ULTIMATE IT SECURITY .COM

SUPERCHARGER™ for Windows Event Collection

Windows Security Log Quick Reference

User Account Changes

4720	Created	4722	Enabled
4723	User changed own password		
4724	Privileged User changed this user's password		
4725	Disabled	4726	Deleted
4738	Changed	4740	Locked out
4767	Unlocked	4781	Name change

Logon Types

2	Interactive
3	Network (i.e. mapped drive)
4	Batch (i.e. schedule task)
5	Service (service startup)
7	Unlock (i.e. unnattended workstation with password protected screen saver)
8	Network Cleartext (Most often indicates a logon to IIS with "basic authentication")
10	Remote Desktop
11	Logon with cached credentials

Logon Failure Codes

0xC0000064	User name does not exist
0xC000006A	User name is correct but the password is wrong
0xC0000234	User is currently locked out
0xC0000072	Account is currently disabled
0xC000006F	User tried to logon outside his day of week or time of day restrictions
0xC0000070	Workstation restriction
0xC00000193	Account expiration
0xC0000071	Expired password
0xC0000133	Clocks between DC and other computer too far out of sync
0xC0000224	User is required to change password at next logon
0xC0000225	Evidently a bug in Windows and not a risk
0xC000015b	The user has not been granted the requested logon type (aka logon right) at this machine

Domain Controller Authentication Events

4768	A Kerberos authentication ticket (TGT) was requested	
4771	Kerberos pre-authentication failed	See Kerberos Failure Codes
4820	A Kerberos TGT was denied because the device does not meet the access control restrictions	

Logon Session Events

4624	Successful logon	Correlate by Logon ID
4647	User initiated logoff	
4625	Logon failure (See Logon Failure Codes)	
4778	Remote desktop session reconnected	
4779	Remote desktop session disconnected	
4800	Workstation locked	
4801	Workstation unlocked	
4802	Screen saver invoked	
4803	Screen saver dismissed	

Kerberos Failure Codes

0x6	Bad user name
0x7	New computer account?
0x9	Administrator should reset password
0xC	Workstation restriction
0x12	Account disabled, expired, locked out, logon hours restriction
0x17	The user's password has expired
0x18	Bad password
0x20	Frequently logged by computer accounts
0x25	Workstation's clock too far out of sync with the DC's

Group Changes		Created	Changed	Deleted	Member	
					Added	Removed
Security	Local	4731	4735	4734	4732	4733
	Global	4727	4737	4730	4728	4729
	Universal	4754	4755	4758	4756	4757
Distribution	Local	4744	4745	4748	4746	4747
	Global	4749	4750	4753	4751	4752
	Universal	4759	4760	4763	4761	4762