HY436 - Software Defined Networks
Assignment 4
Christos Papastamos csd4569

Overview

For the fourt assignment I ran an instance of Artemis using a custom configutation file (code can be found below) to suit the assignment's needs. In the config file there is a prefix watched (snd_assignment4) which is requested from the assignment. The source AS (sdn_assignment4_asn) and the neighbor AS (sdn_assignment4_neighbor) are also set up and a rule connecting ASes and prefixes is present too. Also a monitor is setup according to the basic config file from the git repository

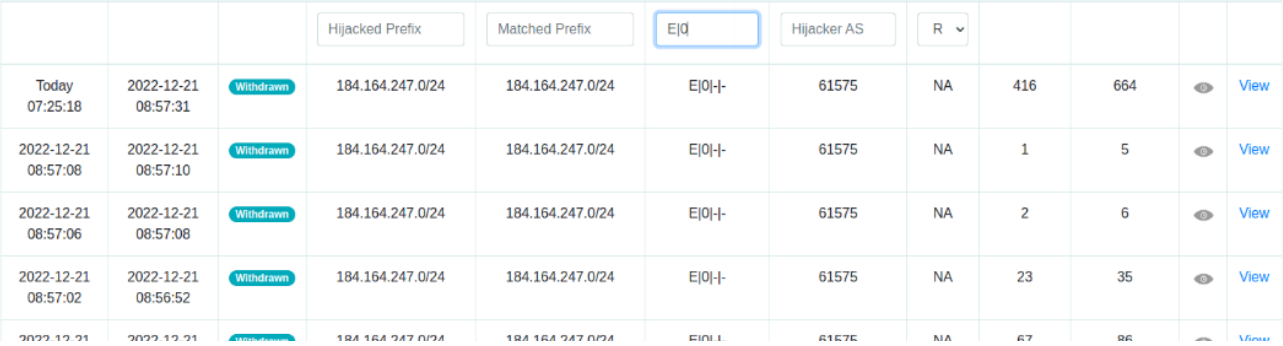
Configuration File:

```
#
# ARTEMIS Configuration File (HY436 Assignment4)
#
# Start of Prefix Definitions
prefixes:
  sdn_assignment4: &sdn_assignment4
  - 184.164.247.0/24
# End of Prefix Definitions

# Start of ASN Definitions
asns:
  sdn_assignment4_asn: &sdn_assignment4_asn
  - 61574
  sdn_assignment4_neighbor: &sdn_assignment4_neighbor
  - 47065
# End of ASN Definitions

# Start of Monitor Definitions
monitors:
  riperis: ['']
  bgpstreamlive:
  - routeviews
  - ris
  bgpstreamkafka:
    host: bmp.bgpstream.caida.org
    port: 9092
    topic: '^openbmp\.router--.+\.peer-as--.+\.bmp_raw'
  bgpstreamhist: '/etc/artemis/'
# End of Monitor Definitions

# Start of Rule Definitions
rules:
- prefixes:
  - *sdn_assignment4
  origin_asns:
  - *sdn_assignment4_asn
  neighbors:
  - *sdn_assignment4_neighbor
  mitigation: manual
# End of Rule Definitions
```

