Windows Event Log Cheat Sheet – Extended

youtube.com/13cubed



Security Event IDs of Interest

Event ID	Description
4800	The workstation was locked.
4801	The workstation was unlocked.
4802	The screen saver was invoked. (Does not establish whether a user was physically present)
4803	The screen saver was dismissed. (Does not establish who was physically present)
4778	A session was reconnected to a Window Station. (Session Name, Client Name, and Client Address)
4779	A session was disconnected from a Window Station. (Includes RDP and other session activity)
***4662**	An operation was performed on an Active Directory object. (DC; replication rights may indicate DCSync)
6416	A new external device was recognized by the system. (Does not establish file access or copying)
4886	Certificate Services received a certificate request. (Request ID and Requester)
4887	Certificate Services issued a certificate. (Requester and Subject; SANs may not appear as a field)
4888	Certificate Services denied a certificate request.
4898	Certificate Services loaded a certificate template. (Not a complete inventory of templates in AD)
4899	A Certificate Services template was updated. (Does not establish exploitation)
4900	Certificate Services template security was updated. (Template permission changes)
4882	The security permissions for Certificate Services changed. (Administrative rights)

**Requires a matching SACL on the DC; replication GUID prefixes: 1131f6aa, 1131f6ad, and 89e95b76*
Control Access (0x100) and the caller provide context; legitimate replication also generates these events

Status and Sub Status Codes (Companion to Event ID 4625)

youtube.com/13cubed



Code	Description
0xC0000064	The account name does not exist. (Repetition may indicate account enumeration)
0xC000006A	The account name is valid but the password is incorrect.
***0xC000006D**	Generic logon failure. (Bad account name or bad authentication information)
0xC000006E	An account restriction prevented the logon. (Credentials were valid; a restriction applied)
0xC000006F	Logon outside the hours permitted for the account.
0xC0000070	Logon from an unauthorized workstation.
0xC0000071	The password has expired.
0xC0000072	The account is disabled.
0xC0000133	The clock difference between the systems is too large.
0xC000015B	The requested logon type has not been granted on the target system.
0xC0000193	The account has expired.
0xC0000224	The password must be changed at the next logon.
0xC0000234	The account is locked out.
0xC0000413	An authentication firewall denied the logon.

**Status identifies the failure; when Status is the generic 0xC000006D, Sub Status carries the specific reason*

Event ID 4776 reports NTSTATUS values from this same set in its Error Code field, where 0x0 indicates success

PreAuthType Codes (Companion to Event ID 4768)

youtube.com/13cubed



Type	Description
0	No Pre-authentication
2	PA-ENC-TIMESTAMP (Password-based Pre-authentication)
***15**	PA-PK-AS-REP_OLD (Legacy Smart Card/Certificate Authentication)
***16**	PA-PK-AS-REQ (Smart Card/Certificate Authentication)

**Certificate authentication alone does not establish abuse; use the result and certificate fields in Event ID 4768*

Microsoft-Windows-Windows Defender/Operational Event IDs of Interest

Event ID	Description
1118	The antimalware platform attempted to take action on a threat, but the action failed.
1119	The antimalware platform encountered a critical error while taking action on a threat.
1121	An attack surface reduction rule blocked an action. (Rule GUID and process details)
1122	An attack surface reduction rule triggered in audit mode. (The rule did not block the action)
5001	Real-time protection was disabled.
***5007**	The antimalware platform configuration changed. (Old/new values, including exclusion changes)
5010	Scanning for malware and other potentially unwanted software was disabled.
5012	Virus scanning was disabled.
5013	Tamper protection blocked a change to Microsoft Defender Antivirus settings.

