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.

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.

You need to know these.

You need to practice these.

Clean what you inherit.

Make the world a better place.

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-Global-Universal-DomainLocal-Resource
- Account-Global-Universal-DomainLocal-Permission

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…

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.

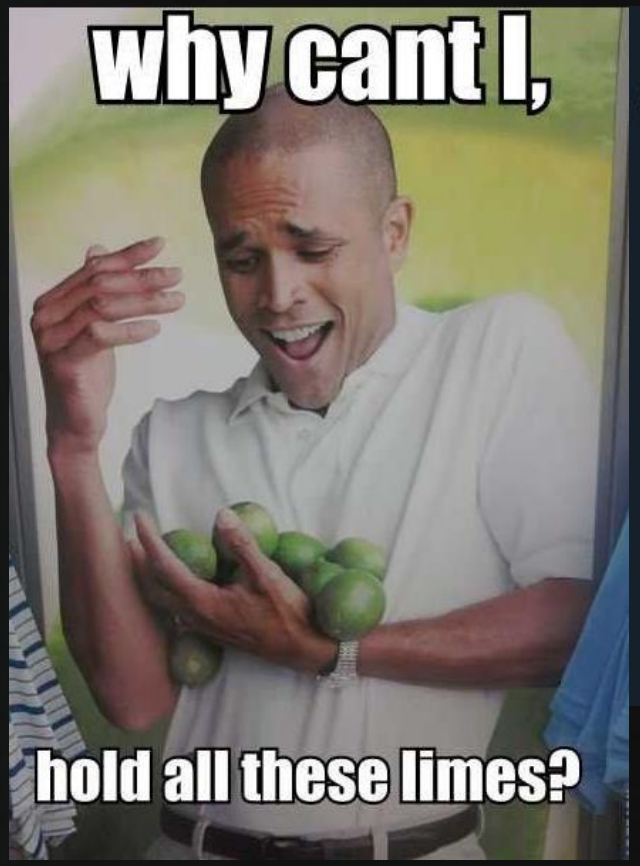
You need to practice these.

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 detstruction
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



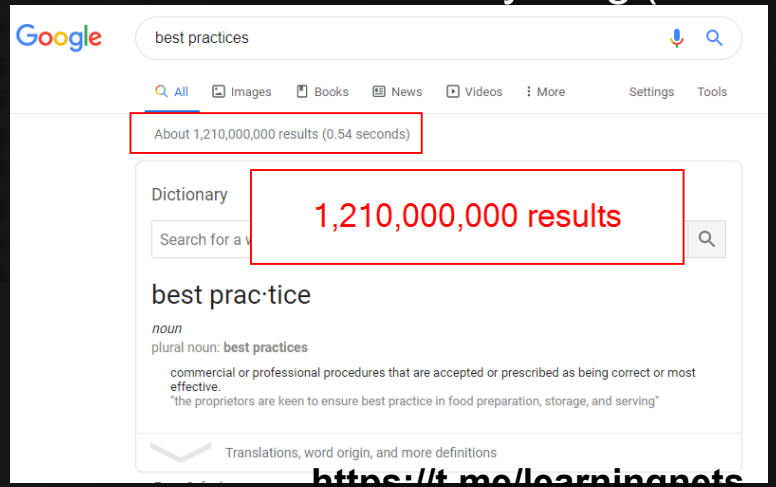
Network Defenses Section to Follow

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

BLACK HILLS Information Security • 2008 •

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*

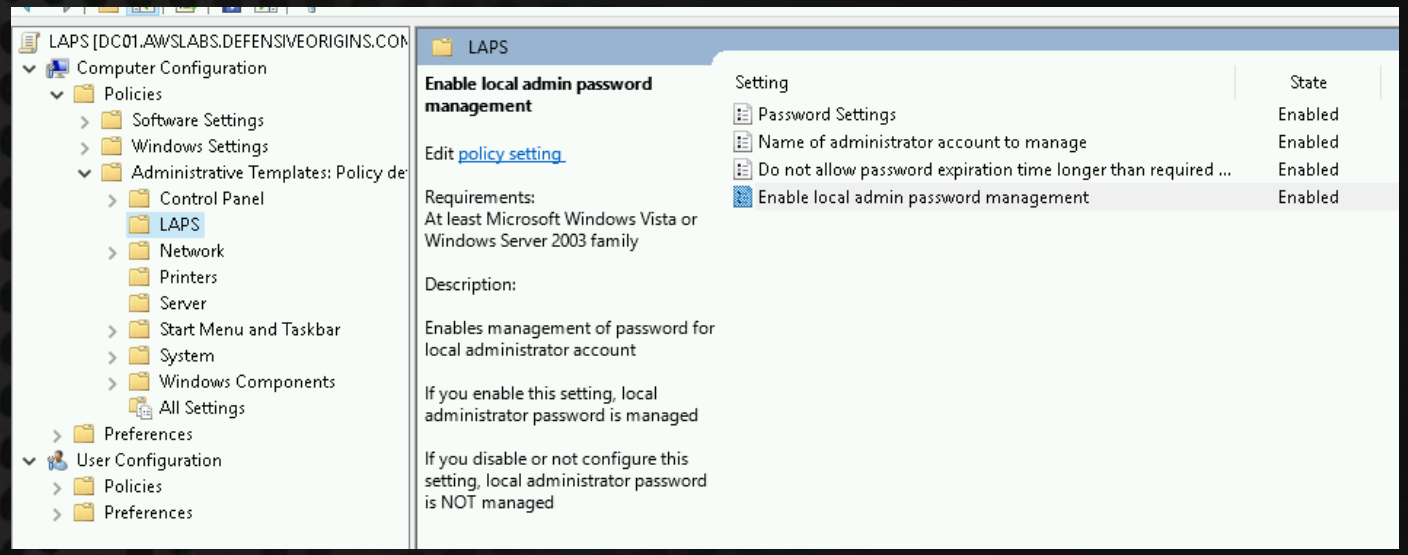
Rename local administrator account? Make it a honey account?

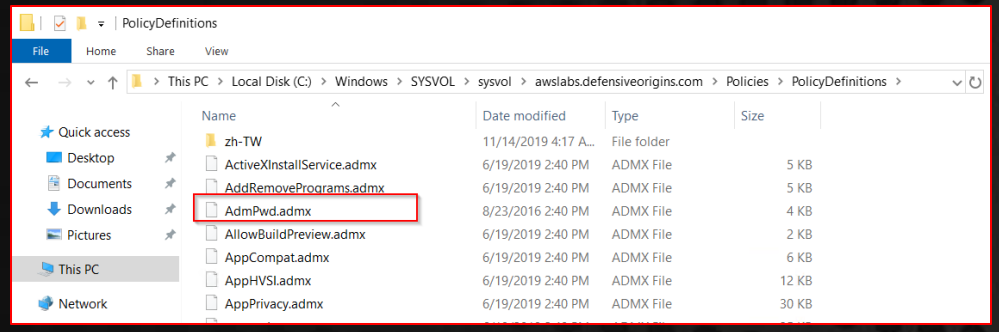
Policy	Policy Setting
Accounts: Administrator account status	Disabled
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to cons...	Not Defined
Accounts: Rename administrator account	Wally.Smith

