PALM SPRINGS An oldie

The VDI lockdown guide: Security truths your users don't want you to know

Who is this dude?

- 2x father, nerd, & hacker since the late '80s, joined the Marines, did some tours in Iraq, and now click and draw on things in the security consulting world to try and make things better.
- Passion for EUC, computer security, scouting, and racing (NASA, SCCA, Chump).
- Founding board member of the World of EUC.
- Security Nerd at VDISEC (Focus on VDI security and privacy).
- Speaker:
 - E2EVC, DerbyCon, XenAppBlog, EUC Masters Retreat, Citrix Synergy, Citrix User Groups, BSides, CUGC XL Events, VMUG Events, and VMWorld.





Presentation goal

- Spoiler alert: There is not one magical silver bullet, Achilles' heel, Infinity Gauntlet, Muramasa Blade, Adamantium, or Kryptonite that will make this problem go away. My goal is to get you to think about:
- Your VDI deployments differently.
- The data in your applications.
- How someone could take your data out or do things they shouldn't be able to.
- One tip you can take back and apply to your deployment after testing to secure it. Don't think you can "secure all the things' after the presentation, but you can make it more secure.



What is this VDI security you speak of?

VDI security self-assessment phase 1

- What do you host in your deployment?
- Is it business critical?
- Is its availability revenue impacting? (back to business critical)
- What kind of data is in it? customer/client, PHI, patents, PI, PCI, banking? Who would want it?
- What can your users do in that session? What can they execute? What do they have access to?
- File shares? Are you sure they are all SMB3 and have secure permissions?



Knocking on the VDI door

- Every deployment is always under attack, all day every day. (Port scans, exploits ran, phishing emails sent, and OSINT and Recon).
- If someone wants to go in, it just takes time and pressure.

VDI cyber threats

- There are lots of people who are making lots of money by hacking each day. It is estimated that it's an
 over one trillion dollar industry.
- A single attacker can make thousands of dollars a day in cryptolocker/ransomware attacks.
- Phishing is another revenue stream for attackers using ransomware or credential harvesting to get credentials.
- If an attacker gets into whaling, the money goes up drastically. Think about Google and Facebook paying over 100 million dollars to bad purchase orders (finance and CEO fraud).
- How many passwords do you **share between accounts** on the internet and work? What is different?
- What do you think your users do with their passwords?

| Bitcoin \$19,766.24 +3.25% | Ethereum \$1,085.95 +5.11% | Binance Coin \$229.30 +4.92% | XRP \$0.315030 +2.84% |
|----------------------------|----------------------------|------------------------------|-------------------------------|
| BTC - \$84,425.65 +3.07% | ETH - \$2,025.04 +7.09% | XRP - \$2.4951 +10.85% | USDT - \$1.0001 -0.00% |
| | | | |

Breaches and leaks

2014-2024 (just a few of the heavy hitters)

- Bad password habits will hurt your business eventually.
- Most people are in at least 5-10 breaches.

DEHASHED 14,453,524,107 COMPROMISED ASSETS



Over 14.4 billion records leaked

0.0 Optimize

- Less things running, less to attack. Plus, better experience for your users and better density.
- Win, win, win.



0.0 Optimize

Project**VRC**.team

- To stay up to date with optimizations, follow @LoginVSI and @G0_euc.
- Turning off all the services and doing all the tweaks also will secure the image, because the only good Winder service is a dead Winder service.
- Running a couple PowerShell optimization scripts can help be the first pass to securing them.

https://www.go-euc.com





0.1: Optimization

Optimization of your image can greatly improve the security of your deployment.

Citrix Optimizer

<u>https://support.citrix.com/article/CTX224676</u>

BISF (Seal script too!, clean up that SCCM and AV settings. Has a GPO to run things)

• <u>https://github.com/EUCweb/BIS-F/releases</u>

VMware Optimizer

<u>https://flings.vmware.com/vmware-os-optimization-tool</u>





1.0 Windows Policies

Secure Windows Policies are one of your best defenses from users and/or attackers from being able to do things they shouldn't.



1.0 Windows Policy Foundation: Passwords

Password policies:

- 20+ passwords remembered.
- 16+ characters (20+ for privileged) (14 recommended by CIS, Microsoft, + many others).
- Complexity turned on (if you have problems with this because of workflow, give your users a better way to log in using badges and/or biometrics).

Fine-grained password policies:

• Heard of them?



Hardening: Baselines-compliance

- Do you have the recommended settings from Microsoft?
- 311 for Windows 11
- 266 for Server 2022

| | Windows 11 9-19-22 Build 22621.382 - 311 | | Server 2022 9-6-21 Build 20348.169 - 266 | | | |
|-------|--|-----|--|-----|--|--|
| | Advanced auditing | 23 | User | 1 | | |
| | Computer | 217 | Security | 62 | | |
| | Tasks | 1 | template | 02 | | |
| | Services | 4 | Computer | 180 | | |
| - And | Security template | 63 | Advanced | 00 | | |
| | User | 3 | auditing | 23 | | |

1.1: The basics-logs

- If something is happening and you don't know it, how will you fix it?
- Failure to configure your logs correctly can lead to a critical oversight. When it's time to apply policies, you might miss crucial errors or successes related to the changes.
- The changes within the baselines are a big deal, especially related to authentication and signing.
 Without the logs, you will just be enabling a policy and praying it won't cause issues.

LIVIN' ON A PR

1.2 Recommended logs

Microsoft security baselines

- 1. Domain controllers
- 2. Servers (File, DB, App + Auth\Access Related)
- 3. Remaining servers
- 4. IT desktops
- 5. HR desktops
- 6. Finance desktops
- 7. Leadership desktops
- 8. Remaining desktops

| Policy Setting Name | Member Server 2022 | Domain Controller | Windows 11 22H2 |
|--|---------------------|---------------------|---------------------|
| Audit Account Lockout | Failure | Failure | Failure |
| Audit Audit Policy Change | Success | Success | Success |
| Audit Authentication Policy Change | Success | Success | Success |
| Audit Computer Account Management | | Success | |
| Audit Credential Validation | Success and Failure | Failure | Success and Failure |
| Audit Detailed File Share | Failure | Failure | Failure |
| Audit Directory Service Access | | Failure | |
| Audit Directory Service Changes | | Success | |
| Audit File Share | Success and Failure | Success and Failure | Success and Failure |
| Audit Group Membership | Success | Success | Success |
| Audit Kerberos Authentication Service | | Success and Failure | |
| Audit Kerberos Service Ticket Operations | | Failure | |
| Audit Logon | Success and Failure | Success and Failure | Success and Failure |
| Audit MPSSVC Rule-Level Policy Change | Success and Failure | Success and Failure | Success and Failure |
| Audit Other Account Management Events | | Success | |
| Audit Other Logon/Logoff Events | Success and Failure | Success and Failure | Failure |
| Audit Other Object Access Events | Success and Failure | Success and Failure | Success and Failure |
| Audit Other Policy Change Events | Failure | Failure | Failure |
| Audit Other System Events | Success and Failure | Success and Failure | Success and Failure |
| Audit PNP Activity | Success | Success | Success |
| Audit Process Creation | Success | Success | Success |
| Audit Removable Storage | Success and Failure | Success and Failure | Success and Failure |
| Audit Security Group Management | Success | Success | Success |
| Audit Security State Change | Success | Success | Success |
| Audit Security System Extension | Success | Success | Success |
| Audit Sensitive Privilege Use | Success and Failure | Success and Failure | Success and Failure |
| Audit Special Logon | Success | Success | Success |
| Audit System Integrity | Success and Failure | Success and Failure | Success and Failure |
| Audit User Account Management | Success and Failure | Success and Failure | Success and Failure |

