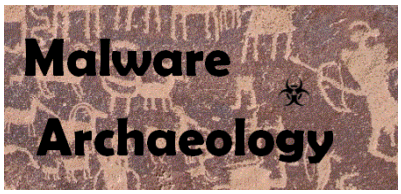
WINDOWS LOGGING CHEAT SHEET - Win 7 thru Win 2012

This "**Windows Logging Cheat Sheet**" is intended to help you get started setting up basic and necessary Windows Audit Policy and Logging. By no means is this list extensive; but it does include some very common items that should be enabled, configured, gathered and harvested for any Log Management Program. Start with these settings and add to it as you understand better what is in your logs and what you need.



DEFINITIONS:

ENABLE: Things you must do to enable logging to start collecting and keeping events.

CONFIGURE: Configuration that is needed to refine what events you will collect.

GATHER: Tools/Utilities that you can use locally on the system to set or gather log related information – AuditPol, WEvtUtil, Find, etc.

HARVEST: Events that you would want to harvest into some centralized Event log management solution like syslog, SIEM, Splunk, etc.

RESOURCES: Places to get more information

- MalwareArchaeology.com/cheat-sheets for more Windows cheat sheets
- ***Log-MD.com*** – The ***Log Malicious Discovery*** tool reads security related log events and settings. Use ***Log-MD*** to audit your log settings compared to the "***Windows Logging Cheat Sheet***" and Center for Internet Security (CIS) Benchmarks. It is a standalone tool to help those with and without a log management solution find malicious activity.
- www.ultimatewindowssecurity.com/securitylog/encyclopedia/Default.aspx - Better descriptions of Event OD's
- www.EventID.Net – Most of the Event ID's
- IIS Error Codes - http://support.microsoft.com/kb/318380 - IIS Error Codes
- http://cryptome.org/2014/01/nsa-windows-event.pdf - Good Article
- http://technet.microsoft.com/en-us/library/dd772712(v=ws.10).aspx – MS Adv Security Audit Policy Descriptions
- https://technet.microsoft.com/itpro/windows/whats-new/whats-new-windows-10-version-1507-and-1511 (new)
- Google! – But of course

ENABLE:

1. LOCAL LOG SIZE: Increase the size of your local logs. Don't worry you have plenty of disk space, CPU is not an issue
   a. Application, System logs - 256k or larger
   b. PowerShell logs - 256k or larger
   c. Security Log - 512,000k (yes this big) (1,024,000)
2. LOCAL SECURITY POLICY: Change Security Options – "***Audit: Force audit policy subcategory settings***" to ***ENABLE***. This sets the system to force use of the "Advanced Audit Policies"
3. GROUP POLICY: All settings mentioned should be set with Active Directory Group Policy in order to enforce these settings enterprise wide. There are cases where the Local Security Policy would be used.

ENABLE:

1. DNS LOGS: Enable DNS Logging. Capture what DNS queries are happening. "***systemroot\System32\Dns\Dns.log***"
   a. Log Packets for debugging
   b. Outgoing and incoming
   c. UDP and TCP
   d. Packet type Request and Response
   e. Queries/Transfers and updates
2. DHCP LOGS: Add your DHCP Logs – "***%windir%\System32\Dhcp.***" This will allow you to detect rogue systems on your network that fall outside your naming convention.
   a. EventID = 10 – New IP address was leased

WINDOWS LOGGING CHEAT SHEET - Win 7 thru Win 2012

Windows Audit Policy settings may be set by the Local Security Policy, Group Policy (preferred) or by command line using 'AuditPol.exe'. Be sure to select "*Configure the following audit events*" box on items that say "*No Audit*" or the policy will not apply. Any that are left blank will break the GPO and auditing will not be applied. ***(N)*** = Will generate large number of events or noise and filtering of events may be needed. ***(C)*** Indicates a setting changed.

CONFIGURE:

1. SYSTEM AUDIT POLICIES: In order to capture what you want and need the following ***Advanced Audit Policies*** must be set. You may expand these to your specific needs, but here is a place to start.