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



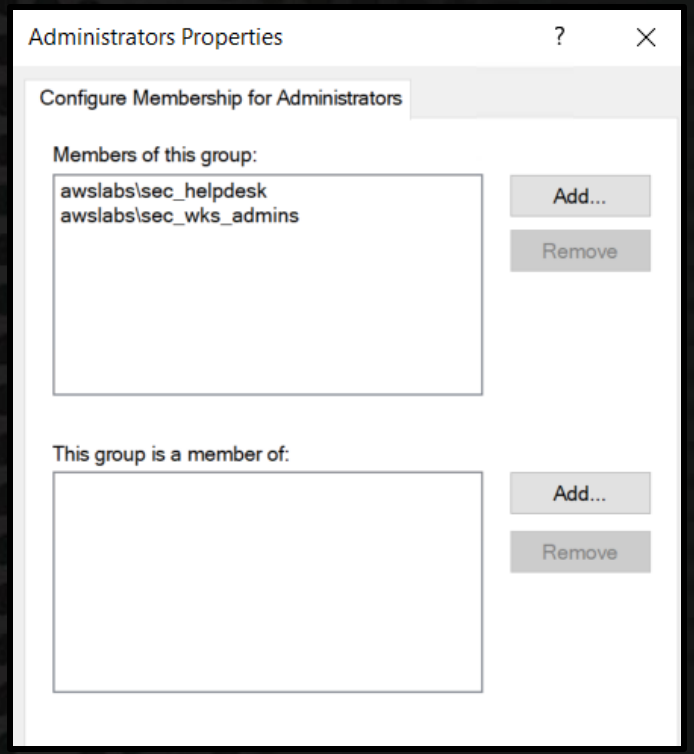


Dealing with Local Admins

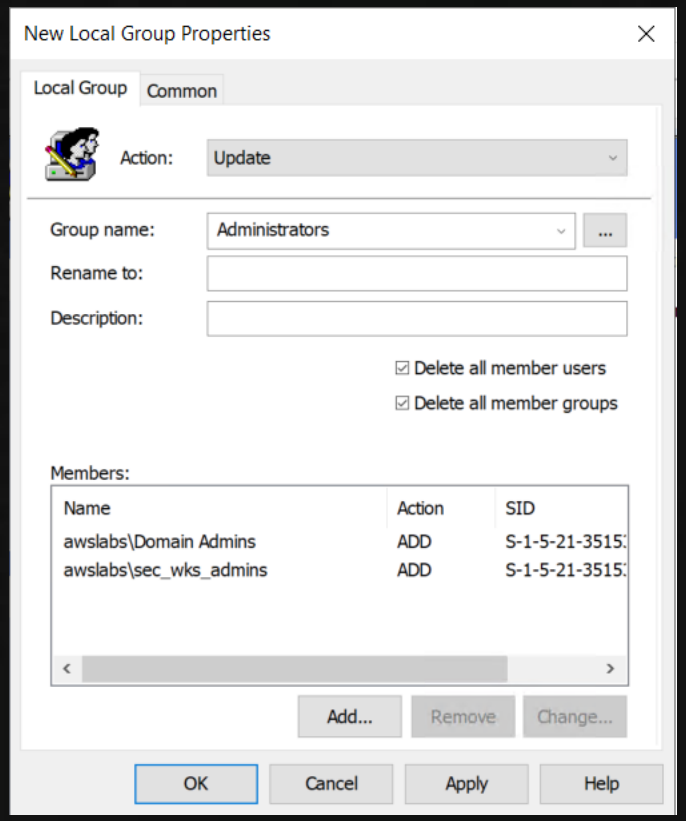
Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Restricted Groups
Members of this group: Add…
Computer Configuration -> Preferences -> Control Panel Settings -> Local Users and Groups
Update Administrators, Delete all members users/groups, Add specifics.

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

Via Policies:

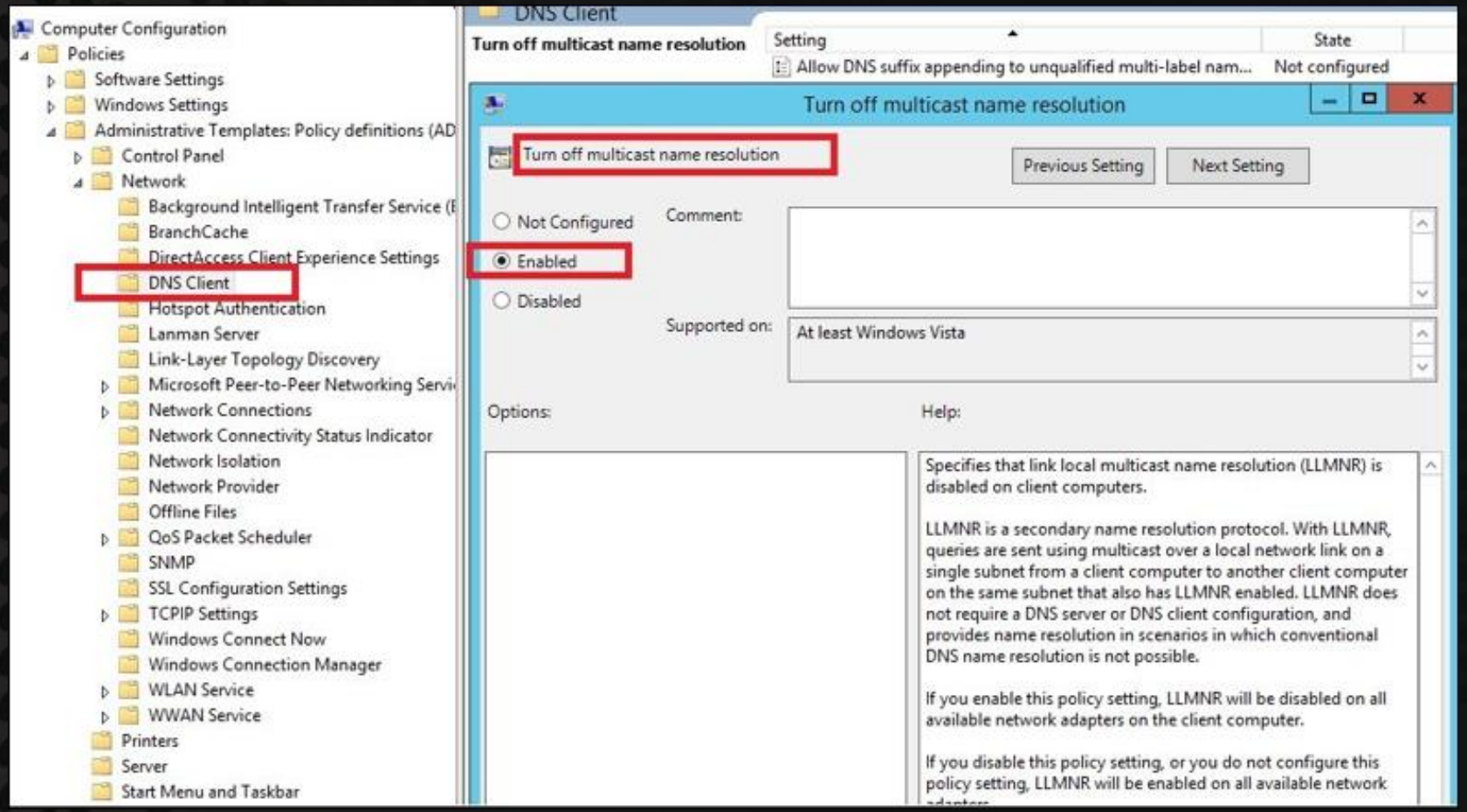


Via Preferences:



Addressing LLMNR
(NBNS and WPAD too)

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



Addressing LLMNR (NBNS and WPAD too)

