-rule-snorby/resu	lts?match_all	=true&se	earch%5B	sensor%5D	0%5Bcolu	ımn%5D=cl	< ☆ 🗆
Add multiplicity         Add multiplicity         Add multiplicity           accountailsSance ifS overtis Sourd         Image: Sensor Source IP         Destination IP         Event Signature         Image: Sensor Source IP         Preder Information           Image: Sensor Source IP         Destination IP         Mr // Mr         N/A         Course Signature Database         View Rule           TCP Header Information         Image: Sensor Source IP         Sensor Source IP         Ark         Off         Res         Fargs         Win         Caun         OP           Sof Port Dre Port Sensor Source IP         Sensor Source IP         Ark         Off         Res         Fargs         Win         Caun         OP           Sof Port Dre Port Sensor Source IP         Se	norbu	SPONSORED BY						We	lcome Administr	rator   <u>Settings</u>   <u>Lo</u> c
Serv. Sensor         Source IP         Destination IP         Event Signature         Timestame           *         is nort.NUL         172.29.0.1         172.29.0.3         Source Advertitie 20000001-11         513 PV           P Header Information         Ver         Hin         Tos         Len         ID         Flags         Off         TT         Proto         Count           Signature Information         Ver         Hin         Tos         Len         ID         Flags         Off         TT         Proto         Count           Signature Information         Ver         Hint         Tos         Len         ID         Flags         Off         TT         Proto         Count           Signature Information         Sig. Revision         Activity (07961.1)         Category         Sig Info         Uew Rule           TCP Header Information         Sig. Revision         Activity (07961.1)         Category         Sig Info         Uew Rule           Signature Information         Signature Information         N/A         Cuery Signature Database         Wew Rule           Signature Information         Signature Information         Signature Information         Signature Information         Uew Rule           Signature Information         Signature In	5									
Sev. Sensor         Source IP         Destination IP         Event Signature         Tendent           *         snort-NULL         172.29.0.3         Statustance         Perform Mass Classification         Revet Export Outloo         Permainer           Source Performation         Ver         Hen         Tos         Len         D         Flags         Off         TL         Proto         Cource           Source Sourc	ashboard M	y Queue (0) Eve	nts Sensors	Search						Administrat
*       •       •       172.29.0.1       172.29.0.3       •       •       •       9	connaissance a	5 events found					Hotkeys	s 🔳 ci	assify Event(s)	More Option
Precoder Information         Perform Mass Classification         Perfo	Sev. Sens	or Source IP	Destination II	P Event Sig	gnature					Timestamp
Source         Destination         Ver         Hien         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         sig. ID         Sig. Revision         Activity (0/7961)         Category         Sig Info         View Rule           1         200001         1         0.00%         N/A         Query Signature Database         View Rule           TCP Header Information          Sig 10996642         0         6         0         2         1024         31663         0           Payload         Dat Port         Seq         Ack         Off         Res         Flags         Win         Csum         URP           36730         50576         3169496642         0         6         0         2         1024         31653         0           Payload         Data         sig 1172.29.0.1         172.29.0.3         Smert-AlertH:3000001-11         5         5         5515 PM           Cod A Note To This Everin:          Sig 10	🗆 ★ 💽 snort	:NULL 172.29.0.1	172.29.0.3	Snort Ale	ert [1:2000	001:1]				5:15 PM
