TDX ARENA

Certification Report

TDX ARENA

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 hacktivists were creating a global campaign against the country. A simulated security challenge was created to aim at preempting the hacktivist 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

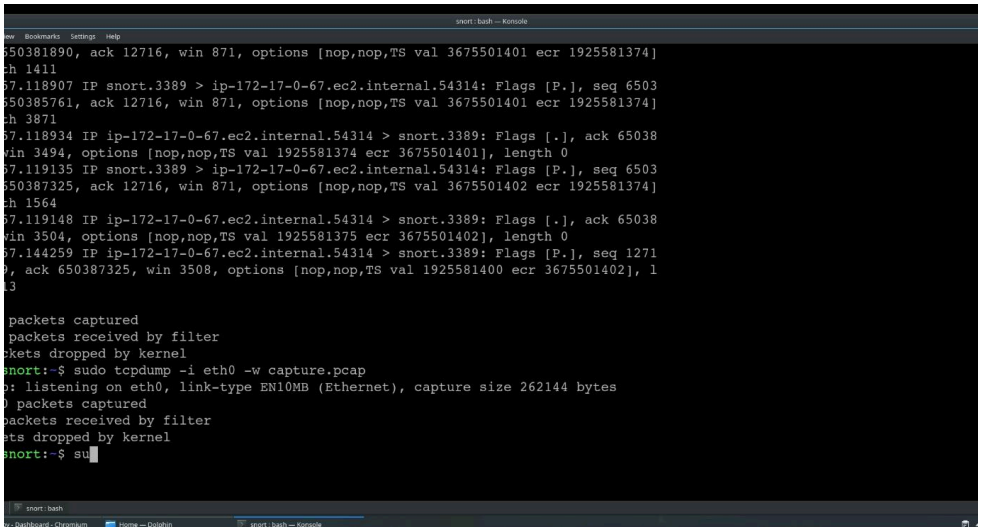
Tools and Technologies Used

- **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.

