WINDOWS ADVANCED LOGGING CHEAT SHEET - Win 7 thru Win 2019

This "**Windows Advanced Logging Cheat Sheet**" is intended to help you expand the logging from the Windows Logging Cheat Sheet to capture more details, and thus noisier and higher impact to log management licensing. These are just a few additional items to help you find targeted items in the logs.

Authored by: David Longenecker, @dnlongen, SecurityForRealPeople.com with contributions and updates by Malware Archaeology

Covered Operating Systems:

Windows 7, Windows 8, Windows 10

Server 2008, Server 2012, Server, 2016, Server 2019

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.

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. Security Log – minimum of 1,024,000k on clients
        i. 2,048,000k on servers
2. GROUP POLICY: While most 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. Consider enabling noisy advanced settings on a small number of endpoints to serve as "canaries" while not overwhelming your log management/SIEM (or SIEM license).

WINDOWS ADVANCED LOGGING CHEAT SHEET - Win 7 thru Win 2019

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.

There are tradeoffs of advanced auditing in that they can generate significantly more events than the auditing recommended in the '***Windows Logging Cheat Sheet***'. The four noisiest noisy events will be:

4688 – Process Create, 4689, Process Terminate, 5156 Filtering Platform Connection (Windows Firewall), and 5158 Filtering Platform Connection (Windows Firewall). This will vary from workstations to servers.

If you enable the additional items mentioned in this cheat sheet, the amount of events that will be generated will rotate your logs faster, thus the logs will have less days of events. You can increase the log sizes so that you collect how long you want local logs to collect. The amount of events will also impact your log management licensing, so there is a tradeoff to collecting more log events, the sizes, and impact to log management licensing.

CONFIGURE:

1. SYSTEM AUDIT POLICIES:

Category/Subcategory	Setting
Object Access	
• Other Object Access Events	Success and Failure

USE CASES:

- Adds 4698 and 4702 events for new and updated scheduled tasks, containing the complete XML of the task (which identifies the user that created the task, complete command line, and schedule details).

CAVEATS: Anything for which a SACL exists, will generate 4662 events according to the SACL.

- More on SACLs: https://msdn.microsoft.com/en-us/library/windows/desktop/aa379321(v=vs.85).aspx

- If BitLocker is enabled, this generates a huge number of 4662 events for WMI Namespace MicrosoftVolumeEncryption. To suppress these events, use the WMI Control snap-in for MMC, right-click on properties, and browse to:

  Root → cimv2 → Security → MicrosoftVolumeEncryption. Click Security → Advanced → Auditing, select the "All / Everyone" entry, edit → Show advanced permissions, and uncheck ALL boxes.

CONFIGURE:

SYSTEM AUDIT POLICIES: Continued

Category/Subcategory	Setting
Detailed Tracking	
• Process Creation	Success and Failure
• Process Termination	Success

USE CASES:

- Triggers a 4688 event for every new process launch, including the process name and path, the parent process name and path are included with Win10 and Server 2016. Earlier versions include only the parent process PID and not the process name.
  - That Office DDE exploit from October 2017? "Creator Process Name: WINWORD.EXE" is big red flag for your investigators.
- 4689 will show when a process terminated. This can be used to track the parent process that launched the item or if the item is still running. This event will create as many events as a 4688, so noisy and

CAVEATS:

- With Process Creation tracking enabled, Chrome 63+ with site isolation (chrome://flags/#enable-site-per-process) is NOISY, generating a high volume of 4688 events for every resource load.

CONFIGURE:

2. SYSTEM AUDIT POLICIES: Continued

Category/Subcategory	Setting
Object Access	
• Filtering Platform Connection	Success and Failure
• Filtering Platform Packet Drop	Success

USE CASES: Find conflicting configurations.

- Windows by default enables Link-Local Multicast Name Resolution, an easily-abused DNS alternative talking on TCP/5355. Windows FW by default blocks the same LLMNR requests, consuming resources and filling the event log with 5152 and 5157 events. Solution: disable LLMNR: **Computer Configuration > Administrative Templates > Network > DNS Client > Turn Off Multicast Name Resolution ➔ Enable**
- Misconfigured domain trust relationships can result in, for instance, DMZ DCs trying to communicate to internal DCs. Look for 5152 and 5157 events between DCs.
- A client unexpectedly listening for new inbound connections (event ID 5154) could be a relay point for an intruder.

