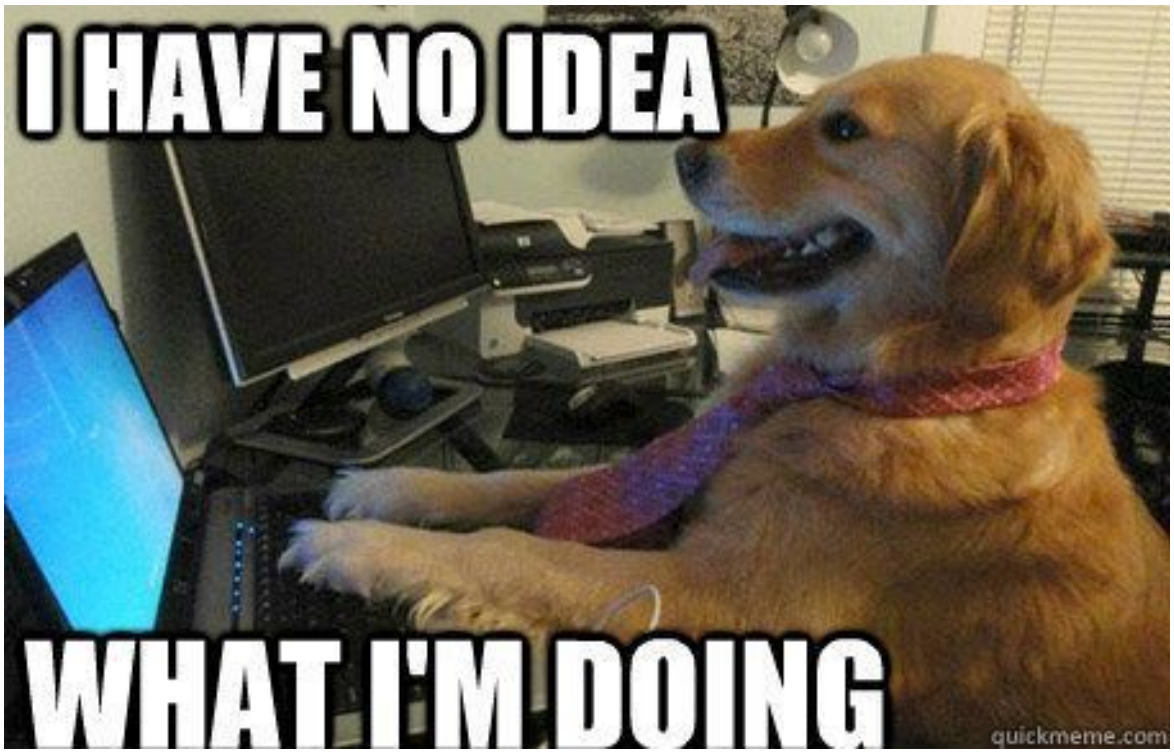
I HAVE NO IDEA
WHAT I'M DOING
quickmeme.com

# Table of Contents

# Hardening Priorities

| **Host** | **Who** | **Services** |
|---|---|---|
| Dell 2 Core (dc1) | Liam | AD/DNS/DHCP |
| Dell 5 Gui (mgmt1) | Ally | Management/Utility/IIS |
| HyperV | Liam | Server 16 |
| Dell 4 Spare | Ally | Possible Firewall |
| Dell 1 Workstation | Liam | DHCP Client |
| Dell 7 Traveler | Ally | Possible orange team use |

# Important Info

| Host | IP | Users | Scored Services/Ports |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

# Hardening Systems Level

Note - Use a temporary User

| # | Task | Command |
|---|---|---|
| 1 | Lockdown local users | Net user<br><br>Take note of users on sheet.<br>Net localgroup “Administrators”<br>Net localgroup “Remote Management Users”<br>Net  localgroup “Remote Desktop Users”<br><br>Net user “username” /active:no |
| 2 | Put powershell into constrained language mode | [Environment]::SetEnvironmentVariable('__PSLockdownPolicy', '4', 'Machine') |
| 3 | Check constrained language mode settings | $ExecutionContext.SessionState.LanguageMode |
| 4 | Get commands that launch on startup. | wmic startup get caption,command<br>Make sure nothing looks too weird… consult google + partner |
| 5 | Disable Teredo | Netsh interface teredo show stat<br>netsh interface teredo set state disabled |
| 6 | Check installed programs | Open Add or Remove Programs<br>Get-WmiObject -Class Win32_Product -ComputerName <remote_computer_name/localhost> |
| 7 | Uninstall any suspicious programs | $app = Get-WmiObject -Class Win32_Product -Filter "Name = '<Package Name>'"<br>$app.Uninstall() |
| 8 | Check Shares for weirdness | Net share |
| 9 | Check for open Sessions | List all sessions connected to this machine<br>NET SESSION<br>List sessions from a given machine<br>NET SESSION \\ComputerName<br>Disconnect all sessions connected to this machine<br>NET SESSION /DELETE<br>Disconnect all sessions connected to this machine (without any prompts)<br>NET SESSION /DELETE /y<br>Disconnect sessions from a given machine<br>NET SESSION \\ComputerName /DELETE |
| 10 | Check for listening ports | Netstat -at<br>Netstat -abon |

