FROM THE SERVER ROOM
VERTIGRATE
TO THE COURTROOM ®

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 &

https://blogs.technet.microsoft.com/askds/2011/09/26/advanced-xml-filtering-in-the-windows-event-viewer/

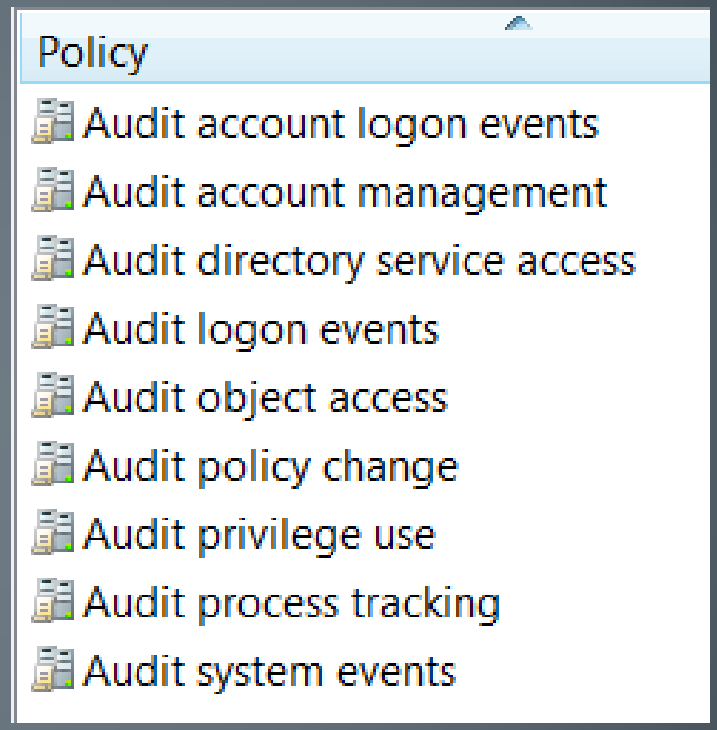
- https://blogs.technet.microsoft.com/kfalde/2015/05/27/some-posh-to-help-with-evt-xpath-filter-creations/

Agenda

- 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

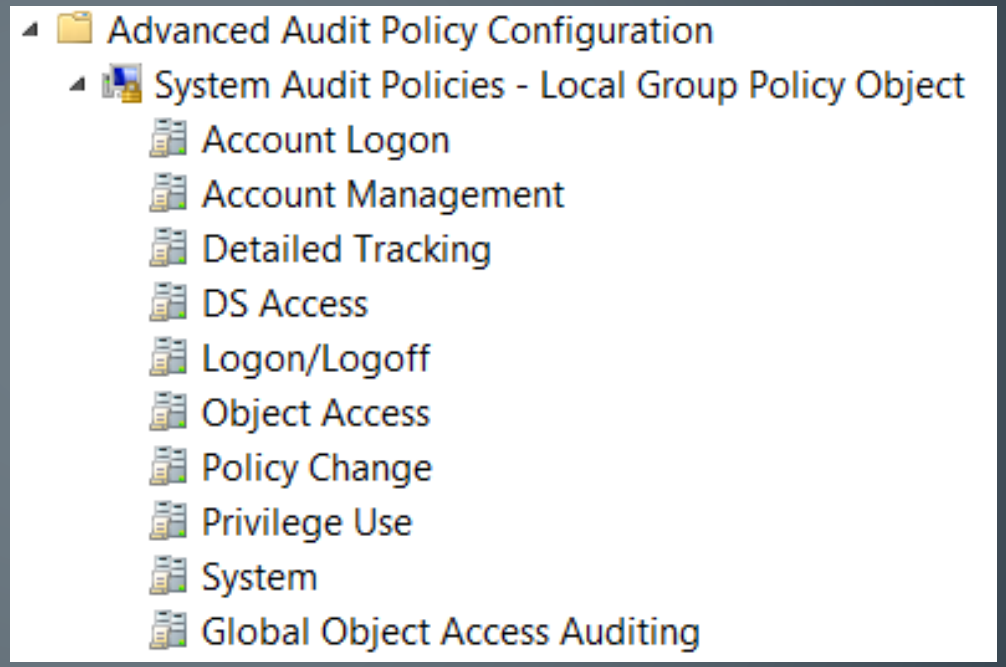
- Big Three Event Logs
  - System
  - Application
  - Security
- Security Log = Nine Categories



