Event IDs for Hunting

Logon Events:
- 4624 - successful logon
- 4625 - failed logon
- 4634 - logoff
- 4647 - user initiated logoff
- 4688 - logon attempted using explicit credentials
- 4768 - Kerberos ticket requested
- 4769 - Kerberos service ticket requested
- 4703 - logon rights adjusted
- 4704 - user right assigned
- 4705 - user right removed
- 4717 - system security access granted
- 4718 - system security access removed
- 4770 - Kerberos service ticket renewed
- 4771 - Kerberos pre-auth failed
- 4772 - Kerberos auth ticket request failed
- 4773 - Kerberos service ticket requested failed
- 4776 - NTLM account auth
- 4777 - DC failed to validate credentials
- 4820 - Kerberos TGT device request denied
- 4821 - Kerberos TGT device / user request denied
- 4824 - Kerberos DES / RC4 pre-auth failed
- 4964 - special group assigned to new logon

Account management logs:
- 4720 - account created
- 4722 - account enabled
- 4725 - account disabled
- 4726 - account deleted
- 4738 - account changed
- 4740 - account locked out
- 4741 - computer account created
- 4742 - computer account changed
- 4743 - computer account deleted
- 4767 - account unlocked
- 6420 - device account disabled
- 6421 - request to enable a device account
- 6422 - device account enabled
- 6423 - device installation forbidden by policy
- 6424 - device installation allowed after having been forbidden

Directory Service Object logs:
- 4739 - domain policy changed
- 5136 - object value added / deleted
  - Action = %%14674 - object added
  - Action = %%14675 - object deleted
- 5137 - object created
- 5138 - object restored
- 5139 - object moved

Sysmon logs:
- 1 - process creation
- 2 - file creation time changed
- 3 - network connection
- 4 - sysmon service state change
- 5 - process terminated
- 6 - driver loaded
- 7 - image loaded
- 8 - remote thread created
- 9 - raw access read, memory / file; e.g. “\\.\”
- 10 - process accessing other process
- 11 - file created
- 12 - registry object create / delete
- 13 - registry value set
- 14 - registry key or value renamed
- 15 - file alternate data stream created
- 17 - named pipe created
- 18 - Named pipe connected
- 19 - WMI filter event registered
- 20 - WMI consumer event registered
- 21 - WMI consumer to filter binding registered
- 22 - DNS query
- 23 - file deleted
- 255 - sysmon error

ScheduledTask logs:
- 4698 - created
- 4699 - deleted
- 4700 - enabled
- 4701 - disabled
- 4702 - updated

Group management logs:
- **Account added**
  - 4728 - security enabled global group
  - 4732 - security enabled local group
  - 4746 - security disabled local group
  - 4751 - security disabled global group
  - 4756 - security enabled universal group
  - 4761 - security disabled universal group
- **Account removed**
  - 4729 - security enabled global group
  - 4733 - security enabled local group
  - 4747 - security disabled local group
  - 4752 - security disabled global group
  - 4757 - security enabled universal group
  - 4762 - security disabled universal group
- **Group created**
  - 4727 - security enabled global group
  - 4731 - security enabled local group
  - 4754 - security disabled local group
  - 4749 - security disabled global group
  - 4744 - security enabled universal group
  - 4759 - security disabled universal group
- **Group deleted**
  - 4730 - security enabled global group
  - 4734 - security enabled local group
  - 4758 - security disabled local group
  - 4753 - security disabled global group
  - 4748 - security enabled universal group
  - 4763 - security disabled universal group
- **Group changed**
  - 4735 - security enabled global group
  - 4737 - security enabled local group
  - 4755 - security disabled local group
  - 4750 - security disabled global group
  - 4745 - security enabled universal group
  - 4760 - security disabled universal group

WMI logs:
- 5857 - provider loaded
- 5858 - query error
- 5860 - temporary consumer
- 5861 - permanent consumer

Network Share Access logs:
- 5140 - share accessed
- 5145 - share checked for desired access

Windows firewall logs:
- 4946 - rule added
- 4947 - rule modified
- 4950 - FW setting changed
- 4954 - FW group policy changed
- 5025 - FW service stopped
- 5031 - app blocked from accepting connection
- 5152 - packet blocked
- 5153 - packet blocked by more restrictive filter
- 5155 - app blocked from creating listening port
- 5157 - network connection blocked
- 5447 - FW filter was changed

