THE VOLATILITY FOUNDATION

Open Memory Forensics Workshop

SSID:

Chantilly, Virginia

November 4, 2013

EMPOWERING INVESTIGATORS

OMFW 2013

- 5th* Annual Open Memory Forensics Workshop
- Venue for advanced digital investigators
- Learn from pioneering researchers and practitioners
- The most exciting and important topics in DFIR
- 100% of the proceeds are donated to charity
- Encourage participation and discussions
- Lightening talks

OMFW Agenda 2013

1300PM	A State of Volatility, AAron
1330PM	Stabilizing Volatility, Ikelos
1400PM	Mastering TrueCrypt and Windows 8/Server Memory, MHL
1440PM	All Your Social Media are Belong to Volatility, Jeff
1500PM	Memory, Volatility, and Threat Intel Life Cycle, Steven and Sean
1530PM	Break
1545PM	Dalvik Memory Analysis and a Call to ARMs, Joe
1615PM	Bringing Mac Memory Forensics to the Mainstream, Andrew
1645PM	Memoirs of a Hindsight Hero: Detecting Rootkits in OS X, Cem
1715PM	Every Step You Take: Profiling the System, Gleeda
1745PM	Closing Comments/Reception

Volatility Development Team

- Core Developers:
  - Mike Auty (ikelos)
  - Andrew Case (attc)
  - Brendan Dolan-Gavitt (moyix)
  - Michael Hale Ligh (MHL)
  - Jamie Levy (gleeda)
  - AAron Walters (labarum)

Thank You!

- The Volatility Community (OOV)
  - Numerous research collaborators/testing/bugs
  - Academia, government, industry, law enforcement
  - Mailing lists, blogs, irc (#volatility)

Volatility 2.3: Highlights

- Mac
  - Mac support officially added to trunk (38 profiles)
  - 32-bit and 64-bit MachO address space support
  - Over 30+ new plugins
- Linux/Android
  - ARM address space support
  - 7 new Linux plugins:
    - linux_check_syscall_arm, linux_check_tty, linux_check_evt_arm, linux_keyboard_notifier, linux_yarascan, linux_volshell
- Address Spaces
  - Expanded virtualization support
    - VMWareSnapshotFile (vmsn, vmss), VirtualBoxCoreDumpElf64
  - Proprietary format support
    - HPAKAddressSpace
  - Metadata: vboxinfo, vmwareinfo, hpakinfo, hpakextract

Volatility 2.3: Highlights

- Windows
  - 14 New Plugins
    - privs - Identify the present and/or enabled windows privileges
    - iehistory - Extract and parse Internet Explorer history and URL cache
    - dumpfiles - Reconstruct memory mapped and cached files
    - unloadedmodules - Show recently unloaded kernel modules
    - shellbags – Shellbag information obtained from the registry
    - mbrparser - Scans for and parses potential Master Boot Records
    - mftparser - Scans for and parses potential MFT entries
    - timeliner - Timelines in body file format, excel spreadsheets, or text
    - dumpcerts - Extract SSL private and public keys/certs
    - poisonivyscan – Detect processes infected with Poison Ivy
    - poinsonivyconfig – Locate and parse the Poison Ivy configuration
    - zuesscan1 – Locate and decrypt Zeus > 1.20 and < 2.0 configs
    - zuesscan2 – Locate and decrypt Zeus >= 2.0 configs
    - citadelscan1345 – Locate and decryp Citadel 1.3.4.5 configs

Volatility 2.3: Highlights

- Windows Plugin Enhancements
  - apihooks: detects duqu style instruction modifications
  - crashinfo: displays uptime, systemtime, and dump type
  - psxview: includes process listings from the GUI APIs
  - svcscan: queries the cached registry for service dlls
  - dlllist: distinguishes static and dynamic loaded dlls
  - screenshot: shows text for window titles