Credit due:
http://blog.dbsnet.fr/disable-netbios-with-powershell

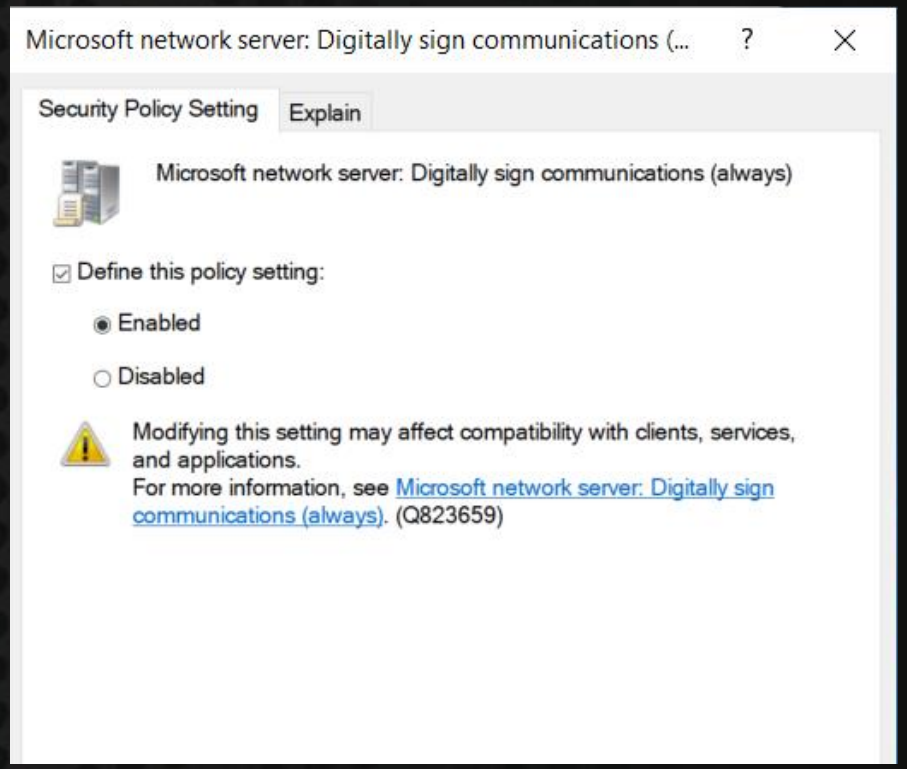
(Deploy that with a GPO ☺)