Source         Destination         Ver         Hien         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         sig. Revision         Activity (0/7961)         Category         Sig Info         .	IP Header Info	rmation				P	erform Mass Cl	lassification	Event Export C	Options Permalink
172.29.0.1 **       172.29.0.3 **       4       5       0       44       29366       0       0       45       6       49879         Signature Information         Category Sig Info         1       2000001       1       0.00%       N/A       Outery Signature Database       View Rule         Notes         Sinort-Null       172.29.0.1       172.29.0.3       Snort-Alert1+2000000+1+1       Sin 5 PM         Sinort-Null       172.29.0.1       172.29.0.3       Snort-Alert1+2000000+1+1       Sin 5 PM         Sinort-Null       172.29.0.1       172.29.0.3       Snort-Alert1+200000+1+1       Sin 5 PM	Source	Destination	Ver	Hlen Tos		ID	Flags	Off		
Generator ID         Sig. ID         Sig. Revision         Activity (0/7951)         Category         Sig Info           1         2000001         1         0.00%         N/A         Query Signature Database         View Rule           TCP Header Information         50576         3169496642         0         6         0         2         1024         3163         0           Payload           Notes           This event currently has zero notes - You can add a note by clicking the button below.           Acte To This Event:           1         12.290.1         172.290.3         Sport-Alert [1:20000011]         5:15 PM           1         12.290.1         172.290.3         Sport-Alert [1:20000011]         5:15 PM           1         1         172.290.3         Sport-Alert [1:20000011]         5:15 PM           1 </td <td>172.29.0.1 🏨</td> <td>172.29.0.3 🗯</td> <td>4</td> <td>5 0</td> <td>44</td> <td>29366</td> <td></td> <td>0</td> <td>45 6</td> <td>49879</td>	172.29.0.1 🏨	172.29.0.3 🗯	4	5 0	44	29366		0	45 6	49879
Generator ID         Sig. ID         Sig. Revision         Activity (0/7951)         Category         Sig Info           1         2000001         1         0.00%         N/A         Query Signature Database         View Rule           TCP Header Information         50576         3169496642         0         6         0         2         1024         3163         0           Payload           Notes           This event currently has zero notes - You can add a note by clicking the button below.           Acte To This Event:           1         12.290.1         172.290.3         Sport-Alert [1:20000011]         5:15 PM           1         12.290.1         172.290.3         Sport-Alert [1:20000011]         5:15 PM           1         1         172.290.3         Sport-Alert [1:20000011]         5:15 PM           1 </td <td>Signature Info</td> <td>rmation</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	Signature Info	rmation								
1       200001       1       0.00%       N/A       Query Signature Database       View Rule         TCP Header Information         Src Port       Dst Port       Seq       Ack       Orf       Res       Flags       Win       Csum       URP         36730       50576       3169496642       0       6       0       2       1024       31663       0         Payload         Notes         This event currently has zero notes - You can add a note by clicking the button below.         Add A Note To This Event         Sinort-NULL       172.29.0.1       172.29.0.3       Snort-Alert [1:2000001:1]       Sin 15 PM         Image: Sinort-NULL       172.29.0.1       172.29.0.3       Snort-Alert [1:2000001:1]       Sin 15 PM         Image: Sinort-NULL       172.29.0.1       172.29.0.3       Snort-Alert [1:2000001:1]       Sin 15 PM         Image: Sinort-NULL       172.29.0.1       172.29.0.3       Snort-Alert [1:2000001:1]       Sin 15 PM         Image: Sinort-NULL       172.29.0.1       172.29.0.3       Snort-Alert [1:2000001:1]       Sin 15 PM         Image: Sinort-NULL       172.29.0.1       172.29.0.3       Snort-Alert [1:2000001:1] </td <td></td> <td></td> <td>ision Activity (</td> <td>0/7961)</td> <td></td> <td>Cate</td> <td>aory Sia</td> <td>Info</td> <td></td> <td></td>			ision Activity (	0/7961)		Cate	aory Sia	Info		