Volatility Roadmap

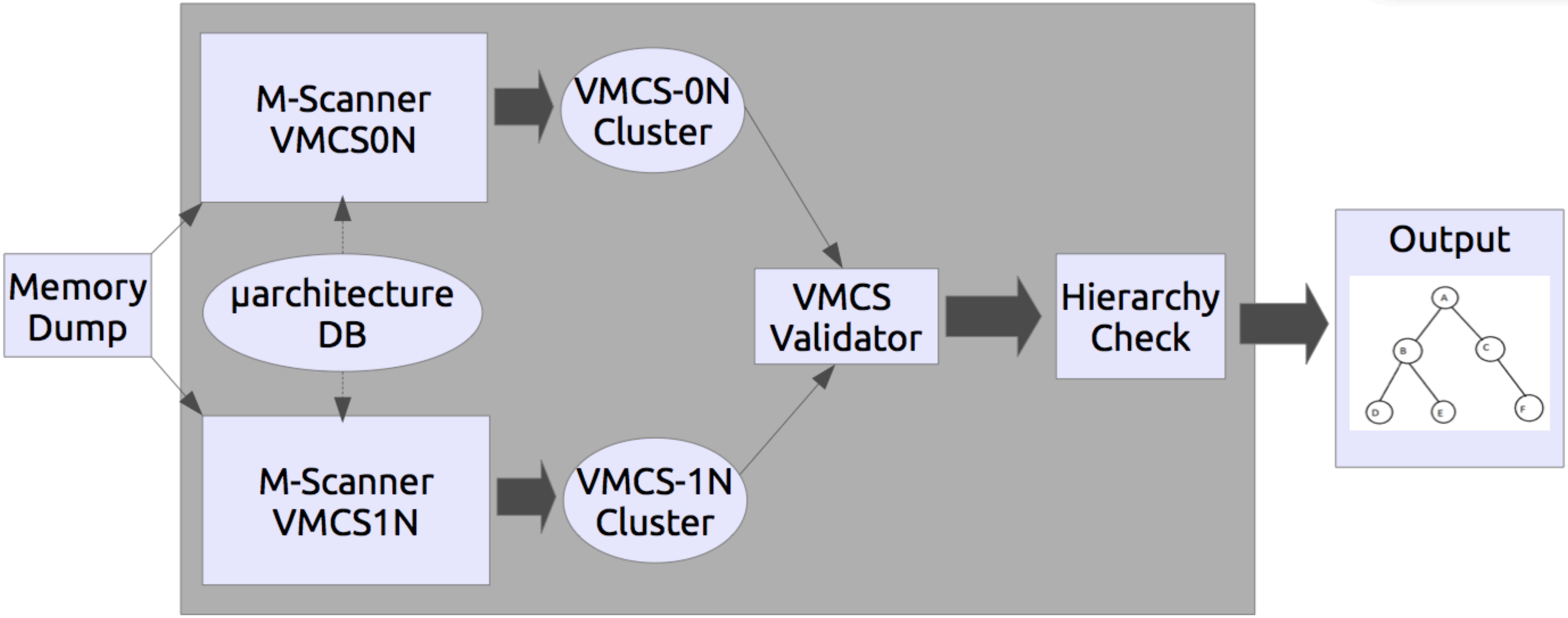
- Volatility Wiki:
  - https://code.google.com/p/volatility/wiki/VolatilityRoadmap
- Volatility 2.4 (April 2014)
  - Window 8/Server 2012
  - Mac 10.9/Mavericks
  - Pool scanner updates
- Volatility 3.0 (2014)
  - "Big Changes": Refactor/Cleanup/API
  - Unicode improvement/Python 3.0
  - Unified plugin output format
  - Pagefile support

1st Volatility 2013 Plugin Contest

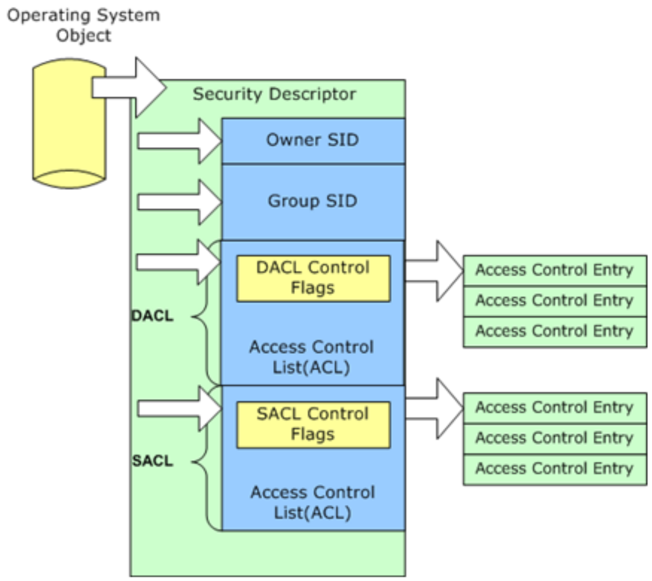
- (Inspired by the Hex-Rays IDA plugin contest)
- Create an innovative and useful extension to Volatility and win the contest!
- Prizes awarded for top 5 submissions:
  - 1: $1500, 2: $500, 3: $250, 4-5: Volatility swag
- Core development team judges
  - creativity, usefulness, effort, completeness, submission date, and clarity of documentation.
- 8 Submissions (15 new plugins!)
- Xen address space/Timeline patches

1st Place: Mariano Graziano

- Actaeon: Analyzing guest VMs in host memory and nested hypervisors (VT-x)