CAVEATS: Windows firewall is NOISY, even after tuning out misconfigurations. Easily 9,000 - 10,000 events per hour per system.

CONFIGURE:

SYSTEM AUDIT POLICIES: Continued

Category/Subcategory	Setting
DS Access	
• Directory Service Access	Success and Failure

USE CASES: Discover AD replication errors.

CAVEATS: If ***Failure*** auditing is enabled, errors in DS Replication will flood the logs with 4662 events, into the tens of millions. You can filter just these failed items out of your log collectors.

More on DS SACLs: https://technet.microsoft.com/en-us/library/dd277403.aspx

CONFIGURE:

SYSTEM AUDIT POLICIES: Continued

Category/Subcategory	Setting
Logon/Logoff	
• Account Lockout	Success and Failure

USE CASES: Pinpoint LDAP authentication failures.

Microsoft's recommendation is auditing for Success only. There is an edge case with third party services that leverage AD, such as LDAP: the 4740 Account Lockout event shows the DC as the source of the lockout, but by enabling Failure auditing for Account Lockout, there will *also* be a 4625 event with TaskCategory=Account Lockout, and with Network Information showing the IP of the application making the LDAP request.

Reference: https://blogs.technet.microsoft.com/pie/2016/10/02/the-source-of-my-account-lockouts-are-my-domain-controllers/

CONFIGURE:

- Enable DNS Client logging. DNS lookups are best processed from your DNS server logs, but Event ID 1001 in the Microsoft/Windows/DNS Client Events channel reports the name server the client is configured to use – useful for detecting malicious DNSChangers and attempts to bypass content controls.
    a. wevtutil sl Microsoft-Windows-DNS-Client/Operational /e:true

WINDOWS ADVANCED LOGGING CHEAT SHEET - Win 7 thru Win 2019

CONFIGURE:

1. Configure non Microsoft Services to log an event when they stop and start. Unfortunately Microsoft Windows does NOT log all services starting and stopping. Microsoft only logs the Windows default services, leaving third party services without any auditing of services stops and starts. The following are the steps needed to configure a service that you want to log starting and stopping. Follow the steps below to enable a service to log events.
    a. SC QUERY > Svcs.txt — Provides the name of each service (SERVICE_NAME)
    b. SC SDSHOW <the_service_name_you_want_to_monitor> > sd.txt — Provides the current DACL
    c. SC SDSET <the_service_name_you_want_to_monitor> <the_big_DACL_string>
        i. Add this to the end of the DACL
            1. (AU;SAFA;RPWPDT;;;WD)
    d. Modify these two Object Access subcategories to ENABLE, if not already set
        i. Auditpol /set /subcategory:"Handle Manipulation" /success:enable /failure:disable
        ii. Auditpol /set /subcategory:"Other Object Access Events" /success:enable /failure:disable
    e. Test by stopping and starting the service and then checking the Security log for a 4656 event and the service you adjusted the settings

Reference:

https://social.technet.microsoft.com/Forums/windows/en-US/7e6d6f95-74cc-48f2-9d17-fae367efd976/service-control-manager-auditing-startstop-events-event-id-7035-or-similar-missing?forum=winservergen

CONFIGURE:

SYSTEM AUDIT POLICIES:

Category/Subcategory	Setting
Privilege Use	
• Sensitive Privilege Use	Success and Failure

USE CASES: Mimikatz credential harvesting.

Watch for non-normal processes calling SeTcbPrivilege privilege

CONFIGURE:

SYSTEM AUDIT POLICIES:

Category/Subcategory	Setting
Detailed Tracking	
• Token Right Adjustment	Success and Failure

USE CASES: Mimikatz credential harvesting.

Watch for non-normal processes calling SeDebugPrivilege privilege

CONFIGURE:

SYSTEM AUDIT POLICIES: Win10 and Server 2016 & later

Category/Subcategory	Setting
Object Access	
• Removable Storage	Success and Failure

USE CASES: Monitor use of Removable media.