| | | |
|---|---|---|
| | | netstat -a -b |
| 11 | Processes | tasklist |
| 12 | Services | Net start |
| 13 | Workstation | net config workstation<br>Note the name |
| 14 | Defender | Windows Defender - Check all the exceptions and remove all<br>Run. |

# Installing Programs

| | | |
|---|---|---|
| 1 | NMAP | |
| 2 | RSAT | |
| 3 | SYSinternals | https://live.sysinternals.com/<br><br>net use x: \\http://live.sysinternals.com<br>xcopy /s x:\ c:\sysinternals<br>net use x: /d |
| 4 | Splunk Forwarder | https://www.splunk.com/en_us/download/universal-forwarder.html |
| 5 | Wireshark | |

# Hardening Active Directory

## Creating New Users

| # | Task | Command |
|---|---|---|
| 1 | Temp User | Net user “Name” * /add /domain /workstation:<FQDN> |
| 2 | Add Admin to these accounts | Account operations<br>Administrators<br>DHCP Administrators<br>DNS Admins<br>Domain Admins<br>Enterprise Admins<br>Event Log Readers<br>Group Policy Creator Owners<br>Performance Log Users<br>Performance Monitor Users<br>Print Operators<br>Remote Desktop Users<br>System Admins<br>Server Operators |

# Group Policy

| # | Task | Command |
|---|---|---|
| 1 | Install Group Policy App | Add Under Roles and Features |
| 2 | Create Harden GPO | |
| | Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment<br><br>Debug programs - Remove all groups/users<br><br>Interactive logon: Message text for users attempting to log on - sometimes an inject “That's against the student code of conduct.”<br><br>Computer Configuration > Administrative Templates > Windows Components > Windows Defender - Turn off Window Defender - Disabled<br>Turn on Windows Firewall<br><br>This Group Policy needs to be applied to all necessary workstations, servers, and domain controllers in the domain.<br><br>**-- These Broke it ---**<br>Computer Configuration > Preferences > Windows Settings > Right click registry > New Registry Item<br>- Action: Create<br>- Hive: HKEY_LOCAL_MACHINE<br>- Key Path: SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters<br>- Value name: SMB1<br>- Value type: REG_DWORD<br>- Value data: 0<br>Allow log on through Terminal Services - Leave blank to disallow login via TS even if it has been started.<br>Deny Access to this computer from the network - Guests;ANON Logon<br>Network security: LAN Manager authentication level - Send NTLMv2 response only\refuse NTLM & LM<br>Network security: Do not store LAN Manager hash value on next password change - Enabled<br>Network access: Do not allow anonymous enumeration of SAM accounts and shares - Enabled<br>Network access: Do not allow anonymous enumeration of SAM accounts - Enabled<br>Network access: Allow anonymous SID/name translation - Disabled | |
| 3 | Create Audit Policy | Apply to All machines |
| | Administrative Templates → Windows Components → Windows PowerShell<br>1. Turn on Module - > Set *<br>2. Scripting Block -> Log Script Block checked<br>3. Transcript -> Include Invo Checked<br>CC -> Policies -> Windows Settings -> Security Settings -> Advanced Audit<br>Audit process tracking - Successes<br>Audit account management - Successes, Failures<br>Audit logon events - Successes, Failures<br>Audit Account Lockout: S&F<br>Audit Other Logon/Logoff Events: S&F | |

| | | |
|---|---|---|
| | Audit Special Logon: S&F | |
| 4 | Create Applocker Policy | Apply to Win1 to Test |
| | Create new Policy<br>CC > POL > SEC > SYS > Application Identity<br>App Locker create default policies<br>Block Powershell<br>Block User Folder | |
| 5 | Create Lockout Policy | |
| | Create a new User lockout, with password<br>Add a new OU<br>Add Lockout to Lockout OU<br>Set lockout threshold to 0<br>Enforce | |
| 6 | Create Service Lockdown | |
| | CC > POL > SEC > SYS ><br>Disable:<br>Telnet, IP Telephony, Print Spooler, Multimedia Class Scheduler | |

