

The Quest for the Kill Chain Killer

Defend Thyself, Thy Networks, and Thy Domains from Thy Enemies



© Black Hills Information Security
@BHInfoSecurity

Biographies



Kent Ickler	Jordan Drysdale
Hacker	Hacker
Pentester	Pentester
Researcher	Researcher
SysAdmin	SysAdmin
Trainer	Trainer



© Black Hills Information Security
@BHInfoSecurity

We were a little stumped…



What Changed in the Last Year?

- Threat vectors moved to the employee's home network
- Supply Chain Management (and CICD gets hacked)…

- But… Ransomware still kicking butt.
- Service Misconfiguration… still… (*cough* unsecured databases)

© Black Hills Information Security
@BHInfoSecurity

Too much fail



And yet…

Targeted attacks are even less needed than before.

Our baselines defenses must grow.



© Black Hills Information Security
@BHInfoSecurity

The Kill Chain –
Its much more than just low hanging 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

© Black Hills Information Security
@BHInfoSecurity

Active Directory Best Practices to Frustrate Attackers



It's easy to make things hard,

But it's not hard to make things easy.

https://www.blackhillsinfosec.com/active-directory-best-practices-to-frustrate-attackers-webcast-write-up/

© Black Hills Information Security | @BHinfoSecurity

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~~ Understand your stack!
Centralized Logging
Internet Filtering – Ingress/Egress
Workstation Internet Proxy –
Honeypots & Cyber Deception
Av/AntiMalware/EDR. Yes, Defender.
Baseline Analyzer – includes MS's RSOP
Ping Castle / Control Path Analysis.
Credential Management
Password Age/Complexity exemptions!?
VPNs… MFA
Reconnaissance

WFH? Yes.

You need to know these.

You need to practice these.

Clean what you inherit.

Make the world a better place.

© Black Hills Information Security
@BHInfoSecurity

Active Directory (still)



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

<u>Job Functional Mail Enabled Security Groups…</u>

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…

© Black Hills Information Security

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.

© Black Hills Information Security
@BHInfoSecurity

Layer Two Protocols

- mDNS
- LLMNR
- NBNS
- DHCP[v6]
- ARP, SNACs

Gather around folks, let's have a chat.

Why are we still talking about this?