Watch for new USB devices being inserted.

CONFIGURE:

SYSTEM AUDIT POLICIES:

Category/Subcategory	Setting
Account Logon	
• Kerberos Authentication Service	Success and Failure
• Kerberos Service Ticket Ops	Success and Failure

USE CASES: Monitor use of Removable media.

Watch for Odd Kerberos failed and types

WINDOWS ADVANCED LOGGING CHEAT SHEET - Win 7 thru Win 2019

HARVEST:

1. WINDOWS FIREWALL:
    a. 5152 – Blocked a *packet*.
    b. 5154 - Permitted an application to *listen* for incoming connections.
    c. 5156 – Permitted a *connection*
        i. *Failed events can catch port scans between clients that do not cross a firewall*
    d. 5157 – Blocked a *connection*
    e. Look for: Direction:, Source Address:, Source Port:, Destination Address: & Destination Port:

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.
    b. For Windows 10 and Server 2016, look for Creator Process Name that ordinarily should not spawn processes (e.g. MS Office apps, Adobe)

HARVEST:

1. SERVICES:
    a. 7009 – SYSTEM log – A timeout was reached (%1 milliseconds) while waiting for the %2 service to connect. Possibly a faulty service, but possibly malicious code masquerading as a service (but not accepting a connection from the Service Control Manager)

HARVEST:

1. DIRECTORY SERVICES:
    a. 4662 – SECURITY Log – An operation was performed on an object.
    Only objects with SACLs cause audit events to be generated, and only when they are accessed in a manner that matches their SACL. More on DS SACLs:

https://technet.microsoft.com/en-us/library/dd277403.aspx

HARVEST:

1. SPECIAL PRIVILEGES: Watch for SeTcbPrivilege use indicating credential harvesting
    a. 4673 – SECURITY Log – Special privileges and the Process Name that calls

HARVEST:

1. Token Rights: Win 10/Server 2016 and later
    a. 4703 – SECURITY Log - Token Right Adjusted and the Process Name that called SeDebugPrivilege

HARVEST:

1. SPECIAL PRIVILEGES: Watch for a user to take on elevated privileges
    a. 4672 – SECURITY Log – Special privileges assigned to new logon.

HARVEST:

1. EXPLICIT CREDENTIALS:
    a. 4648 – SECUREITY Log - logon was attempted using explicit credentials. Watch Process Name and the user and domain they are using.

WINDOWS ADVANCED LOGGING CHEAT SHEET - Win 7 thru Win 2019

HARVEST:

1. DNS SETTINGS:
    a. 1001 – Microsoft-Windows-DNS-Client/Operational Log – Periodically reports the DNS servers configured for the active network interface.
    b. 3008 & 3010 – DNS requests, lots of events, filtering will be necessary

HARVEST:

1. OTHER OBJECT ACCESS EVENTS:
    a. 4656 – SECURITY Log – A handle to an object was accessed. For services that have had their DACLs adjusted, you will find when they are stopped and started with this Event ID

HARVEST: (Enable "Other Object Access Events")

1. SCHEDULED TASKS: Watch for a Process to create or modify scheduled tasks.
    a. 4698 – SECURITY Log – New Task Created
    b. 4702 – SECURITY Log – Task Modified
    c. Learn what is normal (certain AV and MS Office products regularly create new scheduled tasks), then watch for unexpected tasks.

HARVEST:

1. REMOVABLE MEDIA: Monitor for removable USB devices
    a. 6416 – SECURITY - Plug & Play events
    b. 400, 410 - Microsoft-Windows-Kernel-PnP/Configuration – Kernel-PnP events
    c. 10000 – SYSTEM - Microsoft-Windows-UserPnp events
    d. 20001 – SYSTEM - Microsoft-Windows-UserPnp events
    e. 4657 – SECURITY – Requires auditing to be set on specific registry keys. Watch for the following values:
    - Enum\USBSTOR\ - FriendlyName, Service, Class
    - Explorer\MountPoints2\ - MUIVerb
    - Enum\USB\ – New values