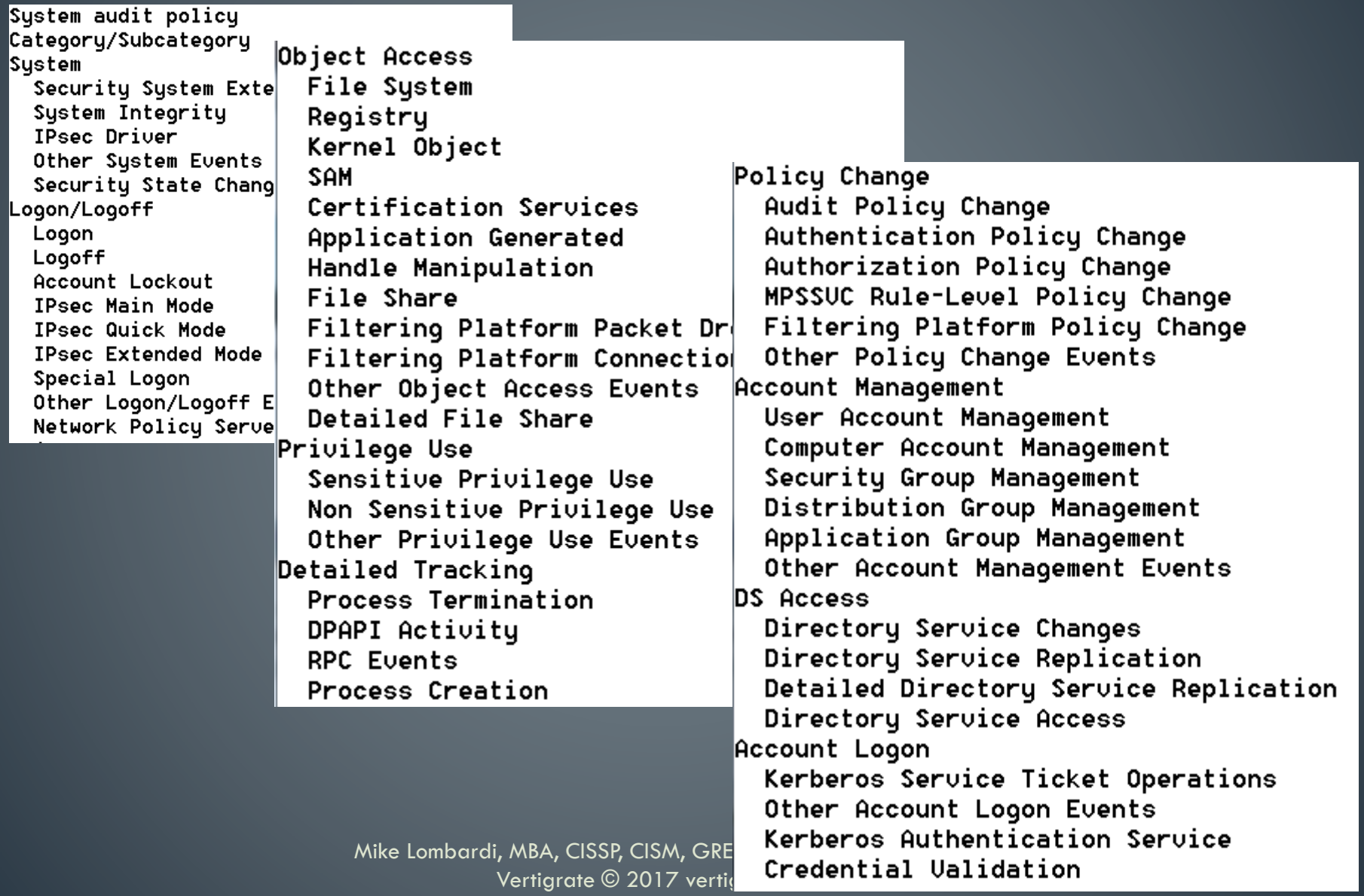
- Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy

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



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…"

Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled

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

Events of Interest

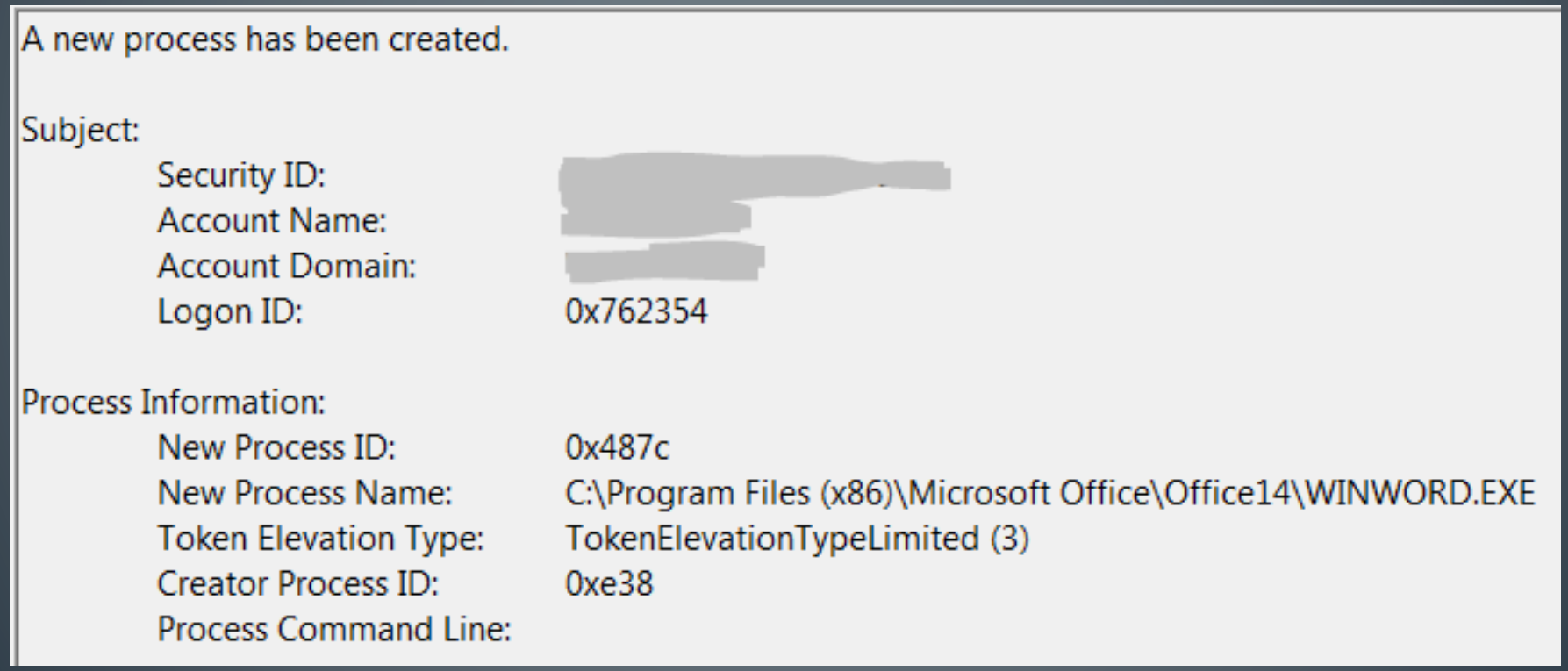
- Logon / Logoff
  - Logon Type
- Process Creation / Termination
- Filtering Platform Connection
- Command Line / PowerShell
- Object Access
  - File System
  - Registry
  - File Share (Detailed)

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.

Process Creation

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



A new process has been created.