More than 50% of *enterprises...*

- *Still have support for LLMNR and NBNS*
- *Allow privesc with this tradecraft*



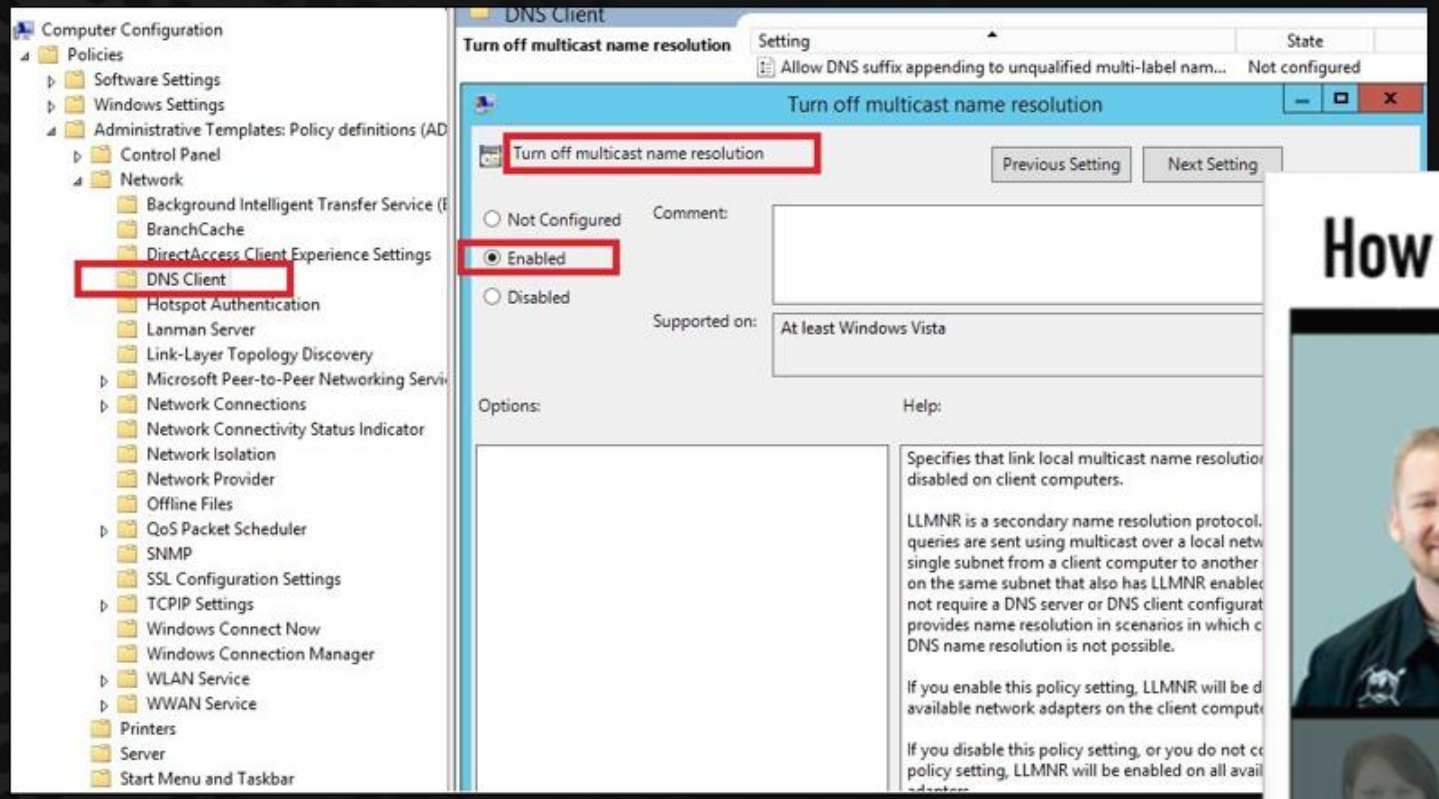


© Black Hills Information Security
@BHInfoSecurity

Addressing LLMNR

(NBNS and WPAD too)

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



https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/ (2018)



© Black Hills Information Security
@BHInfoSecurity

New in 2021!

<RANT Length=3Slides>

This (really) grinds my gears.

The Unaddressing LLMNR

(or)

The disabling of the enabling of the disabling GPO.

(or)

The internet Isn’t always a SysAdmin's best friend.



© Black Hills Information Security
@BHInfoSecurity

Un-Addressing LLMNR
(And making Dentistry Vulnerable)

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

KB5001330

DENTRIX

Unable To Connect To Database / eSync Connectivity Issues / Registration Issues Due To Windows Update - KB5001330 (4/14/2021)

Article Number
000055722

https://hsione.force.com/dentrixguest/s/article/Unable-To-Access-Common-Folder-Due-to-Windows-Update-KB001330

Update 4/14/2021 4:20pm Eastern Time:

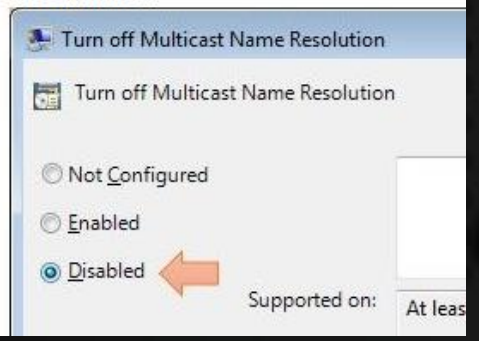
After working with Microsoft, we believe that we have found a solution that allows you to keep the critical Microsoft Security Update installed. It appears that this issue can be resolved by enabling "Link Layer Multi-cast Name Resolution" (LLMNR). Re-enabling this group policy seems to restore proper IP Address resolution which in turn restores connectivity to the Dentrix Database. To enable LLMNR, follow the steps below.

Enable LLMNR Using

1. Go to Start>Run
   - This should
2. Use the Group Policy Editor to navigate to Local Computer Policy > Computer Configuration > Administrative Templates > Network > DNS *Client* (see screenshot 1 below)
3. Double-Click "Turn Off Multicast Name Resolution"
4. Mark the radio button labeled "Disabled" (see screenshot 2 below)
5. Click Apply and OK
6. Open a Windows Command Prompt Window (Start>Cmd.exe) and enter the command ***ipconfig /flushdns*** <press enter> (see screenshot 3 below)

STOP, JUST STOP.

Screenshot 2:



© Black Hills Information Security
@BHInfoSecurity

BLACK HILLS Information Security • 2008 •

New in 2021: Update Madness

This really isn't new at all.

9 days later…

Details

Update 4/23/2021 2:00pm Eastern Time:

Microsoft has issued a KIR (Known Issue Rollback) to Windows 10 HOME edition PCs that have installed the KB 5001330 update. This KIR restores hostname DNS resolution to workgroup PCs where LLMNR has been disabled. Users of Windows HOME edition should have already had this KIR Applied automatically but users of Windows 10 Pro\Enterprise and Server 2019 will need to install it if they wish to disable LLMNR. Activating this KIR and turning off Link Layer Multi-cast Name Resolution will involve multiple steps but combined should take no more than 5 minutes per station. These steps should be completed on the server and all workstations.

Step 2: Re-enable the group policy to disable LLMNR (not applicable to Windows Home users)

Important Notes:

- These steps will reverse the suggestion made in the second update on 4/14/2021
- Windows HOME edition users please contact Henry Schein One Support to have LLMNR disabled via PC Registry

1. Go to Start>Run and type ***GPEdit.msc*** <press enter>
   - This should open the Local Group Policy Editor
2. Use the Group Policy Editor to navigate to ***Local Computer Policy>Computer Configuration>Administrative Template>Network>DNS Client*** (Step 2 Image 2 Below)
3. Double-Click "Turn Off Multicast Name Resolution"

https://hsione.force.com/dentrixguest/s/article/Unable-To-Access-Common-Folder-Due-to-Windows-Update-KB001330

Dentrix: I don't blame you….. mmm…ish

It was a risk-balance.
You had a commitment to getting your customers working fast.
And… you called Microsoft.

<u>But…?</u>
The internet TRUSTED you without regard of context.
They reposted, repasted, affirmed, and told everyone the "fix" to KB5001330 was LLMNR.
ITS BAD. There are posts for unrelated issues of KB5001330 saying "just enable LLMNR" too, because it fixed Dentrix's problems.

