

FROM THE SERVER ROOM

VERTIGRATE

TO THE COURTROOM ®



Windows Advanced Auditing Pump Up the VOLUME

One Incident Responder's Wish List
of Events



SANS



**SIEM &
Tactical
Analytics**
SUMMIT
& TRAINING

Scottsdale, AZ
Nov 28 - Dec 5, 2017

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 &

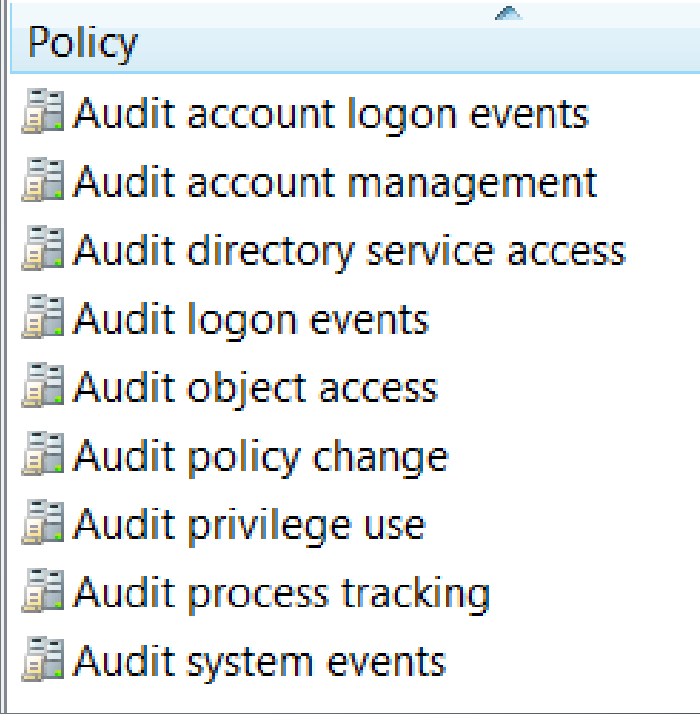
<https://blogs.technet.microsoft.com/askds/2011/09/26/advanced-xml-filtering-in-the-windows-event-viewer/>

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

Agenda

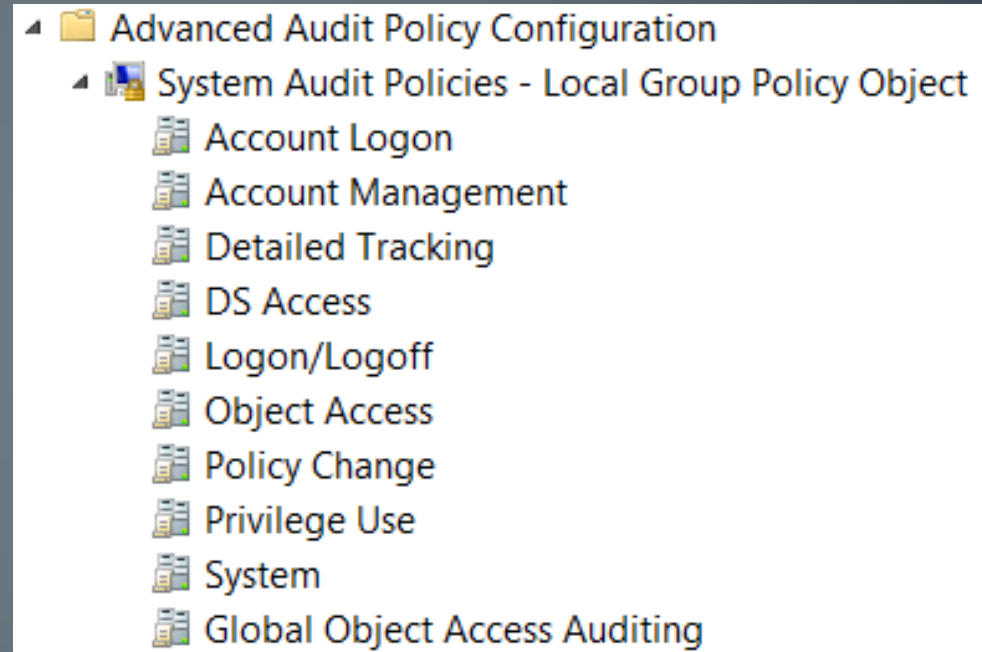
- A Little History on Windows Event Logging
- Windows Advanced Auditing
 - What We Can Get
 - Why We Want It
 - Where to Deploy It
 - How to Find It
- Finding a Needle in a Stack of Needles
 - Native
 - Open Source
 - Commercial
- Other Valuable Events You Already Have

