

TDX ARENA

Certification Report

Araseli Serrano

Final Assessment Report Submission

Case: Pigs Rules

12.24.2024

Executive Summary

As the role of a SOC analyst, challenged in the “The Flying Pig” post office, it was known that a group of hackers were creating a global campaign against the country. A simulated security challenge was created to aim at preempting the hacker campaign to target the nation.

The goal was to sniff all incoming traffic and identify any malicious traffic, and configure Snort IDS rules to alert the system and only capture malicious traffic.

Findings and Analysis

Finding	Finding Details	Description
Rule	alert tcp 10.3.40.16 57842 -> 172.17.0.105 80 (msg:"SYN-ACK packet from 10.3.40.16 to 172.29.0.3 on port 80"; flags:A; sid:1000002; rev:1;)	This rule is customized to alert when all ongoing incoming traffic from the specific IP address and specific port is targeted.
User IP	172.17.0.105	This was the IP that was getting targeted.
Port	80	This was the port which malicious traffic was coming through.
Malicious IP	10.3.40.16	The IP address which the attacker was sending traffic to.
Validation	sudo snort -T -c /etc/snort/snort.conf	This was to test Snort and to verify that the rule was indeed taken into account.

Methodology

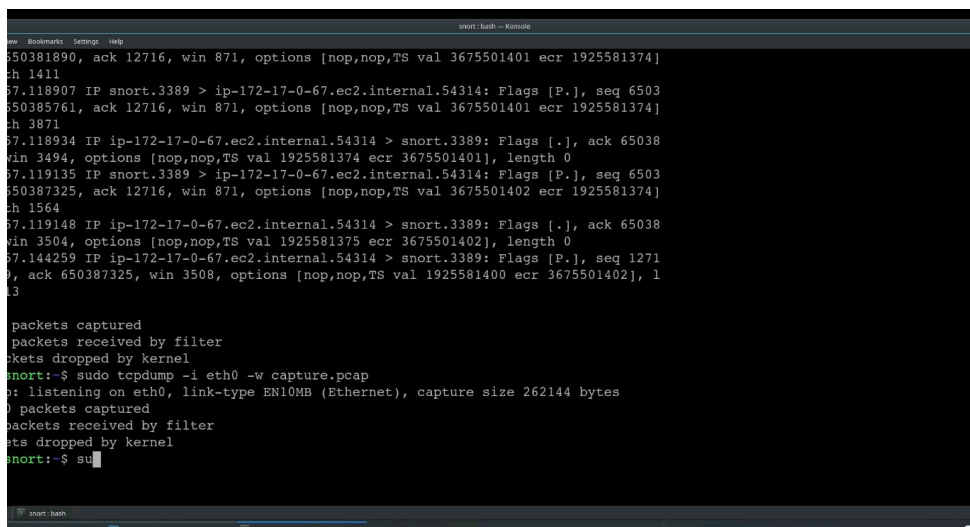
Tools and Technologies Used

- **TCPdump:** TCPdump is a tool to analyze packets that are incoming or outgoing on the network.
- **Snort IDS:** Snort IDS is an open-source intrusion detection program that is designed to monitor traffic in real time.
- **Snorby:** Snorby serves as a GUI for Snort to simplify network security monitoring.

Investigation Process

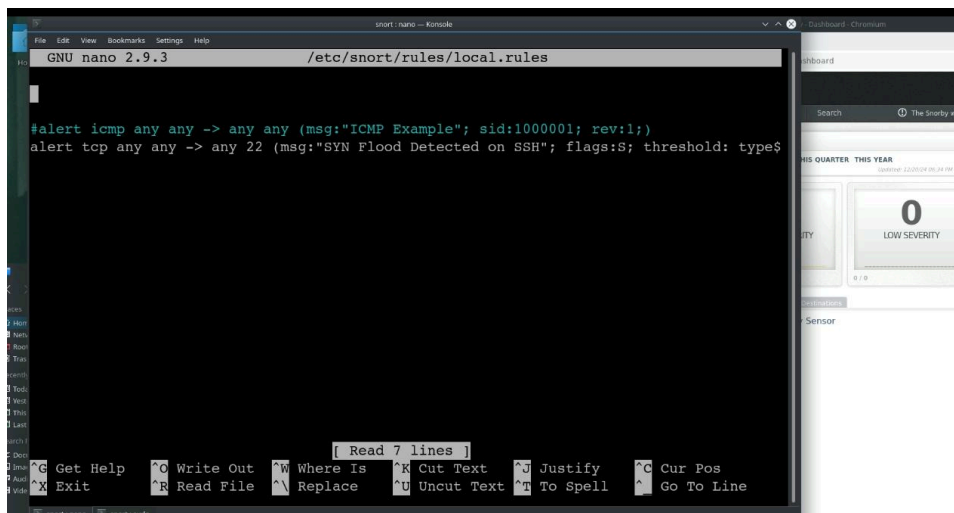
Certain IP addresses and ports might be different in the images due to multiple attempts.

