University of Crete
Computer Science Department
Lecturer: Prof. X. Dimitropoulos
TAs: E. Papadogiannaki, A. Shevtsov,
M. Lakiotakis, A. Hatzivasileiou
Authors: V. Petropoulos, A. Kornilakis

Fall Semester 2022
CS436 - Software Defined Networks
Tasks of **Assignment 4**
Assigned: 08 December 2022
Due: 23 December 2022, 23:59

Assignment 4

Introduction

In this exercise, you will learn about the open-source tool ARTEMIS [9]. ARTEMIS implements a defense approach against BGP prefix hijacking attacks. It is (a) based on accurate and fast detection operated by the AS itself, by leveraging the pervasiveness of publicly available BGP monitoring services, and (b) it enables flexible and fast mitigation of BGP hijacking events.

You will understand how to use ARTEMIS to monitor a network and detect various types of BGP prefix hijacking attacks against this network. The TAs will use the PEERING testbed [8] to advertise a real-world network and conduct BGP hijacking against that network. You will use ARTEMIS to detect and report these events.

This exercise aims to understand the installation and configuration process of ARTEMIS, and use the tool to monitor a network and identify possible BGP prefix hijacking incidents against it. You will get hands-on experience using a tool that is currently operated to monitor and protect large networks across the world.
More details on creating and submitting your report and other deliverables will be provided later in the instructions. Make sure that you follow each step carefully.

ARTEMIS

How to Install

ARTEMIS is built as a multi-container Docker application. Follow the detailed (step-by-step) instructions at ARTEMIS GitHub repository to install and set up a containerized copy of the ARTEMIS tool on your local Linux machine (or on a Linux Virtual Machine in case you don't have Linux installed on your system) using the docker-compose utility.

Important: The *minimum technical requirements* for running ARTEMIS are:

- CPU: 4 cores
- RAM: 4 GB
- HDD: 50 GB free space (in most cases 20-30 GB may suffice)
- OS: Ubuntu Linux 16.04+ (other Linux distributions will work too)

The instructions given at the ARTEMIS GitHub repository are for installation in a Linux distribution. In case you don't have Linux (preferably Ubuntu) installed on your system, you can create a Virtual Machine on VirtualBox [5, 6].

Assignment

Our Network/PEERING Testbed

For this assignment, we have requested an IPv4 prefix from the PEERING testbed [8].
PEERING testbed is a system that provides safe and easy access for researchers and educators to the Internet's BGP routing system. PEERING is connecting (via BGP) with real networks at universities and Internet exchange points around the world, and gives us the ability to run experiments and announce our prefix directly with these networks.
The IPv4 prefix **184.164.247.0/24** and the **ASN 61574** were granted to us for use with the 4th assignment. Our network has one peer/neighbor with ASN 47065.
TAs will administer (announce and/or hijack) the IPv4 prefix during the assignment.

Configure ARTEMIS

After installation, you have to configure ARTEMIS to monitor our ASN and IPv4 prefix. In order to configure and control ARTEMIS, you can use the Web Application[3], and you can access it at localhost using the default credentials:

```
email: admin@admin.com
password: Adm!n1234
```

By default, ARTEMIS is configured to monitor FOTRH's network. You have to modify the ARTEMIS configuration file based on our network; you can find instructions on how to do so on the corresponding wiki page [1].
If you have configured ARTEMIS correctly, you will be able to observe the announcements/withdrawals of our IP prefix; also, you will be able to see the detected Hijacks. To record BGP hijacks, you have to let ARTEMIS run for a few hours. Finally, you should create one user (the username should contain your academic number (AM)) using the Web UI and give him admin rights.

Files to submit

After recording a few Hijacks against our network you should take screenshots with the details of different types of Hijacks and include them in your report and make some comments on each hijack type. Also, you should submit the JSON file containing the *Hijack table* data, as well as the JSON file containing the *BGP updates table* data - there is a 'DOWNLOAD TABLE' button above each table. Finally, you should also submit a copy of your configuration file of ARTEMIS.

How to submit your report

Please submit your report as a PDF file (also submit the configuration file and the JSON files) using the TURNIN submission program [7]:

- Login to one of the CS department's systems.
- Create a folder named ask4.
- Place in ask4 the PDF report and other files that you want to submit.
- Use 'cd' to make the directory one level above ask4 your current working directory.
- Issue the following command:

```
turnin assignment4@hy436 ask4
```

The deadline for submission is: **December 23, 23:59**
Your report should answer all the related questions and include the wanted screenshots to get the full grade. Points will be subtracted for missing logs or incorrect reports. The penalty for late submission is 10% per day. The submitted code will be tested for plagiarism using plagiarism-detection software. Any attempt to plagiarize will be accordingly punished with a 0 grade. The exercise weight is 25% of the overall lab grade.

Debriefing

All the students who have submitted their report/logs are requested to attend the debriefing session, where a sample solution will be presented by the assistants and a discussion of the exercise will follow. The date of the debriefing session will be announced via announcement in Moodle forum.

Oral Exam

All the students who have submitted their reports/logs are requested to attend the oral exam session to present their solutions to the teaching assistants. A timeslot during the oral exam session will be assigned to each student using Doodle.

Attention:

- **Each student will only be examined during the timeslot assigned.**
- **During this session, both Assignments 3 and 4 will be examined.**
- **Both the timely submission and the oral exam session will contribute to the grading of the assignment.**

Asking for help

For any issues you may encounter regarding the exercise, please ask the teaching assistants during the exercise sessions (14:00-16:00) on 08/12, 15/12 and 22/12, or post your question on Moodle forum.
Before contact, please make sure that you have formulated your question clearly and that you have already studied the ARTEMIS wiki [4] and the ARTEMIS installation guide tutorial [2] thoroughly.

Good luck!

References

[1] Artemis Configuration . https://bgpartemis.readthedocs.io/en/latest/basicconf/.

[2] Artemis GitHub repository. https://github.com/FORTH-ICS-INSPIRE/artemis#how-to-install-and-setup.

[3] Artemis Web Application . https://bgpartemis.readthedocs.io/en/latest/webapp/.

[4] Artemis Wiki. https://bgpartemis.readthedocs.io/en/latest.

[5] Creating a New Virtual Machine in VirtualBox. https://docs.oracle.com/cd/E26217_01/E26796/html/qs-create-vm.html.

[6] Creating a New Virtual Machine in VirtualBox. https://medium.com/dfclub/create-a-virtual-machine-on-virtualbox-47e7ce10b21.

[7] Turnin User Guide. https://medium.com/dfclub/create-a-virtual-machine-on-virtualbox-47e7ce1

[8] Brandon Schlinker, Todd Arnold, Italo Cunha, and Ethan Katz-Bassett. PEERING: Virtualizing BGP at the Edge for Research. In *Proc. ACM CoNEXT*, Orlando, FL, December 2019.

[9] Pavlos Sermpezis, Vasileios Kotronis, Petros Gigis, Xenofontas Dimitropoulos, Danilo Cicalese, Alistair King, and Alberto Dainotti. Artemis: Neutralizing bgp hijacking within a minute. *IEEE/ACM Trans. Netw.*, 26(6):2471–2486, dec 2018.