Hunting Malware with Volatility

About ME

- Attacker
- Defender
- Alphabet Soup = OSCP, MCSA, Security +, Net +, A +
- Blog: pentest-labs.org
- Twitter: @bostonlink
- I Script in Python and am learning Ruby =)
- Now for the good stuff

Rules of the presentation and demos

I don’t know everything therefore here are the rules =)

I have to drink if:

- I mess up a command
- I fat finger a command
- I WANT TOO =)

Volatile data

What is Volatile Data?

- Data that can be lost if live response/forensics is not done
- Includes:
  - Processes
  - Network Connections
  - Open Files
  - File Handles (Previously Open files)
  - ETC…

How can we obtain Volatile data?

- Live Response Procedures
  - Multiple Commands
  - Cmd.exe
  - Netstat –anbo
  - Sysinternal tools
  - Must pipe output into text files for further analysis
  - Text files are good but I want all volatile data for analysis =)
- Acquiring a memory dump for analysis has all volatile data stored within memory.
  - One command
  - Less time and one file to analyze

Why does my computer do this?

OR This – Depends on the subscription right!!

Or this?

Anti-Virus always works! Right?

And This

The 50/50 Battle – disk images are only half the battle!

Acquiring disk images for static analysis is only half the battle in malware analysis.

A memory image and disk image can give you the full picture of the state of the system you are analyzing.

What is volatility?

Volatility is an open-source collection of command line tools written in python, it is used for the extraction of digital artifacts (evidence) from volatile memory (RAM) images.

Using volatility you can:

- List all processes
- List existing and recently closed network connections
- List file handles
- Extract executable running
- Dump the addressable space for the process
- And many many more options

Image format support

- Raw Image of memory (DD, MEM)
- Windows crash dumps
- Hibernation files (Sleep mode or hibernation)

Volatility has the ability to output the contents of windows crash dumps and hibernation files to a raw image format such as dd.

Current Operating System Support

Windows:

- 32bit Windows XP Service Pack 2 and 3
- 32bit Windows 2003 Server Service Pack 0, 1, 2
- 32bit Windows Vista Service Pack 0, 1, 2
- 32bit Windows 2008 Server Service Pack 1, 2
- 32bit Windows 7 Service Pack 0, 1