**Configuration changes can also result from maintenance (Old/new values identify the change)*



Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
Event IDs of Interest

Event ID	Description
39	Session *x* has been disconnected by session *y*. (May reflect user or administrative activity)
***40**	Session *x* has been disconnected, reason code *y*.
41	Session arbitration started. (User and session details)
42	Session arbitration finished. (Does not establish that the desktop or shell was reached)

**Reason codes depend on context and Windows build; correlate the session ID with surrounding events*

Microsoft-Windows-TerminalServices-RemoteConnectionManager/Admin Event IDs of Interest

Event ID	Description
1158	Remote Desktop Services accepted a connection from a client IP address. (Does not establish a logon)

Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational Event IDs of Interest

Event ID	Description
131	The server accepted a new TCP connection. (Client IP address and port; may include failed attempts)

System (Service Control Manager Provider) Event IDs of Interest

Event ID	Description
7040	The start type of a service changed. (Old/new start modes; persistence or defense impairment)



Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
Event IDs of Interest

Event ID	Description
2004	A rule was added to the Windows Firewall exception list. (Rule, modifying application, and user)
2005	A rule was modified in the Windows Firewall exception list.
2006	A rule was deleted from the Windows Firewall exception list.
***2071**	A rule was added to the Windows Firewall exception list. (Variant on newer Windows builds)
***2073**	A rule was modified in the Windows Firewall exception list. (Variant on newer Windows builds)
***2052**	A rule was deleted from the Windows Firewall exception list. (Variant on newer Windows builds)

**Event IDs vary by Windows build; the event message and ErrorCode identify the action and result*

Microsoft-Windows-TaskScheduler/Operational Event IDs of Interest

Event ID	Description
140	The user *x* updated the Task Scheduler task *y*. (Existing Scheduled Task)
200	Task Scheduler launched an action. (ActionName and task instance ID)
201	Task Scheduler completed an action. (ResultCode; completion alone does not establish success)

Microsoft-Windows-PowerShell/Operational Event IDs of Interest

Event ID	Description
4103	A PowerShell command or pipeline was logged. (Module Logging; command and parameter details)

Security Event IDs of Interest



Event ID	Description
4724	An attempt was made to reset an account's password. (Actor, target, and audit success/failure)
4726	A user account was deleted. (Actor and target account)
4738	A user account was changed. (Changed attributes and actor)
4740	A user account was locked out. (Caller Computer Name, where populated)
4732	A member was added to a security-enabled local group. (Member SID and target group)
4733	A member was removed from a security-enabled local group.
4728	A member was added to a security-enabled global group. (DC; actor, member SID, and target group)
4729	A member was removed from a security-enabled global group. (DC)
4756	A member was added to a security-enabled universal group. (DC; actor, member SID, and target group)
4757	A member was removed from a security-enabled universal group. (DC)
4699	A scheduled task was deleted. (Security audit evidence and actor details)
4702	A scheduled task was updated. (TaskContentNew XML contains actions, triggers, and principal)
4719	The system audit policy was changed. (Affected subcategory and auditing changes)
***1101**	Audit events were dropped by the transport. (Potential gap in the record; does not establish tampering)
4657	A registry value was modified. (Old/new data)
4663	An attempt was made to access an object. (Records access rights used; object, process, and Accesses)
5136	A directory service object was modified. (DC; Active Directory attribute changes)

**1101 uses Microsoft-Windows-Eventlog; other entries use Microsoft-Windows-Security-Auditing*

Microsoft-Windows-Sysmon/Operational Event IDs of Interest

youtube.com/13cubed



Event ID	Description
1	A process was created. (Image, command line, parent, hashes, and ProcessGuid)
***3**	A network connection was detected. (Process, protocol, IP addresses, and ports)
***7**	An image was loaded into a process. (Image path, hashes, and signature)
8	A thread was created in another process. (Source/target process and start address; possible injection)
***10**	A process opened another process. (Target process and GrantedAccess; includes access to LSASS)
11	A file was created or overwritten. (Process and target path)
12-14	A registry object was created/deleted (12), a value was set (13), or a key/value was renamed (14).
16	The Sysmon configuration was changed.
19-21	A WMI filter (19), consumer (20), or consumer-to-filter binding (21) was registered.
22	A DNS query was performed. (Process, query name, status, and results; includes failed and cached queries)
23/26	A file was deleted. (23 also archives the file; 26 logs deletion without archiving)
25	Process image tampering was detected. (Includes techniques such as process hollowing)

**Events 3 and 7 are disabled by default; all event types depend on Sysmon version, configuration, and filters*
Process access alone does not establish credential dumping; ProcessGuid connects activity on the same host

Microsoft-Windows-WMI-Activity/Operational Event IDs of Interest

Event ID	Description
5861	A permanent WMI filter-to-consumer binding was recorded. (Does not establish payload execution)