Windows (CCDC 2016)

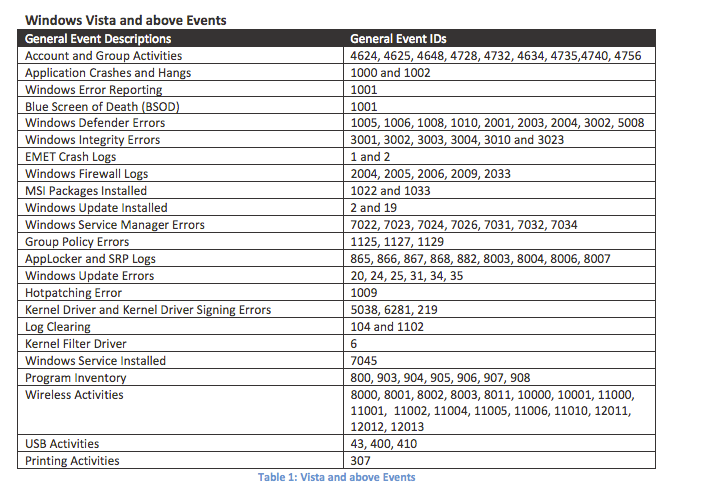
**MS09-050**

1. ONLY IF NOT R2 09-050: regedit -> HKEY\_LOCAL\_MACHINE -> System -> CurrentControlSet -> Services -> LanmanServer -> Parameter -> right click & add new DWORD -> smbv2 (set value to 0) -> right click & add new DWORD smbv1 (set value to 1)

**Services**

* Disable rcp over http
* Disable Remote Registry
* Disable Print Spooler
* Disable Remote Desktop
* Find out what services/ ports we need up for scoring

**Event Logs**

1. Eventvwr.msc to bring up event viewer -> Create custom view -> Windows logs -> event relevant event ids or select critical from event level
2. Some good event ids to look for:
   1. 4625: Login failure -- could tell us if we are getting brute forced
   2. 4720: User account created -- if we didn’t create a new user then this is NOT GOOD
   3. others:   
      

**Scheduled Tasks / Startup Scripts**

1. Check task scheduler and view hidden tasks
2. To check startup scripts: Msconfig -> Boot, Startup, Services

**Monitoring Network Connections**

1. Show connections that have been “ESTABLISHED” every 30 seconds  
    netstat -abo 30 | findstr ESTABLISHED
2. Show connections that have been “LISTENING” every 30 seconds  
    netstat -abo 30 | findstr LISTENING

**Change User Access Settings**

1. Control Panel -> User Accounts -> Turn user account control on or off -> turn it on -> restart

**Group Policy & SRP**

1. gpmc.msc -> Default Domain Policy -> Windows Settings -> Security Settings
   1. Account Policies
      1. Password Policies
      2. Account lockout policies
   2. Local Policies
      1. User Rights assignment
         1. forced shutdown from remote system -> Remove all
         2. Allow logon Locally -> administrators
      2. Security Options
         1. Accounts: Guest account -> Disable & rename guest account
         2. Accounts: Admin -> Rename the admin account
         3. Domain Member: Max machine account password age
         4. Network Access: No anonymous enum -> Enable
         5. Network Access: Allow anonymous SID Trans -> Disable
         6. Network Security: Lan Manager authen -> Send NTLMv2 response only\ use NTLM & LM
         7. Network Security: Do not store LAN manager hash -> Enable
         8. Shutdown: Allow system shutdown without having to logon -> Disable
         9. Network Security: Force logoff when logon hours have expired -> Enable
         10. Interactive Logon: Message text for users attempting to logon
      3. Audit Policy
         1. Audit process tracking -> Successes
         2. Audit account management -> Successes, failures
         3. Audit logon events -> successes, failures
         4. Audit account logon events -> successes, failures
   3. System Services
      1. Disable services that we do not need
   4. Firewall
   5. User Configuration
      1. Policies
         1. Admin templated -> all setting
            1. Password protect screen saver
            2. screen saver timeout
2. Stop programs from running in Temp folder(C:\Windows\temp)
   1. gpmc.msc -> right click domain name & create new GPO
      1. Right click the new policy -> edit
      2. Computer config -> windows settings -> security settings -> file system -> right click & add file
         1. browse to folder & click ok
         2. Configure ntfs file/ folder permissions -> click ok
3. Push out all Group Policies updates
   1. In CMD(may need to be running as admin) run gpupdate /force
   2. restart all systems

**Disabling Sticky Keys**

* Control Panel -> Accessibility Options -> Uncheck all checkboxes for sticky keys, filter keys, toggle keys -> General tab -> check apply all settings to logon desktop & Apply all settings to defaults for new users

**Disable Ease of Access**

* In CMD run: reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Utilman.exe" /v "Debugger" /t REG\_SZ /d "systray.exe" /f
* or remove utilman.exe