**CYT245 Assignment 6 winter 2024 - 4%**

**Individual work**

Objectives: learn practical steps of using YARA by utilizing rules from the repository.

* <https://yara.readthedocs.io/en/latest/>

Your task is to follow the steps as described and perform them on your own computer. The list of steps include:

* Installing YARA
* Getting a set of rules to use
* Download a specific rule file
* Running YARA

Stop at this step, do not proceed to the section “How to write your own YARA rule”.

As usual, make screenshots to demonstrate your work and put them into MS Word document. Include Screen 0 and your comments.

**Task 1. Install Yara – 1%**

[**https://medium.com/bugbountywriteup/intro-to-malware-detection-using-yara-eacab8373cf4**](https://medium.com/bugbountywriteup/intro-to-malware-detection-using-yara-eacab8373cf4)

Follow the workflow from the article and install Yara on your computer.

**Task 2. Work on Yara rules available at github**

Step1 – 1%.

Go to

[rules/CVE-2018-4878.yar at master · Yara-Rules/rules · GitHub](https://github.com/Yara-Rules/rules/blob/master/cve_rules/CVE-2018-4878.yar)

Consult YARA documentation and write the comment to this YARA rule, which is one of the CVE set of rules. Describe in details what kind of filtering is established by this rule.

Include your comments into MS Word document.

Step 2 – 1%. Do the same for

[rules/EMAIL\_Cryptowall.yar at master · Yara-Rules/rules · GitHub](https://github.com/Yara-Rules/rules/blob/master/email/EMAIL_Cryptowall.yar)

Consult YARA documentation and write the comment to this YARA rule, which is one of the email set of rules. Describe in details what kind of filtering is established by this rule.

Include your comments into MS Word document.

Step 3 – 1%. Work with Yara documentation to see in more details how to run the rules:

[Running YARA from the command-line — yara 4.2.1 documentation](https://yara.readthedocs.io/en/latest/commandline.html)

Following recommendations, run the downloaded Cryptowall rule against any file with a suitable content.

Make screenshots, comments, and include into MS Word document.

**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)
* What is this (e.g. lab1, assignment 1, etc )
* Author’s name

**Sample: CYT245Lab1\_Peter**

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