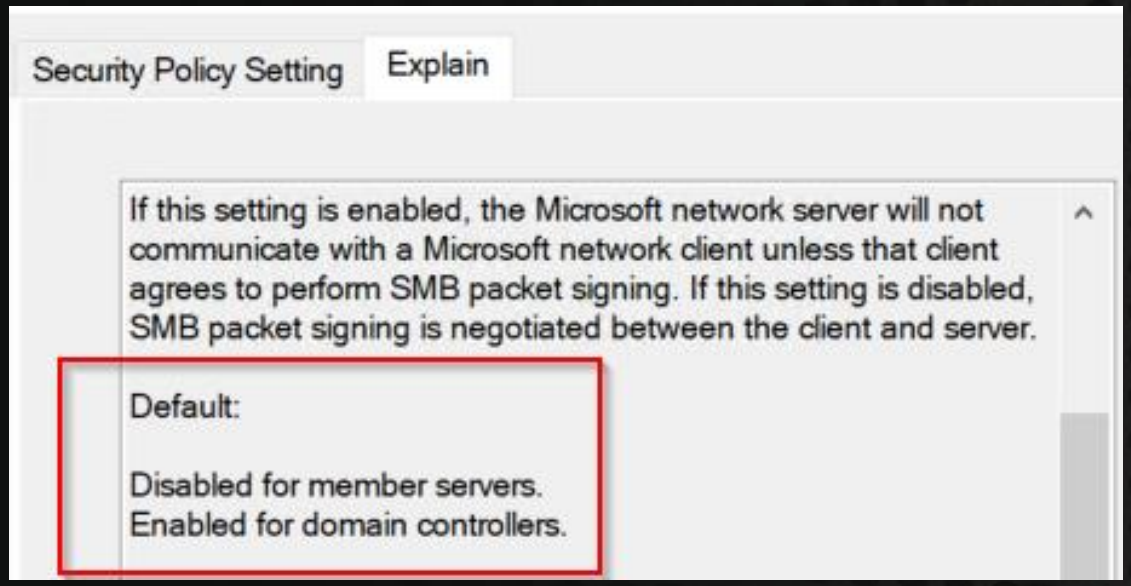
```
Write-Host("----- Disable NetBIOS by updating Registry -----")

$key = "HKLM:SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces"

Get-ChildItem $key |
foreach {
Write-Host("Modify $key\$($_.pschildname)")
$NetbiosOptions_Value = (Get-ItemProperty "$key\$($_.pschildname)").NetbiosOptions
Write-Host("NetbiosOptions updated value is $NetbiosOptions_Value")
}

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)

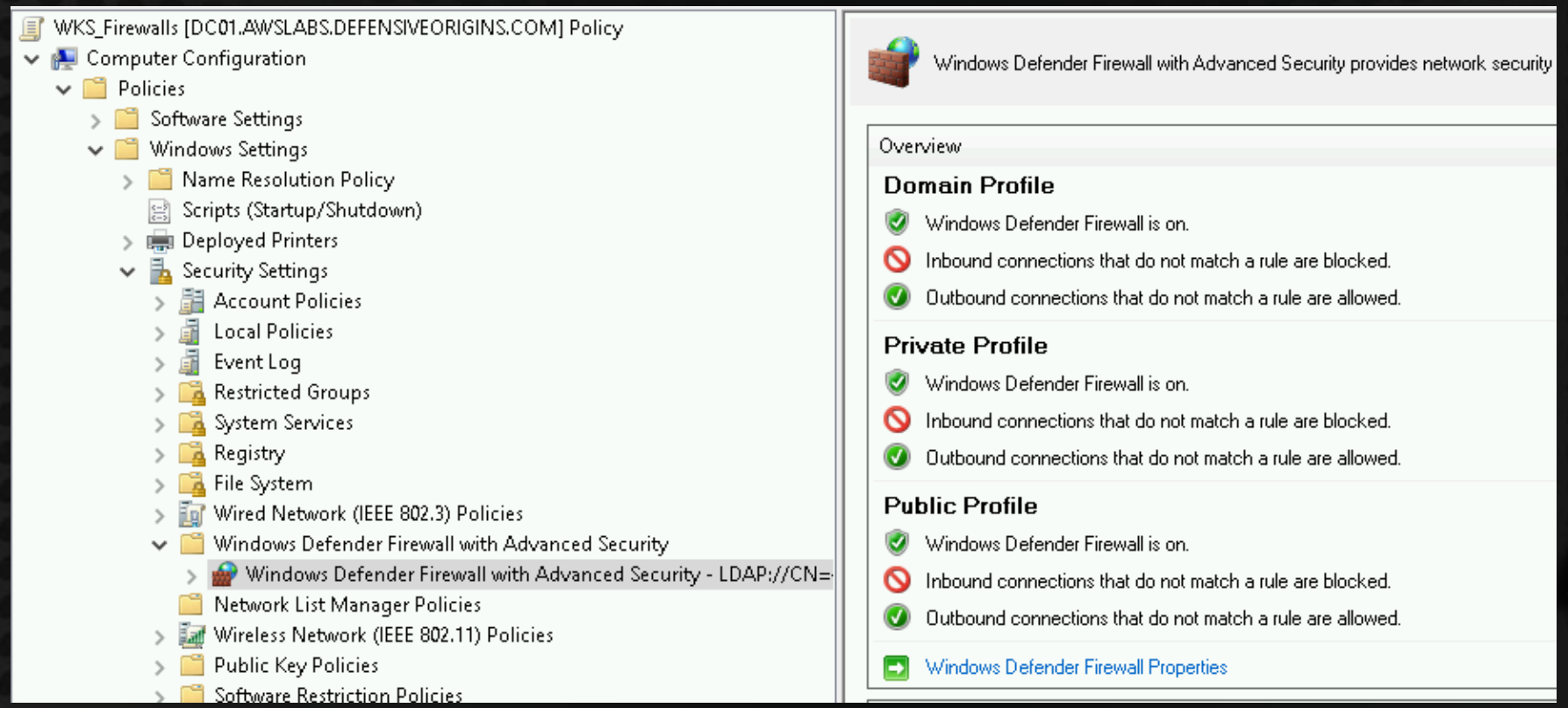




Configuring Host Based Firewalls

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

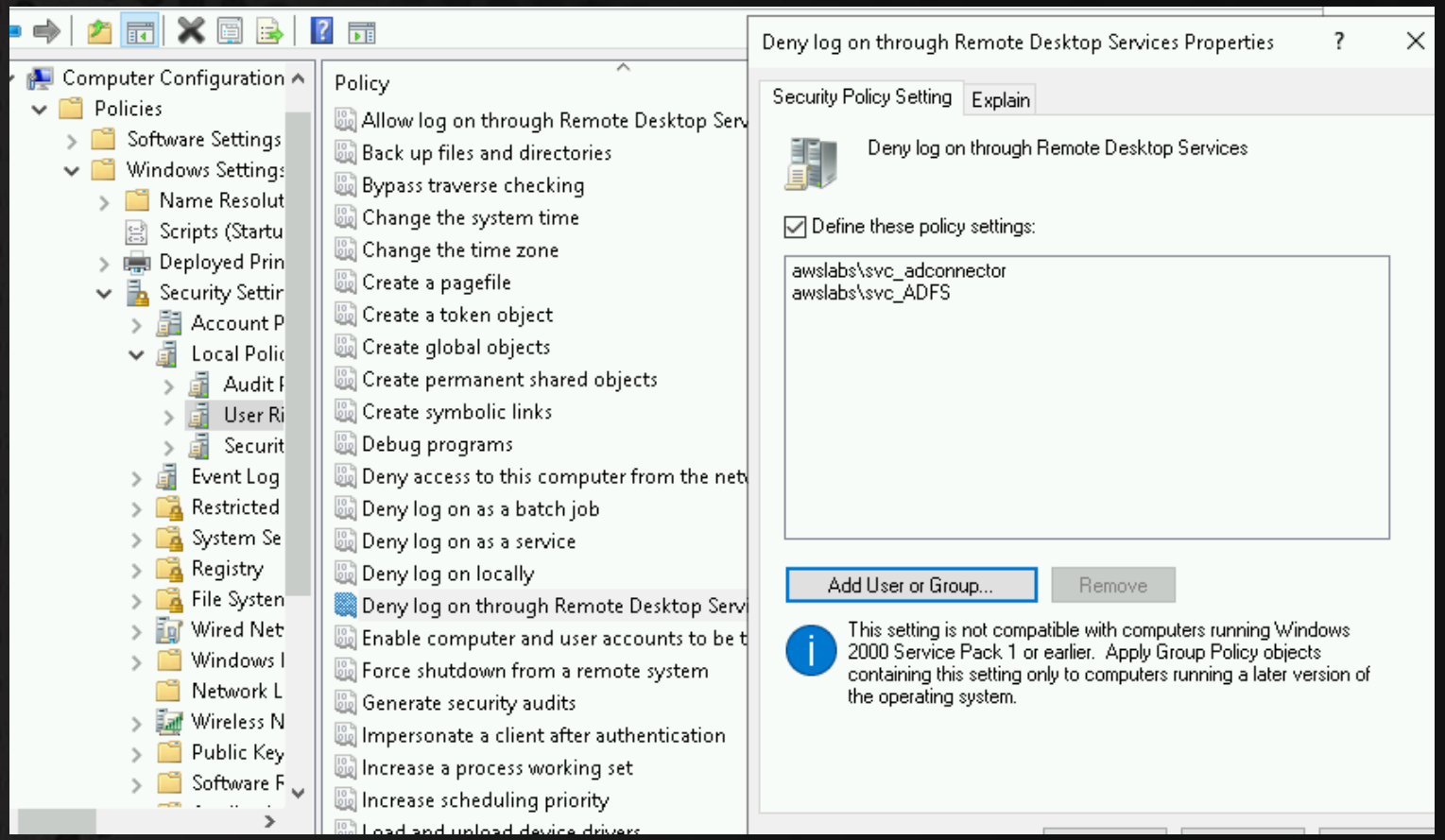
Start by turning them on. Really.
Your workstations don't need to talk to each other.
But, like Fine-Grained Password Policies, you might need something a bit more...*fine-grained...*



