Homework 10

Incident Response / Memory Analysis
CIS 4930 / CIS 5930
Offensive Computer Security
Spring 2014

Due 11:59PM Friday April 25
Electronic turn in (Turn in via email to: redwood@cs.fsu.edu)
The email must be titled in the following format:
[OCS2014] hw10 <your last name>
(where <your last name> is your last name)
i.e.: [OCS2014] hw10 redwood

LATE SUBMISSIONS WILL NOT BE ACCEPTED

Worth: 100 points

Overview

You are expected to download and install the volatility (2.1 or 2.2) framework (either on your host machine, or in a virtual machine). You will also need your hands on a linux system (preferably virtual machine). The easiest (to work with) route would be to take a debian distro of your choice (ubuntu, backtrack 5R3, etc...) and follow the respective instructions at https://code.google.com/p/volatility/wiki/VolatilityIntroduction?tm=6

Otherwise for windows users, the standalone installer at https://code.google.com/p/volatility/downloads/list should work decently. But you'll still need access to a linux system for many of these tools - so it will just double your work.

You will also need IDA.

Related Help / Tutorial:

If you'd like to get some practice with an already solved challenge using volatility, see http://www.honeynet.org/challenges/2010_3_banking_troubles. There is a great writeup which will provide you a nice guide/how-to-reference for this rest of this homework : http://honeynet.org/files/Forensic_Challenge_3_-_Banking_Troubles_Solution.pdf

Homework Files

Download from https://code.google.com/p/volatility/wiki/SampleMemoryImages

- zeus.vmem
- be2.vmem

Download from http://dougee652.blogspot.com/2011/04/malware-memory-images.html

- xp-clean.tgz
- xp-infected.tgz

Questions

Getting Started

Use the xp-clean.bin and the xp-infected.bin memory dumps with volatility to answer the following questions. This will be a good starting point as you will have a clean and infection state of a system to compare the outputs of the various volatility plugins you might use. For instance try the "malfind" plugin on both the clean and infection versions --- and you might notice that the tools/plugins are not perfect. In fact it is best to familiarize yourself with the documentation for each plugin:

- https://code.google.com/p/volatility/wiki/CommandReference22
- https://code.google.com/p/volatility/wiki/CommandReferenceMal22
- https://code.google.com/p/volatility/wiki/CommandReferenceRegistryApi22
- https://code.google.com/p/volatility/downloads/detail?name=CheatSheet_v2.3.pdf

1. [**5 points**] What new processes are there between xp-clean and xp-infected? (Ignore wind32dd)

2. [**10 points**] What connections have been opened between xp-clean and xp-infected (Give source => Dest IP info)? Which processes control these connections (Give PID, and process name if possible).

3. [**5 points**] One of the processes from part 2 might be closed. It is common for malware to move around on a system, so did this process spawn any new processes? If so provide details (PID + process name)

4. [**10 points**] Use procmemdump to dump this new process or processes. Then open up the dumped file in IDA (IDA demo 6 will work fine, and is free: https://www.hex-rays.com/products/ida/support/download_demo.shtml).
   What libraries is the process loading (give their names)?

5. [**5 points**] One of these libraries should be suspicious. List some of the shady functions that this process is importing from the suspicious dll.

6. [**15 points**] Dump all the dlls from the xp-infected.bin image and find the suspicious DLL mentioned in #5 (hint grep will be useful). From this dll answer the following with IDA:
   a. Does this dll export the same number of functions that the process that uses it imports from it?

   b. How many does it export?

   c. How many from this dll does the process from #4 import?

7. [**15 points**] Processes and even DLL's can load and unload DLLs on the fly. Functions from DLLs can be accessed either by their function string name, or by their ordinal. Now analyze the strings of this dll (as simple as running "strings" on the dll in linux) and answer the following:
   a. What crypto related functions does this dll seem to involve?

   b. What networking / connection related functions does this dll seem to involve?

Zeus:

Zeus is a particularly nasty and aggressive piece of malware. Answer the following questions with the vmem snapshot of a machine infected by zeus:

1. [**5 points**] What processes are current running in this snapshot?

2. [**10 points**] How many of those processes have been potentially infected by Zeus?

Black Energy (be2)

Black Energy is a notorious botnet tool (see http://threatpost.com/en_us/blogs/inside-black-energy-2-botnet-072110). Answer the following with the be2.vmem file:

1. [**10 points**] What are the open connections in this vmem file?

2. [**10 points**] What can you tell about the process or processes that the connections belong to? Does a bot always have to be connected to the botnet?