Was the LLMNR risk acknowledged (before 9 days later)?
Why did this even happen? SMBv1? Programming in protocol margins?
Do you test your typical customer environments with OS updates? CICD?
What even are "Best Practices"? For Clients? For Vendors? … For MSPs?

© Black Hills Information Security

New in 2021: Update Madness

This really isn't new at all.



- Addresses an issue that might cause File Explorer and other applications to stop responding for several minutes. This issue occurs after a client reconnects to the corporate network and attempts to use mapped drives to access file shares on the corporate network.
- Addresses an issue that prevents Server Message Block 1 (SMB1) clients from accessing the SMB share after restarting the LanmanServer service.

KB5000842 optional update caused problems.

But…

KB5001330 April Cumulative Update (mandatory) included it.

Hey MSPs – I don't blame you either (ish)… except…

What happened to testing updates before rollout?

Hey Internet – I don't blame you either. We all want those sweet social-media upvotes too… (or something)/s.

© Black Hills Information Security

@BHInfoSecurity

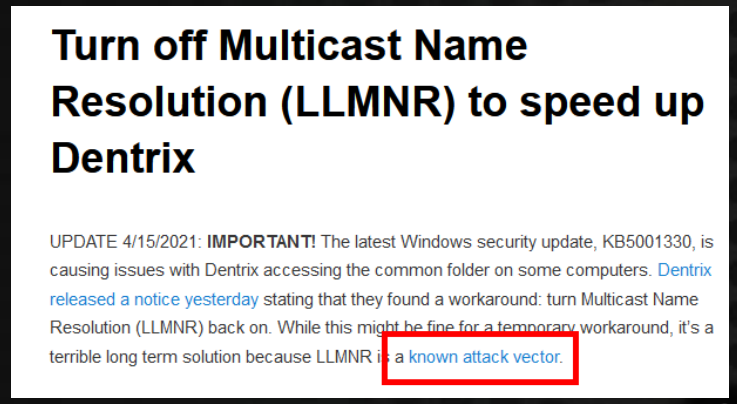
https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/

</RANT>

THANK YOU for everyone on the forums, Reddit, Twitter, etc. that linked our blog in the KB5001330 craziness.
Sometimes "Best Practices" are ignored for expediency.
Your reminders of the risks of "quick fixes" may have saved someone's data (and business).

There are many, many others that sounded the alarms at the danger of enabling LLMNR.

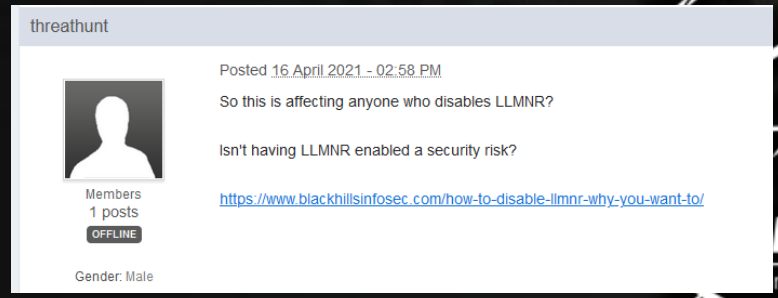
Thank you to all that did. Here are a couple examples:



Turn off Multicast Name Resolution (LLMNR) to speed up Dentrix

UPDATE 4/15/2021: **IMPORTANT!** The latest Windows security update, KB5001330, is causing issues with Dentrix accessing the common folder on some computers. Dentrix released a notice yesterday stating that they found a workaround: turn Multicast Name Resolution (LLMNR) back on. While this might be fine for a temporary workaround, it's a terrible long term solution because LLMNR is a known attack vector.

https://www.jasonshah.com/turn-off-multicast-name-resolution-llmnr-to-speed-up-dentrix-treatment-planner/



threathunt

Posted 16 April 2021 - 02:58 PM

So this is affecting anyone who disables LLMNR?

Isn't having LLMNR enabled a security risk?

https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/

Members
1 posts
OFFLINE

Gender: Male

https://www.bleepingcomputer.com/forums/t/748863/kb5001330-dns-issues-anyone/page-3