Limiting/Restricting Network Logons

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

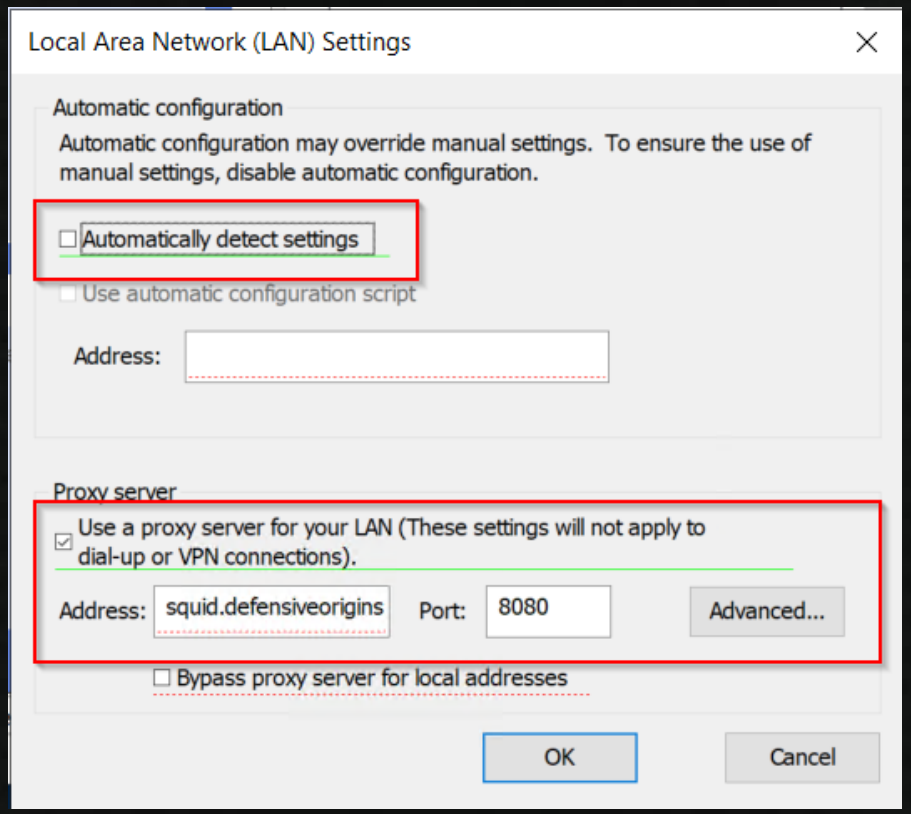
Why would a service account I cracked via kerberoasted hashes easily because the password was set to never expire by an admin in the late 90s need RDP to a DC?



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.

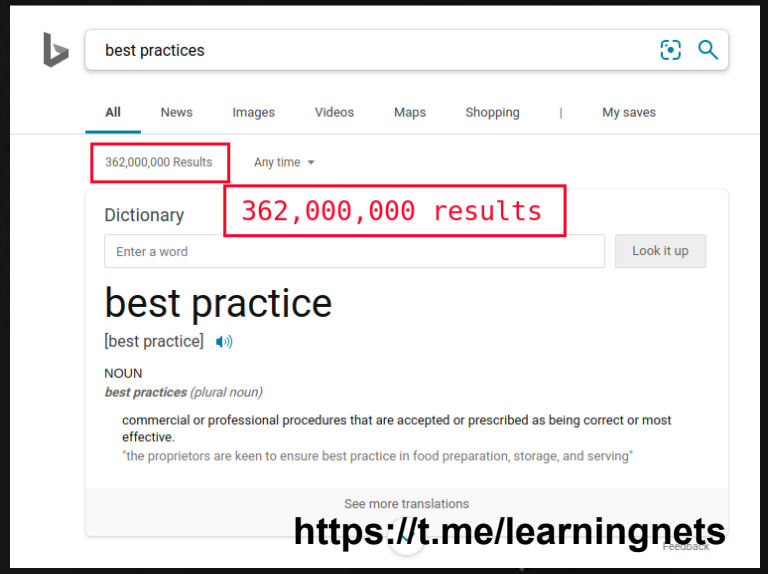
Network Logging and Alerting Section to Follow

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

"BEST PRACTICES"*

for network alertery.

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



https://t.me/learningnets

BLACK HILLS Information Security • 2008 •

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...

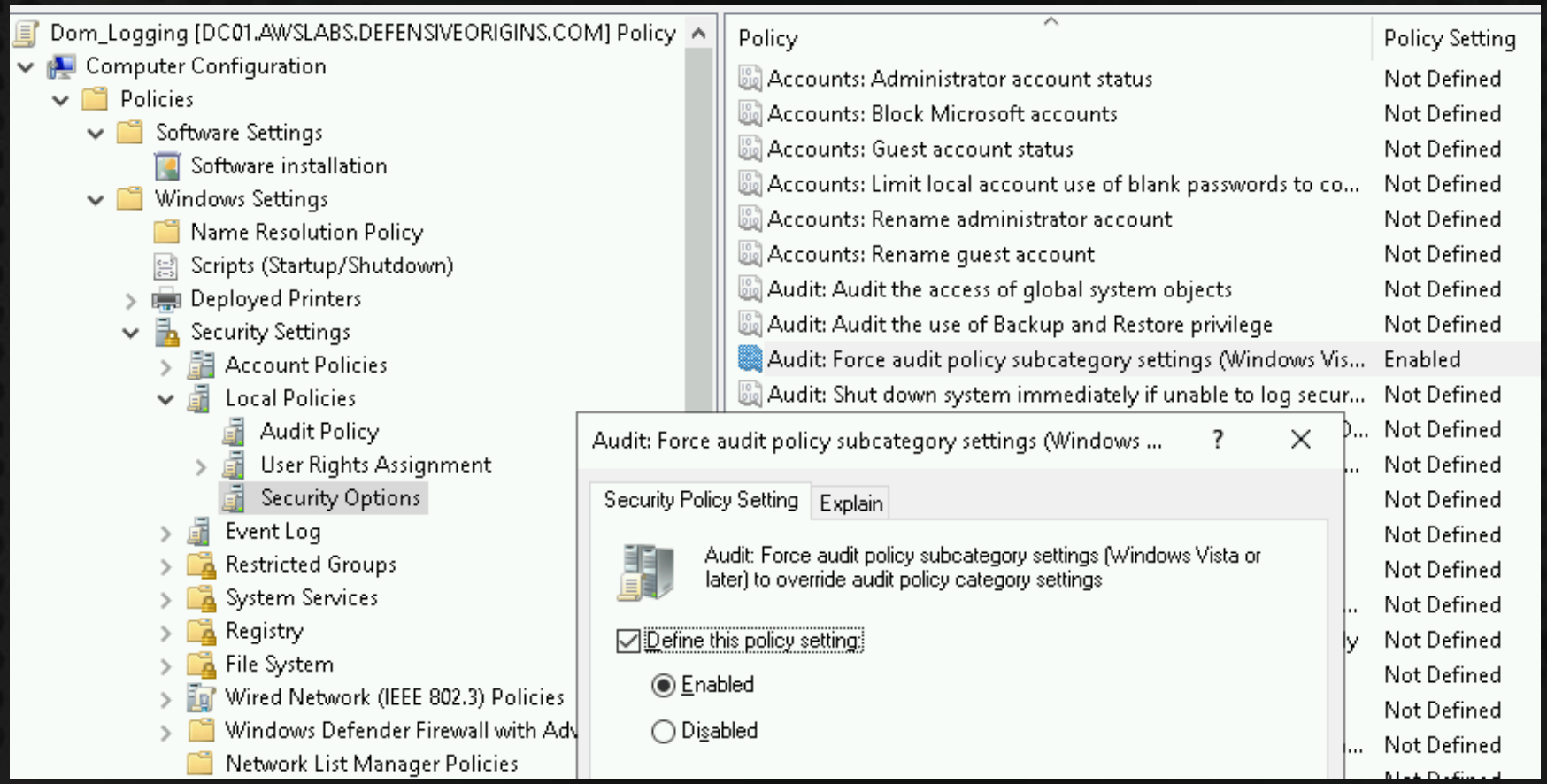
The IoC's might be in there somewhere...right? *wrong*

