Windows Advanced Auditing
Pump Up the VOLUME
One Incident Responder's Wish List of Events
A Little Background

- Founder and president of Vertigrate
- Digital forensics, incident response, and malware reverse engineering
- Proactively engages with business and security teams of all sizes on blue team engagements.
- SANS Community Instructor
- Volunteers as
  - Arizona chapter’s President of the High Technology Crime Investigation Association (HTCIA),
  - Membership Director of the Phoenix chapter’s Membership Director Information Systems Security Association (ISSA),
  - State Bar of Arizona’s Technology Committee.
- Certification Hound:
  - CISSP, CISM, GREM, GCFE, GCIH, GPEN, CCME
Special Thanks to:

- **Michael Gough** &
  www.malwarearchaeology.com

- **Kurt Falde** &
A Little History on Windows Event Logging
Windows Advanced Auditing
  • What We Can Get
  • Why We Want It
  • Where to Deploy It
  • How to Find It
Finding a Needle in a Stack of Needles
  • Native
  • Open Source
  • Commercial
Other Valuable Events You Already Have
Windows Event Logging

• Big Three Event Logs
  • System
  • Application
  • Security

• Security Log = Nine Categories

• Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy
Windows Advanced Auditing

- Introduced with Server 2008 / Vista Release
- Security Log = Ten Categories Containing Fifty-Three Sub-Categories
- Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration
## Windows Advanced Auditing Categories

### System Audit Policy
- **Category/Subcategory**
  - **System**
    - Security System Extensibility
    - System Integrity
    - IPSec Driver
    - Other System Events
    - Security State Change
  - Logon/Logoff
  - Logon
  - Logoff
  - Account Lockout
  - IPSec Main Mode
  - IPSec Quick Mode
  - IPSec Extended Mode
  - Special Logon
  - Other Logon/Logoff Events
  - Network Policy Server

### Object Access
- **Category/Subcategory**
  - **Object Access**
    - File System
    - Registry
    - Kernel Object
    - SAM
    - Certification Services
    - Application Generated
    - Handle Manipulation
    - File Share
    - Filtering Platform Packet Draining
    - Filtering Platform Connection
    - Other Object Access Events
    - Detailed File Share
    - Privilege Use
    - Sensitive Privilege Use
    - Non-Sensitive Privilege Use
    - Other Privilege Use Events
    - Detailed Tracking
    - Process Termination
    - DPAPI Activity
    - RPC Events
    - Process Creation

### Policy Change
- **Category/Subcategory**
  - **Policy Change**
    - Audit Policy Change
    - Authentication Policy Change
    - Authorization Policy Change
    - Microsoft Rule-Level Policy Change
    - Filtering Platform Policy Change
    - Other Policy Change Events

### Account Management
- **Category/Subcategory**
  - **Account Management**
    - User Account Management
    - Computer Account Management
    - Security Group Management
    - Distribution Group Management
    - Application Group Management
    - Other Account Management Events

### DS Access
- **Category/Subcategory**
  - **DS Access**
    - Directory Service Changes
    - Directory Service Replication
    - Detailed Directory Service Replication
    - Directory Service Access

### Account Logon
- **Category/Subcategory**
  - **Account Logon**
    - Kerberos Service Ticket Operations
    - Other Account Logon Events
    - Kerberos Authentication Service
    - Credential Validation
What You Need To Know

• Off by Default
• Will Not Display Values on 2008 R2 / WIN7 via GUI
• Auditpol.exe /get /category:*
  • Shows all 53 options and their current values
• Provides Ability to Log All Sorts of Good Stuff
What You Need To Know

Security Options: Enable “Audit: Force audit policy subcategory settings…”

Computer Configuration > Windows Settings > Security Settings > Event Log = 1GB – 4GB

YOU'RE GOING TO NEED

A BIGGER LOG
Events of Interest

- Logon / Logoff
  - Logon Type
- Process Creation / Termination
- Filtering Platform Connection
- Command Line / PowerShell
- Object Access
  - File System
  - Registry
  - File Share (Detailed)
**Logon / Logoff**

- 4624: An account was successfully logged on.
- LOGON TYPES:
  - 2: Interactive – hands on keyboard
  - 3: Network – lots of these events
  - 9: RunAs
  - 10: RDP Logon
  - 4: Batch – associated with Scheduled Task
  - 5: Service – second only to type 3
  - 7: Unlock
  - 8: NetworkClearText
  - 11: Cached Interactive
- 4634: An account was logged off.