# Event Logs

| | | |
|---|---|---|
| 1 | Powershell Remoting | 4624,4672,4103, 4104, 53504, 400, 403, 800, 91, 198 |
| | **4624** Logon Type 3 Source IP/Logon User Name<br>**4672** Logon User Name Logon by an a user with administrative rights<br>Microsoft-WindowsPowerShell%4Operational.evtx<br>**4103, 4104** – Script Block logging Logs suspicious scripts by default in PS v5 Logs all scripts if configured<br>**53504** Records the authenticating user<br>Windows PowerShell.evtx<br>**400/403** "ServerRemoteHost" indicates start/end of Remoting session<br>**800** Includes partial script code Microsoft-WindowsWinRM%4Operational.evtx<br>**91** Session creation<br>**168** Records the authenticating user | |
| 2 | WMI WMIC | 4624,4672, 5857,5860, 5861 |
| | security.evtx<br>**4624** Logon Type 3 Source IP/Logon User Name<br>**4672** Logon User Name Logon by an a user with administrative rights<br>Microsoft-Windows-WMIActivity%4Operational.evtx<br>**5857** Indicates time of wmiprvse execution and path to provider DLL – attackers sometimes install malicious WMI provider DLLs<br>**5860, 5861** Registration of Temporary (5860) and Permanent (5861) Event Consumers. Typically used for persistence, but can be used for remote execution. | |
| 3 | Services | 4624,4697,7034,7035,7036,7040,7045 |
| | security.evtx<br>**4624** Logon Type 3 Source IP/Logon User Name<br>**4697** Security records service install, if enabled Enabling non-default Security events such as ID **4697** are particularly useful if only the Security logs are forwarded to a centralized log server<br>system.evtx<br>**7034** – Service crashed unexpectedly<br>**7035** – Service sent a Start/Stop control<br>**7036** – Service started or stopped<br>**7040** – Start type changed (Boot \| On Request \| Disabled)<br>**7045** – A service was installed on the system | |
| 4 | Scheduled Tasks | 4624,4672,4698,4702,4699,4700,4701,106,140,141,200,201 |
| | security.evtx<br>**4624** Logon Type 3 Source IP/Logon User Name<br>**4672** Logon User Name Logon by a user with administrative rights Requirement for accessing default shares such as C$ and ADMIN$<br>**4698** – Scheduled task created<br>**4702** – Scheduled task updated<br>**4699** – Scheduled task deleted<br>**4700/4701** – Scheduled task enabled/disabled<br>Microsoft-Windows-Task Scheduler%4Maintenance.evtx | |

| | | |
|---|---|---|
| | **106** – Scheduled task created<br>**140** – Scheduled task updated<br>**141** – Scheduled task deleted<br>**200/201** – Scheduled task executed/completed | |
| 5 | PsExec | 4624,4672,5140,7045 |
| | security.evtx<br>**4624** Logon Type 3 (and Type 2 if "-u" Alternate Credentials are used) Source IP/Logon User Name<br>**4672** Logon User Name Logon by a user with administrative rights Requirement for access default shares such as C$ and ADMIN$<br>**5140** – Share Access ADMIN$ share used by PsExec system.evtx<br>**7045** Service Install | |
| 6 | Map Network Shares | 4624, 4672, 4776, 4768, 4769, 5140, 5145 |
| | Security Event Log – security.evtx<br>**4624** Logon Type 3 Source IP/Logon User Name<br>**4672** Logon User Name Logon by user with administrative rights Requirement for accessing default shares such as C$ and ADMIN$<br>**4776** – NTLM if authenticating to Local System Source Host<br>**4768** – TGT Granted Source Host Name/Logon User Name Available only on domain controller<br>**4769** – Service Ticket Granted if authenticating to Domain Controller Destination Host Name/Logon User Name Source IP Available only on domain controller<br>**5140** Share Access<br>**5145** Auditing of shared files – NOISY! | |
| 7 | Remote Desktop | 4624,4778,4779,131,98,1149,21,22,25,41 |
| | Security Event Log – security.evtx<br>**4624** Logon Type 10 Source IP/Logon User Name<br>**4778/4779** IP Address of Source/Source System Name Logon User Name<br>Microsoft-WindowsRemoteDesktopServicesRdpCoreTS%4Operational.evtx<br>**131** – Connection Attempts Source IP/Logon User Name<br>**98** – Successful Connections<br>Microsoft-Windows-Terminal Services-RemoteConnection Manager%4Operational.evtx<br>**1149** Source IP/Logon User Name • Blank user name may indicate use of Sticky Keys<br>Microsoft-Windows-Terminal Services-LocalSession Manager%4Operational.evtx<br>**21, 22, 25** Source IP/Logon User Name<br>**41** Logon User Name | |

# Other

## NMAP

```
nmap -sS -T4 -A -sC -oA Output --stylesheet
https://raw.githubusercontent.com/honze-net/nmap-bootstrap-xsl/master/nmap-bootstrap.xsl <IP>
```

# Normal State Configurations

Nmap Scan
Service list
Netstat list
Get-WindowsFeature
Process
Startup