Windows Event Logging

- Big Three Event Logs
 - System
 - Application
 - Security
 - Security Log = Nine Categories
- 
- The screenshot shows a window titled "Policy" with a list of audit categories. Each category is preceded by a small icon representing a document with a checkmark. The categories listed are:
- Audit account logon events
 - Audit account management
 - Audit directory service access
 - Audit logon events
 - Audit object access
 - Audit policy change
 - Audit privilege use
 - Audit process tracking
 - Audit system events
- 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	Object Access	
Security System Extension	File System	
System Integrity	Registry	
IPsec Driver	Kernel Object	
Other System Events	SAM	
Security State Change	Certification Services	Policy Change
Logon/Logoff	Application Generated	Audit Policy Change
Logon	Handle Manipulation	Authentication Policy Change
Logoff	File Share	Authorization Policy Change
Account Lockout	Filtering Platform Packet Driver	MPSSUC Rule-Level Policy Change
IPsec Main Mode	Filtering Platform Connection	Filtering Platform Policy Change
IPsec Quick Mode	Other Object Access Events	Other Policy Change Events
IPsec Extended Mode	Detailed File Share	Account Management
Special Logon	Privilege Use	User Account Management
Other Logon/Logoff Events	Sensitive Privilege Use	Computer Account Management
Network Policy Service	Non Sensitive Privilege Use	Security Group Management
	Other Privilege Use Events	Distribution Group Management
	Detailed Tracking	Application Group Management
	Process Termination	Other Account Management Events
	DPAPI Activity	DS Access
	RPC Events	Directory Service Changes
	Process Creation	Directory Service Replication
		Detailed Directory Service Replication
		Directory Service Access
		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...”

 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



imgflip.com

Mike Lombardi, MBA, CISSP, CISM, GREM, GCFE, GCIH, GPEN -
Vertigate © 2017 vertigate.com

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:	[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:	

Process Termination

- 4689: A process has exited
- WHY: Establish a timeline

```
A process has exited.

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

Process Information:
  Process ID:    0x487c
  Process Name:  C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE
  Exit Status:   0x0
```

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

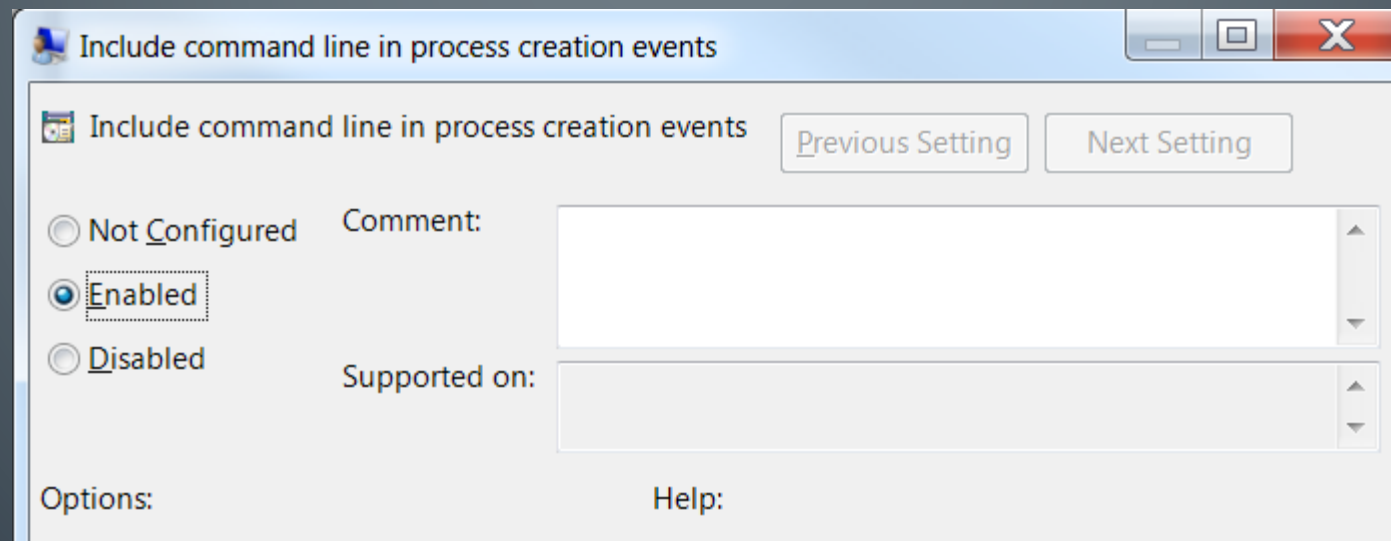
Filter Information:
    Filter Run-Time ID: 0
    Layer Name:         Connect
    Layer Run-Time ID: 48
```



- 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