Subject:

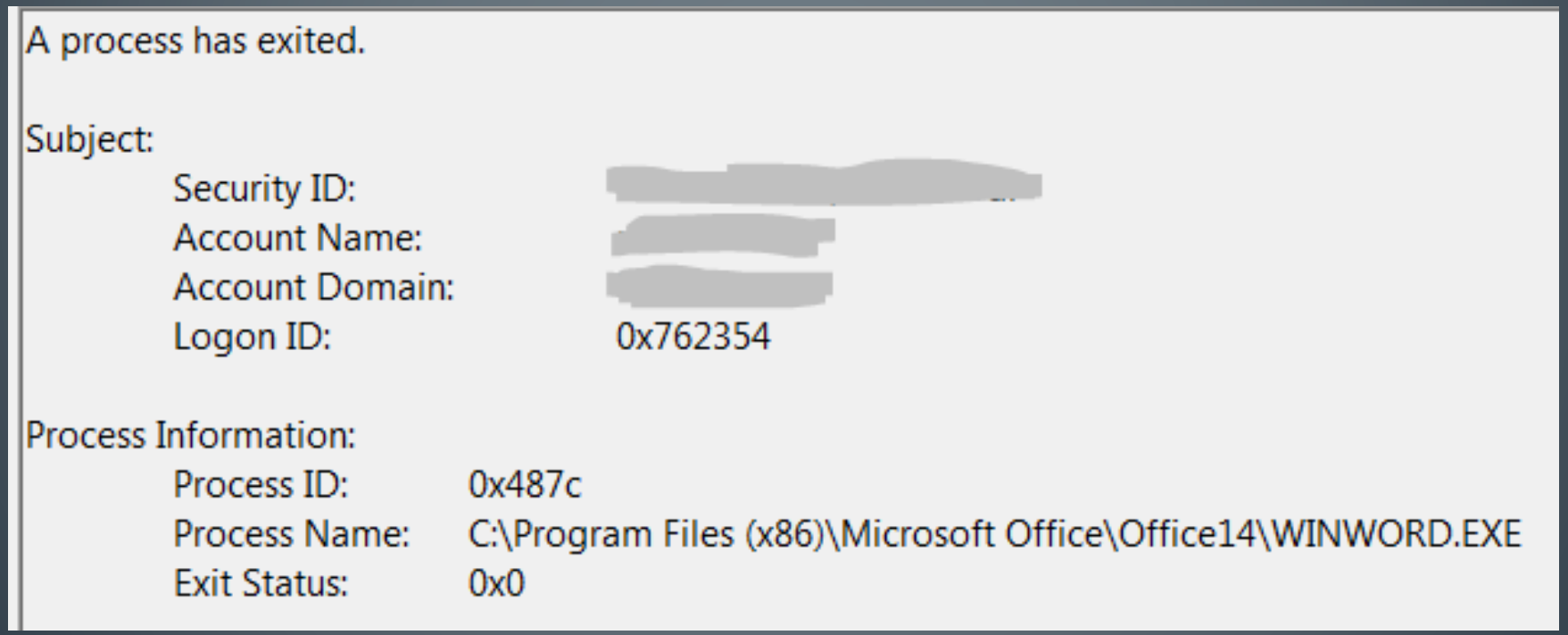
Security ID:	[redacted]
Account Name:	
Account Domain:	
Logon ID:	0x762354

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:	

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
Source Port:	10037
Destination Address:	52.18.63.80
Destination Port:	80
Protocol:	6