4.1: The basics-logs

- 1. Domain controllers
- 2. Servers (File, DB, App + Auth\Access Related)
- 3. Remaining servers
- 4. IT desktops
- 5. HR desktops
- 6. Finance desktops
- 7. Leadership desktops
- 8. Remaining desktops

| Policy Setting Name | Member Server 2022 | Domain Controller | Windows 11 22H2 |
|--|---------------------|---------------------|---------------------|
| Audit Account Lockout | Failure | Failure | Failure |
| Audit Audit Policy Change | Success | Success | Success |
| Audit Authentication Policy Change | Success | Success | Success |
| Audit Computer Account Management | | Success | |
| Audit Credential Validation | Success and Failure | Failure | Success and Failure |
| Audit Detailed File Share | Failure | Failure | Failure |
| Audit Directory Service Access | | Failure | |
| Audit Directory Service Changes | | Success | |
| Audit File Share | Success and Failure | Success and Failure | Success and Failure |
| Audit Group Membership | Success | Success | Success |
| Audit Kerberos Authentication Service | | Success and Failure | |
| Audit Kerberos Service Ticket Operations | | Failure | |
| Audit Logon | Success and Failure | Success and Failure | Success and Failure |
| Audit MPSSVC Rule-Level Policy Change | Success and Failure | Success and Failure | Success and Failure |
| Audit Other Account Management Events | | Success | |
| Audit Other Logon/Logoff Events | Success and Failure | Success and Failure | Failure |
| Audit Other Object Access Events | Success and Failure | Success and Failure | Success and Failure |
| Audit Other Policy Change Events | Failure | Failure | Failure |
| Audit Other System Events | Success and Failure | Success and Failure | Success and Failure |
| Audit PNP Activity | Success | Success | Success |
| Audit Process Creation | Success | Success | Success |
| Audit Removable Storage | Success and Failure | Success and Failure | Success and Failure |
| Audit Security Group Management | Success | Success | Success |
| Audit Security State Change | Success | Success | Success |
| Audit Security System Extension | Success | Success | Success |
| Audit Sensitive Privilege Use | Success and Failure | Success and Failure | Success and Failure |
| Audit Special Logon | Success | Success | Success |
| Audit System Integrity | Success and Failure | Success and Failure | Success and Failure |
| Audit User Account Management | Success and Failure | Success and Failure | Success and Failure |

4.2: The basics-logs

Standards for all systems, or at least servers and desktops. We don't have floppy drives, so crank it up.

Local event log policies matter too:

- 1. Prevent local guest group from accessing application log
- 2. Prevent local guest group from accessing security log
- 3. Retain application log
- 4. Retain security log
- 5. Retain system log
- 6. Retention method for application log
- 7. Retention method for security log
- 8. Retention method for system log

| | Retain application log | Properti | es | | ? | × | |
|-----------------|---------------------------|----------------------|----|--------|----|-----|---|
| | Security Policy Setting | Explain | | | | | |
| | Retain app | lication lo <u>c</u> | 3 | | | | |
| | Define this policy | setting | | | | | |
| | Overwrite events 7 🍦 d | older thar ays | 1: | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | E |
| | | | | | | | 区 |
| | | | | | | | X |
| | | | | | | | |
| | | | OK | Cancel | Ap | ply | |
| $\overline{\ }$ | YITKA | N A | | | | Y | |

1.3: The basics-logs-what to use

- Splunk on top of it being able to ingest almost any log known by modern nerds. It also is an SIEM for a lot of clients (security information event management). Its biggest downside is price and knowing how much you will need to do what you need to do.
- 2. Sentinel, LogRhythm, IBM, McAfee, ArcSight, Rapid7, Solarwinds, AlienVault, and many more.
- 3. ELK or other variants make some servers give it lots of storage and get ready to RTFM and make all kinds of cool things.



COMPLETENESS OF VISION

As of June 2022

© Gartner, Inc.

Figure 1: Magic Quadrant for Security Information and Event Management

1.4: PowerShell logging

- If you allow PowerShell in your VDI deployment or just anywhere in general:
- https://www.blackhillsinfosec.com/powers hell-logging-blue-team/
- https://blogs.technet.microsoft.com/ashle ymcglone/2017/03/29/practical-powershell-security-enable-auditingand-logging-with-dsc/

Event ID 4103:)



| nnd | Filtered: Log: Microsoft-Wind | ows-PowerShell/Operational; Source: ; Event ID: 4103. Number of events: | 51 | |
|----------------------|--|---|---|-------------------------|
| J'''S | Level | Date and Time | Source | Event ID Task Category |
| | (1) Information | 9/4/2019 8:17:55 PM | PowerShell (Microsoft-Windows-PowerShell) | 4103 Executing Pipeline |
| | Unformation | 9/4/2019 8:17:55 PM | PowerShell (Microsoft-Windows-PowerShell) | 4103 Executing Pipeline |
| | Information | 9/4/2019 8:17:55 PM | PowerShell (Microsoft-Windows-PowerShell) | 4103 Executing Pipeline |
| | Information | 9/4/2019 & 17:55 PM | Powershell (Microsoft-Windows-Powershell) | 4103 Executing Pipeline |
| | Unformation | 9/4/2019 8:17:55 PM | PowerShell (Microsoft- Windows- PowerShell) | 4103 Executing Pipeline |
| | Distormation | 9/4/2019 8:17:52 PM | Powershell (Microsoft-Windows-Powershell) | 4103 Executing Pipeline |
| | Disformation | 9/4/2019 8:02:47 PM | Powershell (Microsoft-Windows-Powershell) | 4103 Executing Pipeline |
| | Disformation | 9/4/2019 8/02/47 PM | Powershell (Microsoft-Windows-Powershell) | 4103 Executing Pipeline |
| | Disformation | 9/4/2019 6(02)47 PM | PoweShell (Microsoft-Windows-PoweShell) | 4103 Executing Pipeline |
| | Bloformation | 9/4/2019 8:02:47 PM | PowerShell (Microsoft-Windows-PowerShell) | 4103 Executing Pipeline |
| | | 9/4/2019 8:02:47 PM | PowerShell (Microsoft-Windows-PowerShell) | 4103 Executing Pipeline |
| | Disformation | 0/A/2010 8-02-47 DEA | DowerChall (Microsoft-Windows-DowerChall) | 4102 Execution Dinalina |
| ميرميل | Event (102 DeverChall (Misserth) | Nordaux Daux-Chall) | | ~ |
| eral: | General Details | vinacionale ovversioneny | | |
| | CommandInvocation/Write-Ho | t): "Weite-Host" | | |
| owers | ParameterBinding(Write-Host): Connecting to localhost with th | name="Object"; value=" e credentials Administrator : System.Security.SecureString | | |
| <u>/ashle</u> | Context: Severity = Informational Host Name = ConsoleHost Host Version = 51,171348 Host ID = d30863a3-7167-4 Host Application = C:Villin Engine Version = 5,117134 Runspace ID = 513/a124-24 Pipeline ID = 17 Command Type = Cmdlet | 8 12f-9672-12d144088e542 dows/System32/WindowsPowerShell/v1.0/powershell.exe 558 94-498c-6337-d68a99feb101 4ost | | |
| <u>g-</u> | Script Name = C:\User\ad Command Path = Sequence Number = 42 User = LAB\administrator Connected User = Shell ID - Microsoft Power | ministrator/Desktop/demo.ps1 | | Ţ |
| | Log Name: Microsoft-V Source: PowerShell Event ID: 4103 Level: Information User: LAB\admini OpCode: To be used i More Information: <u>Event Log C</u> | Indows-PowerShell/Operational Microsoft-Wind Loggett: 9/4/2019/8:17:55 PM Task Category: Executing Pipeline Keywords: None Strator Computen VMW-L-W10Jab.ntwrk01.net when operation i Infine Help | | |
| 41219 | | TALAR | NITIVIA | |
| Catting | | ^ | | Ctate |
| secong | | | | State |
| E Set the default so | urce path for | Update-Help | | Not configured |
| 📓 Turn on Module l | Logging | | | Enabled |
| Turn on PowerSh | ell Script Bloc | k Logging | | Enabled |