```
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
```

Windows Auditing and Logging Continued

Computer Configuration -> Policies -> Windows Settings-> Security Settings-> Local Policies -> Security Options
Audit: Force audit subcategory settings…: Enabled

Enable the force of audit policy to override “basic” and enforce “advanced” auditing

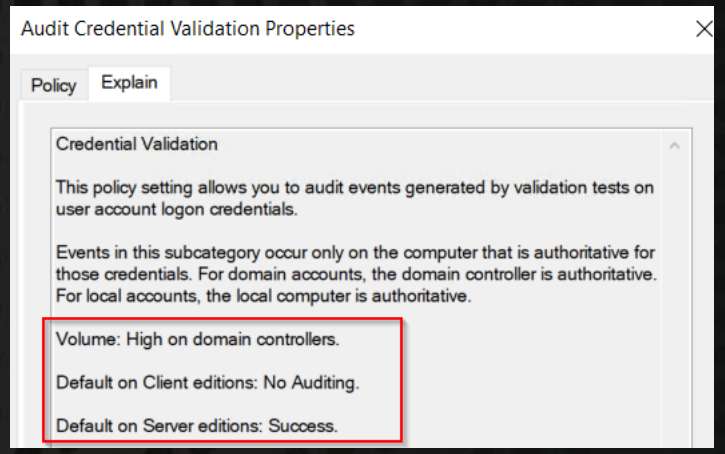


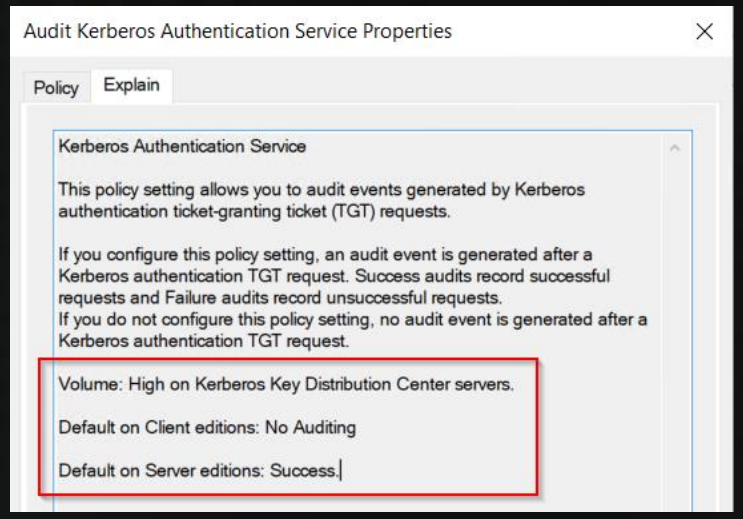
Kerberos Ticket Operations

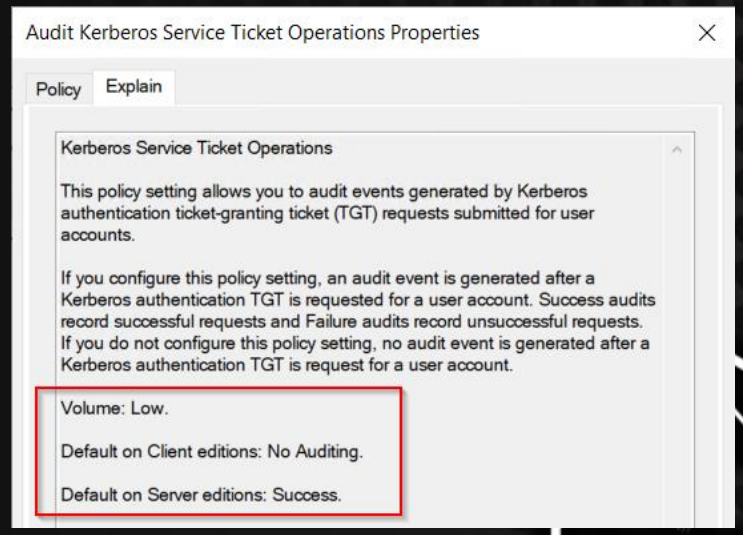
Computer Configuration -> Policies -> Windows Settings-> Security Settings-> Advanced Audit Policy Configuration -> Audit Policies -> Account Logon
Audit Credential Validation: Success and Failure
Audit Kerberos Authentication Service: Success and Failure
Audit Kerberos Service Ticket Operations: Success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