Results

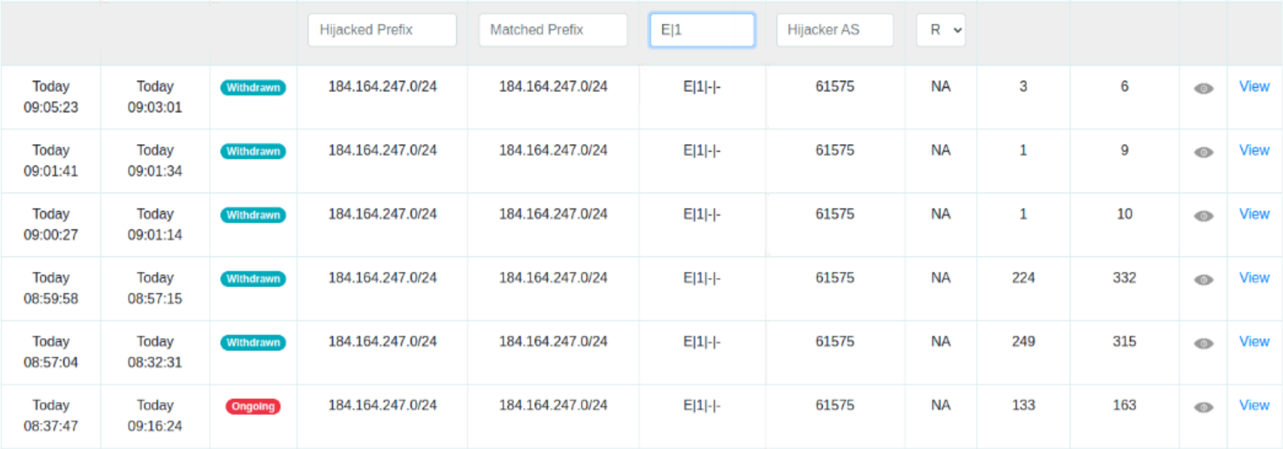
In the screenshots included below are the hijacks found by Artemis. In total two types of hijacks were picked up by my implementation, E|0|-|- and E|1|-|-. E|0|-|- means that there was a hijack for the exact prefix (sdn_assignment4) with an illegal origin. E|1|-|- means that there was a hijack for the exact prefix (sdn_assignment4) with a legal origin but an illegal first hop. In the second screenshot an ongoing hijack can also be noticed!

E|0|-|- hijacks:



			Hijacked Prefix	Matched Prefix	E|0	Hijacker AS	R				
Today 07:25:18	2022-12-21 08:57:31	Withdrawn	184.164.247.0/24	184.164.247.0/24	E|0|-|-	61575	NA	416	664	👁	View
2022-12-21 08:57:08	2022-12-21 08:57:10	Withdrawn	184.164.247.0/24	184.164.247.0/24	E|0|-|-	61575	NA	1	5	👁	View
2022-12-21 08:57:06	2022-12-21 08:57:08	Withdrawn	184.164.247.0/24	184.164.247.0/24	E|0|-|-	61575	NA	2	6	👁	View
2022-12-21 08:57:02	2022-12-21 08:56:52	Withdrawn	184.164.247.0/24	184.164.247.0/24	E|0|-|-	61575	NA	23	35	👁	View
2022-12-21	2022-12-21	Withdrawn	184.164.247.0/24	184.164.247.0/24	E|0|-|-	61575	NA	67	86	👁	View

E|1|-|- hijacks:



			Hijacked Prefix	Matched Prefix	E|1	Hijacker AS	R				
Today 09:05:23	Today 09:03:01	Withdrawn	184.164.247.0/24	184.164.247.0/24	E|1|-|-	61575	NA	3	6	👁	View
Today 09:01:41	Today 09:01:34	Withdrawn	184.164.247.0/24	184.164.247.0/24	E|1|-|-	61575	NA	1	9	👁	View
Today 09:00:27	Today 09:01:14	Withdrawn	184.164.247.0/24	184.164.247.0/24	E|1|-|-	61575	NA	1	10	👁	View
Today 08:59:58	Today 08:57:15	Withdrawn	184.164.247.0/24	184.164.247.0/24	E|1|-|-	61575	NA	224	332	👁	View
Today 08:57:04	Today 08:32:31	Withdrawn	184.164.247.0/24	184.164.247.0/24	E|1|-|-	61575	NA	249	315	👁	View
Today 08:37:47	Today 09:16:24	Ongoing	184.164.247.0/24	184.164.247.0/24	E|1|-|-	61575	NA	133	163	👁	View