Enabled

Enabled

Turn on PowerShell Transcription

E Turn on Script Execution

1.4: PowerShell logging

- 1. Remove admin application access
- 2. Remove common jailbreak points
- 3. Lock down the desktop and start menu
- 4. Lock down File Explorer





Windows Policy-we have to work, too

- 1. Make a new GPO.
- 2. Link it to your Test OU.
- 3. Change the security of the policy to "Deny" for your admin groups. You may need to apply this to your VDI admin groups and others to make sure the server can still be worked on when something isn't functioning and to perform routine maintenance.

|)I-Lockdown | | |
|---|--|------------|
| cope Details Settings Delegatio | n | |
| hese groups and users have the spe | cified permission for this GPO | |
| iroups and users: | VDI-Lockdown Security Settings | × |
| Name | All LB | |
| 😣 Authenticated Users 🛛 📕 | VDI-Lockdown Security Settings X | |
| Citrix-Admins (VDILOCKDOWNG) | | |
| Domain Admins (VDILOCKDOV) Section: Section: | Security | ^ |
| ENTERPRISE DOMAIN CONTR | - | |
| SYSTEM . | Group or user names: | |
| | STATES AND A CREATOR OWNER | dmins) 🗡 |
| | Authenticated Users | > |
| | SYSTEM | Remove |
| | Citrix-Admins (VDII OCKDOWNGUID\Citrix-Admins) | Deny |
| | Domain Admine (VDILOCKDOWNGUID) Domain Admine) | |
| | | |
| | | |
| | Add Remove | |
| | | |
| | Permissions for Citrix-Admins Allow Deny | vanced |
| | | |
| | | |
| | Create all child objects | Apply |
| | Delete all child objects | |
| | Apply group policy | |
| | Special permissions | |
| Add Remov | | Advanced |
| | For special permissions or advanced settings, Advanced | |
| | click Advanced. | |
| | | |
| | | VIY |
| | OK Canad Arabi | |
| | UK Cancel Apply | |
| | | ᆲᅛᆛᆘᄉᆘ |

Windows Policy: 1. Admin applications-part 1

 Disable Run (This is the Windows noisy cricket)
 GPO: User Configuration \ Policies \ Administrative Templates \ Start Menu and Taskbar \ Remove Run



• Disable CMD

GPO:User Configuration/Administrative Templates/System/Prevent access to the command prompt

Disable PowerShell

AppLocker - Powershell.exe and Powershell_ise.exe

Windows Policy: 1. Admin applications-part 1

- Control Panel
- GPO: User Configuration/Administrative Templates/Control Panel/Prohibit access to the Control Panel
- System
- GPO: User Configuration/Policies/Administrative Templates/System/Enable-Prevent access to registry editing tools
- Restrict Admin Apps
- Computer Configuration/Policies/Windows Settings/Security Settings/File System
 - %AllUsersProfile%\Microsoft\Windows\Start Menu\Programs\Administrative Tools
 - %AllUsersProfile%\Microsoft\Windows\Start Menu\Programs\System Tools\Windows PowerShell.Ink
 - %AllUsersProfile%\Microsoft\Windows\Start Menu\Programs\Administrative Tools\Server Manager.Ink
 - And much More!

Windows Policy: 1. Admin applications-part 2

- Windows Update
- Computer Configuration/Policies/Administrative Templates/Windows Components/Windows Installer/
- Enable: Remove access to use all Windows Update features
- Enable: Prevent users from using Windows Installer to install updates and upgrades
- Enable always: Turn off Windows Installer
- Enable: Do not display 'Install Updates and Shut Down' option
- Disable: Allow non-administrators to receive update notifications
- Credentials
- GPO: User Configuration/Policies/Administrative Templates/Windows Components/Credentials User Interface/do not display the password reveal button: Enable

Windows Policy: 2. Common jailbreaks-part 1

• GPO: User

Configuration\Policies\Administrative Templates\System\Restrict these applications from being launch from Help

cmd.exe,powershell.exe,powershell_ise.ex
 e,notepad.exe,iexplore.exe,wordpad.exe,re
 gedit.exe,chrome.exe

| Restrict these progr | ams from being | launched from H | Help | | | — | | \times |
|---|-----------------|-----------------|---|--|--|--|--------------------------------------|---------------|
| Restrict these progr | rams from being | launched from H | lelp | Previous Settin | ng Nex | t Setting | | |
| Not Configured Enabled | Comment: | | | | | | | ^ |
| O Disabled | | | | | | | | ~ |
| | Supported on: | At least Window | vs Server 2003 | operating syste | ms or Wind | ows XP Profe | ssional | $\hat{}$ |
| Options: | | | Help: | | | | | |
| Enter executables separ | rated by commas | : | This po being run f | licy setting allow rom online Help. | ws you to re | strict progran | ns from | \neg |
| Example: calc.exe,paint | .exe | | If you programs f policy settin want to res | nable this policy om being run fr 1g, enter the file trict, separated b | y setting, yo om Help. W names nam by commas. | u can preven hen you enal les of the pro | t specified ble this grams you | |
| @VD | ltec | kõr | lf you can run all | lisable or do not applications from | configure t n online Hel | his policy set lp. | ting, user | 5 |
| vellege | en fiy | gioi | Note: | 'ou can also restr e Software Restri Configuration\Se | rict users fro iction Policy ecurity Settin | om running aj v settings avai ngs. | pplication lable in | s |
| | | | Note: T Configurati used, any p launched fr | his policy settin on and User Con rograms listed in om Help | g is available ofiguration. o either of th | e under Com If both are set nese locations | puter ttings are cannot | |
| L | | | | | OK | Cancel | | tiva No Se |
| | | | | | | | | |
| JAL | | | | | | | | Л |

Windows Policy: 2. Common jailbreaks-part 2

Does your application use the file menu or something else?

- File Open can be your enemy also, and your mitigation mileage may vary depending on the application.
- GPO: User Configuration/Administrative Templates/File Explorer/
 - Remove File Menu from File Explorer
- You may have to use other solutions to remove menus and locations from your application that are not controllable by policy. Avetco, Ivanti (Application Manager) & PolicyPak
- So many applications will have a default location inside a file directory that users have access to even with Restrict drives. Don't send everyone to the same path, park it in the profile.