HARVEST: **Application Whitelisting**

1. APPLOCKER: Watch for triggers to AppLocker events (8000-8027)
    a. 8004 – Filename not allowed to run
2. Software Restriction Policies: Watch for triggers to denied execution or installation of files in folders you lock down, such as "***C:\Users***" where most droppers and malware initially execute
    b. 866 – Access to <*filename*> has been restricted
    c. 1007 – The installation of <*filename*> is not permitted by software restriction policy

HARVEST: **Kerberos (**Domain Controllers only)

1. Kerberoasting: Watch for certain values ()
    a. 4769 – SECURITY - For the combo of
    b. Ticket_Encryption_Type="0x17"
    c. Ticket_Options="0x40810000"
2. Spraying: Watch for failed attempts in mass that indicate Kerberos spraying
    a. 4771 – Failures

WINDOWS ADVANCED LOGGING CHEAT SHEET - Win 7 thru Win 2019

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; adjust to suit your needs
        iii. /rd:true = newest events first
        iv. /f:text = format text, also can do XML
    b. ***Process launches*** - WevtUtil qe Security /q:"*[System[(EventID=4688)]]" /c:5 /rd:true /f:text
    c. ***Modified Service Stopped*** - WevtUtil qe Security /q:"*[System[(EventID=4656)]]" /c:5 /rd:true /f:text
    d. ***Scheduled Task Installed or Modified*** – *WevtUtil qe Security* /q:"*[System[(EventID=4698 or EventID=4702)]]" /c:5 /rd:true /f:text
    e. ***Special Privileges assigned*** - *WevtUtil qe Security* /q:"*[System[(EventID=4672)]]" /c:5 /rd:true /f:text

GATHER:

2. AUDITPOL: Use this utility to view your current log settings

    g. List all Policies categories: ***AuditPol /List /Subcategory:****
    h. List what is SET: ***AuditPol /get /category:****
    i. List what is SET for a subcategory:
        - ***AuditPol /get /subcategory:"Object Access"***

GATHER:

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

MONITOR:

1. **Windows firewall blocked packets and connections – Security Log** - Following are some log management ideas to catch unusual or suspicious behavior.
    a. **(5152 & 5157) – Sort by Source IP on count of events.** Blocked packets and connections are noisy, but certain sources will show up in the event logs of many endpoints. If it's not a known vulnerability scanner, why are connections from it being blocked by every single endpoint?
    b. **(5156 Success) – Sort by Source IP on count of events.** Network sweeps to ports that are open result in allowed connection events on many targets from the same source. WannaCry for example scans IP ranges for port 445; infected systems will show up in a top-sources list.
    c. **(5156 Failed) –** Will show port scans failed connection to ports that are not open. Monitor using a count of failed port requests > 5 or what suits your environment
2. **Users accessing a large number of systems – Security Log**
    a. **(4624) – Sort on username by count of Workstation.** You already harvest this event ID if you have followed the "***Windows Logging Cheat Sheet***". Use it to discover lateral movement through your network. Filter out known sysadmin and service accounts. What normal users log on to an abnormal number of systems?
3. **Service stopped or started** – For services that have had their DACLs adjusted, this will show the stopping and starting of the modified service
    a. **(4656) –** A handle to an object was requested, Object Name (Service Name) and Accesses (Stopped or Started)
4. **Unexpected administrators and privileged users – Security Log**
    a. **(4672)** – This event indicates a privileged user, or one that is able to elevate privileges. Filter out SYSTEM (Local System) as Special Privileges are normal for it; look for Subject that is not or should not be a system administrator.
5. **Unusual parent processes – Security Log**
    a. **(4688)** – You already harvest this event ID if you have followed the Windows Logging Cheat Sheet. Windows 10 and Server 2016 record the Creator Process Name. A New Process Name of cmd.exe or powershell.exe, with a Creator Process Name of WinWord.exe or AcroRd32.exe could indicate a macro, or it could indicate an exploit.
6. **Unauthorized DNS settings – Microsoft-Windows-DNS-Client/Operational Log –**
    a. **(1001)** – DNSChanger and related malware changed the DNS settings on a system, using fake name lookup responses to facilitate MitM attacks. Clever users might replace a preferred DNS with their own to bypass content filters. In both cases, Event ID 1001 reports the DNS settings for the active interface. Keep in mind that mobile clients move and typically get their DNS settings from each network via DHCP. Unless you control DNS settings even when clients are off-network, correlate this against another source to only alert to changes while the client is on a controlled network.
    b. **(3008, 3010)** – General DNS query. Filter out known good items and only collect what is new and odd. If a web proxy is used, these events do not need to be collected unless there is an event.