© Black Hills Information Security
@BHInfoSecurity

Addressing NBNS

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 -----")
```

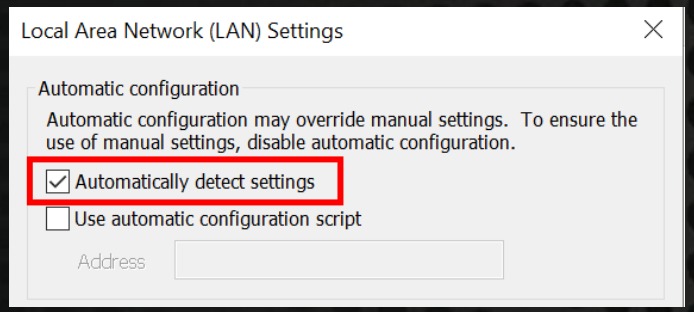


© Black Hills Information Security
@BHInfoSecurity

Addressing WPAD

WPAD MiTM Internet Filtering? Ok. Else?
Disable WPAD
This involves regkey based GPOs, gross (but effective).

Protocol	Length	Info
LLMNR	84	Standard query 0xaee8 A wpad
LLMNR	64	Standard query 0xaee8 A wpad



- (maybe not) less gross:
  - create an invalid wpad A record in DNS.

    After Windows Vista, LLMNR is used only if DNS Fails.

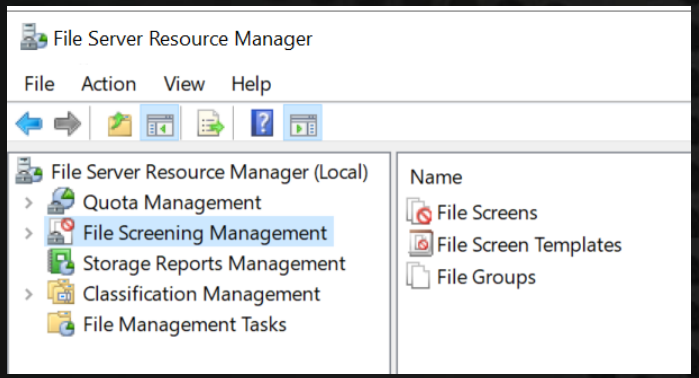
- (This will break Win 10 <= 1703 Registration /w AzureAD) [get >1703]
  - 1703 is EOL anyway :D

© Black Hills Information Security
@BHInfoSecurity

File Shares

- File Server Resource Manager (FSRM)
  - Disable the creation of LNK, URL, extensions of your choice
- Search your file shares for:
  - password
  - cred (covers credit card and credential*)
  - *.kdbx
  - *.vmdk *.vhd *.ova *.wim
  - Thousands of other terms, too...
    - Because your adversaries will
      - And so will your pentesters
      - Ransomware? Raccine





© Black Hills Information Security
@BHInfoSecurity

SMB Signing

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

- Lock it down.
- Easy win.



Disastrous vulnerability combinations

Step 1a: LLMNR / NBNS / mDNS lying around
Or
Step 1b: LNK / URL dropper files in shares

Step 2: No Signing? Relay poisoned responses

Step 3: No firewalls? No logon restrictions?



© Black Hills Information Security
@BHInfoSecurity

IPv6

- Control your endpoints, lest they get "MITM6'd" - Kyle Avery

```
mitm6 -d domain.segment
```

Some basic concepts (use /120s to align with IPv4 /24s)

- RA: router advertisement (attacker goes here)
- RS: router solicitation (client asks around)
- AAAA: DNSv6 records (attacker hijacks request/response pairs)

Step 2: No Signing? Relay poisoned responses

Step 3: No firewalls? No logon restrictions?



© Black Hills Information Security
@BHInfoSecurity

LDAP Channel Binding



When SMB signing is enforced...

...LDAP / LDAPS relay is an option