All those enabled audit functions still miss Kerberoasting.

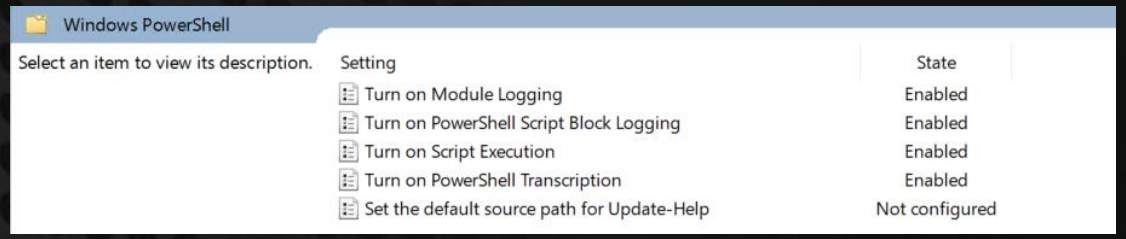
Subcategory	Audit Events
Audit Credential Validation	Success and Failure
Audit Kerberos Authentication Service	Success and Failure
Audit Kerberos Service Ticket Operations	Success and Failure
Audit Other Account Logon Events	Not Configured





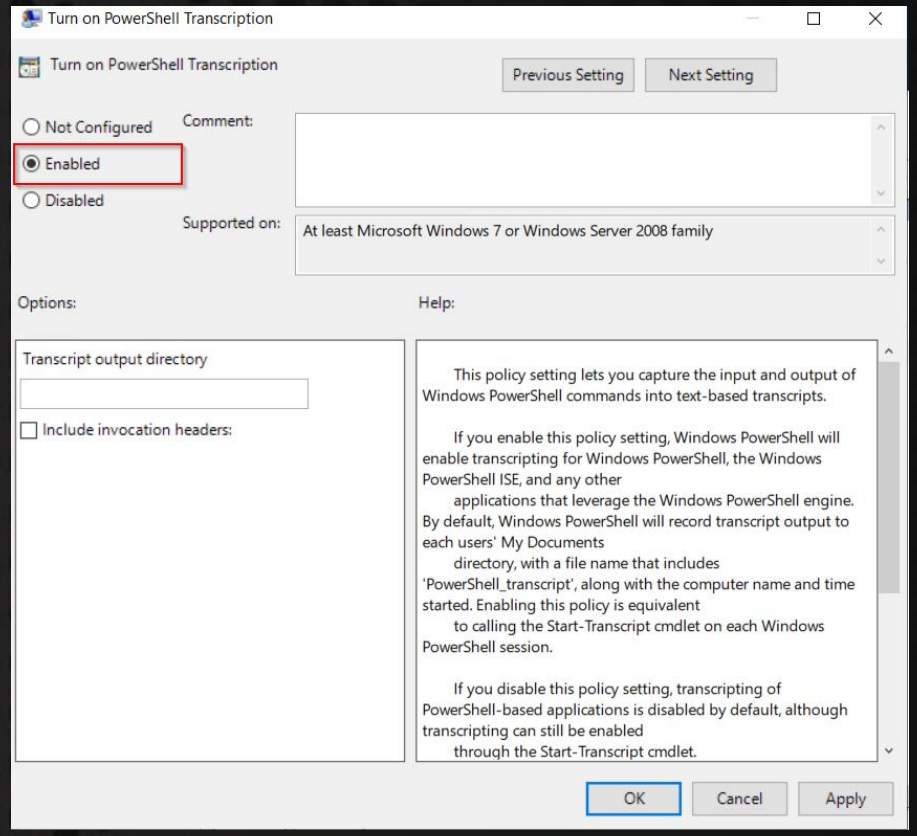


PowerShell and CMD Transcription

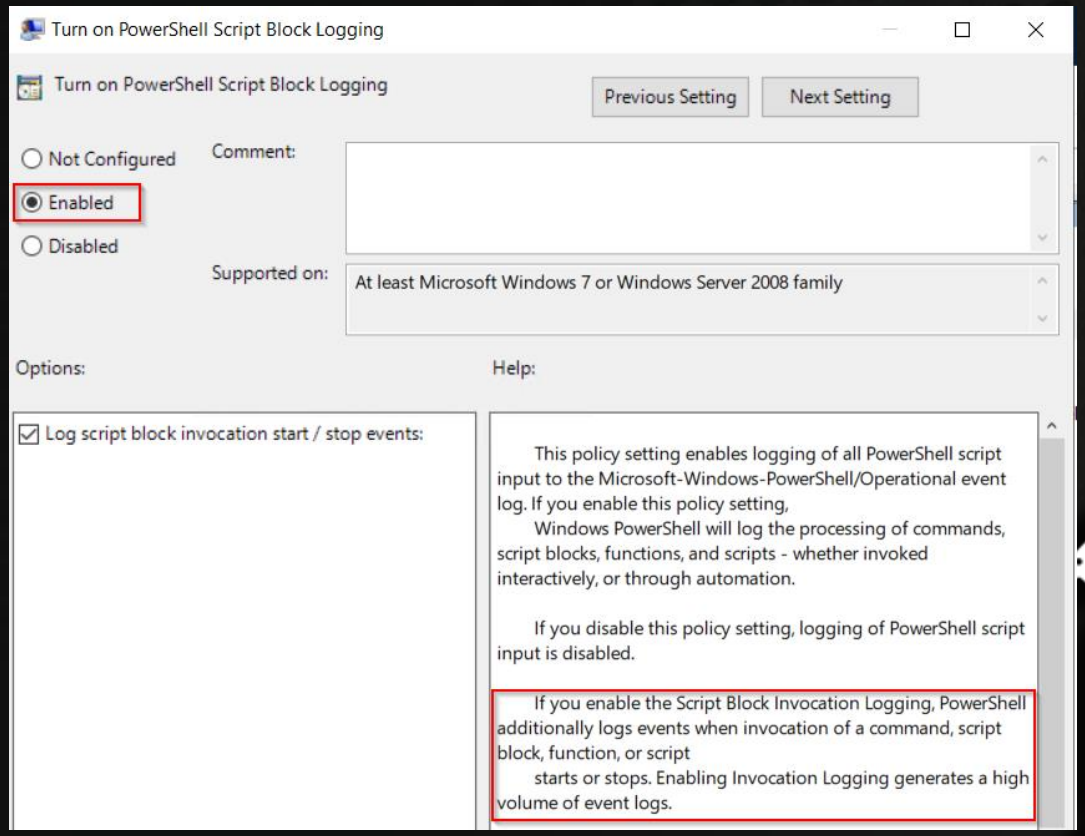


Computer Configuration -> Administrative Templates -> Windows Components -> Windows Powershell
Turn on Powershell Transcription: Enabled
Turn on Script Execution: Enabled, Allow only signed scripts
Turn on PowerShell Script Block Logging: Enabled, Log script block invocation start / stop events
Turn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

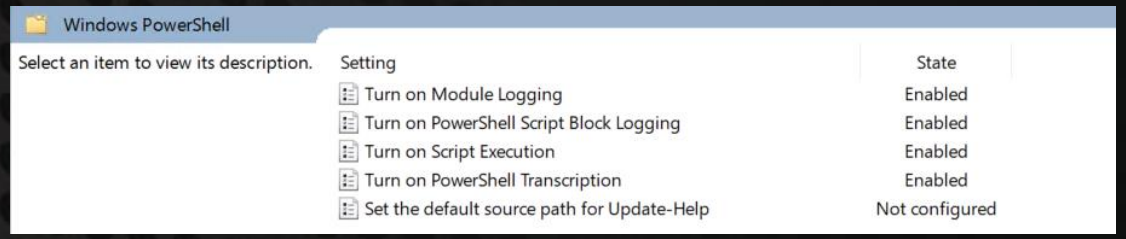
