CYBER502x Computer Forensics

Unit 4: Windows Forensic Acquisition

I: Windows Memory Acquisition and Analysis

Investigations in windows involves…

- Acquire the Evidence
- Preserve the Evidence
- Analyze the Evidence
- Report

Basic imaging steps

- Obtain volatile data (including RAM) if possible
- Image drives and removable media

Collect volatile data from Windows

- System Information
- Processes Information
- Network Information
- Logon users
- Clipboard contents
- Command History
- MAC Times

Commands to collect volatile data from Windows systems

Display system date and time	`date /T; time /T`
Display when was the system rebooted	`uptime`
Display system information	`psinfo`
Check whether the network interface is running in a promiscuous mode	`ipconfig`
Look for unusual processes and services	`tasklist /svc; psservices; pslist`
List currently loaded dlls	`listdlls;  process explorer;`
View open files	`psfile; openfiles`
Show network connections	`netstat; fport`
List logged in users	`psloggedon; logonsessions`
View clipboard contents	`pclip`
View logs	Windows Event Viewer

Helix3 from e-fense

- Helix3 Pro is a commercial tool, Helix (2009R1) version is free
- http://www.e-fense.com
- Operates in two different modes
  - In a windows live mode: collecting data from a live system
  - In a bootable CD mode: in-depth analysis of a dead machine

Memory forensics – why?

- Used by forensic investigators in
  - Malware detection
    - objects hidden by rootkits (processes, threads, connections etc.)
    - memory-resident malware
    - unpacked/unencrypted images
  - Password recovery
  - …

Physical Memory Acquisition

- Comae Memory Toolkit (formerly MoonSols Windows Memory Toolkit)
  - https://comae.typeform.com/to/XIvMa7
  - Includes DumpIt (win32dd + win64dd), hibr2bin, etc.
  - Can be launched from a USB thumb drive
- Open source physical memory acquisition tool

Other memory acquisition tools

- Host-based
  - winen.exe from Guidance Software
  - MemoryDD from ManTech
  - FTK imager from Access Data
  - Belkasoft Live RAM Capturer
- Remote
  - F-response by By Agile Risk Management LLC
  - FTK from Access Data

Memory Analysis tools

- WindowsSCOPE by WindowsSCOPE Cyber Forensic
- Redline/Memoryze from FireEye
- The Volatility Framework by the Volatility Foundation
- Rekall Memory Forensics Framework from Google
- Google Rapid Response (GRR)
- Cold boot attack by Princeton University

The Volatility Framework

- https://github.com/volatilityfoundation/volatility/wiki
- a Python-based toolkit can extract information from both Windows and Linux/Unix memory images
  - imageinfo, pslist, psscan, thrdscan, dlllist, modules, sockets, sockscan, connections, connscan, hivelist, malfind…
  - vol.py –f memfile imageinfo
  - Vol.py --profile=WinXPSP3x86 connscan –f memfile
  - Example: http://sketchymoose.blogspot.de/2012/11/memory.html

Other volatility plugins

- Cryptoscan
  - Based on “RAM is Key: Extracting Disk Encryption Keys From Volatile Memory” by Brian Kaplan,
  - Scans a memory image to recover TrueCrypt passphrases
  - vol.py --profile= WinXPSP3x86 cryptoscan –f memfile
- Suspicious
  - Displays the command line used in “suspicious” processes
- hivelist and hivescan
  - Finds hive offsets in memory images

Rekall Memory Forensics Framework

- Google's memory acquisition and analysis framework
  - For Windows, Linux, and Mac
- http://www.rekall-forensic.com/
- http://www.rekall-forensic.com/docs/Manual/tutorial.html

Google Rapid Response (GRR)

- GRR - GRR Framework
  - https://github.com/google/grr-doc
  - An incident response framework
  - Focus on remote live forensics
  - Using both Rekall and Sleuthkit
  - Client: python agent for Linux, OS X, and Windows
  - Server: Ubuntu Server 14.04 64-bit

GRR (Cont'd)

- GRR server sends action requests (flow or hunt) to clients
  - actions are blocks of code executed by the agent on the endpoint machine, then return the results
- Investigator initiates requests through the web-based GUI or the GRR console
  - OS-level and raw file system using SleuthKit
  - Memory acquisition and analysis using Rekall
- Communication between client and server using AES256 encryption

Cold boot attack

- Princeton researchers found that RAM isn't automatically erased when it no longer has power
- You can pull power first, and then reboot and grab the contents of RAM
- Tools - https://citp.princeton.edu/research/memory/code/
  - RAM imaging tools
    - Scraper.bin (in a usb),
    - Boot from this usb which dumps RAM to this usb