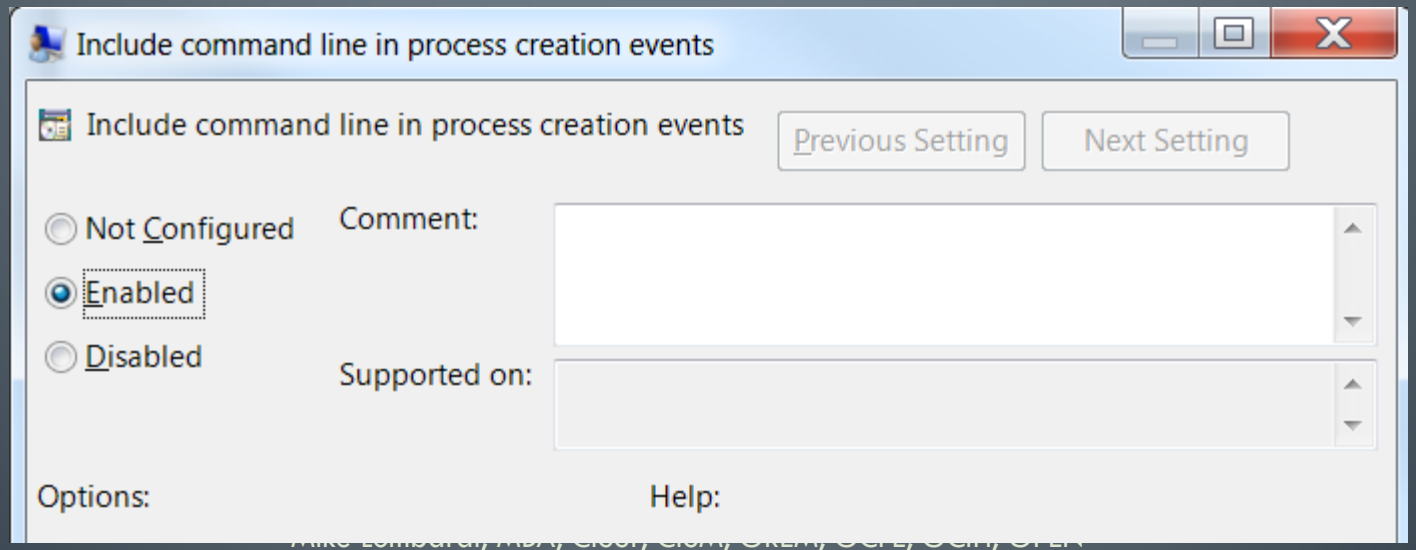
Filter Information:

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

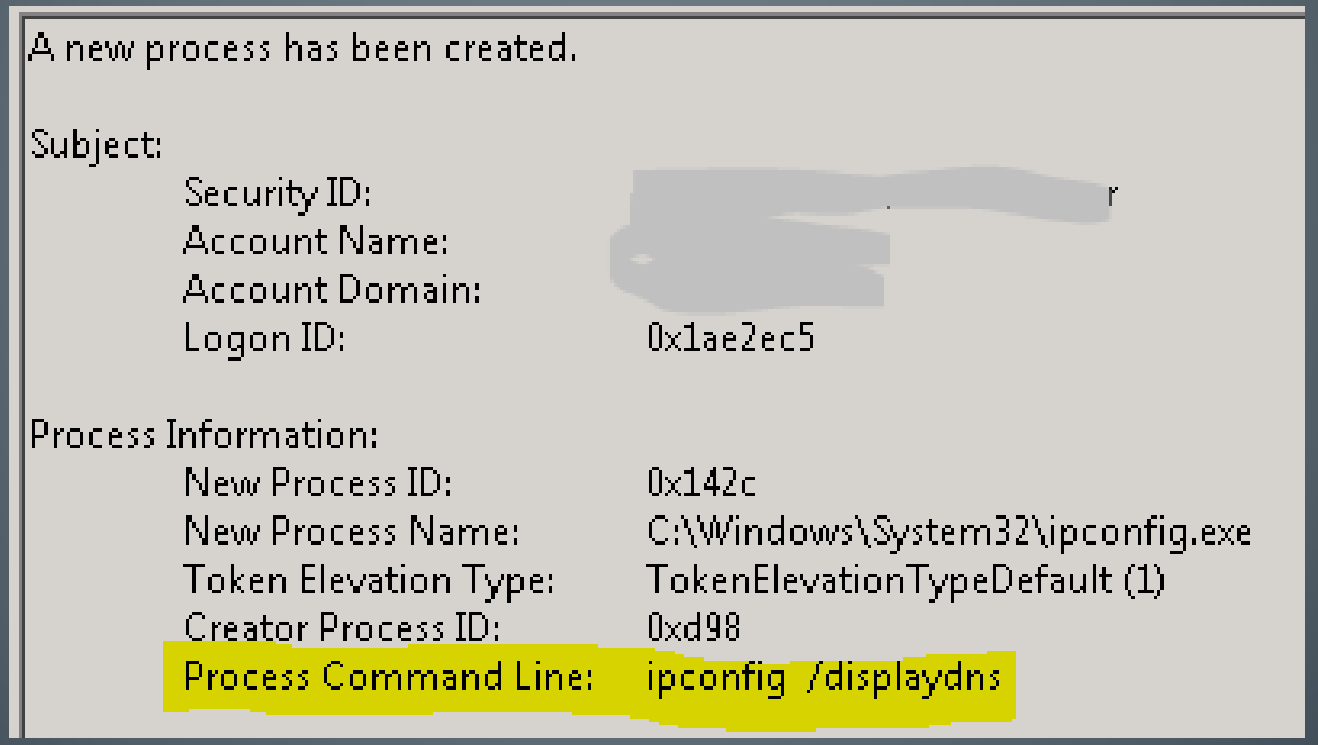
Logging The Command Line

- 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

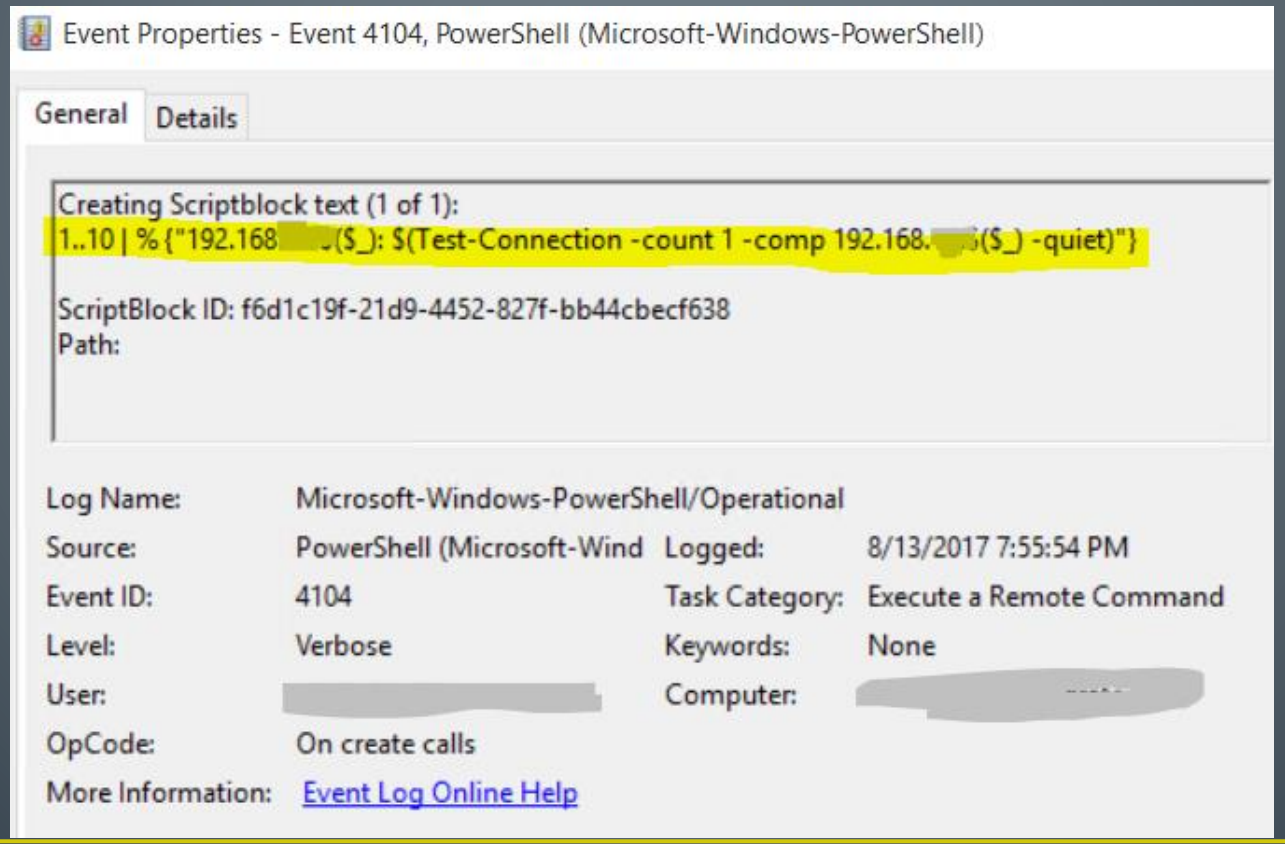


Logging PowerShell

- 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
  - https://www.microsoft.com/en-us/download/details.aspx?id=36991
  - https://www.microsoft.com/en-us/download/details.aspx?id=53430
- Careful if credentials are being passed on command line.