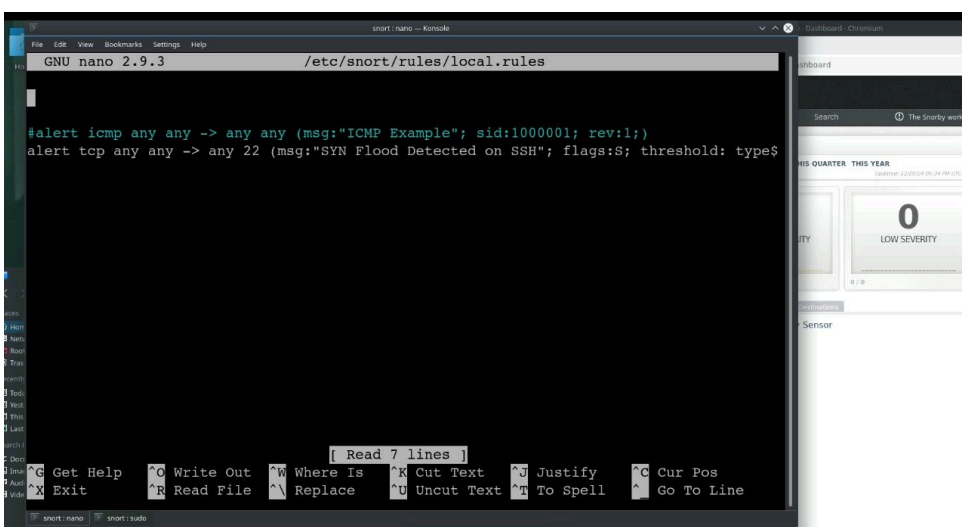
Investigation Process

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

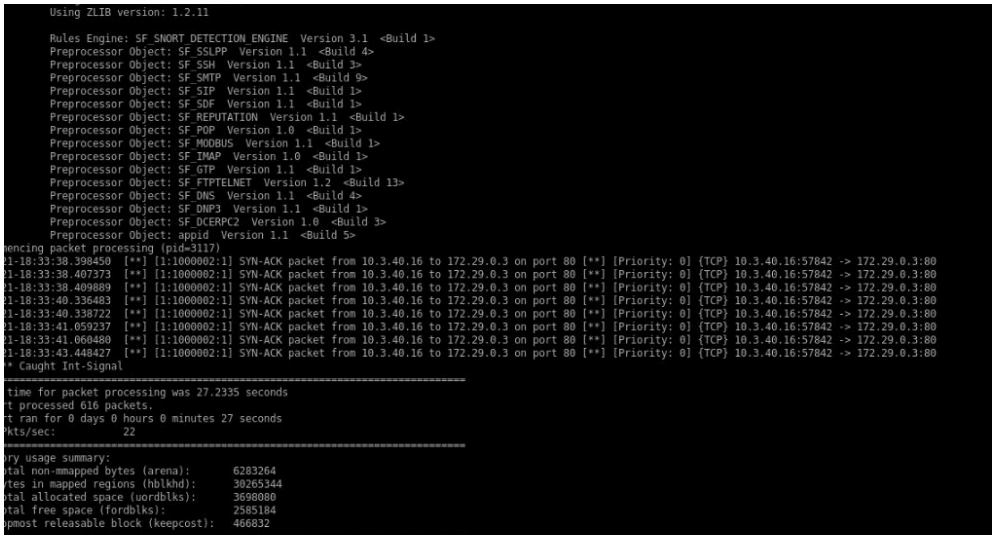
1. I started by doing a TCPdump and capturing them to look through and analyze for any anomalies on incoming traffic.



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



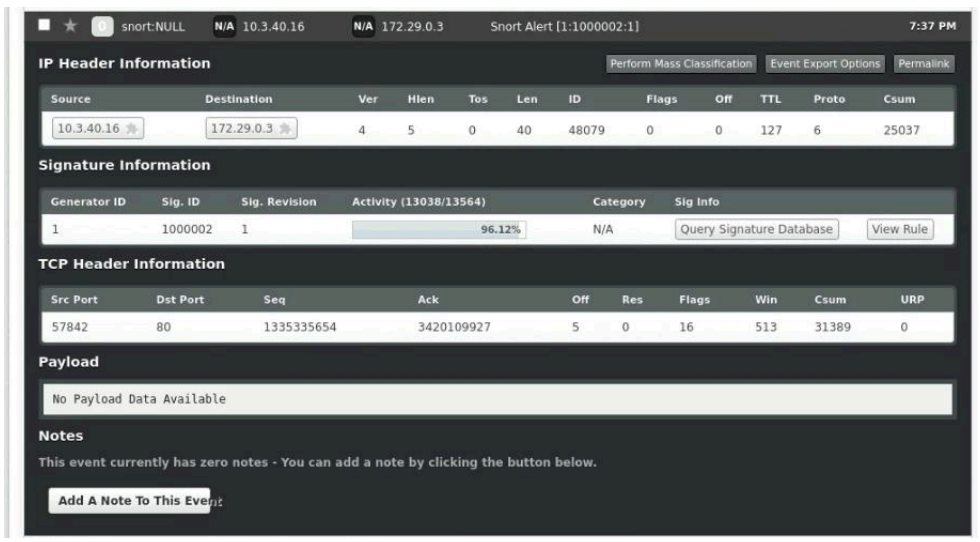
3. After setting the rule alert, all malicious packets were being identified.



```
        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_SDF  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_MODBUS  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_DNP3  Version 1.1  <Build 1>
        Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
        Preprocessor Object: appid  Version 1.1  <Build 5>
encing packet processing (pid=3117)
1-18:33:38.398450  [**] [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
1-18:33:38.407373  [**] [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
1-18:33:38.409889  [**] [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
1-18:33:40.336483  [**] [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
1-18:33:40.338722  [**] [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
1-18:33:41.059237  [**] [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
1-18:33:41.060480  [**] [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
1-18:33:43.448427  [**] [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
===============================================================================
ry usage summary:
tal non-mmapped bytes (arena):       6283264
tes in mapped regions (hblkhd):      30265344
tal allocated space (uordblks):      3698080
tal free space (fordblks):           2585184
pmost releasable block (keepcost):   466832
```

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



Recommendations

Based on the findings, it is recommended to:

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