Locked Out of Harden Network

*\*\*Note: I have verified and tested on Windows Server 2016*

*\*\*Conditions: BIOS – Boot from DVD is enabled; MUST not be Bitlocker yet.*

***Backup Sticky Keys***

1. Insert a Windows OS Installation Disk into Server/Computer.
   1. Grab Windows OS (.iso) file and burn to DVD.
   2. Boot to DVD.
2. Select “Repair your Computer”
   1. You will see this on the bottom left of the Wizard window.
   2. Click on “Troubleshoot” tab.
   3. Then, click on “Command Line Prompt”.
3. Command Line – Know where you’re looking at!!
   1. WinPE – CMD
      1. By Default, you will be at the “x:” drive within WinPE (aka bootable disk).
      2. You want run “diskpart” command, and then type in “list volume”
         1. You want to specifically look for the C drive for the OS your locked out on.
            1. \*\*CAUTION\*\*: The C drive could be a different letter and not “C”.
      3. Change to the C drive, drive letter and continue below with my notes.
4. Back up original Sticky Key file.
   1. Use this command. “copy c:\windows\system32\sethc.exe c:\”
   2. Then, use this command. “copy c:\windows\system32\cmd.exe c:\windows\system32\sethc.exe”
   3. Reboot your Server/Computer to the login screen.

***Re-Edit your GPO’s When Locked Out!!***

1. After Rebooting and being at the login screen.
   1. Press the “Shift” button on the keyboard 5 time’s.
      1. The admin command prompt will pop up.
2. Re-edit your GPO’s.
   1. Use this command to get to your GPO’s.
      1. “gpedit”
3. Your sign-in method is not allowed.
   1. If you hardened your systems and get this when you try to login in, “Deny log on locally” GPO is set for Domain admins and local admin’s.
      1. Computer Configuration 🡪 Windows Settings 🡪 Security Settings 🡪 Local Policies 🡪 User Rights Assignment 🡪 Deny log on locally
4. **IMPORTANT:** Once you got back in your harden network, you need to move sethc.exe back to its original location. Boot back up using your Windows OS Disc and get into the command prompt again.
   1. Use this command. “copy c:\sethc.exe c:\windows\system32\sethc.exe”

***Reset Forgotten Domain Account Password***

1. After “Backing Sticky Keys” steps.
   1. After Rebooting and being at the login screen. Press the “Shift” button on the keyboard 5 time’s. The admin command prompt will pop up.
   2. Use this command line. “net user AccountName MyNewPassword”
      1. Input the already established account username and input a new password.
   3. Computer Management Console (GUI)
      1. CMD 🡪 “compmgmt.msc”
2. **IMPORTANT:** Once you got back in your harden network, you need to move sethc.exe back to its original location. Boot back up using your Windows OS Disc and get into the command prompt again.
   1. Use this command. “copy c:\sethc.exe c:\windows\system32\sethc.exe”