CS 6345 – Digital Forensics

Assignment-1

Stage-2

Ravi Sankar Gogineni-R117788968

Your job is to investigate the content of a given malicious pdf file. Using the PDF analyzing tools offered by the REMnux tool, spider monkey, sctest, or PDF Stream Dumper, address the following questions/activities:

1. Report the number of objects in the file.

2. Determine whether the file is compressed or not.

3. Determine whether the file is obfuscated or not.

4. Find and Extract JavaScript.

5. De-obfuscate JavaScript.

6. Extract the shell code.

7. Create a shell code executable

8. Analyze shell code and determine what is does or even execute it using sctest or spider monkey. 9. What is the secret code?

**Answers:**

The stage 2 of the assignment is executed using pdf stream dumper.

1. Report the number of objects in the file.

**Answer:** The number of objects in the file are **38**

Graphical user interface, text, application, email

Description automatically generated

1. Determine whether the file is compressed or not.

**Answer:** Yes, the file is compressed. As there are filters in the given pdf file (analyzed using pdf stream dumper), we can say that the file is compressed.

Graphical user interface, application, Word

Description automatically generated

1. Determine whether the file is obfuscated or not.

**Answer**: Yes, the file is obfuscated. As the header contains the launch action, we can write that the file is obfuscated.

Graphical user interface, text, application, email

Description automatically generated

1. Find and Extract JavaScript.

**Answer**: The extract JavaScript is shown below.

Graphical user interface, text, application, email

Description automatically generated

1. De-obfuscate JavaScript.

**Answer:** The De-obfuscated JavaScript is shown below:

Graphical user interface, text, application, email

Description automatically generated

1. Extract the shell code.

**Answer:** The extracted shell code is:

Graphical user interface, text, application

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

1. Create a shellcode executable.

**Answer**: The created shellcode is shown below:

Graphical user interface, application

Description automatically generated

Graphical user interface, text

Description automatically generated

1. Analyze shell code and determine what is does or even execute it using sctest or spider monkey.

**Answer**: Before the execution of shell code, we got the data as Ip address, I-port or mac address etc. But due to the change of shell code we get an error.

Graphical user interface, text

Description automatically generated

1. What is the secret code?

**Answer**: The secret code is hocuspocus.

Graphical user interface, text, application, email

Description automatically generated