Src Port         Dst Port         Seq         Ack         Off         Res         Flags         Win         Csum         URP           36730         50575         3169496642         0         6         0         2         1024         31663         0           Payload           No Payload Data Available         Version of the second of					.00%				ture Database	View Rule
Src Port         Dst Port         Seq         Ack         Off         Res         Flags         Win         Csum         URP           36730         50575         3169496642         0         6         0         2         1024         31663         0           Payload           No Payload Data Available         Version of the second of	TCP Header Inf	formation								
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         Intervent         Interven			Sea	Ack	Off	Res	Flags	Win	Csum	URP
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 Events           Add A Note To This Events           Snort-NULL         172.29.0.1         172.29.0.3         Snort-Alert [h:2000001:h]         5:15 PM <ul> <li>Image: Image: Image</li></ul>										
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 Events           Add A Note To This Events           Snort-NULL         172.29.0.1         172.29.0.3         Snort-Alert [h:2000001:h]         5:15 PM <ul> <li>Image: Image: Image</li></ul>	Pavload									
Notes           This event currently has zero notes - You can add a note by clicking the button below.           Add A Note To This Event           a         0 snort:NULL         172.29.0.1         172.29.0.3         Snort Alert [1:2000001:1]         5:15 PM           a         0 snort:NULL         172.29.0.1         172.29.0.3         Snort Alert [1:2000001:1]         5:15 PM           a         0 snort:NULL         172.29.0.1         172.29.0.3         Snort Alert [1:2000001:1]         5:15 PM           a         0 snort:NULL         172.29.0.1         172.29.0.3         Snort Alert [1:2000001:1]         5:15 PM           a         0 snort:NULL         172.29.0.1         172.29.0.3         Snort Alert [1:2000001:1]         5:15 PM           a         0 snort:NULL         172.29.0.1         172.29.0.3         Snort Alert [1:2000001:1]         5:15 PM           a         0 snort:NULL         172.29.0.1         172.29.0.3         Snort Alert [1:2000001:1]         5:15 PM           a         0 snort:NULL         172.29.0.1         172.29.0.3         Snort Alert [1:2000001:1]         5:15 PM           a         0 snort:NULL         172.29.0.1         172.29.0.3         Snort Alert [1:2000001:1]         5:15 PM           a         0 snort:NULL         172.29.0.1	_	Available								
This event currently has zero notes - You can add a note by clicking the button below.         Add A Note To This Event <ul> <li></li></ul>	no raycoud buch									
Add A Note To This Events         Add A Note To This Events         Snort:NULL       172.29.0.1       172.29.0.3       Snort Alert [1:2000001:1]       5:15 PM         Snort:NULL       172.29.0.1       172.29.0.3       Snort Alert [1:2000001:1]       5:15										
Image: State			ou can add a note	by clicking th	ne button	below.				
snort:NULL       172.29.0.1       172.29.0.3       Snort Alert [1:2000001:1]       5:15 PM         Snort:NULL       172.29.0.1       172.29.0.3       Snort	This event curren	tly has zero notes - Y	ou can add a note	by clicking th	ne button	below.				
snort:NULL       172.29.0.3       Snort-Alert [1:2000001:1]       5:15 PM         snort:NULL       172.29.0.1       172.29.0.3       Snort-Alert [1:2000001:1]	This event curren	tly has zero notes - Y	ou can add a note	by clicking th	ne button	below.				