RAM imaging tools

- citp.princeton.edu/research/memory/code
  - Scraper.bin: A bootable image to dump the memory to a usb
  - Usbdump: Dump the RAM from the USB to your forensics system
  - Aeskeyfind and rsakeyfind: searches for AES keys ad RSA keys
- A small executable that you can boot
  - either from a USB disk
  - or over the network via remote network boot (PXE)
- It could be used to recover encryption keys
  - When machine is locked, suspend or hibernated

Memory anti-forensics

- Dementia (Dec. 2012)
  - modifies the memory dump of a machine in its acquisition mode.
  - defeats memory analysis on Windows OS by hiding operating system objects (processes)
  - http://events.ccc.de/congress/2012/Fahrplan/events/5301.en.html

Attention-deficit-disorder (ADD)

- Physical memory anti-analysis tool designed to pollute memory with fake artifacts
- Shmoocon 2014
- Proof of concept for Windows 7 SP1 x86
- https://code.google.com/p/attention-deficit-disorder/

Appendix

Commands to collect volatile data from Windows

psinfo

- www.sysinternals.com
- Can be run either locally or remotely
- Provide System Info
  - Type of installation
  - Install date
  - Kernel version
  - Service pack
  - Processors information
  - Registered organization and owner

Psinfo options

- -h: list installed hotfixes
- -s: list installed applications
- -d: display disk partition size, format and free space
- Psinfo –s > c:\forensicsInfo\sysinfo.txt
- Psinfo –s \\xx.xx.xx.xx

Running processes

- Processes Information
  http://technet.microsoft.com/en-us/sysinternals/bb896649.aspx
  - Psservices
  - Pslist
- Note: Do not reveal the presence of the rootkit or the other processes that the rootkit has hidden
- Identify specific services associated with the svchost process
  - Tlist.exe for Windows 2000
    - Tlist –s > c:\auditResult\tlist.txt
    - from the \Support directory of the Window 2000 installation CD-ROM
  - Tasklist /svc for Windows XP later
- Find a particular service based on process ID
  - Tasklist /FI “PID eq processID “

Currently loaded DLLs (From Sysinternals)

- ListDLLs
  - View the currently loaded DLLs for a process or all running processes
    - listdlls notepad.exe
- Process Explorer
- If processes are hidden, the DLLs will not shown

View open files

- The tools show files that are opened locally or remotely on a system
  - Handle
    - Shows the open files for all the running processes including the path to the file. It may reveal malicious processes.
  - net file, open shared files
  - psfile
    - http://technet.microsoft.com/en-us/sysinternals/bb897552.aspx
  - Openfiles
    - Windows builtin command
    - queries, displays, or disconnects files opened locally or by network users
    - http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/openfiles.mspx?mfr=true

Logged on users

- Psloggedon
  - Shows the name of the user currently logged on locally and remotely via a mapped share
  - www.microsoft.come/technet/sysinternals/systemInformation/psloggedon.mspx
- Net sessions
  - Show usernames that remotely login and their ip addresses
- Logonsessions
  - From sysIntermals
  - Shows all the active logon sessions on a system including who is logged on, when and what processes are running.
- Note:
  - All the above does not show the ones logged on via a backdoor.

Open ports

- Tools for external port scanning
  - **Nmap**
  - Foundstone's ScanLine (**sl.exe**)
    - `Sl –t 1-2999 –u 1-2999 –v –o c:\auditResult\sl.txt`
  - Foundstone's SuperScan
- Get a list of open ports through host (disable firewall temporarily)
  - **netstat** –ano
    - displays all connections and listening ports
  - Associate ports with particular services
    - Foundstone's **fport** (fport can not run against a remote machine)
    - diamondCS' **OpenPorts**

Network Status

- Ipconfig may provide this information
- Tools that tells whether the NIC is in promiscuous mode
  - Promiscdetect
  - Promqry
    - Can be run against remote systems

Event Log files

- Event logs for the system
  - SECEVENT.EVT
  - SYSEVENT.EVT
  - APPEVENT.EVT
- These files are written with a binary format
- Windows uses Event Viewer to read the log files.
- EnCase EnScript: Windows Event Log parser will also parse this files.

.EVT files

- SECEVENT.EVT
  - Stores security-related events, including failed login and attempts to access files without permissions.
- SYSEVENT.EVT
  - Stores system events functioning, for example, the failure of a driver or the inability of a service to start.
- APPEVENT.EVT
  - Stores application events such as databases, Web servers, User applications.