Windows Policy: 2. Common jailbreaks-part 2

• Office Products (control where they open default documents)

• Restricted browsing settings

Default open locations per product

| Se Approve Locations | X |
|--|--|
| Approve Locations | Previous Setting Next:Setting |
| Not Configured Comment: Enabled | ^ |
| O Disabled Supported on: At least | Windows Server 2008 R2 or Windows 7 |
| Options: | Help: |
| List of Approved Locations: Show Enter the name of the Location as Value Name, ar path as the Value. | Adds locations, such as c:\Windows or \\server\share, to the list of approved locations for use with Restricted Browsing. When Restricted Browsing is active, the Save As dialog box is restricted such that the user can navigate only to the locations and the children of the locations specified in this list. To allow easier access to these approved locations, consider adding them to the Places bar by using the Places Bar Locations setting for the File Open/Save dialog box. If there are no approved locations in the Places bar, the dialog box may not be able to open. To activate Restricted Browsing, use the Restricted Browsing/Activate Restricted Browsing setting. Note: You must set this policy setting first before the "Activate Restricted Browsing." |
| @VDIHa | TEX D |
| Vellesseurfi | OK Cancel Apply |
| XXX | |
| $\diamond \dot{\Phi} \times \times$ | $\phi \phi X X \phi \phi$ |
| | |

Windows policy: 3.1 Desktop lockdown-part 1

GPO: User
 Configuration/Administrative
 Templates/Desktop/Hide
 network locations icon on
 desktop

| Setting | State |
|--------------------------------|----------------|
| Enable Active Desktop | Not configured |
| Disable Active Desktop | Not configured |
| Prohibit changes | Not configured |
| E Desktop Wallpaper | Not configured |
| Prohibit adding items | Not configured |
| E Prohibit closing items | Not configured |
| Prohibit deleting items | Not configured |
| Prohibit editing items | Not configured |
| 🖾 Disable all items | Not configured |
| Add/Delete items | Not configured |
| Allow only bitmapped wallpaper | Not configured |

Windows Policy: 3.2 Start Menu Lockdown-part 1

| | 📔 Start Menu and Taskbar | | | |
|---------------------------------------|---|--|---------------------|----------------|
| | Select an item to view its description. | Setting | | State |
| | | Notifications | | |
| | | Add Search Internet link to Start Menu Clear history of recently opened docume | nts on exit | Not configured |
| | | E Clear the recent programs list for new use | ers | Not configured |
| | | E Clear tile notifications during log on | | Not configured |
| Start Menu | | E List desktop apps first in the Apps view | | Not configured |
| | | Search just apps from the Apps view | | Not configured |
| | | E Add Logoff to the Start Menu | menu size | Not configured |
| GPO: User | | E Go to the desktop instead of Start when s | igning in | Not configured |
| _ | | E Gray unavailable Windows Installer progra | ams Start Menu sh | Not configured |
| Configuration/Administrative | | Turn off personalized menus | | Not configured |
| e en ligar actor i / lar in her act e | | E Lock the Taskbar | | Not configured |
| Templates/Start menu and | | Start Layout Add "Run in Separate Memory Space" chi | eck box to Run dial | Not configured |
| remplates/start mena and | | Turn off notification area cleanup | | Not configured |
| | 1 | E Remove Balloon Tips on Start Menu item | s | Not configured |
| taskbar/ Remove Network | Setting | | State | red |
| | Hide "Set Program Access | and Computer Defaults" page | Not configur | red red |
| connections from Start Menu | E Hide "Get Programs" page | and computer behavits page | Not configur | ed red |
| | Hide Vertrigrams page | - | Not configure | red |
| | | age | Not configur | ed red |
| | Hide "Programs and Featu | ires" page | Not configure | ed red |
| | E Hide the Programs Contro | ol Panel | Not configur | ed red |
| | Hide "Windows Features" | | Not configure | ed red |
| | Hide "Windows Marketpla | ice" | Not configur | ed red |
| | | | | |

Windows Policy: 4. Windows Explorer lockdown-part 1

- GPO: User Configuration/Administrative Templates/File Explorer/
- Hide these specified drives in My Computer
- Remove "Map Network Drive" and "Disconnect Network Drive"
- No Computers Near Me in Network Locations
- No Entire Network in Network Locations
- Remove search button
- Turn off display of recent search entries in the File Explorer Search Box (if search disabled, not needed)

- Allow only per user or approved shell extensions
- Remove File Menu from File Explorer
- Display the Menu bar in File Explorer
- Hides the Manage Item on the File Explorer context
 Menu
- Remove Share Documents from My Computer
- Turn off Windows+X Hotkeys
- Remove Security tab
- Remove Hardware tab

Top 10 desktop group polices for desktops and apps

- 1. Remove Run and CMD and PS Access
- 2. Restrict all drives
- 3. Restrict help programs
- 4. AppLocker all administrative applications
- 5. If the "Internets" isn't needed, then block traffic with proxy or blackhole proxy
- 6. <u>Remove all unnecessary items in the Start Menu and desktop</u>
- 7. Lock down File Explorer (menu bar, file menu, network locations)
- 8. Remove Mapped Network Drives (Only Map drives if you have to)
- 9. Remove Control Panel, Remove Windows Installer Rights
- 10. Restrict Application Execution to only the known goods (long haul)

Don't forget PowerShell (both flavors) and ISE (both flavors)

x86 and x64

| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | | X Windows PowerShell ISE | |
|--|--------------|------------------------------------|--|
| Your system administrator has blocked this program. For more information, or system administrator. | contact your | File Edit View Tools Debug Add-one | |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | | X I write-host "PartyTime123.p | is in the House!!!!" |
| Your system administrator has blocked this program. For more information, or system administrator. | ontact your | | |
| C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe | | × | |
| Your system administrator has blocked this program. For more information, or system administrator. | contact your | PS C:\Windows\System32\WindowsPo | werShell\v1.0> write-host "PartyTime123.ps1 is in the House!!!!" |
| | UN | PS (+\Windows\Sveton32\WindowsPo | mershellivi o |
| C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell_ise.exe | THUR HIM T | × | |
| | | | |
| Your system administrator has blocked this program. For more information, system administrator. | Action | User | Name |
| | Allow | BUILTIN\Administrators | (Default Rule) All files |
| | Allow | Everyone | (Default Rule) All files located in the Program Files folder |
| | Allow | Everyone | (Default Rule) All files located in the Windows folder |
| | 🚫 Deny | PARTYTIME123\ThunderDomeUsers | %SYSTEM32%\WindowsPowerShell\v1.0\powershell.exe |
| | () Deny | PARTYTIME123\ThunderDomeUsers | %SYSTEM32%\WindowsPowerShell\v1.0\powershell_ise.exe |

Office Products: Tons of other settings

Default open and save locations

So many applications will have a default location inside a file directory that users have access to even with Restrict drives. Don't send everyone to the same path—park it in the profile.

