**CYT245 Assignment 2. Exploratory Data Analysis of IP addresses**

**Individual work.**

**This Assignment is based on materials from Chapter 4 of the book “Data-Driven Security”. We are not able to run the code because the code posted is made on R. However, we still are able to run some actions with the tools, and learn the methods implemented with the code. You should work on the materials provided in the Chapter and answer the following questions.**

**Objectives:**

* **Learn often used operations performed by security professionals on IP addresses in order to obtain better data feeds for the analysis**
* **Learn additional sources of external trusted data feeds you can utilize in your work with IPs.**

**Task 1. Read the Chapter 4 materials and answer the following questions – 1%**

1. **Why would you need to convert dotted-decimal presentation of IP address to integer form?**
2. **Why would you need to do segmenting, or grouping, of IP addresses?**
3. **Explain CIDR prefix format.**
4. **Explain what is AS and ASN. How it can be useful for segmenting or grouping task?**
5. **Play with** [**https://www.maxmind.com/en/home**](https://www.maxmind.com/en/home)**. Describe the value of the services and data provided (you are not supposed to buy anything there, just go through description)**
6. **Why would you need to augment IP address data?**
7. **Play with** [**www.iana.org**](http://www.iana.org)**. Describe what kind of information you can obtain from this service.**

**STOP reading at the point when you see the title “Association/Correlation, Causation, and Security Operation Center Analysts Gone Rogue”**

**Task 2. Implement the following Use Case – 2%**

**Context: You are security analyst of the AAA company, and you are given the task to do analysis of IP addresses associated with the threat alert.**

**Your actions:**

1. **Connect to AlienVault site and retrieve certain network indicators (individual and CIDR)**

[**https://otx.alienvault.com/pulse/642d624ccd3a7cca31c9e252?utm\_userid=tato1234&utm\_medium=InProduct&utm\_source=OTX&utm\_content=Email&utm\_campaign=new\_pulse\_from\_following**](https://otx.alienvault.com/pulse/642d624ccd3a7cca31c9e252?utm_userid=tato1234&utm_medium=InProduct&utm_source=OTX&utm_content=Email&utm_campaign=new_pulse_from_following)

You see the list of IOCs associated with this threat. Work on Network IOCs only (ignore FileHashs). Open Details and see information related to network – observe IPs, domain names, ASN, country.

To document your result, download IOCs in csv format, and extend the structure with additional columns IPadress, Location, ASN, nameservers.

P.S. Version of csv file is enclosed into the Assignment 2 task on BB.

1. **Obtain geolocation of via Maxmind services and compare the versions of geolocation (from AlienVault and MaxMind).** 
   * [**http://freegeoip.net**](http://freegeoip.net)
   * [GeoIP2 Web Service Demo | MaxMind](https://www.maxmind.com/en/geoip2-precision-demo)

**Comment on your observations. Include comparison of the results obtain from all sources of information you worked.**

1. **Report the results:**
   * **Make screenshots of the steps 1 and 2 implementations.**
   * **Provide your comments.**

**END of the Assignment Workflow**

**Submission includes:**

* **MS Word document uploaded to the BB. Include 0-screen as the proof of ownership. The name of the document must follow Submission Upload Requirements (see below).**
* **Answers to the questions from Task1**
* **Screenshots and comments for the actions 1 and 2, Task 2**

**Submission Upload Requirements**

Make online submission to BB, only one submission from your team.

If you have more than one document, wrap it up to ZIP, 7ZIP, or RAR folder

Name the file you will uploading as indicated below. The name must include:

* Course ID (CYT245)
* Section
* What is this (e.g. lab1, assignment 1, etc )
* Author(s) by name(s)

**Sample: CYT245MLab1\_PeterJohnMohammadSue**

**Note: submissions that do not follow the requirements will not be accepted**