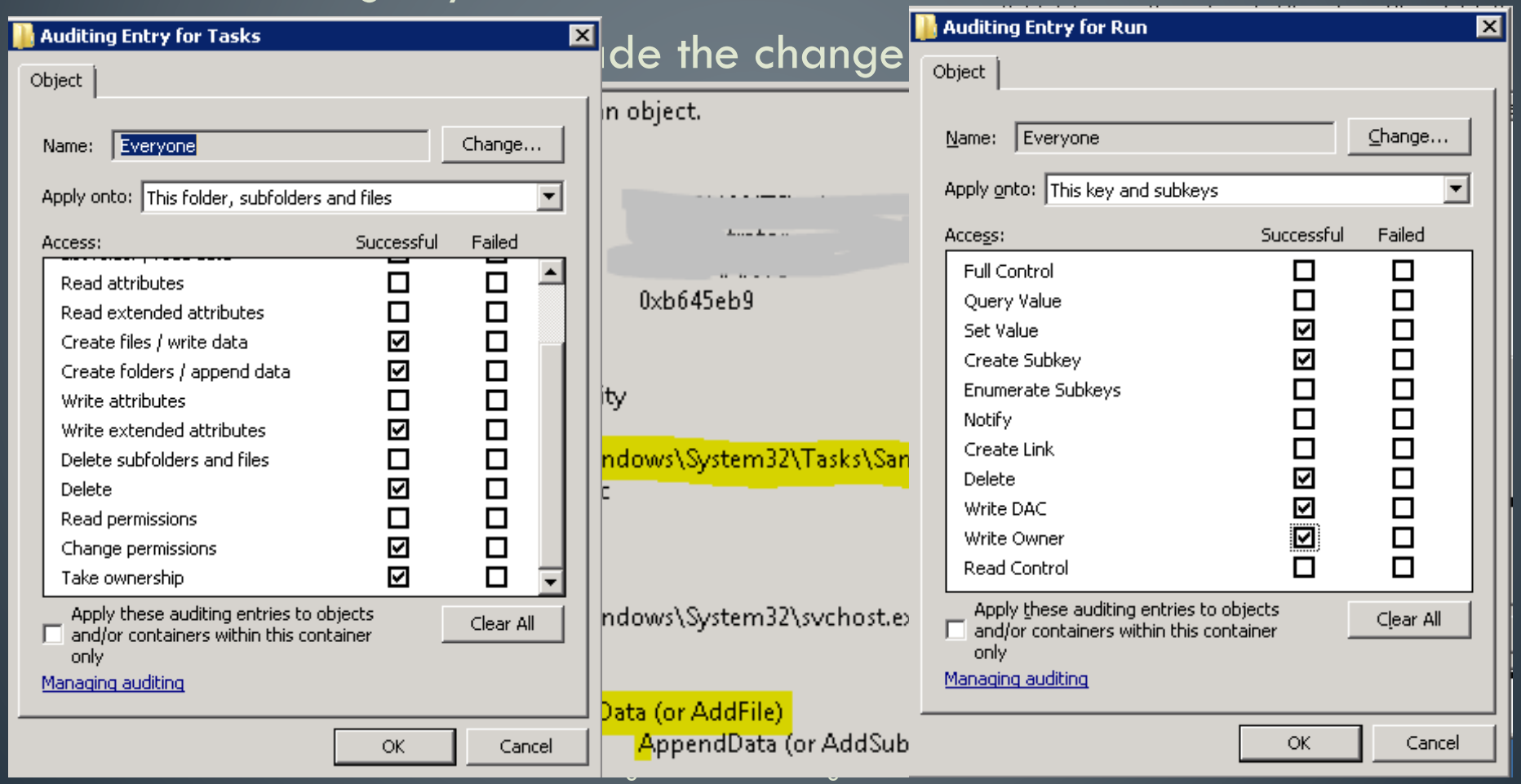
Reading PowerShell Log

- Event Viewer > Application and Services > Microsoft > Windows > PowerShell
  - Event 4104 – Execute a Remote Command