Mike Lombardi, MBA, CISSP, CISM, GREM, GCFE, GCIH, GPEN - Vertigrate © 2017 vertigrate.com
Process Creation

- **4688**: A new process has been created
- **WHY**: Find the offending process

A new process has been created.

Subject:
- Security ID: [redacted]
- Account Name: [redacted]
- Account Domain: [redacted]
- Logon ID: 0x762354

Process Information:
- New Process ID: 0x487c
- New Process Name: C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE
- Token Elevation Type: TokenElevationTypeLimited (3)
- Creator Process ID: 0xe38
- Process Command Line: [redacted]
Process Termination

• 4689: A process has exited
• WHY: Establish a timeline
Platform Filtering Connection

- **5156**: Windows Filtering Platform has permitted a connection
- **WHY**: Discover who is calling out and to whom

The Windows Filtering Platform has permitted a connection.

**Application Information:**
- **Process ID**: 18556
- **Application Name**: \\device\harddiskvolume2\program files (x86)\microsoft office\office14\winword.exe

**Network Information:**
- **Direction**: Outbound
- **Source Address**: 192.168.xx.xx
- **Source Port**: 10037
- **Destination Address**: 52.18.63.80
- **Destination Port**: 80
- **Protocol**: 6

**Filter Information:**
- **Filter Run-Time ID**: 0
- **Layer Name**: Connect
- **Layer Run-Time ID**: 48
• Did anyone notice the Process ID?
• 4688 & 4689: Process ID = 0x487c
• 5156: Process ID = 18556
Logging The Command Line

- TWO Requirements:
  - Include command line in process creation events
    - Via: Local Computer Policy > Computer Configuration > Administrative Templates > System > Audit Process Creation
  - Audit Process Creation

- Careful if credentials are being passed on command line.
Process Creation with Command Line

- 4688: A new process has been created
- NOW we see what was entered on command line

A new process has been created.

Subject:
- Security ID: [redacted]
- Account Name: [redacted]
- Account Domain: [redacted]
- Logon ID: 0x1ae2ec5

Process Information:
- New Process ID: 0x142c
- New Process Name: C:\Windows\System32\ipconfig.exe
- Token Elevation Type: TokenElevationTypeDefault (1)
- Creator Process ID: 0x9d8

Process Command Line: ipconfig /displaydns
Logging PowerShell

• Three Settings:
  • Via: Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Windows PowerShell
    • Turn on Module Logging: Enable (* for all modules)
    • Turn on PowerShell Script Block Logging: Enable
    • Turn on PowerShell Transcription: Enable & set location

• Side Note: 2008 R2 needs updated ADMX’s

• Careful if credentials are being passed on command line.
Reading PowerShell Log

- Event Viewer > Application and Services > Microsoft > Windows > PowerShell
- Event 4104 – Execute a Remote Command
<table>
<thead>
<tr>
<th>Monitor Sensitive Areas with File Object Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 4663: An attempt was made to access an object</td>
</tr>
<tr>
<td>• 4657: A registry value was modified</td>
</tr>
</tbody>
</table>

Mike Lombardi, MBA, CISSP, CISM, GREM, GCFE, GCIH, GPEN

Vertigrate © 2017 vertigrate.com
Since We’re On Scheduled Tasks...

- 4698: A scheduled task was created

A scheduled task was created.

Subject:
Security ID:
Account Name:
Account Domain:
Logon ID: 0xb645eb9

Task Information:
Task Name: \Sample Task
Task Content:
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
<RegistrationInfo>
<Date>2017-08-20T12:57:50.5497483</Date>
<Author>
<Actions Context="Author">
<Exec>
<Command>%COMSPEC%</Command>
<Arguments>%SYSTEMDRIVE%\Windows\Temp\Task_List_Out.txt</Arguments>
</Exec>
</Actions>
</Author>
</Task>
WHAT DO YOU MEAN

YOU DON'T KNOW WHERE TO START?
Start Small

• Advanced Auditing
  • Detailed Tracking:
    • Process Creation: Success & Failure = 4688
    • Process Termination: Success & Failure = 4689
  • Logon/Logoff
    • Logoff: Success = 4634
    • Logon: Success & Failure = 4624 & 4625
    • Other Logon/Logoff Events: Success & Failure = 4649, & 4800-4802
  • Object Access
    • Other Object Access Events: Success = 4698 (Scheduled Task)
  • Policy Change
    • Audit Policy Change: Success & Failure = 4719 & 4912
  • Command Line (4688) & PowerShell Logging
    • PowerShell in PowerShell Log = 4104
Build From There