```
python3.9 ntlmrelayx.py -6 -t ldaps://dc01 -wh bhis-wpad
 --add-computer bhops47 --delegate-access -ts -of /opt/work/relays
 --dump-gmsa --dump-laps --sid -l /opt/work/loots
 --escalate-user john.strand
```

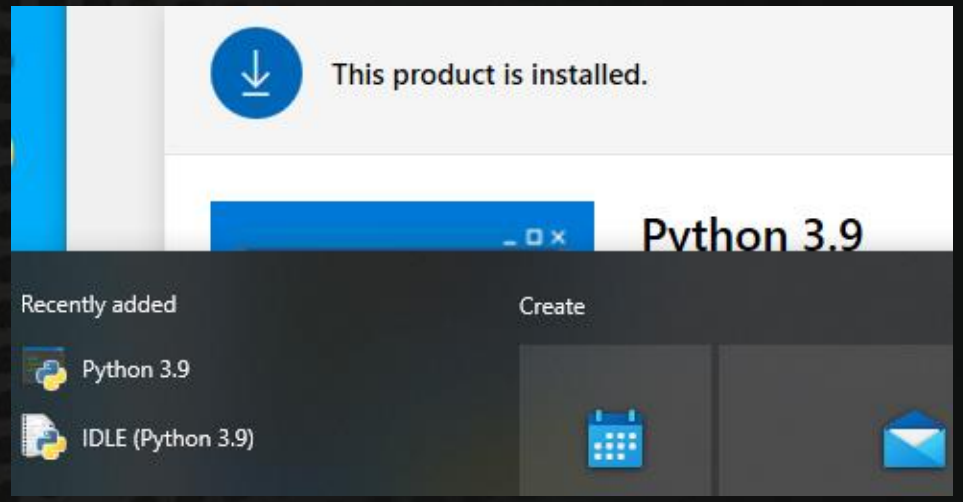
Unless you enforce LDAP signing or channel binding on your DCs

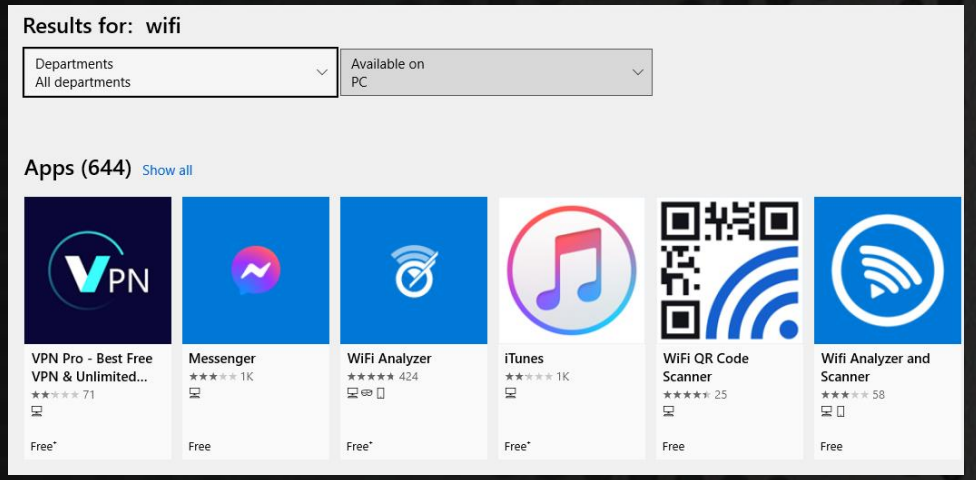


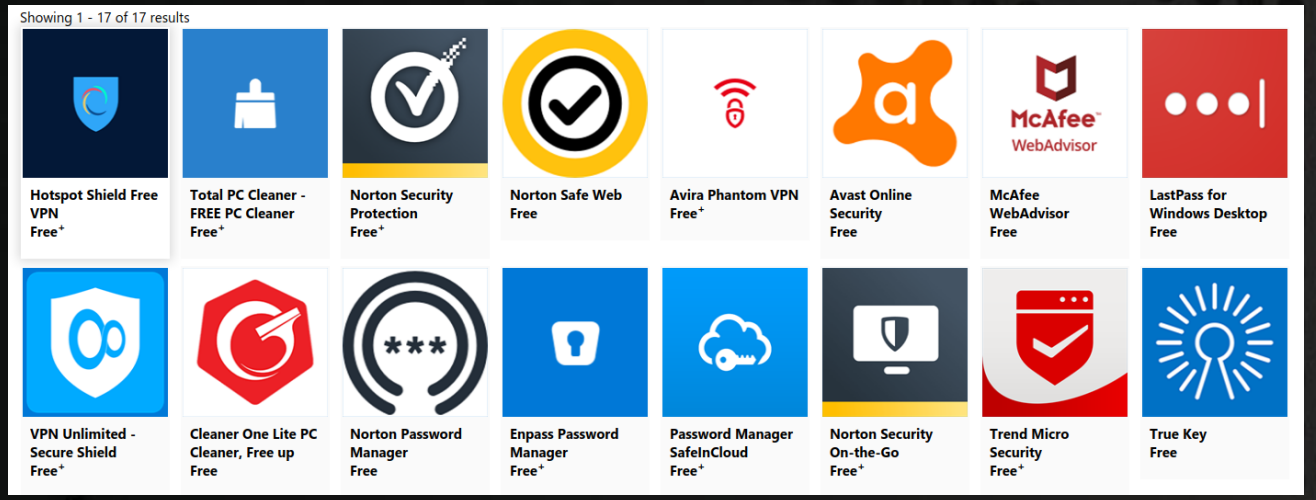
© Black Hills Information Security
@BHInfoSecurity

Microsoft Store

- The gift that keeps on giving. MS made it hard to get rid of...
- Port scanners, PrivEsc tools, and Python
- Why shouldn't users install IDLE?



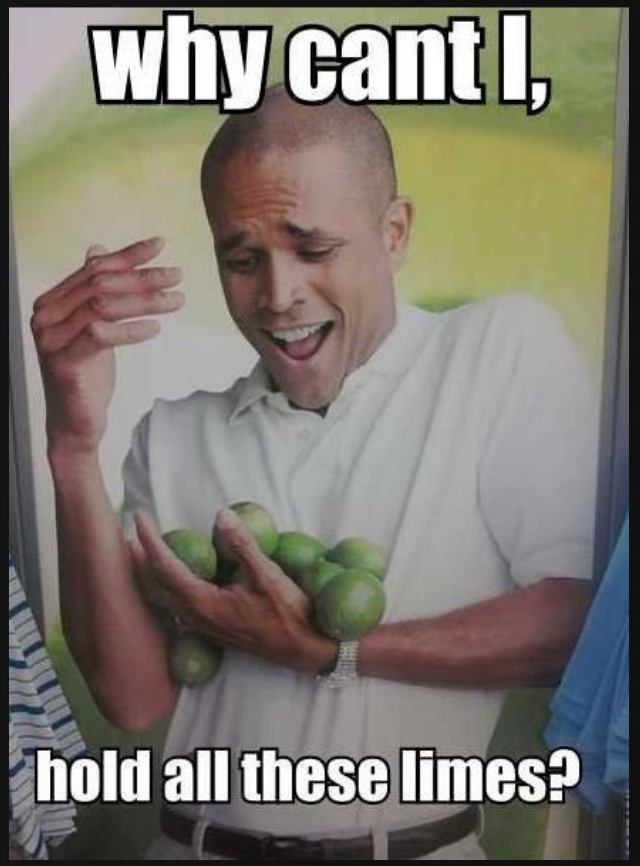




© Black Hills Information Security
@BHInfoSecurity

Top ~~10…13…16~~… Too Many GPOs to Cover Them All

Local admin Rename / LAPS
Event Logs / Sysmon / WEF
LLMNR / NBNS / WPAD
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
App Control / 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
NetCease



Original Material:

Group Policies That Kill Kill Chains

You can almost completely secure your environment with proper AD construction and GPOs

https://www.blackhillsinfosec.com/webcast-group-policies-that-kill-kill-chains/

© Black Hills Information Security
@BHInfoSecurity

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

LAPS!

You'll need the Administrative template files

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

LAPS gotcha of importance – cleartext local admin password stored in schema.

Restrict access with ADSIEdit

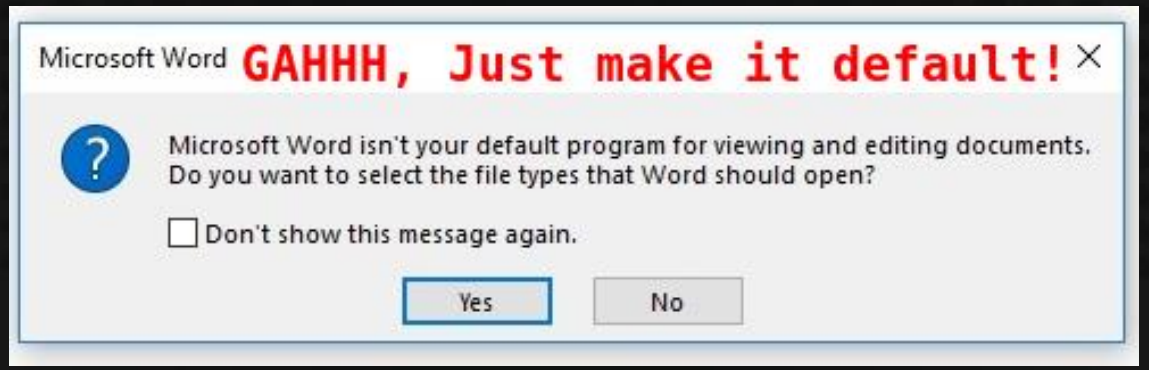
© Black Hills Information Security

Network Logons

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

- **Deny access to this computer from the network**
  - Can limit the impact of user compromise
- Also "**Protected Users**" configuration
  - No more weak Kerb keys (RC4)
  - No more Pass the Hash
  - No more unconstrained delegation
  - No more cleartext cached creds





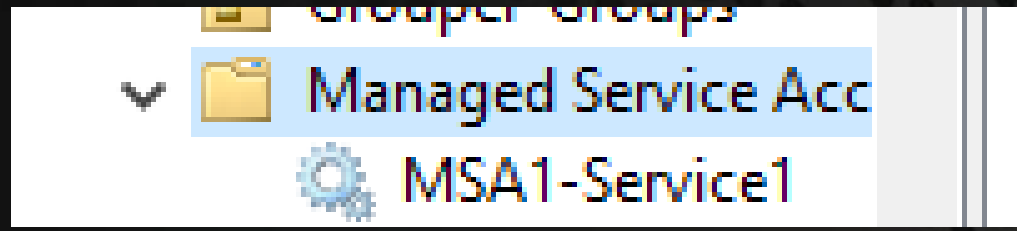
© Black Hills Information Security
@BHInfoSecurity

Managed Service Accounts

Please replace Bob and Linda's SQL accounts with these

- Standalone MSAs
  - Single password managed account
- Group MSAs
  - Best used for clustered solutions that require a single principal