snort:NULL       172.29.0.1       172.29.0.3       Snort-Alert [1:2000001:1]       5:15 PM         > 10       snort:NULL       172.29.0.1       172.29.0.3       Snort-Alert [1:2000001:1]       5:15 PM         > 10       snort:NULL       172.29.0.1       172.29.0.3       Snort-Alert [1:2000001:1]       5:15 PM         > 10       snort:NULL       172.29.0.1       172.29.0.3       Snort-Alert [1:2000001:1]       5:15 PM         > 10       snort:NULL       172.29.0.1       172.29.0.3       Snort-Alert [1:2000001:1]       5:15 PM         > 10       snort:NULL       172.29.0.1       172.29.0.3       Snort-Alert [1:2000001:1]       5:15 PM         > 10       snort:NULL       172.29.0.1       172.29.0.3       Snort-Alert [1:2000001:1]       5:15 PM         > 11       snort:NULL       172.29.0.1       172.29.0.3       Snort-Alert [1:2000001:1]       5:15 PM         > 11       snort:NULL       172.29.0.1       172.29.0.3       Snort-Alert [1:2000001:1]       5:15 PM         > 11       snort:NULL       172.29.0.1       172.29.0.3       Snort-Alert [1:2000001:1]       5:15 PM         > 11       snort:NULL       172.29.0.1       172.29.0.3       Snort-Alert [1:2000001:1]       5:15 PM         > 11       snort:NULL <t< td=""><td>This event curren Add A Note To</td><td>tly has zero notes - Y This Eve<mark>n</mark>t</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>5:15 PM</td></t<>	This event curren Add A Note To	tly has zero notes - Y This Eve <mark>n</mark> t								5:15 PM
snort:NULL       172.29.0.1       172.29.0.3       Snort Alert [1:2000001:1]       5:15 PM         snort:NULL       172.29.0.1       172.29.0.3       Snort Alert [1:2000001:1]       5:15 PM         snort:NULL       172.29.0.1       172.29.0.3       Snort Alert [1:2000001:1]       5:15 PM         r       o       snort:NULL       172.29.0.1       172.29.0.3       Snort Alert [1:2000001:1]       5:15 PM         r       o       snort:NULL       172.29.0.1       172.29.0.3       Snort Alert [1:2000001:1]       5:15 PM         r       o       snort:NULL       172.29.0.1       172.29.0.3       Snort Alert [1:2000001:1]       5:15 PM         r       o       snort:NULL       172.29.0.1       172.29.0.3       Snort Alert [1:2000001:1]       5:15 PM         r       o       snort:NULL       172.29.0.1       172.29.0.3       Snort Alert [1:2000001:1]       5:15 PM         r       o       snort:NULL       172.29.0.1       172.29.0.3       Snort Alert [1:2000001:1]       5:15 PM         r       o       snort:NULL       172.29.0.1       172.29.0.3       Snort Alert [1:2000001:1]       5:15 PM         r       o       snort:NULL       172.29.0.1       172.29.0.3       Snort Alert [1:2000001:1]       5:15 PM	This event curren         Add A Note To <ul> <li></li></ul>	tly has zero notes - Y This Eve <mark>nt</mark> :NULL 172.29.0.1	172.29.0.3	Snort Ale	ert [1:2000	001:1]				5:15 PM 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         Snort-Alert [1:2000001:1]         5:15 PM           *         0         snort:NULL         172.29.0.1         Snort-Alert [1:2000001:1]         5:15 PM	Add A Note To         Add A Note To $ \Rightarrow  \boxed{ \ }  \text{snort}  \\         \Rightarrow  \boxed{ \ }  \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	tly has zero notes - Y This Eve <mark>nt</mark> :NULL 172.29.0.1 :NULL 172.29.0.1	172.29.0.3 172.29.0.3	Snort-Ale	ert [1:2000 ert [1:2000	<del>001:1]</del> 001:1]				
snort:NULL         172.29.0.1         172.29.0.3         Snort Alert [1:2000001:1]         5:15 PM            snort:NULL         172.29.0.1         172.29.0.3         Snort Alert [1:2000001:1]         5:15 PM            snort:NULL         172.29.0.1         172.29.0.3         Snort Alert [1:2000001:1]         5:15 PM            snort:NULL         172.29.0.1         172.29.0.3         Snort Alert [1:200001:1]         5:15 PM             snort:NULL         172.29.0.1         172.29.0.3         Snort Alert [1:2000001:1]         5:15 PM             snort:NULL         172.29.0.1         172.29.0.3         Snort Alert [1:2000001:1]         5:15 PM              snort:NULL         172.29.0.1         172.29.0.3         Snort Alert [1:2000001:1]         5:15 PM	Add A Note To	tty has zero notes - Y <b>This Eve</b> pt :NULL 172.29.0.1 :NULL 172.29.0.1 :NULL 172.29.0.1	172.29.0.3 172.29.0.3 172.29.0.3	Snort Ale Snort Ale Snort Ale	ert [1:2000 ert [1:2000 ert [1:2000	001:1] 001:1] 001:1]				5:15 PM