Restrict paths for open and saving (test, test, and test)

| Activate Restricted Browsing | – 🗆 X | Approve Locations | w Contents 🔓 — 🗆 🗙 |
|-------------------------------|--|--|---------------------------|
| Activate Restricted Browsing | Previous Setting Next Setting | Approve Locations Previous Setting Next Setting List | t of Approved Locations: |
| O Not Configured Comment: | ^ | O Not Configured Comment: | Value name 🔺 Value |
| Enabled | | Enabled | C:\Users\%usemame%\Office |
| ○ Disabled | ~ | O Disabled | |
| Supported on: | At least Windows Server 2008 R2 or Windows 7 | Supported on: At least Windows Server 2008 R2 or Windows 7 | |
| | × | | |
| Options: | Help: | Options: Help: | |
| | When Pertricted Provision is activated the raws as dialog how will | | |
| Microsoft Access | be restricted such that the user will only be able to navigate to | List of Approved Locations: Show | |
| Microsoft Excel | those locations and the children of those locations specified in the "Restricted Browsing\Approve Locations" policy setting. If | Enter the name of the Location as Value Name, and such that the user can navigate only to the locations and | |
| Microsoft SharePoint Designer | you want to enable the "Approve Locations" policy setting, you must first enable the "Approve Locations" policy setting first. | path as the Value. children of the locations specified in this list. | |
| Microsoft InfoPath | | To allow easier access to these approved locations, consi | OK Cancel |
| Microsoft OneNote | | setting for the File Open/Save diang box. If there are no | |
| Microsoft Outlook | | approved locations in the Places bar, the dialog box may not be able to open. | |
| Microsoft PowerPoint | | To activate Restricted Browsing, use the Restricted | NANTINIAN |
| Microsoft Project | | Browsing/Activate Restricted Browsing setting. Note: You must | NAIYIANAIY |
| Microsoft Publisher | willion with and | Browsing." | |
| Microsoft Visio | A COLORIDA A COLORIDA | Milleanse | |
| Microsoft Word | | | |
| | v | willionanthy | |
| | OK Cancel Apply | OK Cancel Apply | |

MACROS: Level 1

Are MACROs needed in Office 2019?
 No, they are only required for about 1% of use cases. For the other 99%, we should disable them to avoid unnecessary risks.

Load the Office 2016 GPO Pack

 User configuration > Administrative templates > Microsoft Word
 2016 > Word options > Security > Trust
 Center-"Block macros from running in
 Office from the internet".

| | m running in Offic | Previous Setting Next Setting | |
|--------------------------|--------------------|---|---|
| ○ Not <u>C</u> onfigured | Comment: | | ^ |
| • Enabled | | | |
| O <u>D</u> isabled | | | Y |
| | Supported on: | At least Windows Server 2008 R2 or Windows 7 | ^ |
| | | | ٧ |
|)ptions: | | Help: | |
| | | In Office files that come from the internet. If you enable this policy setting, macros are blocked from running, even if "Enable all macros" is selected in the Macro Settings section of the Trust Center. Also, instead of having the choice to "Enable Content," users will receive a notification that macros are blocked from running. If the Office file is saved to a trusted location or was previously trusted by the user, macros will be allowed to run. If you disable or don't configure this policy setting, the settings configured in the Macro Settings section of the Trust Center determine whether macros run in Office files that come from the Internet. | |
| | | | ~ |

MACROS: Level 2

Windows

components > Windows Defender Antivirus > Windows Defender Exploit Guard >

 Attack surface reduction: "Configure attack surface reduction rules"



MACROS: Level 3

- 1. Training, training, and training
- 2. Don't click on all the things
- 3. There are no take backs on clicking things
- 4. Check the emails
- 5. Check twice and click once



Contents of this document are protected. To view this content, please click "Enable Editing" from the yellow bar and then click "Enable Content"




Unpatched systems are how almost all vulnerabilities work.

2.0 Patches

2.0 Patches

In almost every scan I do, there are unpatched systems. Number one problems in applying patches:

- No one tests the applications.
- We don't cook it-we just serve it.
- So many admins must apply the patches and test them.
- Most of us only have the time to just smoke test, click it opens, feels right.



2.0 Patches

Apply all the patches?

- Sounds cool until one breaks something for thousands of users.
- So many deployments tested in prod for so many reasons.

What to do?

- Find a way to make a test deployment
- Full test deployment
- Test master image
- Test desktop pool
- Test pre-production desktop pool

DIDN'T PATCH YOUR SERVERS? BOLD MOVE COTTON

2.0 Patches

Methods of mayhem

- Group Policy
- Intune
- Click Windows update
- Snapshots all day every cay

Automation is key Keeping a schedule is a must!



Project Evergreen (Module to update common Windows apps): <u>https://stealthpuppy.com/evergreen/#evergreen</u> Automation framework (Make a golden image monthly instead of patching): <u>https://xenappblog.com/automation-framework-master-class/</u>

3.0 Application control

You know what you publish, but finding out what to block can be fun.

3.0 Application control

Some apps are just bad mmkayyy

This is one of the most commonly overlooked methods to securing a VDI deployment. That is why this is before antivirus on my top 8.

VDI deployments in most cases are deployed with a known set of applications because you are publishing them. In most cases, what needs to be allowed to run is the same list of published application in the console and the add/remove programs on a known good image.

The gotchas are what do the users open after opening the application you published to them.

Major methods of doing this:

- AppLocker
- PolicyPak: Amazing other things, got Java? Least privilege manager, browser (Edge is a PDF reader?)
- UEM
- Ivanti Application Manager
- Avetco
- Most AVs can also do it, check with your vendor to find out which is better for you.

Most of these solutions will allow you to take baby steps, too.

3.1: Application control-deployment phases

Where to start?

Level 0 setup audit only default policies (Exe, installer, script, and packages) Level 1 admin applications (PowerShell and other places)

• Make sure users are not able to launch admin tools that can cause problems.

Level 2 - LOLBins (fun times)

• Block some of the known applications and scripts that can bypass AppLocker and/or do bad things.

Level 3 - Main applications (long process)

Step by step, we want to only allow the good and eventually get rid of the "allow any", like a firewall, along
with blocking things instead of just auditing.





Oddvar Moe @api0cradle https://lolbas-project.github.io

Good files gone wrong

LOLBins are files that are native to Windows that users will, by default, have access to and have unexpected superpowers.

- Executing code
- Passthrough of unsigned code through a signed file that is allowed
- Compiling code
- File operations
- UAC bypass
- Surveillance
- Dump process info
- Log evasion
- DLL side-loading hijacking

LOLBins

Execute

Open the target .EXE using the Program Compatibility Assistant.

pcalua.exe -a calc.exe

Usecase:Proxy execution of binary Privileges required:User OS:Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10 Mitre:<u>T1218</u>

Open the target .DLL file with the Program Compatibility Assistant.

pcalua.exe -a \\server\payload.dll

Usecase:Proxy execution of remote dll file Privileges required:User OS:Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10 Mitre:<u>T1218</u>

Open the target .CPL file with the Program Compatibility Assistant.

pcalua.exe -a C:\Windows\system32\javacpl.cpl -c Java

Usecase:Execution of CPL files Privileges required:User OS:Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10 Mitre:T1218

LOLBins

OFF THE LAND BINA

Oddvar Moe @api0cradle https://lolbas-project.github.io

AppInstaller.exe Aspnet_Compiler.exe At.exe Atbroker.exe Bash.exe Bitsadmin.exe CertOC.exe CertReq.exe Certutil.exe Cmd.exe Cmdkey.exe cmdl32.exe Cmstp.exe ConfigSecurityPolicy.exe Control.exe Csc.exe Cscript.exe DataSvcUtil.exe Desktopimgdownldr.exe Dfsvc.exe

