Week 3 Activity

Background

This week's activity is in three parts:

- Parts 1 and 2 are assessable and to be started during your tutorial/lab session.
- Part 3 is optional and not assessed.

Part 2 is based on training scenarios produced by George Mason University and made available as Digital Corpora[1] under a National Science Foundation grant.

Part 1

Activity

During the Week 3 Lecture, we saw how Volatility can be used to examine a memory dump. Repeat the cridex exercise for yourself. Make contemporaneous notes and take copies as needed e.g. screenshots, output text files.

Try to complete the activity in tutorial/labs. You may complete the report at home.

Materials

Volatility framework (pre-loaded in Kali Linux and COMP6445 Win10 image)
cridex.mem memory dump (pre-loaded in Kali Linux and COMP6445 Win10 image)
Optional - BinText (if using Windows and pre-loaded on COMP6445 Win10 image)
Optional – You might want to experiment with graphviz (pre-loaded on COMP6445 Win10 image) to create diagrams

Instructions

See slides for Week 3 Lecture.

Assessment

Prepare a one-page report explaining the process. Use a short essay style (an expert report is not needed for this activity).

Marking

0.5 = complete and submit activity
up to 1 = Explanation is clear and simple for a lay reader
up to 1.5 = Uses clear diagrams to explain the linkages e.g. between named processes using their Process ID (PID) and Parent Process ID (PPID)

[1] https://digitalcorpora.org/

Part 2

Activity

The Bulk Extractor tool is available on the COMP6445 Win10 image and the Kali Linux image. The file BEWorkedExamplesStandalone.pdf is on WebCMS (as well as on the Win10 image) and it was two worked examples. For this part, we will focus on the second worked example which starts on page 13 i.e. NPS DOMEX Users Image.

You may want to experiment more with Bulk Extractor at home.

Materials

Bulk Extractor (pre-loaded on COMP6445 Win10 image and Kali Linux)
The NPS DOMEX Users image is called nps-2009-DOMEXUSERS.E01 (pre-loaded in Kali Linux and COMP6445 Win10 image)

Stick to only the AES option for extraction during the lab (otherwise you will be waiting too long).

Assessment

Up to 0.5 marks = provide the output text file for the AES key
Up to 1 mark = provide evidence of other Bulk Extractor artefacts

Part 3 (optional)

This is a challenge activity and is not assessed. Can you extract the AES key from the NPS DOMEX image without using Bulk Extractor? Write up how you did this on the WebCMS blog for Week 3.