M. Kaan Arici 16.12.2024
Mandatory 2.3 - Suricata Rules

Overview

This exercise focuses on creating and testing custom Suricata IDS rules to detect potential network threats, such as the downloading of specific files, unauthorized authentication attempts, and SYN flood attacks.

1. **Creating a Rule to Detect ncat.exe Download** Created a custom Suricata rule to detect the downloading of ncat.exe from http://www.kallas.dk/ncat.exe.

   alert http any any -> any any (msg:"DABE Possible disallowed tool: ncat"; content:"ncat.exe"; http_uri; nocase; sid:7000003; rev:2;)

   This rule checks if any ip from any source checks if the payload of an HTTP packet has ncat.exe in it and gives a warning.

2. **Creating a Rule to Detect Basic Authentication Attempts** Designed a rule to detect basic authentication attempts from the homenet to http://www.kallas.dk, using a test URL https://kallas.dk/basic.php.

   alert http $HOME_NET any -> 165.232.77.195 any (msg:"Homenet attempted login to kallas.dk";http_method; content:"GET";http.header; content:"Authorization"; sid:7000004; rev:1;)

   This rule checks if any from the home net tries to sign in at kallas.dk, it checks if it's a post request and /basic.php to check if the user is actively trying to sign in. Flow just adds that the post request should come from the client trying to sign into kalls.dk.

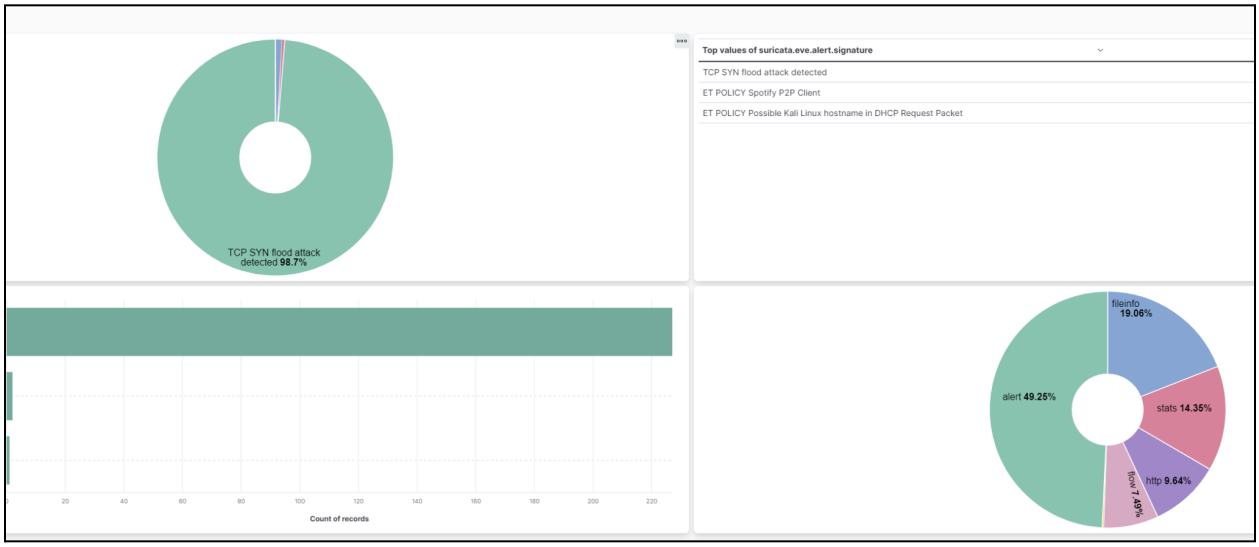
3. **Analyzing and Testing TCP SYN Flood Rule** Analyzed a Suricata rule meant to detect a TCP SYN flood attack, tested it with a Scapy flood, and modified the rule as needed to ensure it effectively detected the attack.

   a. Original:

   alert tcp any any -> 192.168.238.2 any (msg:"TCP SYN flood attack detected"; flags:S; threshold: type threshold, track by_dst, count 20 , seconds 60; classtype:denial-of-service;priority:5 ;sid: 7000100; rev:1;)

Explanation:

- This rule looks for TCP packets with the SYN flag set (flags:S).
- The threshold option means the rule will trigger only if 20 packets are seen within 60 seconds, tracking by destination IP (track by_dst).
- The rule alerts for Denial-of-Service (DoS) attack behavior, classified in classtype as denial-of-service (DOS).
- The priority:5 overrides any default priority set by the class and assigns input priority.



b. <u>Updated IP Range:</u>

alert tcp any any -> 192.168.106.2 any (msg:"TCP SYN flood attack detected"; flags:S; threshold: type threshold, track by_dst, count 20 , seconds 60; classtype:denial-of-service;priority:5 ;sid: 7000100; rev:2;)

This version of the rule updates the destination IP to my router's IP (192.168.106.2).

c. <u>Usage of Flags:</u>

alert tcp any any -> 192.168.106.2/24 any (msg:"TCP SYN flood attack detected"; tcp.flags:S; threshold: type threshold, track by_dst, count 20 , seconds 60; classtype:denial-of-service;priority:5 ;sid: 7000100; rev:3;)

This rule now includes proper flag usage, with tcp.flags:S to explicitly look for the SYN flag in TCP packets. It also triggers alerts for any source IP within my network, targeting the router's IP range (192.168.106.2/24) on any destination port.