Diantz.exe

Diskshadow.exe Dllhost.exe Dnscmd.exe **Esentutl.exe** Eventvwr.exe Expand.exe Explorer.exe Extexport.exe Extrac32.exe Findstr.exe fltMC.exe Forfiles.exe Ftp.exe GfxDownloadWrapper.exe Gpscript.exe Hh.exe

IMEWDBLD.exe le4uinit.exe leexec.exe llasm.exe Infdefaultinstall.exe Installutil.exe Jsc.exe Makecab.exe Mavinject.exe Microsoft.Workflow.Compiler.exe Print.exe Mmc.exe MpCmdRun.exe Msbuild.exe Msconfig.exe Msdt.exe Mshta.exe Msiexec.exe

Netsh.exe Register-cimprovider.exe Odbcconf.exe Regsvcs.exe **OfflineScannerShell.exe** OneDriveStandaloneUpdater.exe Replace.exe Pcalua.exe Pcwrun.exe Pktmon.exe Pnputil.exe Presentationhost.exe Sc.exe **PrintBrm.exe** Psr.exe Rasautou.exe Reg.exe Regasm.exe Regedit.exe Tttracer.exe **Regini.exe** vbc.exe

Regsvr32.exe Rpcping.exe Rundll32.exe Runonce.exe Runscripthelper.exe Schtasks.exe Scriptrunner.exe SettingSyncHost.exe Stordiag.exe SyncAppvPublishingServer.exe Ttdinject.exe

LOLBins

Verclsid.exe Wab.exe Wmic.exe WorkFolders.exe Wscript.exe Wsreset.exe wuauclt.exe Xwizard.exe Advpack.dll Comsvcs.dll leadvpack.dll leaframe.dll Mshtml.dll Pcwutl.dll Setupapi.dll Shdocvw.dll Shell32.dll Syssetup.dll Url.dll Zipfldr.dll adplus.exe AgentExecutor.exe Appvlp.exe Bginfo.exe Cdb.exe coregen.exe csi.exe DefaultPack.EXE Devtoolslauncher.exe dnx.exe Dotnet.exe

OFF THE LAND BINARY Dxcap.exe Excel.exe Fsi.exe FsiAnyCpu.exe Mftrace.exe Msdeploy.exe msxsl.exe ntdsutil.exe Powerpnt.exe Procdump(64).exe rcsi.exe

Remote.exe

Sqlps.exe

Sqldumper.exe

SQLToolsPS.exe

Squirrel.exe te.exe Tracker.exe Update.exe VSIISExeLauncher.exe VisualUiaVerifyNative.exe vsjitdebugger.exe Wfc.exe Winword.exe Wsl.exe CL_LoadAssembly.ps1 CL_Mutexverifiers.ps1 CL_Invocation.psl Manage-bde.wsf Pubprn.vbs Syncappvpublishingserver.vbs

Oddvar Moe @api0cradle

https://lolbas-project.github.io

UtilityFunctions.ps1 winrm.vbs Pester.bat

AaronLocker

https://blogs.msdn.microsoft.com/aaron_margosis/tag/aaronlocker/ https://github.com/Microsoft/AaronLocker

@AaronMargosis

- Documentation is 81 pages, and it is amazing
- AaronLocker's strategy can be summed up as if a non-admin could have put a program or script onto the computer-i.e., it is in a user-writable directory-and not allow it to execute unless it has already been specifically allowed by an administrator. This will stop execution if a user is tricked into downloading malware, if an exploitable vulnerability in a program the user is running tries to put malware on the computer, or if a user intentionally tries to download and run unauthorized programs (from its documentation).

Windows Defender application control

- To get started, you need to make your golden image with all your applications installed (layering gets complicated).
- No GPO for this, image-specific (can use Intune).
- Run the discovery scripts.
- Review the findings of the applications installed and allow for all users or assign to specific users (admin applications).
- Then run the deployment scripts to only allow those applications to be ran.
- Anything the user downloads or access that isn't defined in this system will not be able to execute.
- If you install any new applications, you will need to recapture the installed applications, adjust the rules, and roll out the new one.
- <u>https://docs.microsoft.com/en-</u> <u>us/windows/security/threat-protection/windows-</u> <u>defender-application-control/windows-defender-</u> <u>application-control-deployment-guide</u>

| PowerShell | 🗅 Copy | | |
|--|--------|--|--|
| cp \$MEMCMPolicy \$LamnaPolicy | | | |
| Give the new policy a unique ID, descriptive name, and initial version number: | | | |
| PowerShell | 🗅 Copy | | |
| Set-CIPolicyIdInfo -FilePath \$LamnaPolicy -PolicyName \$PolicyName -ResetPolicyID Set-CIPolicyVersion -FilePath \$LamnaPolicy -Version "1.0.0.0" | | | |
| Modify the copied policy to set policy rules: | | | |
| PowerShell | 🗅 Сору | | |
| Set-RuleOption -FilePath \$LamnaPolicy -Option 3 # Audit Mode Set-RuleOption -FilePath \$LamnaPolicy -Option 6 # Unsigned Policy Set-RuleOption -FilePath \$LamnaPolicy -Option 9 # Advanced Boot Menu Set-RuleOption -FilePath \$LamnaPolicy -Option 12 # Enforce Store Apps Set-RuleOption -FilePath \$LamnaPolicy -Option 13 # Managed Installer Set-RuleOption -FilePath \$LamnaPolicy -Option 14 # ISG Set-RuleOption -FilePath \$LamnaPolicy -Option 16 # No Reboot Set-RuleOption -FilePath \$LamnaPolicy -Option 17 # Allow Supplemental Set-RuleOption -FilePath \$LamnaPolicy -Option 19 # Dynamic Code Security | | | |
| Add rules to allow windir and Program Files directories: | | | |
| PowerShell | 🗅 Сору | | |
| <pre>\$PathRules += New-CIPolicyRule -FilePathRule "%windir%*" \$PathRules += New-CIPolicyRule -FilePathRule "%0SDrive%\Program Files*"</pre> | | | |

FSLOGIX Fake the funk with masking

- This is a great way to at an image.
- Deploy the FSLogix files
- Run the rule editor and l and then choose which
- This has a benefit of allc pools, but users based (
- There are 2x files that ar directory, and then you
- This doesn't prevent use fake the funk pretty well
- <u>https://docs.microsoft.c</u>

| | 🗰 Rule Set: Contoso_1 | | | _ | | × |
|---|-----------------------|---------|------------|------------|------|-----|
| | O Blank Dula Cat | | | | | |
| FSLogix Apps RuleEditor | | | - 🗆 | × | | |
| 🌐 Assignments | _ | | × | | | ^ |
| Rule Set: | | | | | | |
| Assignment | | Applies | | | | |
| 📽 Everyone | | No | | | | |
| | | | Quick Laur | nch\Use | | ~ |
| | | | rt Menu\P | rogram | | |
| | | | | | | 0% |
| | | | | | Cano | cel |
| Set As Template Move Up | Move Down Add | Remove | | | n | |
| Rule Set does apply to user/group | | | | | | |
| Rule Set does not apply to user/group | | | Kev/Val | > ue: 1 | | |
| AD Reporting | OK Cancel | Apply | | | | |

4.0 Session policies

Secure session policies are one of your best defenses from users and/or attackers being able to do things they shouldn't. Windows Policies can only go so far.