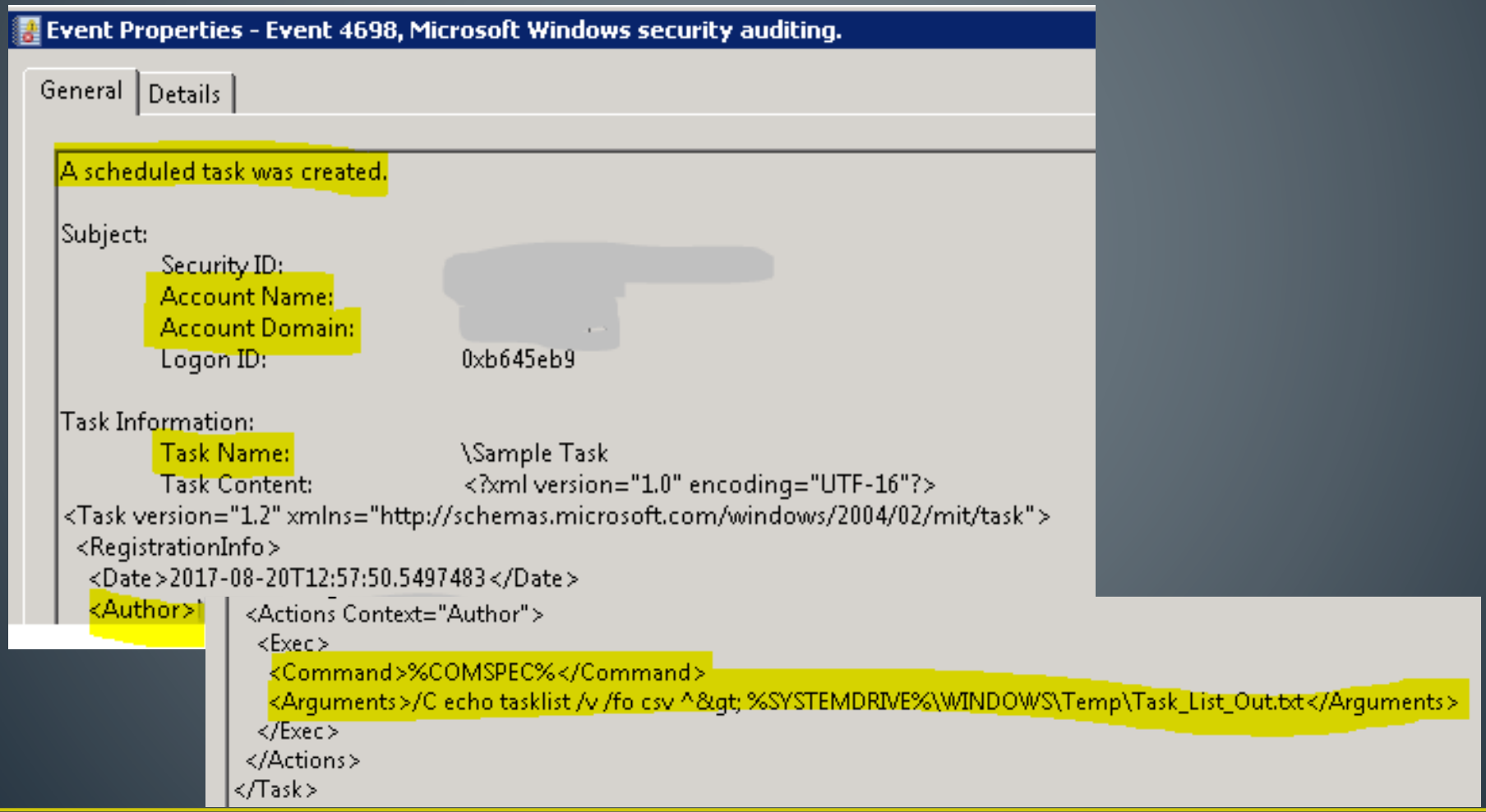
Monitor Sensitive Areas with File Object Access

- 4663: An attempt was made to access an object
- 4657: A registry value was modified



Since We're On Scheduled Tasks…

- 4698: A scheduled task was created




WHAT DO YOU MEAN
YOU DON'T KNOW WHERE TO START?
imgflip.com

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

Keep Going…

- 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??

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>
```

Wevtutil and PowerShell

- Wevutil 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
imgflip.com

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

QUESTIONS?

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