```
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:  0xd98
  Process Command Line: ipconfig /displaydns
```

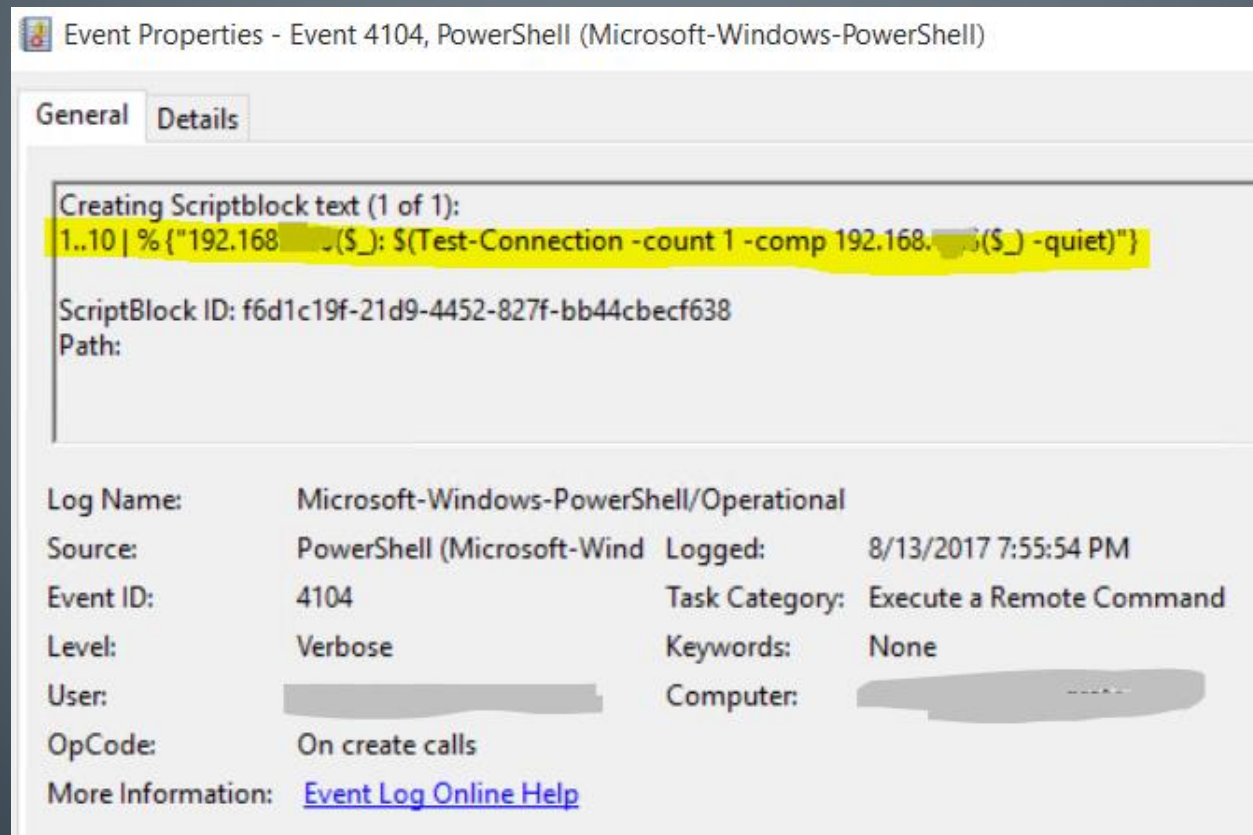
Logging PowerShell

- 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
 - <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



The screenshot shows the 'Event Properties' window for Event 4104 in the PowerShell log. The 'Details' tab is active, displaying the scriptblock text that was executed. The text is highlighted in yellow and reads: `1..10 | % {"192.168.1.10 ($_) : $(Test-Connection -count 1 -comp 192.168.1.10 ($_) -quiet)"}`. Below the scriptblock text, the ScriptBlock ID is shown as `f6d1c19f-21d9-4452-827f-bb44cbe6f638`. The 'Path' field is empty. At the bottom, a summary table provides additional details about the event.

Log Name:	Microsoft-Windows-PowerShell/Operational		
Source:	PowerShell (Microsoft-Wind	Logged:	8/13/2017 7:55:54 PM
Event ID:	4104	Task Category:	Execute a Remote Command
Level:	Verbose	Keywords:	None
User:	[REDACTED]	Computer:	[REDACTED]
OpCode:	On create calls		
More Information:	Event Log Online Help		

Monitor Sensitive Areas with File Object Access

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

Auditing Entry for Tasks

Object

Name:

Apply onto:

Access:	Successful	Failed
Read attributes	<input type="checkbox"/>	<input type="checkbox"/>
Read extended attributes	<input type="checkbox"/>	<input type="checkbox"/>
Create files / write data	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Create folders / append data	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write attributes	<input type="checkbox"/>	<input type="checkbox"/>
Write extended attributes	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delete subfolders and files	<input type="checkbox"/>	<input type="checkbox"/>
Delete	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read permissions	<input type="checkbox"/>	<input type="checkbox"/>
Change permissions	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Take ownership	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Apply these auditing entries to objects and/or containers within this container only