```
New-ADServiceAccount -Name MSA1-Service1 -Path "CN = Managed Service Accounts, DC=dteclass, DC=com" -DNSHostName
MSA1.DTEClass.com
Set-ADServiceAccount -Identity MSA1-Service1 -PrincipalsAllowedToRetrieveManagedPassword AZRWWEBS1000000$
```



© Black Hills Information Security
@BHInfoSecurity

Application Controls



We may preach this one often, and understand it is a challenge (but so is ransomware to cleanup)

- Implement restrictions that prevent standard users from accessing cmd.exe, powershell.exe, and powershell_ise.exe.
- Use Microsoft **AppLocker** and/or **Windows Defender Application Control** to implement comprehensive application allowlisting
- Prevent standard users from accessing dangerous built-in utilities including (not limited to):
  - csc.exe (all instances) / cscript.exe / installutil.exe (all instances) / msbuild.exe (all instances) / mshta.exe / regasm.exe (all instances) / regsrv32.exe / runscripthelper.exe / wscript.exe
- The Microsoft Windows (or other host-based) firewall policy should be used to prevent commonly abused binaries from communicating over the network.



© Black Hills Information Security
@BHInfoSecurity

Speaking of RansomWare…

Did you see the Emergency Webcast?





BTW: Raccine
https://github.com/Neo23x0/Raccine

© Black Hills Information Security
@BHInfoSecurity

Firewalls

Limit access to SMB ports, at a minimum.
UDP 137, TCP 139, TCP 445

^ Over the Internet ? Don't give out hashes.

RPCs over SMB are more terrifying...like instantiating a dcsync...