snort:NULL         172.29.0.1         172.29.0.3         Snort Alert [1:2000001:1]         5:15 PM           * 0         snort:NULL         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	Add A Note To            ☆         ①         snort         ☆         ①         snort         ☆         ①         snort         ☆         ①         snort         ☆         ③         Snort         ④         ③         Snort         ①         Snort	tty has zero notes - Y <b>This Even</b> y: :NULL 172.29.0.1 :NULL 172.29.0.1 :NULL 172.29.0.1	172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3	Snort Ale Snort Ale Snort Ale Snort Ale	rt [1:2000 rt [1:2000 rt [1:2000	001:1] 001:1] 001:1] 001:1]				5:15 PM 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	Add A Note To       Add A Note To	tty has zero notes - Y <b>This Ever</b> y: :NULL 172.29.0.1 :NULL 172.29.0.1 :NULL 172.29.0.1 :NULL 172.29.0.1 :NULL 172.29.0.1	172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3	Snort-Ale Snort-Ale Snort-Ale Snort-Ale Snort-Ale	ert [1:2000 ert [1:2000 ert [1:2000 ert [1:2000 ert [1:2000	001:1] 001:1] 001:1] 001:1] 001:1]				5:15 PM 5:15 PM 5:15 PM
Image: short:NULL         172.29.0.1         172.29.0.3         Short-Alert [1:2000001:1]         5:15 PM           Image: short:NULL         172.29.0.1         172.29.0.3         Short-Alert [1:2000001:1]         5:15 PM	Add A Note To	tty has zero notes - Y This Every: :NULL 172.29.0.1 :NULL 172.29.0.1 :NULL 172.29.0.1 :NULL 172.29.0.1 :NULL 172.29.0.1 :NULL 172.29.0.1 :NULL 172.29.0.1	172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3	Snort Ale Snort Ale Snort Ale Snort Ale Snort Ale Snort Ale	rt [1:2000 rt [1:2000 rt [1:2000 rt [1:2000 rt [1:2000 rt [1:2000	001:1] 001:1] 001:1] 001:1] 001:1] 001:1]				5:15 PM 5:15 PM 5:15 PM 5:15 PM
snort:NULL         172.29.0.1         172.29.0.3         Snort Alert [1:2000001:1]         5:15 PM	This event curren Add A Note To Add A Note To Add A Note To Snort S	tty has zero notes - Y           This Every:           ::NULL         172.29.0.1           :NULL         172.29.0.1	172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3	Snort-Ale Snort-Ale Snort-Ale Snort-Ale Snort-Ale Snort-Ale Snort-Ale	rt [1:2000 rt [1:2000 rt [1:2000 rt [1:2000 rt [1:2000 rt [1:2000 rt [1:2000	001:1] 001:1] 001:1] 001:1] 001:1] 001:1] 001:1] 001:1]				5:15 PM 5:15 PM 5:15 PM 5:15 PM 5:15 PM 5:15 PM 5:15 PM
	This event curren Add A Note To Add A Note To Add A Note To Snort S	tty has zero notes - Y           This Every:           :NULL         172.29.0.1	172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3	Snort-Ale Snort-Ale Snort-Ale Snort-Ale Snort-Ale Snort-Ale Snort-Ale Snort-Ale Snort-Ale Snort-Ale	rt [1:2000 rt [1:2000 rt [1:2000 rt [1:2000 rt [1:2000 rt [1:2000 rt [1:2000 rt [1:2000	001:1] 001:1] 001:1] 001:1] 001:1] 001:1] 001:1] 001:1] 001:1]				5:15 PM 5:15 PM 5:15 PM 5:15 PM 5:15 PM 5:15 PM 5:15 PM
	This event curren Add A Note To Add A Note To Add A Note To a snort a	tty has zero notes - Y           This Every:           :NULL         172.29.0.1           :NULL         172.29.0.1	172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3 172.29.0.3	Snort-Ale Snort-Ale Snort-Ale Snort-Ale Snort-Ale Snort-Ale Snort-Ale Snort-Ale Snort-Ale Snort-Ale Snort-Ale	rt [1:2000 rt [1:2000 rt [1:2000 rt [1:2000 rt [1:2000 rt [1:2000 rt [1:2000 rt [1:2000	001:1] 001:1] 001:1] 001:1] 001:1] 001:1] 001:1] 001:1] 001:1]				5:15 PM 5:15 PM 5:15 PM 5:15 PM 5:15 PM 5:15 PM 5:15 PM 5:15 PM 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.

Sev. Ser	FOT E	ource IP	Destination	. 10	Event Sig	nature						Timestam
		72.29.0.1	172.29.0.3		Snort-Ale		001:11					5:15 PM
IP Header Inf	ormation						B	erform Mass Cl	assification	Even	t Export Opti	ions Permalink
Source	Des	stination	Ver	Hlen	Tos	Len	ID	Flags	o <del>rr</del>	TTL	Proto	Csum
172.29.0.1 救	1 17	2.29.0.3 🚸	4	5	0	44	29366	0	0	45	6	49879
Signature Inf	ormation											
Generator ID	Sig. ID	Sig. Revision	Activit	y (0/796)	1)		Cate	gory Sig	Info			
1	2000001	1			0.	00%	N/A	Qu	ery Signat	ure Dal	tabase	View Rule
TCP Header I	nformation											
Src Port	Dst Port	Seq			Ack	off	Res	Flags	Win		Csum	URP
36730	50576	31694	96642		0	6	0	2	1024		31663	0
Payload												
No Payload Da	ta Available	,										
Notes												
		o notes - You ca										