4.0 Session policies-AVD Cloud PC

Intune or GPO to the desktops

| Do not allow Clipboard redirection | Restrict clipboard transfer from client to server |
|---|---|
| Do not allow COM port redirection | Restrict clipboard transfer from client to server (User) |
| Do not allow drive redirection | Restrict clipboard transfer from server to client |
| Do not allow LPT port redirection | Restrict clipboard transfer from server to client (User) |
| Do not allow smart card device redirection | Restrict clipboard transfer from client to server |
| Do not allow supported Plug and Play device redirection | Restrict clipboard transfer from client to server: (Device) |
| Do not allow video capture redirection | Restrict clipboard transfer from client to server (User) |
| Do not allow WebAuthn redirection | Restrict clipboard transfer from client to server: (User) |
| | |
| | |
| | Restrict clipboard transfer from server to client (User) |

https://learn.microsoft.com/en-us/azure/virtual-desktop/clipboard-transfer-direction-data-types?tabs=intune

4.0 Session policies-AVD Cloud PC

Default pools

| Hit Test1 RDP Properties | 5 🖈 … | | | |
|-------------------------------|--|--|--|--|
| | | | | |
| Overview | | | | |
| Activity log | Each host pool has a set of default RDP | properties and values. You can add other properties to the default set or override | the default values by setting custom RDP properties.Learn more | |
| 玲 Access control (IAM) | | | | |
| 🔶 Tags | Connection information Session behaviour Device redirection Display settings Advanced | | | |
| 🗙 Diagnose and solve problems | Audio and video | | | |
| 🛧 Resource visualizer | Microphone redirection ① | Not configured | \sim | |
| ✓ Settings | Redirect video encoding ① | Not configured | $\overline{\neg}$ | |
| 🗹 Scaling plan | | | | |
| RDP Properties | | Not configured | ➤ | |
| Properties | Audio output location ① | Play sounds on the local computer (default) | ~ | |
| Networking | | | | |
| 🕓 Scheduled agent updates | Camera redirection | Not configured | \neg | |
| Locks | - | | | |
| → Manage | MTP and PTP device redirection ① | Redirect portable media players based on the Media Transfer Protoc | <u>~</u> | |
| Application groups | Drive/storage redirection ① | Redirect all disk drives, including ones that are connected later (defa | \checkmark | |
| 🍵 MSIX packages | Clipboard redirection ① | Clipboard on local computer is available in remote session (default) | \checkmark | |
| 🕎 Session hosts | COM ports redirection ① | COM ports on the local computer are available in the remote sessio | \searrow | |
| > Monitoring | Keyboard redirection | Not configured | \neg | |
| > Automation | | | | |
| > Help | Location service redirection U | Not configured | <u>×</u> | |
| | Printer redirection ① | The printers on the local computer are available in the remote sessio | ∽ | |
| | Smart card redirection ① | The smart card device on the local computer is available in the remo | \checkmark | |
| | WebAuthn redirection ① | WebAuthn requests in the remote session are redirected to the local | \sim | |
| | USB device redirection ① | Redirect all USB devices that are not already redirected by another h | \sim | |
| | Save Discard changes | | | |

https://learn.microsoft.com/en-us/azure/virtual-desktop/redirection-configure-drives-storage?tabs=intune&pivots=azure-virtual-desktop

4.0 Session policies-AVD Cloud PC

Cloud PC & AVD Default Session Settings

| Risk | Setting | Default setting |
|-------------|---------------------------|-----------------|
| High | Copy\Paste | Allowed (Bi) |
| High | Client Fixed Drives | Allowed |
| High/Medium | Printer Mapping | Allowed |
| High/Medium | Client Webcam Mapping | Prohibited |
| High/Medium | Client USB Mapping | Allowed |
| High/Medium | Location Redirection | Prohibited |
| Medium/Low | COM Mapping | Allowed |
| Medium/Low | Audio Redirection | Allowed |
| Low | Microphone Mapping | Prohibited |
| Low | SmartCard Redirection | Allowed |



5.0 Antivirus

If you have a solution of 100% application blocking, you still need something to catch the "others" and known bad things.

5.0 Antivirus

- When we first started down the XenApp world and then the VDI world, AV has been the big debate at many levels.
- Typical AV weaknesses:
 - Too much overhead, ProjectVRC went over this in 2013. You can lose 10-30% of your density.
 - Doesn't understand multi-user OS with RDS/XenApp.
 - Causes frequent updates to the image, which can add a whole lot of time to maintain the image.
 Requires frequent DAT updates that, in some cases, can crash some systems just keeping it up to date.
 - They all have complicated policies that don't know Citrix/VMware in general of some basic exclusions.
 - Most are not Hypervisor-aware, which means tons of agents and not using basic guest introspection that is available from XenServer, ESX and Hyper-V now.

5.0 Antivirus

- Bit9 NextGen detonate and deny
- BitDefender HVI=Hypervisor Integration (XenServer, ESX and HyperV)
- Cylance NextGen, Al
- <u>Carbon Black NextGen</u>
- CrowdStrike NextGen + others
- Kaspersky classic huge solution options
- McAfee classic huge solution options
- Microsoft Defender ATP classic + cloudy
- Palo and Cisco classic huge solution options with sprinkles of clouds
- Symantec classic huge solution options
- TrendMicro classic + guest introspection

CROWDSTRIKE "THE BIG ONE"

JULY 19TH, 2024

imgflip.com

ung sup o

6.0 Windows features There are some new things you might like

Windows 10: Build equal but different security

• 20H2

- Windows Defender Updates for APT and AIR
- Windows Defender Application Guard for Office
- 21H1
 - Windows Defender Application Guard (WDAG) Updates
- 21H2
 - WPA3
- 22H1
 - Who knows 😊 I would guess more Defender things.

Windows 11: Building up, but starting over

• 11-21H2

- Windows Defender updates
- Windows Defender Application Guard + Office
- Windows Hello Updates + TPM requirements
- Windows Security Baseline updates
- 11-22H2
 - Credential Guard (on by default)
 - Smart app control
- 11-23H2
 - Passwordless enhancements (Passkey)
- 11-24H2
 - SMB Signing required
 - SMB NTLM Block
 - LAPs updates

Local administrator password solution (LAPS)

- No more single admin password for all systems!
- Management of local account passwords
 - Domain joined computers
 - Passwords stored in Active Directory
 - ACL protected
 - Randomly generated
- Managed by:
 - Group Policy
 - PowerShell
 - Agent
- ENSURE you delegate the right permissions to the right group!
- Find-AdmPwdExtendedrights -identity <OU name> | Format-Table (audit it)





7.0 SSL

Don't accept a man in the middle attack every day. Replace default certificates.

| 00- | https://server-vcenter.vkernel.local/ | 🔽 🄄 🔀 Bing | <u>.</u> |
|-------------|--|--|--------------|
| 🔶 Favorites | Certificate Error: Navigation Blocked | 🦄 🔹 🖾 👻 🚍 🕶 Page 🔹 Safety | Tools ▼ |
| 8 | There is a problem with this website's securi | ty certificate. | <u>_</u> |
| _ | The security certificate presented by this website was no | t issued by a trusted certificate authority. | |
| | Security certificate problems may indicate an attempt to server. | fool you or intercept any data you send to the | |
| | We recommend that you close this webpage and do | o not continue to this website. | |
| | 🥙 Click here to close this webpage. | | |
| | 😵 Continue to this website (not recommended). | | |
| | More information | | |
| | | | |
| K | | XXXXXXXX | XX |
| AN | | | |

TLS basics for all external connections

Run your SSL Labs test (for the win!) https://www.ssllabs.com/ssltest/analyze.html

Don't forget to check this box before you test.