```
bba640a7d6de18c87b1c3546bbea96
SMB         10.10.98.10     445    dc01             HREWWKS1000000$:des-cbc-md5:2a45f292f16
a7
SMB         10.10.98.10     445    dc01             HREWAPPS1000002$:aes256-cts-hmac-sha1-9
43f9d190408483127f60cf06f6ee7dc76099b40cbf487c363b0d41b2cda0e79
SMB         10.10.98.10     445    dc01             HREWAPPS1000002$:aes128-cts-hmac-sha1-9
29dd5ad00e604e02bc6b2e9df289a9c
SMB         10.10.98.10     445    dc01             HREWAPPS1000002$:des-cbc-md5:c2d9bcdaef
5b5
SMB         10.10.98.10     445    dc01             [+] Dumped 16619 NTDS hashes to /root/.
/logs/dc01_10.10.98.10_2021-01-28_023329.ntds of which 4081 were added to the database
^C
itadmin@localhost:/opt/CrackMapExec$
```





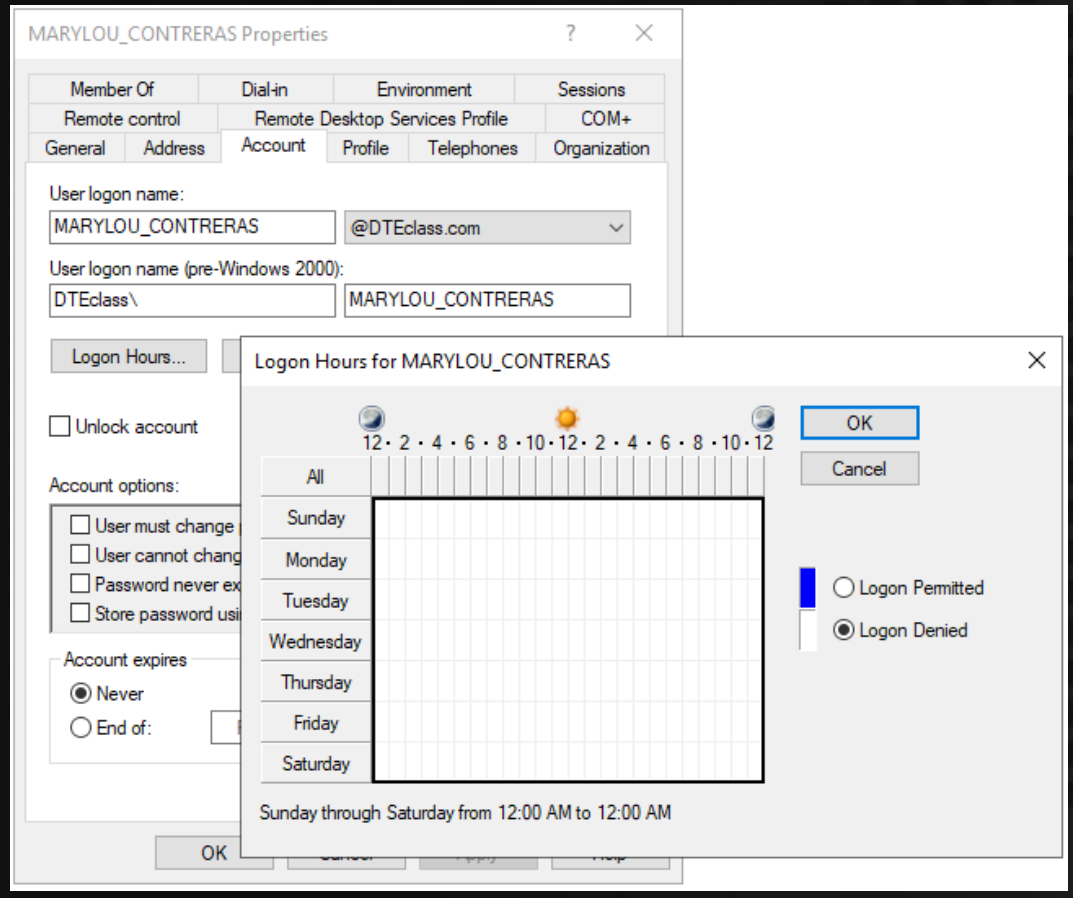
© Black Hills Information Security
@BHInfoSecurity

Canary Accounts, Services

- User Accounts; Internal / External
- Monitored for Login

- Set Logon times
- Logon at least once

- Make Documents
- Set Alerts!



© Black Hills Information Security
@BHInfoSecurity

Network Analysis



RITA is free

- Feed it Bro/Zeek logs
- Reap the benefits
  - Learn about your network's egress / ingress traffic
  - Find beacons before lettered agencies knock on your door

Major Features

The framework ingests Bro/Zeek Logs, and currently supports the following major features:

- Beaconing Detection: Search for signs of beaconing behavior in and out of your network
- DNS Tunneling Detection: Search for signs of DNS based covert channels
- Blacklist Checking: Query blacklists to search for suspicious domains and hosts

BLACK HILLS Information Security 2008

© Black Hills Information Security
@BHInfoSecurity

ACTIVE COUNTERMEASURES

Credentials to Rule Them All

- Credential Abuse:
  - Password Reuse
  - Password Sprays
  - Password Cracking
- Credential Hardening:
  - Password Policies
  - Password Management
  - New MS Playbooks ----->

New in 2021!

https://docs.microsoft.com/en-us/security/compass/incident-response-playbooks

Password spray investigation

04/29/2021 • 17 minutes to read •

This article provides guidance on identifying and investigating password spray attacks
remedial action to protect information and minimize further risks.

This article contains the following sections:

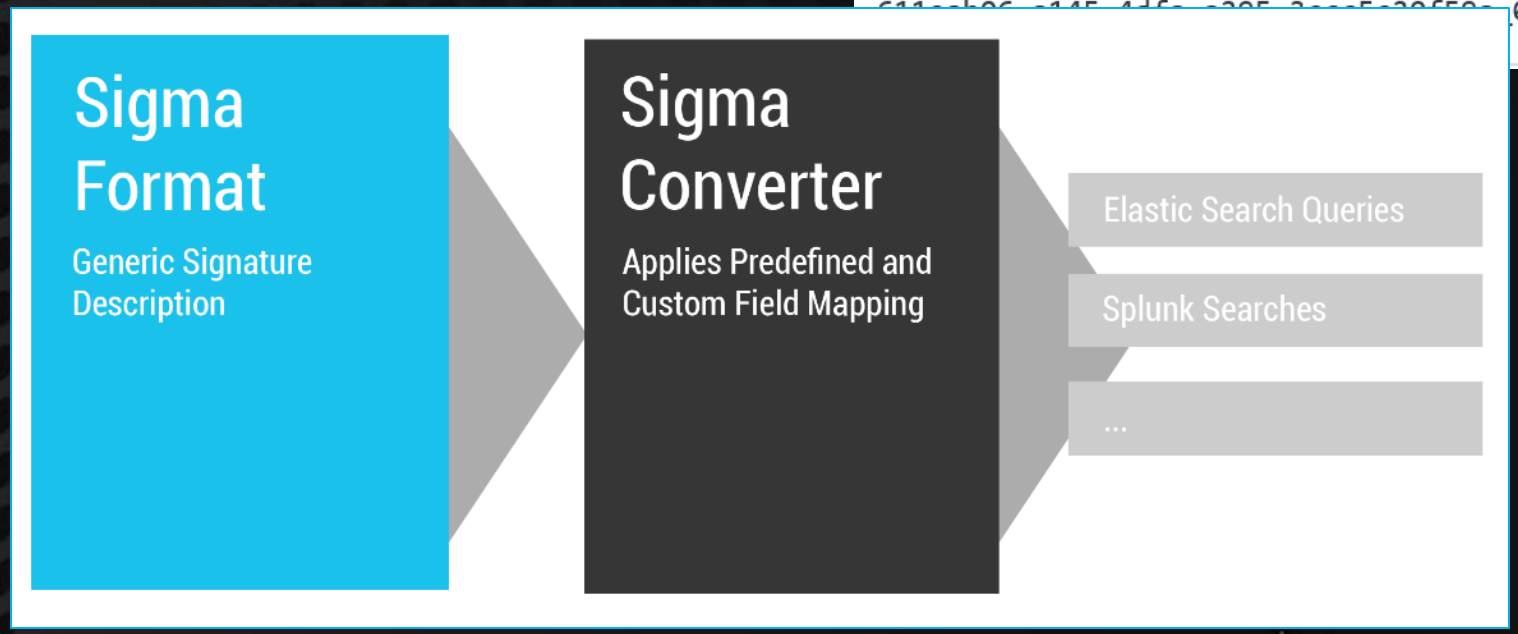
© Black Hills Information Security
@BHInfoSecurity

Logging, Detection, Visualization

Logging is hard.
Sigma is awesome.
And you can be too.