Powershell Transcription.



Powershell Script Block Logging.

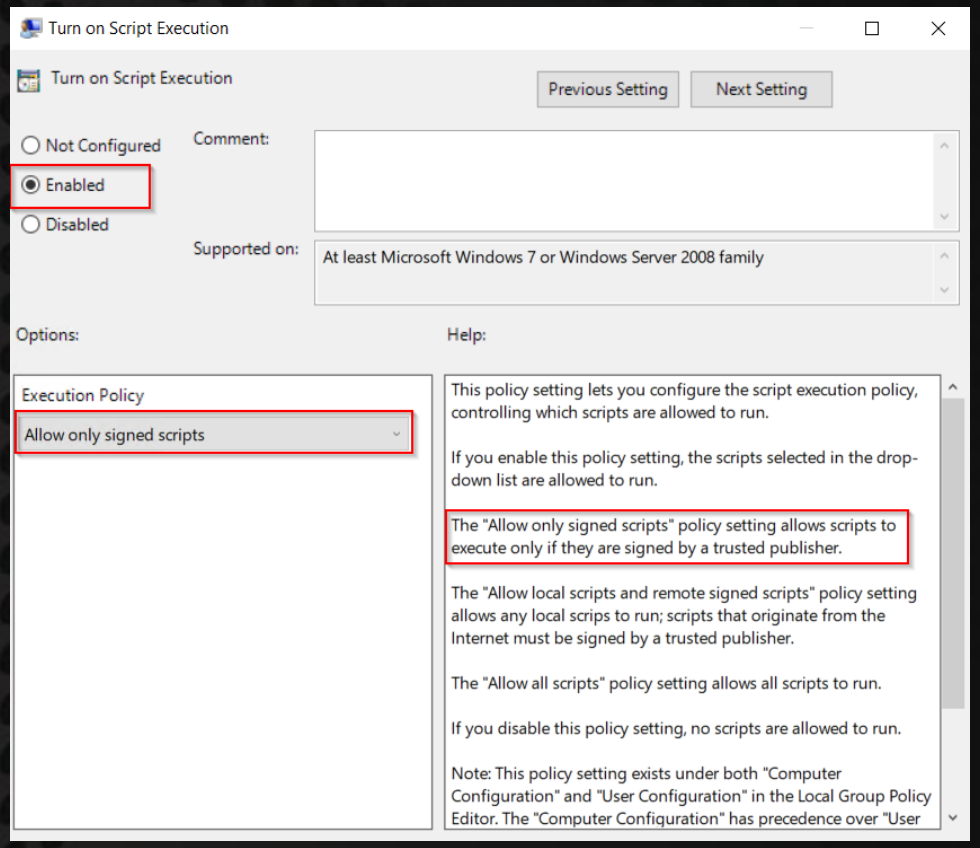


PowerShell and CMD Transcription

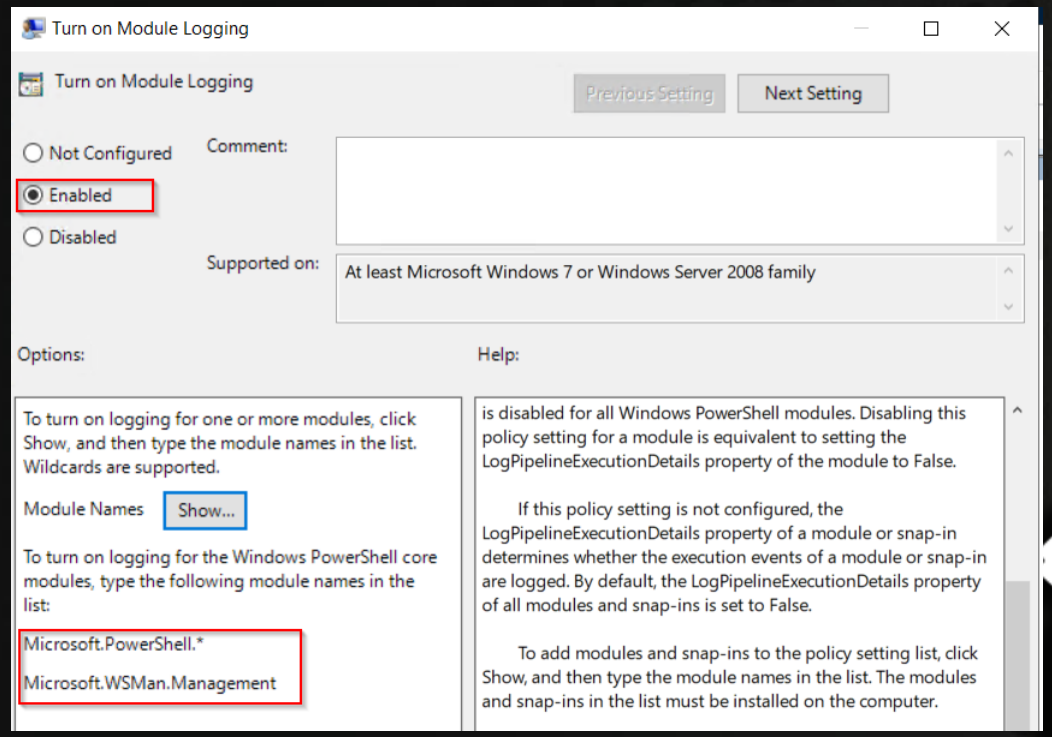


Computer Configuration -> Administrative Templates -> Windows Components -> Windows Powershell
Turn on Powershell Transcription: Enabled
Turn on Script Execution: Enabled, Allow only signed scripts
Turn on PowerShell Script Block Logging: Enabled, Log script block invocation start / stop events
Turn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

Script Execution.



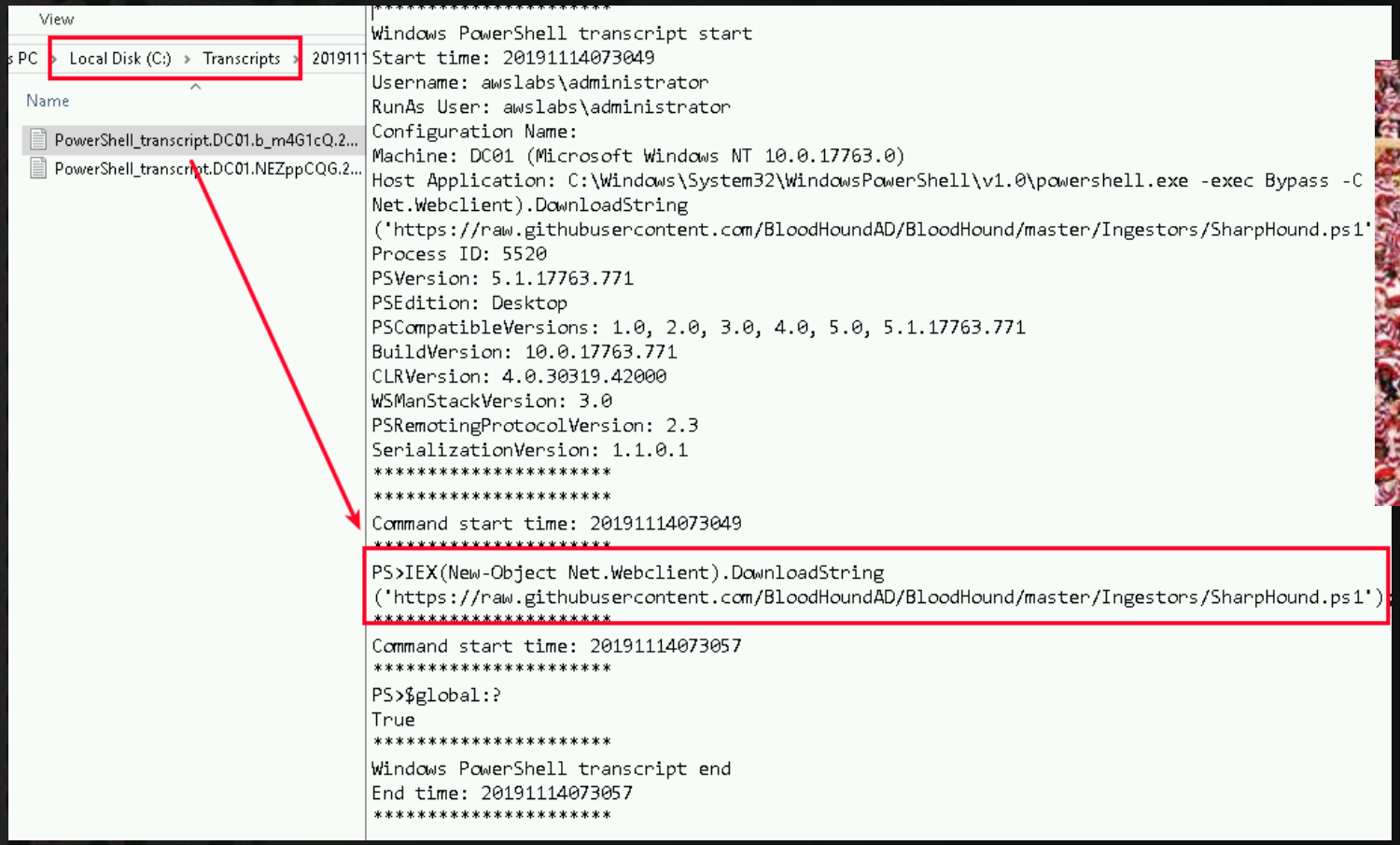
Module Logging



BLACK HILLS Information Security • 2008 •

Transcription Results

Found you!

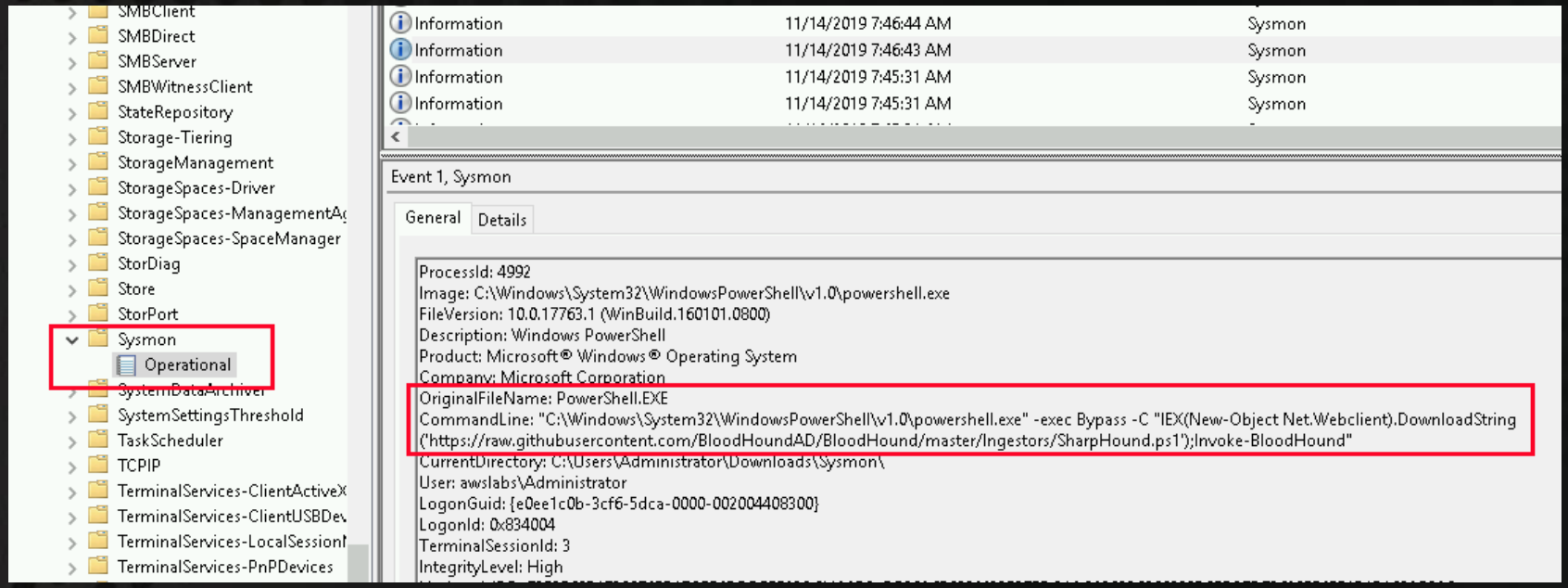


Installing SysMon

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/



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”