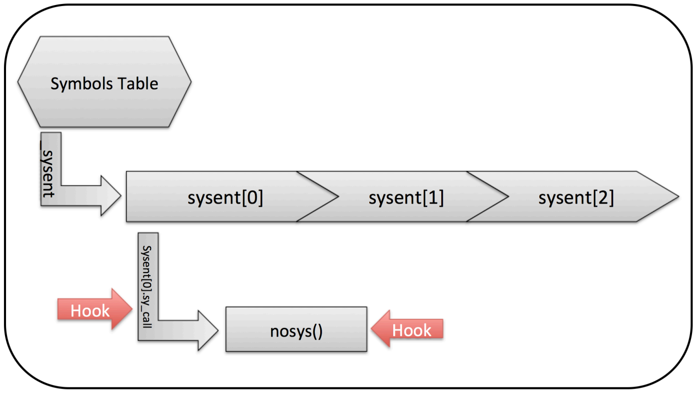
2nd Place: Cem Gurkok



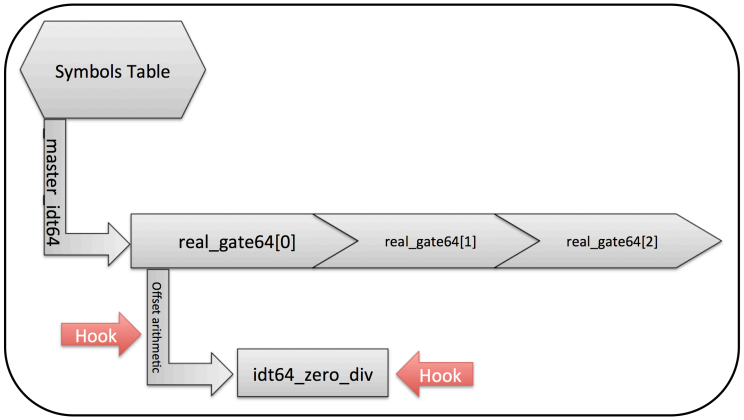
```
0xfffffa800123b060 explorer.exe
SecurityDescriptor
      Control
        SE_DACL_PRESENT
        SE_SACL_AUTO_INHERITED
        SE_SACL_PRESENT
        SE_SELF_RELATIVE
      SACL
        ACE
          Mask
            PROCESS_TERMINATE
          Flags
            NO_INHERITANCE_SET
          Sid
            Name:  (Medium Mandatory Level)
            SID: S-1-16-8192
          Type: SYSTEM_MANDATORY_LABEL
          Size: 20
      DACL
        ACE
          Mask
            PROCESS_CREATE_PROCESS
            PROCESS_CREATE_THREAD
            PROCESS_DUP_HANDLE
            PROCESS_QUERY_INFORMATION
            PROCESS_QUERY_LIMITED_INFORMATION
            PROCESS_SET_INFORMATION
            PROCESS_SET_QUOTA
            PROCESS_SUSPEND_RESUME
            PROCESS_TERMINATE
            PROCESS_VM_OPERATION
            PROCESS_VM_READ
            PROCESS_VM_WRITE
            Read DAC
            Syncronize
            Write DAC
            Write Owner
          Flags
            NO_INHERITANCE_SET
          Sid
            Name: None
            SID:
S-1-5-21-459936167-2938841458-497108533-1000
          Type: ACCESS_ALLOWED
          Size: 36
        ACE
          Mask
            PROCESS_CREATE_PROCESS
            PROCESS_CREATE_THREAD
            PROCESS_DUP_HANDLE
            PROCESS_QUERY_INFORMATION
            PROCESS_QUERY_LIMITED_INFORMATION
            PROCESS_SET_INFORMATION
            PROCESS_SET_QUOTA
            PROCESS_SUSPEND_RESUME
            PROCESS_TERMINATE
            PROCESS_VM_OPERATION
            PROCESS_VM_READ
            PROCESS_VM_WRITE
            Read DAC
            Syncronize
            Write DAC
            Write Owner
          Flags
            NO_INHERITANCE_SET
          Sid
            Name:  (Local System)
            SID: S-1-5-18
```