List out the System audit policy

- ***Command:*** AuditPol /get /category:*

Category/Subcategory	Setting
Account Logon	
• Credential Validation	Success and Failure
• Kerberos Authentication Service	No Auditing
• Kerberos Service Ticket Oper	No Auditing
• Other Account Logon Events	Success and Failure
Account Management	
• Application Group Management	Success and Failure
• Computer Account Management	Success and Failure
• Distribution Group Management	Success and Failure
• Other Acct Management Events	Success and Failure
• Security Group Management	Success and Failure
• User Account Management	Success and Failure
Detailed Tracking	
• DPAPI Activity	No Auditing
• Plug and Play (10/2016)	Success
• Process Creation	Success and Failure (N)
• Process Termination	Success and Failure (N)
• RPC Events	Success and Failure
• Audit Audit Token Right Adj (10/2016)	Success (N)
DS Access	
• Detailed Directory Service Repl	No Auditing
• Directory Service Access	No Auditing
• Directory Service Changes	Success and Failure
• Directory Service Replication	No Auditing
Logon/Logoff	
• Account Lockout	Success
• Group Membership (10/2016)	Success
• IPsec Extended Mode	No Auditing
• IPsec Main Mode	No Auditing
• IPsec Quick Mode	No Auditing
• Logoff	Success
• Logon	Success and Failure
• Network Policy Server	Success and Failure
• Other Logon/Logoff Events	Success and Failure
• Special Logon	Success and Failure
• User / Device Claims (8/2012)	No Auditing

CONFIGURE:

SYSTEM AUDIT POLICIES: Continued

To set an item:

- Auditpol /set /category:"Account Management" /success:enable /failure:enable

Category/Subcategory	Setting
Object Access	
• Application Generated	Success and Failure
• Certification Services	Success and Failure
• Central Policy Staging (8/2012)	No Auditing
• Detailed File Share	Success
• File Share	Success and Failure
• File System	Success
• Filtering Platform Connection	Success (Win FW) (N)
• Filtering Platform Packet Drop	No Auditing
• Handle Manipulation	No Auditing (N)
• Kernel Object	No Auditing (C)
• Other Object Access Events	No Auditing
• Removable Storage (8/2012)	Success and Failure
• Registry	Success
• SAM	Success (C)
Policy Change	
• Audit Policy Change	Success and Failure
• Authentication Policy Change	Success and Failure
• Authorization Policy Change	Success and Failure
• Filtering Platform Policy Change	Success (Win FW)
• MPSSVC Rule-Level Policy Change	No Auditing
• Other Policy Change Events	No Auditing
Privilege Use	
• Non Sensitive Privilege Use	No Auditing
• Other Privilege Use Events	No Auditing
• Sensitive Privilege Use	Success and Failure
System	
• IPsec Driver	Success
• Other System Events	Failure
• Security State Change	Success and Failure
• Security System Extension	Success and Failure
• System Integrity	Success and Failure
Global Object Access Auditing – ignore for now	

WINDOWS LOGGING CHEAT SHEET - Win 7 thru Win 2012

CONFIGURE:

1. WEvtUtil: Use this utility to configure your log settings
   a. WevtUtil gl Security – List settings of the Security Log
   b. WevtUtil sl Security /ms:524288000 or /ms: 1048576000 if File & Registry auditing, Windows Firewall and Process Create are all enabled – Set the Security log size to the number of bytes
   c. WevtUtil sl Security /rt:false – Overwrite as needed
2. FILE AUDITING: Configuring auditing of folders and specific files will allow you to catch new file drops in key locations where commodity and advanced malware often use. To understand what, where and why to audit files and folders, refer to the "***Windows File Auditing Cheat Sheet***" for more detailed information.
3. REGISTRY AUDITING: Configuring auditing of registry keys will allow you to catch new keys, values and data in autorun and other locations where commodity and advanced malware often use. To understand what, where and why to audit registry keys, refer to the "***Windows Registry Auditing Cheat Sheet***" for more detailed information.
4. REG.EXE: Use this utility to query what is in a Key or the data within a key or value
   a. Query a Key and all values - ***Reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\Run"***
   b. Query a Key and all values - ***Reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce"***
   c. Query a Key and all values - ***Reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Run"***
   d. Query a Key and all values - ***Reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce"***
   e. Query a known value of a Key:
   Reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v malware

CONFIGURE:

5. Command Line Logging: One of the most important logging items that you can collect is what was executed on the command line when something executes. Microsoft added this capability into the release of Windows 8.1 and Windows Server 2012 R2 and later versions. In Feb 2015 a patch was made available to add this feature to all Windows 7 and Windows 2008 Server with the following patch:
   - ***https://support.microsoft.com/en-us/kb/3004375 - KB3004375 Patch to add Command Line Logging***

   A registry key or GPO change is required to add the "Process Command Line" entry to every event ID 4688 event. The following is the key, value and data that must be set to collect this crucial information:
   - "hklm\software\microsoft\windows\currentversion\policies\system\audit" – Value = ProcessCreationIncludeCmdLine_Enabled - REG_DWORD = 1