[Managing auditing](#)

Auditing Entry for Run

Object

Name:

Apply onto:

Access:	Successful	Failed
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Query Value	<input type="checkbox"/>	<input type="checkbox"/>
Set Value	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Create Subkey	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enumerate Subkeys	<input type="checkbox"/>	<input type="checkbox"/>
Notify	<input type="checkbox"/>	<input type="checkbox"/>
Create Link	<input type="checkbox"/>	<input type="checkbox"/>
Delete	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write DAC	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write Owner	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read Control	<input type="checkbox"/>	<input type="checkbox"/>

Apply these auditing entries to objects and/or containers within this container only

[Managing auditing](#)

Since We're On Scheduled Tasks...

- 4698: A scheduled task was created

Event Properties - Event 4698, Microsoft Windows security auditing.

General | Details

A scheduled task was created.

Subject:

Security ID: [REDACTED]

Account Name: [REDACTED]

Account Domain: [REDACTED]

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>C echo tasklist /v /fo csv ^> %SYSTEMDRIVE%\WINDOWS\Temp\Task_List_Out.txt</Arguments>
</Exec>
</Actions>
</Task>



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??



Order Now
Only \$29⁹⁹ plus S & H

**DR. AMP'S
GOLD DIGGING SHOVEL**

**P. O. BOX 479
TWIN PEAKS, WA**
allow 2 - 4 weeks for delivery

SRWTIME

f t

Some Tools to Help

- How do you find what you're looking for?
 - Windows Event Viewer... meh
 - Wevtutil... better
 - Free Tools
 - EVTExtract (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

- Wevtutil does not support wildcards...
 - But PowerShell Does
- Good for quick and dirty searching

EXAMPLE

```
wevtutil ql 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
 - EVTExtract (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