Home Projects Qualys Free Trial Contact

Submit

You are here: Home > Projects > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.

Hostname: something.gateway

Do not show the results on the boards

hterenceluk.blogspot.com/2018/06/scoring-a-grading-from-qualys-ssl-labs.html los.//www.vcloudinfo.com/2018/08/how-to-get-a-from-qualys-ssllabs-on.html



DNS Certification Authority Authorization (CAA) Policy found for this domain. MORE INFO »





8.0 Multifactor

Requiring more than a username and password will drastically slow down or prevent the attack chain from proceeding.



8.0 Multifactor

- This is a great defense to potential attackers.
 - If you have other entry points that do not use it, its effectiveness will go down, but that also means the attack will pivot through something that might not be yours.
- In some deployments, it may not be possible based on how it is used operationally.
- Do or do not, there is no try 😊
- Solutions
 - Paid
 - SAML IDP (Okta, Ping CYBERSECURITY CISC
 - DUO
 - Azure MFA
 - Proximity Badges
 - Many more

MGM Resorts' ransomware attack started with a single phone call

MGM — NEWS

Social engineering allegedly ¹/₁ed to MGM attack: \$13 billion firm's cybersecurity "defeated by a 10-minute conversation"?

Entra ID: Conditional Access-MFA Party

Do it!

Home > Conditional Access

See Conditional Access | Policies

 $\langle \langle \rangle$

Overview

I Policies

- Insights and reporting
- 🔀 Diagnose and solve problems

Manage

- Named locations
- Custom controls (Preview)
- 🧹 Terms of use
- VPN connectivity
- Authentication contexts
- Q Authentication strengths
- I Classic policies

Monitoring

- Sign-in logs
- Audit logs

Troubleshooting + Support

New support request

+ New policy + New policy from template $\,\,\overline{\uparrow}\,\,$ Upload policy file $\,\,$ What if $\,\,$ C Refr

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organizat

| All policies | Microsoft-managed policies | |
|--------------|----------------------------|----------|
| 12 | 🛱 0 | |
| Total | out of 12 | |
| ✓ Search | | Y Add fi |

12 out of 12 policies found

| Policy name | State |
|---|-------------|
| | |
| Require compliant or hybrid Azure AD joined device or multifactor authentic | Report-only |
| Require multifactor authentication for Azure management | On |
| Require multifactor authentication for Microsoft admin portals | Report-only |
| Require multifactor authentication for admins | On |
| Require multifactor authentication for all users | On |
| Require multifactor authentication for guest access | Report-only |
| Require phishing-resistant multifactor authentication for admins | Report-only |

MFA vs none

<u>MFA (4-5)</u>

- 1. Physical possession of phone
- 2. Passcode, fingerprint, or a face
- 3. Locate the app
- 4. Open the app (may have to enter a PIN)
- 5. Need the UN and password

SMS is not ideal as if an individual is targeted, their phone number can be cloned so that MFA requests go to an attacker's phone.

<u>No MFA (1)</u>

1. Need the UN and password

Directory security

Default Entra ID or hybrid connected will have a failing school score if you don't change settings in GPO, Intune, Azure, and other locations.

Microsoft Secure Score Overview Recommended actions History Metrics & trends Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it. Applied filters: **Filter** Your secure score Actions to review Comparison Include Recently added To address Risk accepted Rearessed Planned Secure Score: 50.37% Your score 50.37 / 100 5 99 0 0 0 517.82/1028 points achieved Recently updated Organizations of a similar size 48.16 / 100 0 Top recommended actions Recommended action Score impact Status Category 2222 202 non in in the set and a set in the set and and Block abuse of exploited vulnerable signed drivers +0.88% O To address Device O To address Block untrusted and unsigned processes that run fr... +0.88% Device Breakdown points by: Category ldentity/ 38.93% ○ To address Encrypt all BitLocker-supported drives +0.88% Device Data 55.56% Block executable files from running unless they me... +0.88% To address Device Device Block Office applications from injecting code into o... +0.88% O To address Device Block Adobe Reader from creating child processes O To address +0.88%Device Points achieved Opportun Block all Office applications from creating child pro... +0.88% O To address Device Block JavaScript or VBScript from launching downl... +0.88% O To address Device

If your CIO or CISO sees this GUI, your new job will be fixing these things nearly full-time.

MFA pro tips

- Start with IT
- High-stakes employees (C-suite, finance)
- Leadership
- Everyone else


9.0 Micro-segmentation

Micro-segmentation



- VLANs are cool.
- No ACLs between them are not cool.
- Everything shouldn't be able to talk to everything.





VDI logging

What did we learn?

- Thanks to the Nov 24 update (auto update to server 2025).
- And a very special thanks to Crowdstrike in Jun 2024.
- Pick your Windows updates.
- Pick your upgrade groups:
 - No two of the same role should be updated at the same time.
- Europe will always have it worse because of the time zones.
- Luck is involved with so many products for when your tenant gets the update.
- Maybe run two AVs?

Timing is everything!



The final countdown

- 1. Apply secure group policies (don't let users get to anything they don't need).
- 2. Apply Windows patches.
- 3. Ensure your session policies allow users access to only what they need.
- 4. Use application control (users can only run what they need and everything else is blocked).
- 5. Run antivirus to catch the wildcards that may show up.
- 6. Use some of the Windows security features.
- 7. Make sure you SSL everything you can.
- 8. Use MFA.
- 9. Use micro-segmentation.
- 10. Logging (Windows event & PowerShell logs).
- 11. Secure endpoints.
- 12. Use security best practices (min domain admins, admin role groups, firewalls).





Ramming speed=broken doors/doors left open. Business priorities of new beat the needs of now

What's the biggest enemy to IT security?



Questions?

Patrick Coble @VDIHacker

VDISecurity.org







Extras (Do we have time yo?)

Special security callouts for AVD/Cloud PC

https://learn.microsoft.com/en-us/security/zero-trust/azure-infrastructure-avd

| Component | Responsibility |
|-------------------------------|---------------------|
| Identity | Customer or partner |
| User devices (mobile and PC) | Customer or partner |
| App security | Customer or partner |
| Session host operating system | Customer or partner |
| Deployment configuration | Customer or partner |
| Network controls | Customer or partner |
| Virtualization control plane | Microsoft |
| Physical hosts | Microsoft |
| Physical network | Microsoft |
| Physical datacenter | Microsoft |

https://learn.microsoft.com/en-us/azure/virtual-desktop/security-recommendations#sharedsecurity-responsibilities

Security testing/audits

- Are you doing regular external vendor audits?
- Are you doing vulnerability assessments or security audits?
- Are you doing penetration tests?
- Are you using different companies each year?
- There are many differences in these tests, and the cost makes a significant difference in any location. You get what you pay for.

Patterns over time



Defense in depth-it's easy, they said