   You can configure it to start collecting with the following command:

   - reg add "hklm\software\microsoft\windows\currentversion\policies\system\audit" /v ProcessCreationIncludeCmdLine_Enabled /t REG_DWORD /d 1

WINDOWS LOGGING CHEAT SHEET - Win 7 thru Win 2012

GATHER:

1. AUDITPOL: Use this utility to view your current log settings
    a. List all Policies categories: ***AuditPol /List /Subcategory:****
    b. List what is SET: ***AuditPol /get /category:****
    c. List what is SET for a subcategory:
        - ***AuditPol /get /category:"Object Access"***
2. Reg.exe: Use this utility to query the registry
    a. ***Changes to AppInit_Dlls*** - reg query "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows" /v AppInit_Dlls
    b. ***Changes to Services Keys*** - reg query "HKLM\System\CurrentControlSet\Services"
    c. ***Changes to Machine Run Key*** - reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\Run"
    d. ***Changes to Machine RunOnce Key*** - reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce"
    e. ***Changes to User Run Key*** - reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Run"
    f. ***Changes to User RunOnce Key*** - reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce"
    g.
3. SC.exe: Use this utility to query the services (sc /? For help)
    a. ***List all services in any state*** – sc.exe query state= all (Note: 'space' after the = sign)
    b. ***Look for a specific service*** – sc.exe query state= all | find /I "telnet"
    c. After finding the 'Display_Name' then look for the 'Service_Name' to get the short name

GATHER:

1. WEvtUtil: Use this utility to query your logs
    a. WevtUtil qe Security – query the Security Log for events
        i. Lots of flags here so read help "WevtUtil -?"
        ii. /c:5 = Read 5 events
        iii. /rd:true = newest events first
        iv. /f:text = format text, also can do XML
    b. ***Success & Failed Logons*** - WevtUtil qe Security /q:"*[System[(EventID=4624 or EventID=4625)]]" /c:5 /rd:true /f:text >Parsed\%computername%_Logon_Events_Win7.log
    c. ***User Account Change*** - WevtUtil qe Security /q:"*[System[(EventID=4738)]]" /c:5 /rd:true /f:text >Parsed\R_%computername%_User_Account_Change_Win7.log
    d. ***New Service Installed*** - WevtUtil qe Security /q:"*[System[(EventID=7045)]]" /c:5 /rd:true /f:text >Parsed\R_%computername%_New_Service_Installed_Win7.log
    e. ***User Account Changes*** - wevtutil qe Security /q:"*[System[(EventID=4725 or EventID=4722 or EventID=4723 or EventID=4724 or EventID=4726 or EventID=4767)]]" /c:10 /f:text
2. Filtering Log Results: Use this method to filter lines within the logs
    a. ***Registry Changed – Find entries with 'Object Name'*** - WevtUtil qe Security /q:"*[System[(EventID=4657)]]" /c:5 /rd:true /f:text |find /i"Object Name"
    b. ***File or Registry Changed – Find entries with 'Object Name'*** - WevtUtil qe Security /q:"*[System[(EventID=4663)]]" /c:50 /rd:true /f:text |find /i "Object Name"
    c. ***Files – Find new files with 'Wbem'*** - WevtUtil qe Security /q:"*[System[(EventID=4663)]]" /c:50 /rd:true /f:text |find /i "wbem"

WINDOWS LOGGING CHEAT SHEET - Win 7 thru Win 2012

HARVEST:

1. LOG CLEAR: Watch for log clear messages
    a. 104 – SYSTEM Log – The Application or System log was cleared
    b. 1102 – SECURITY Log – The audit log was cleared
2. TASKS: Watch for a Process to start and call other processes
    a. 4698 – SECURITY Log – New Task Created
3. DRIVER: Watch for an issue with a driver
    a. 40 – Issue with Driver
4. OS VERSION: What OS do machines have
    a. 6009 – Lists OS version, Service Pack and processor type

HARVEST:

1. ACCOUNTS: Monitor for attempts to change an account password
    a. 4720 – A user account was created
    b. 4724 – An attempt was made to reset an accounts PW
    c. 4735 – Local Group changed
    d. 4738 – User account password changed

HARVEST:

1. PROCESSES: Watch for a Process to start and call other processes
    a. 4688 – SECURITY Log – New Process Name, look for Creator Process ID to link what process launched what
2. INSTALLER: Watch for the Windows Installer activity
    a. 1022 – Windows Installer ***updated the product***
    b. 1033 – Windows Installer ***installed the product***
    c. 1034 – Windows Installer ***removed the product***
3. WINDOWS UPDATE: Watch for the Windows Update Agent activity.
    a. 18 = Ready, 19 = Installed, 20= Failure
4. WINDOWS TIME: Watch for the Windows Service synchronization. Make sure your sources are what they are supposed to be.
    a. 35 – Time Service sync status and source
5. APPLICATION ERROR: Watch for application crashes.
    a. 1000 – (Application Log) Application Fault
6. TASKSCHEDULER LOG: Enable this log and watch for Created Task and Deleted Task.
    a. 129 – Created, 141 – Deleted (New)

HARVEST:

1. SERVICES: Found in the SYSTEM log
    d. 7045 - Message=A service was installed in the system.
    e. 7040 - Message=The start type of the XYZ service was changed from auto start ***to disabled***.
    f. 7000 - Message=The XYX service ***failed to start*** due to the following error: The service did not respond to the start or control request in a timely fashion.
    g. 7022 - Message=The XYZ service hung on starting.
    h. 7024 - Message=The XYZ ***service terminated with service-specific error*** %%2414.
    i. 7031 - Message=The XYZ service ***terminated unexpectedly***. It has done this 1 time(s). The following corrective action will be taken in 60000 milliseconds: Restart the service.
    j. 7034 - Message=The XYZ service ***terminated unexpectedly***. It has done this 1 time(s).
    k. 7035 – Service sent a request to Stop or Start
    l. 7036 – Service was Started or Stopped

HARVEST:

1. AUDIT POLICY: Watch for changes to the Audit Policy that are NOT "SYSTEM"
    a. 4719 – System audit policy was changed

HARVEST:

1. APPLOCKER: Watch for triggers to AppLocker events (8000-8027)
    a. 8004 – Filename not allowed to run
2. SRP: Watch for triggers to Software Restriction Policies
    b. 866 – Access to <*filename*> has been restricted

WINDOWS LOGGING CHEAT SHEET - Win 7 thru Win 2012

HARVEST:

1. NEW FILE ADDED: Watch for the creation of new files. Requires File auditing of the directory(s) that you want to monitor
    b. 4663 – Accesses: WriteData (or AddFile)
    c. GREAT for CryptoWare & Malware drops

HARVEST:

1. REGISTRY: Monitor certain Keys for Add, Changes and Deletes. Setting auditing on the Specific keys is required.
    a. 4657 – A Registry value was modified

HARVEST:

1. LOGON TYPE: Monitor for what type of logons occur
    a. 4624 - Message=An account was ***successfully logged on***.
        i. Type 2 – Interactive – GUI
        ii. Type 3 – Network – Net Use
        iii. Type 4 – Batch
        iv. Type 5 – Service
        v. Type 7 – Unlock
        vi. Type 8 – Network Clear Text
        vii. Type 9 – New Credentials (RDP Tools)
        viii. Type 10 – Remote Interactive (RDP)
        ix. Type 11 – Cached Interactive (laptops)
    b. 4625 - Message = An account ***failed to log on***.

HARVEST:

2. FIREWALL: Windows Filtering Platform - Watch for Inbound and Outbound connections – ***Requires Windows Firewall to be enabled***
    a. This is the noisiest of all Events. Generating easily 9,000 - 10,000 events per hour per system
    b. Storage is required to utilize this event
    c. 5156 – Message=The Windows Filtering Platform has permitted a connection. Look for:
        i. Direction:, Source Address:, Source Port:, Destination Address: & Destination Port:

HARVEST:

1. SYSTEM INTEGRITY: Watch for files with page images with bad hashes
    a. 6281 – Failed – “page hashes of an image file are not valid”

HARVEST:

1. EMAIL / VPN: Monitor for failed and successful logins to your VPN and Webmail application. Consider emailing user if login is from a new IP not in your exclude list
    a. sc_status=401 – Failed OWA login
    b. "reason = Invalid password" – Failed VPN login - Cisco

HARVEST:

1. REGISTRY: Watch for the creation or modification of new registry keys and values
    a. 4657 – Accesses: WriteData (or AddFile)
        i. HKLM, HKCU & HKU – Software\Microsoft\Windows\CurrentVersion
            1. Run, RunOnce
        ii. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows
            1. Watch ***AppInit_Dlls***
        iii. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt
            1. Watch ***Connection time of USB Devices***
        iv. HKLM\System\CurrentControlSet\Services
            1. Watch for ***NEW Services***
        v. HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR
            1. Watch for ***NEW USB devices***