**MALWARE ANALYSIS TOOLS AND TECHNIQUES**

**PRACTICAL TEST 2**

|  |  |  |
| --- | --- | --- |
| **Name** |  | **Date:**  26 Jan 2023  **Duration:**  1.5 hours |
| **Student ID** |  |

**Instructions**

1. This is a closed book test, however students are allowed to bring in and refer to ONE printed or handwritten A4 page with necessary details relevant to his test.
2. Students need to turn on “Airplane Mode” on their laptops and remember to continuously “save” the downloaded document while they are filling it up with their answers. Connecting to the Internet at any point during the test is considered cheating.
3. Extract the following archives on to the desktop. The password for the malwares is "malware" (without the quotes)

* Web.zip
* Document.zip

1. This paper is 60 Marks.
2. Submission of the answers document is via POLITEMall Assignment submission. Permission must be taken before connecting the host OS to the Internet to upload the answer document. Name of the word document must be in the following format: P0X\_StudentFullName\_MATTPT2.docx

**Question 1 (25 marks)**

1. Briefly describe the steps to analyse web.html. Provide detailed screenshots as evidence for each of the steps.

(15 marks)

Hint: Using the SciTE Text Editor’s search option, you will notice more than one occurrence of document.write() instructions, try to deofuscated as much code as you can.

1. List down and briefly explain important network and/or host-based indicators found in web.html

(10 marks)

**Question 2 (30 marks)**

1. Briefly describe the steps to analyse Document.docm. Provide screenshots as evidence for each of the steps, including usage of strings2 and SSview tools.

(15 marks)

1. Examine the extracted macro and briefly describe the nature of the malicious code by indicating any host/network-based indicators if any.

(10 marks)

1. Use the provided document\_extract.py open this .py file in a Text Editor, study and understand it and know how to use it. Then analyse the output generated by this .py file using BinText. List down and justify 5 interesting strings.

(10 marks)