• Advanced Auditing
  • Object Access
    • File Share: Success & Failure = 5140
    • File System: Success = 4663
    • Filtering Platform Connection: Success = 5156 & 5158
    • Registry: Success = 4657

• Set File Object Access Auditing Switch on Sensitive Areas

• PRO TIP: Search for “consent.exe” in 4624 to find UAC prompts
Set File Object Access Auditing Switch on Sensitive Areas

- Any storage areas containing sensitive data
- Plus, standard Windows locations like...
  - HKLM and USER Run Keys
  - HKLM\System\CurrentControlSet\Services
  - HKLM\CurrentControlSetEnum\USBSTOR
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt
    - Plus %windir%\inf\setupapi.dev.log
Not Sure Which Options to Turn On?

• Event-o-Pedia
  • http://eventopedia.cloudapp.net

• Logging Cheat Sheets
  • https://www.malwarearchaeology.com/cheat-sheets/
I’ve Turned Everything ON… Now What??

Order Now Only $29.99

DR. AMP’S GOLD-DIGGING SHOVEL

P. O. BOX 479
TWIN PEAKS, WA

allow 2 - 4 weeks for delivery
Some Tools to Help

• How do you find what you’re looking for?
  • Windows Event Viewer… meh
  • Wevtutil… better
  • Free Tools
    • EVTXtract (python)
    • Parse-Evtx (perl)
    • Log2timeline (perl)
    • LogParser (Microsoft)
  • Commercial Tools
XPath Filter

• Does not support wildcards
• Works with Windows Event Forwarding
• Use Kurt Falde’s Xpath Filter PS1 Script to start, then refine…

EXAMPLE

<QueryList>
  <Query Id="0" Path="Security">
    <Select Path="Security">
      *[EventData[Data[@Name='NewProcessName'] and
      (Data='C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe')]]
    </Select>
  </Query>
</QueryList>

Mike Lombardi, MBA, CISSP, CISM, GREM, GCFE, GCIH, GPEN - Vertigate © 2017 vertigrate.com
Wevtutil and PowerShell

• Wevtutil does not support wildcards...
  • But PowerShell Does

• Good for quick and dirty searching

EXAMPLE

wevtutil qe security /q:"*[System[(EventID=4688)]]" /c:500
/rd:true /f:text | Select-String "powershell.exe" -Context 23,4
Get-WinEvt

• Does not support wildcards
  
  • Get-WinEvent -FilterHashtable @{Logname="Security"; ProviderName="Microsoft-Windows-Security-Auditing"; ID=4688; Data="'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe "
  
  • "C:\Windows\System32\wscript.exe"
  • "C:\Windows\System32\cscript.exe"
  • "C:\Windows\System32\cmd.exe"
  • Don’t forget "C:\Windows\SysWOW64" paths
More Tools

• Free Tools
  • EVTXtract (python)
  • Parse-Evtx (perl)
  • Log2timeline (perl)
  • LogParser (Microsoft)

• Commercial Tools
  • Any SIEM
  • Event Log Explorer
WE'RE RUNNING OUT OF TIME
What if you don’t have Advanced Auditing Enabled?

• System Logs
  • 20MB Default Size
• Task Scheduler
  • 10MB Default Size
• Security Log… maybe
  • 20MB Default Size
  • Depends upon the amount of activity
Microsoft Log Size Recommendations

• Per August 14, 2015 Guidance
  • Up to 4GB per log
  • Cumulative size of all logs 16GB
  • Applies to all 64-bit Windows releases

  • https://support.microsoft.com/en-us/help/957662/recommended-settings-for-event-log-sizes-in-windows
What you can LOOK FOR if you don’t have Advanced Auditing Enabled?

- **Security Logs**
  - 4624 & 4634: Successful Logon & Logoff (Don’t Forget Logon Types)

- **System Logs**
  - 7045: Service Installation
  - 7034 / 7031: Service Crashed
  - 7040: Service configured to interact with desktop

- **Task Scheduler**
  - 106: New Scheduled Task... maybe
    - Highly perishable at default size
    - ~20K events, ~7 days

- **Windows Defender**
  - 20MB Default Size
  - Depends upon the amount of activity
Where to Find Me:
• LinkedIn
• Twitter @vertigrate
• www.vertigrate.com
• Supporting HTCIA and ISSA Meetings
• SANS Events

SANS Mentor or Community SEC504
Hacker Tools, Techniques, Exploits & Incident Handling
GCIH