```
sigmac -t elastalert -c
sigmarulehere > elastalertrule.yml
```

rule_name
c539afac-c12a-46ed-b1bd-5a5567c9f045_0 Remote PowerShell Session 03
17d619c1-e020-4347-957e-1d1207455c93_0 Active Directory Replication from Non Machine Account
Windows-dcsync-non-dc_0
e4a6b256-3e47-40fc-89d2-7a477edd6915_0 System File Execution Location Anomaly
[illegible]0 Mimikatz DC Sync



- Splunk
- ElasticSearch Query Strings
- ElasticSearch Query DSL
- Kibana
- Elastic X-Pack Watcher
- Logpoint
- Microsoft Defender Advanced Threat Protection (MDATP)
- Azure Sentinel / Azure Log Analytics
- Sumologic
- ArcSight
- QRadar
- Qualys
- RSA NetWitness
- PowerShell
- Grep with Perl-compatible regular expression support
- LimaCharlie
- ee-outliers
- Structured Threat Information Expression (STIX)
- LOGIQ
- uberAgent ESA

Defending The Enterprise

16 Hour Course

- Reno, Nevada (June 15-16) + Virtual
- Virtual (July 13-16)

COURSE SCHEDULE

Dates/Times:	Dates/Times:
Tue, June 15, 2021 9:00 AM – 5:00 PM PDT	Tue, July 13, 2021 11:00 AM – 4:00 PM ET
Wed, June 16, 2021 9:00 AM – 5:00 PM PDT	Wed, July 14, 2021 12:00 PM – 4:00 PM ET
Event Type: In Person	Thu, July 15, 2021 12:00 PM – 4:00 PM ET
Event: Way West 2021	Fri, July 16, 2021 12:00 PM – 4:00 PM ET
Location: Nugget Casino Resort, Sparks, NV	Event Type: Virtual
Instructor: Kent Ickler	Instructors: Kent Ickler and Jordan Drysdale
Register to attend this course in-person here	Register to attend this course virtually here

https://wildwesthackinfest.com/training/defending-the-enterprise/

WILD WEST HACKIN' FEST

DEFENSIVE ORIGINS

BLACK HILLS Information Security 2008

© Black Hills Information Security
@BHInfoSecurity

Questions

- Black Hills Information Security
  - http://www.blackhillsinfosec.com
  - @BHInfoSecurity
- Jordan and Kent
  - @rev10d
  - @krelkci



© Black Hills Information Security
@BHInfoSecurity