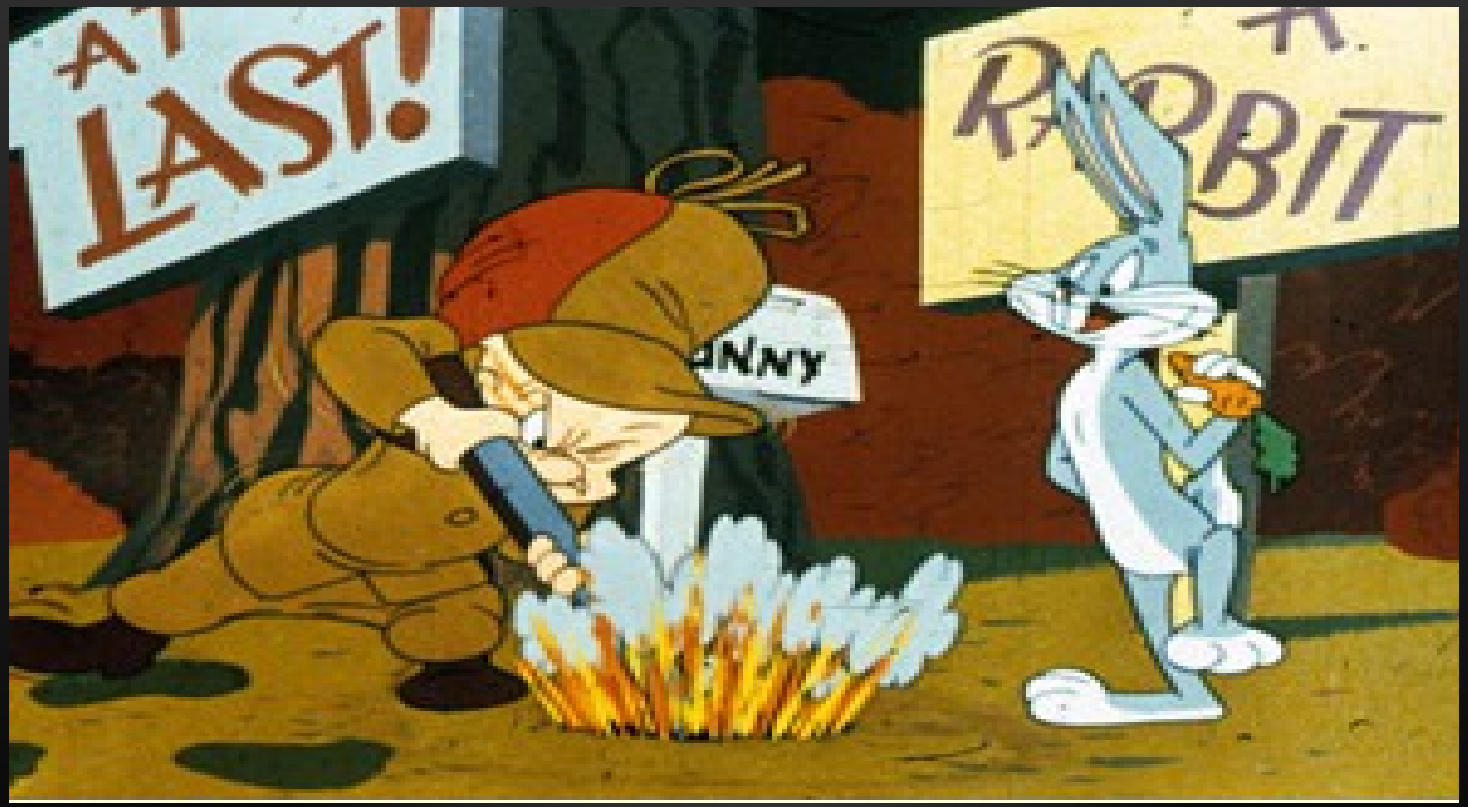
No Mac OSX, No Linux, But the developers are currently talking about supporting Linux memory images in the next release after 2.0.

Volatility can not

- Analyze 64bit images of RAM
- Acquire memory images (memory dumps)

That's about it =) It's a tool that is useful not a tool that does your job.

Feel like Elmer FUD!!



Did I mention the plug-ins?

- Volatility has the ability to easily script plug-ins (in python of course)
- Multiple plugins ship with volatility by default and provide basic memory analysis functionality.
- Since the project is open source the community actively develops new plugins.

A lot of Default Plug-INS =)

Malware.py plug-in

- Provides multiple plugins useful for malware identification and analysis.
- Actively developed by Michael Hale Ligh.
- Introduced in the Malware Analysts Cookbook
- We will use some of the plug-ins during demo time.

Then Elmer FUD turns into this

Uses of Malware.py

- Listing potentially malicious API Hooks (iat, inline, kernel)
- Listing processes that have malicious injections
- Malfind plug-in with yara integration – lists injections with known malware signatures
- Psxview finds hidden processes
- And More…….

API Hooking

hooking covers a range of techniques used to alter or augment the behavior of an operating system, of applications, or of other software components by intercepting function calls or messages or events passed between software components. Code that handles such intercepted function calls, events or messages is called a "hook".

No need for this because!!!!

- WE ALWAYS TRUST FIREWALLS
- WE ALWAYS TRUST ANTI-VIRUS
- WE ALWAYS TRUST IDS/IPS
- WE ALWAYS TRUST THOSE TRUSTY SIGNATURES

My Take on the statements above is

THIS ==➔

Anti-Virus always works! Right?

Demo time

References

- https://www.volatilesystems.com/default/volatility
- http://code.google.com/p/volatility/wiki/CommandReference
- http://code.google.com/p/malwarecookbook/source/browse/trunk/malware.py
- http://mnin.blogspot.com/

Questions??? See Below!! =)