1. I started by doing a TCPdump and capturing them to look through and analyze for any anomalies on incoming traffic.



```
snort:~$ sudo tcpdump -i eth0 -w capture.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
0 packets captured
0 packets received by filter
0 packets dropped by kernel
snort:~$ sudo tcpdump -i eth0 -w capture.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
0 packets captured
0 packets received by filter
0 packets dropped by kernel
snort:~$ su
```

2. A rule to alert when certain incoming traffic was customized to target the incoming Ip address to the port it was coming through.



```
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 22 (msg:"SYN Flood Detected on SSH"; flags:S; threshold: type$
```

- After setting the rule alert, all malicious packets were being identified.

```
Using ZLIB version: 1.2.11
Rules Engine: SF_SNORT DETECTION ENGINE Version 3.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SOF Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_MQDBUS Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DMPP Version 1.1 <Build 1>
Preprocessor Object: SF_DCEPC2 Version 1.0 <Build 3>
Preprocessor Object: appid Version 1.1 <Build 5>
Finishing packet processing (pid=3117)
11-18-33:38.398450 [**] [1:1000002:1] SYN-ACK packet from 10.3.40.16 to 172.29.0.3 on port 80 [**] [Priority: 0] (TCP) 10.3.40.16:57842 -> 172.29.0.3:80
11-18-33:38.407373 [**] [1:1000002:1] SYN-ACK packet from 10.3.40.16 to 172.29.0.3 on port 80 [**] [Priority: 0] (TCP) 10.3.40.16:57842 -> 172.29.0.3:80
11-18-33:38.409809 [**] [1:1000002:1] SYN-ACK packet from 10.3.40.16 to 172.29.0.3 on port 80 [**] [Priority: 0] (TCP) 10.3.40.16:57842 -> 172.29.0.3:80
11-18-33:40.336483 [**] [1:1000002:1] SYN-ACK packet from 10.3.40.16 to 172.29.0.3 on port 80 [**] [Priority: 0] (TCP) 10.3.40.16:57842 -> 172.29.0.3:80
11-18-33:40.338722 [**] [1:1000002:1] SYN-ACK packet from 10.3.40.16 to 172.29.0.3 on port 80 [**] [Priority: 0] (TCP) 10.3.40.16:57842 -> 172.29.0.3:80
11-18-33:41.059237 [**] [1:1000002:1] SYN-ACK packet from 10.3.40.16 to 172.29.0.3 on port 80 [**] [Priority: 0] (TCP) 10.3.40.16:57842 -> 172.29.0.3:80
11-18-33:41.060480 [**] [1:1000002:1] SYN-ACK packet from 10.3.40.16 to 172.29.0.3 on port 80 [**] [Priority: 0] (TCP) 10.3.40.16:57842 -> 172.29.0.3:80
11-18-33:42.448427 [**] [1:1000002:1] SYN-ACK packet from 10.3.40.16 to 172.29.0.3 on port 80 [**] [Priority: 0] (TCP) 10.3.40.16:57842 -> 172.29.0.3:80
+ Caught Int-Signal
-----
time for packet processing was 27.2335 seconds
t processed 616 packets.
t ran for 0 days 0 hours 0 minutes 27 seconds
Kts/sec: 22
-----
Memory usage summary:
Total non-mapped bytes (arena): 6283264
Bytes in mapped regions (hblkhd): 30265344
Total allocated space (wordblks): 3698080
Total free space (fordblks): 2585184
Largest releasable block (keepcost): 466832
```

- Alerts and information on traffic were being captured on Snorby.

short:NULL N/A 10.3.40.16 N/A 172.29.0.3 Snort Alert [1:1000002:1] 7:37 PM

IP Header Information

Perform Mass Classification Event Export Options Permalink

Source	Destination	Ver	Hlen	Tos	Len	ID	Flags	Off	TTL	Proto	Csum
10.3.40.16	172.29.0.3	4	5	0	40	48079	0	0	127	6	25037

Signature Information

Generator ID	Sig. ID	Sig. Revision	Activity (13038/13564)	Category	Sig Info
1	1000002	1	96.12%	N/A	Query Signature Database View Rule

TCP Header Information

Src Port	Dst Port	Seq	Ack	Off	Res	Flags	Win	Csum	URP
57842	80	1335335654	3420109927	5	0	16	513	31389	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](#)

Recommendations

Based on the findings, it is recommended to:

- Configure monitoring rules to alert any suspicious ongoing traffic.
- Regularly educating or conducting training to inform users the importance of
- Perform regular testing to ensure that rules and alerts are being accounted for.
- Ensure Snorby is configured and connected to the system to capture any forwarding alerts detected