**Basic Hardening**

**Remove all AD Users from an AD Group (without removing the Administrator)**

Get-ADGroupMember -Identity “Domain Admins” | Where-Object -Property Name -ne -Value “Administrator” | ForEach-Object {Remove-ADGroupMember “Domain Admins” $\_}

**Disable AD User Accounts**

PS C:\> Get-ADUser -Filter 'Name -notlike "Admin\*"' -SearchBase "DC=minions,DC=galactic" | Disable-ADAccount

Apply local security policies to DC, and then to default GPO

***Local Security Policies -> Local Policies -> Security Options***

Accounts:

Block Microsoft Accounts - Enabled

Guest Account Status - Disabled

Limit Local Account use of blank passwords to console logon only - Enabled

Rename Administrator account - rename and record info with Windows team

Devices:

Prevent users from installing printer drivers - Enabled

Restrict CD-ROM access to locally logged-on user only - Enabled

Interactive Logon:

Display user information when the session is locked - Do not display user information

Do not display last username - Enabled

Do not require CTRL + ALT + DEL - Disabled

Network Access:

Do not allow anonymous enumeration of SAM accounts - Enabled

Let Everyone permissions to apply to anonymous users - Disabled

Recovery Console:

Allow automatic administrator logon - Disabled

***Local Security Policies -> Local Policies -> User Rights Assignment***

Deny logon as batch job/service/via Remote Desktop Services - Guest (user) and Guests (group)

***Local Security Policies -> Local Policies -> Audit Policy***

Enable account logon events, logon events, account management, and policy changes

Enable Windows Firewall, block incoming traffic by default

* Create rules to allow for services scored by ISE

Disable Remote Access

* Run sysdm.cpl, navigate to “Remote”, and check “Don’t allow remote connections to this computer”
* Ensure “Allow remote assistance connections to this computer” is unchecked

Check installed programs either via Control Panel or running appwiz.cpl

* Remove any remote access programs (i.e. TeamViewer, Supremo, GoTo, VNC, etc.)

Deploy Sysinternals suite and run TCPViewer for real time review of network traffic to machine

View open ports using netstat (through cmd) or by running resmon.exe and navigating to Network (highly recommended)

Disable all local users on non-DC machines through lusrmgr.msc or “net user <username> /active:no”

***Powershell commands that only need to be run once at competition start***

**Disable Scripts in PowerShell**

Set-ExecutionPolicy Restricted

**Disable Remote PowerShell**

Disable-PSRemoting -Force

**Disable SMBv1 (Windows 8/2012+)**

Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol

**Disable SMBv2 (Windows 8/2012+)**

Set-SmbServerConfiguration -EnableSMB2Protocol $false

**Disable SMBv1 (Windows 7/2008 and below)**

Set-ItemProperty -Path “HKLM:\SYSTEMCurrentControlSet\Services\LanmanServer\Parameters” SMB1 -Type DWORD -Value 0 -Force

**Disable SMBv2 (Windows 7/2008 and below)**

Set-ItemProperty -Path “HKLM:\SYSTEMCurrentControlSet\Services\LanmanServer\Parameters” SMB2 -Type DWORD -Value 0 -Force