Rootkit Detection in OS X

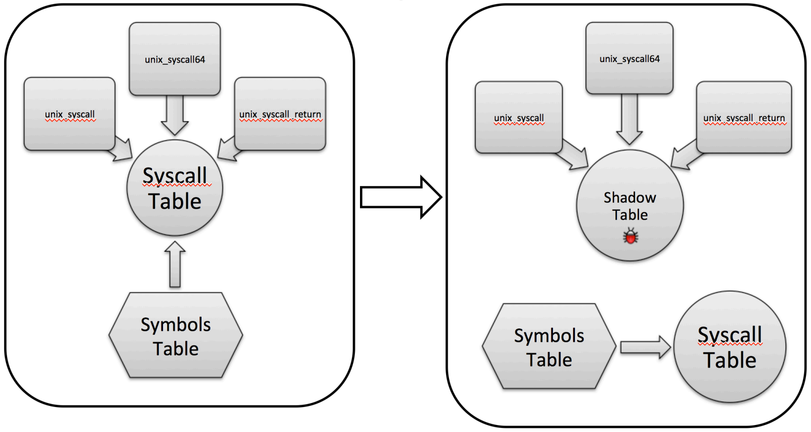
Syscall Table



Hooking the IDT



Shadow Syscall Table

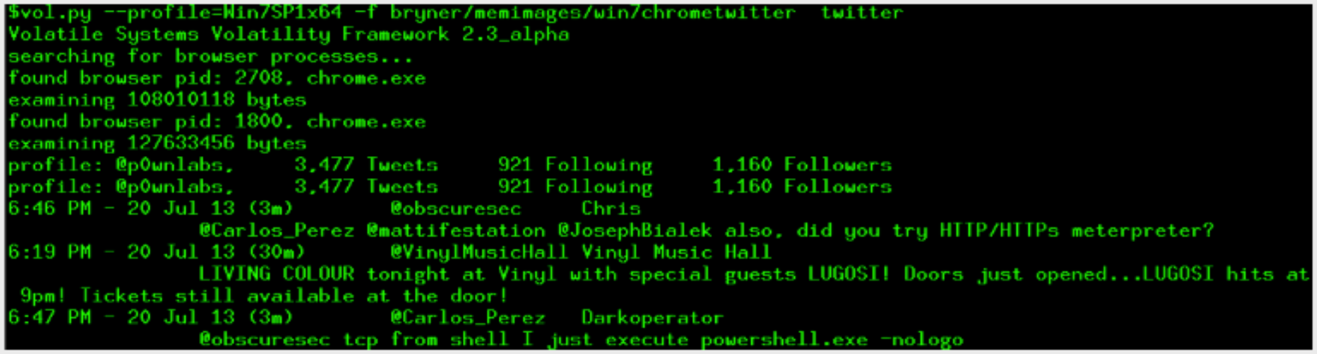


3rd Place: Jeff Bryner

volatility social media plugins

ssl everywhere causes browsers to limit disk storage

memory is where it's at!



```
$vol.py --profile=Win7SP1x64 -f bryner/memimages/win7chrometwitter  twitter
Volatile Systems Volatility Framework 2.3_alpha
searching for browser processes...
found browser pid: 2708, chrome.exe
examining 108010118 bytes
found browser pid: 1800, chrome.exe
examining 127633456 bytes
profile: @p0wnlabs,     3,477 Tweets     921 Following     1,160 Followers
profile: @p0wnlabs,     3,477 Tweets     921 Following     1,160 Followers
6:46 PM - 20 Jul 13 (3m)        @obscuresec     Chris
                @Carlos_Perez @mattifestation @JosephBialek also, did you try HTTP/HTTPs meterpreter?
6:19 PM - 20 Jul 13 (30m)       @VinylMusicHall Vinyl Music Hall
                LIVING COLOUR tonight at Vinyl with special guests LUGOSI! Doors just opened...LUGOSI hits at
 9pm! Tickets still available at the door!
6:47 PM - 20 Jul 13 (3m)        @Carlos_Perez   Darkoperator
                @obscuresec tcp from shell I just execute powershell.exe -nologo
```

1st Volatility 2013 Plugin Contest

- 4th Place
  - Carl Pulley: Annotating Windows Samples with nearest Symbol Information (i.e. execution stack, pointers)
  - Edwin Smulders: Linux process information, stack analysis, syscall registers
- 5th Place
  - Jamaal Speights: Extracting Network Packets
- Honorable Mention:
  - Jeremy Jones: Converting VMware suspended state to Illumos format

Volatility Foundation

- Volatility development is supported by an independent foundation
  - US 501(c)(3) Nonprofit (filed)
- The Volatility Foundation was established:
  - to support the development of Volatility
  - to promote the use of Volatility and memory analysis in the forensics community
  - to defend the intellectual property and the framework's longevity
  - to advance the state of the art in memory analysis research
- But….development driven by Volatility community

Board of Directors

- AAron Walters, **Pres. and Chairman of the Board**
- Michael Hale Ligh, **Secretary/Treasurer**
- Mike Auty, **Volatility Core Team**
- Andrew Case, **Volatility Core Team**
- Jamie Levy, **Volatility Core Team**

Contributor License Agreement

- Protect the contributors, the foundation, and users
- Dual shared ownership property rights and intellectual property license
- The contributor is representing that they are authorized to submit the code and granting its use in Volatility
- Does not restrict how developers use their own code.
- Allows the Volatility Foundation to defend the project should there be a legal dispute

Download Volatility 2.3

https://code.google.com/p/volatility/

http://volatility-labs.blogspot.com/

@volatility

Join the community!