MONITOR:

8. **Abuse of Service Control Manager to launch malicious code – SYSTEM Log**
    a. **(7045 followed by 7009)** This may be a faulty service, but can also indicate Service Control Manager was used to install and run malicious code that is not a valid service. The 7009 event indicates SCM cannot connect to the expected new service – but the code has already run. *Credit: @maridegrazia*

9. **Watch for signs Kerberoasting** – SECURITY Log – Domain Controllers only
    a. **(4769**) Kerberos tickets can show unusual behavior. Watch for the combination of:
        i. Ticket_Encryption_Type="0x17"
        ii. Ticket_Options="0x40810000"

10. **Watch for signs of Kerberos spraying** – SECURITY Log – Domain Controllers only
    a. **(4771)** Kerberos ticket failures. Watch for large volumes in short periods that indicate Kerberos spraying

11. **Watch for signs of credential harvesting – SECURITY Log**
    a. **(4673)** Watch for Processes that are not LSASS.exe or other known users of the SeTcbPrivilege privilege. Credential harvesters such as Mimikatz will make this call by any name. Normal items call this regularly, malicious processes will be new and few.

12. **Lateral movement on endpoints – SECURITY Log**
    a. **(5140 & 5145)** On endpoints watch for users connecting to more than one workstation or server. The credential used can also be telling. Watch for counts > 2 to 4 systems by the same account.

13. **Watch for new Scheduled Tasks being created – SECURITY & TaskScheduler Logs**
    a. (4698 – Security log) New tasks are rare and usually well-known such as Chrome or GoogleUpdate. A great way to persist a reboot is by a scheduled task. Watch for new tasks and filter out known good ones.
    b. (106 – TaskScheduler log) New tasks are rare and usually well-known such as Chrome or GoogleUpdate. A great way to persist a reboot is by a scheduled task. Watch for new tasks and filter out known good ones.

14. **USB Devices – Several logs – If monitoring Removable Storage USB devices is needed**
    a. Security Log – Monitor those events that indicate new USB devices are installed
    b. System Log - Monitor those events that indicate new USB devices are installed
    c. Use Registry Auditing to monitor specific keys that will register new USB devices being plugged in. Please read the "***Windows Registry Auditing Logging Cheat Sheet***" for more on auditing registry keys

MORE 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.
- 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

Event Log Analysis:

- https://sect.iij.ad.jp/d/2018/05/044132/training_material_sample_for_eventlog_analysis.pdf

Windows Command abused by attackers:

- https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html

Lateral Movement:

- https://www.jpcert.or.jp/english/pub/sr/Detecting%20Lateral%20Movement%20through%20Tracking%20Event%20Logs_version2.pdf

DFIR & Threat Hunting:

- http://findingbad.blogspot.com/2017/12/a-few-of-my-favorite-things-continued.html

Win Event Forwarding:

- https://blogs.technet.microsoft.com/jepayne/2017/12/08/weffles/

USB/Removable storage use:

- https://github.com/palantir/windows-event-forwarding/blob/master/wef-subscriptions/External-Devices.xml
- https://speakerdeck.com/ropnop/fun-with-ldap-kerberos-and-msrpc-in-ad-environments?slide=85

Kerberos:

- https://docs.microsoft.com/en-us/windows-hardware/drivers/usbcon/how-to-capture-a-usb-event-trace

Detect things like Mimikatz or requests for credentials:

- https://blogs.technet.microsoft.com/nathangau/2018/01/25/security-monitoring-a-possible-new-way-to-detect-privilege-escalation/