NPS / Radius logs:
- 6272 - access granted
- 6273 - access denied
- 6274 - discarded user request
- 6276 - quarantined user
- 6277 - access granted but host did not meet defined health policy
- 6278 - access granted and host passed health policy check

Object event logs:
- 4656 - handle to object requested
- 4657 - registry value modified
- 4658 - handle to object closed
- 4659 - handle to object requested to delete it
- 4660 - object deleted
- 4661 - handle to object requested
- 4662 - operation performed on object
- 4663 - attempt made to access object
- 4664 - attempt to create hard link
- 4670 - object permissions changed
- 4674 - operation attempted on privileged object
- 4715 - audit policy of object changed
- 4817 - auditing settings on object changed
- 4907 - audit settings on object changed

Workstation logs:
- 4800 - locked
- 4801 - unlocked
- 4802 - screen saver started
- 4803 - screen saver dismissed
- 4778 - remote session reconnected
- 4779 - remote session disconnected
- 4825 - remote session access denied

Certificate service logs:
- 4876 - backup started
- 4877 - backup completed
- 4878 - restore started
- 4879 - restore completed
- 4880 - service started
- 4881 - service stopped
- 4882 - security permissions changed
- 4883 - archived key retrieved
- 4884 - cert imported
- 4885 - audit filter changed
- 4886 - cert request
- 4887 - cert approved and issued
- 4888 - cert request denied
- 4889 - cert request state set to pending
- 4890 - settings for cert services changed
- 4891 - a setting changed
- 4892 - property changed
- 4893 - key archived
- 4894 - imported archived key
- 4895 - CA cert published to AD
- 4896 - rows deleted from cert DB
- 4897 - role seperation enabled
- 4898 - template loaded
- 4899 - template updated
- 4900 - template security updated

COM logs:
- 5888 - object modified
- 5889 - object deleted
- 5890 - object added

SID history logs:
- 4765 - SID history added to account
- 4766 - SID history add to account failed
- 4830 - SID history removed from an account

TPM / TBS logs:
- 4671 - TBS attempted access blocked
- 4909 - TBS local policy changed
- 4910 - TBS group policy change

Misc. Event logs:
- 1102 - event Log cleared
- 4616 - system time changed
- 4622 - LSA loaded security package
- 4649 - replay attack detected
- 4664 - file hard link created
- 4697 - service installation
- 4673 - privileged service called
- 4719 - system audit policy changed
- 4782 - account password hash was accessed
- 4906 - crash on audit fail value changed
- 6281 - Invalid page hashes of image file

Misc. Fields and Values of Interest

Account performing action:
- Subject

Account on which action was performed:
- Member
- Target

Logon Type:
- 2 - Interactive
- 3 - Network
- 4 - Batch
- 5 - Service
- 7 - Unlock
- 8 - Network Cleartext
- 9 - New Credentials
- 10 - Remote Interactive
- 11 - Cached Interactive

Failed Logon Status:
- 0xC0000064 - Account Name Does Not Exist
- 0xC000006A - Incorrect Password
- 0xC0000072 - Account Disabled
- 0xC000006F - Outside of Time Restrictions
- 0xC0000070 - Workstation Restriction
- 0xC0000193 - Account Expired
- 0xC0000071 - Expired Password
- 0xC0000133 - Clocks Out of Sync
- 0xC000005E - No Logon Servers Available
- 0xC000006D - Bad Username or Auth Info
- 0xC000006E - Bad user name or bad password
- 0xC00000DC - Sam Server in Wrong State to Perform Desired Operation
- 0xC000018C - Trust Relationship Between the Primary Domain and Trusted Domain Failed
- 0xC0000192 - Netlogon Service Not Started
- 0xC00002EE - Error Occurred During Logon
- 0xC0000413 - Specified Account Not Allowed by Auth Firewall
- 0xC0000224 - Change Password Next Logon
- 0xC0000225 - Windows Bug - Not a Risk
- 0xc000015B - Not Granted Logon Right
- 0xC0000234 - Account is currently locked out

4703 Interesting privileges:
- **Elevated privileges**
  - SeBackupPrivilege
  - SeDebugPrivilege
  - SeLoadDriverPrivilege
  - SeChangeNotifyPrivilege
  - SeShutdownPrivilege
  - SeTcbPrivilege
  - SeAssignPrimaryPrivilege
  - SeTakeOwnershipPrivilege
  - SeRestorePrivilege
  - SeCreateTokenPrivilege
  - SeEnableDelegationPrivilege
- **System elevated privileges**
  - SeImpersonatePrivilege
  - SeAssignPrimaryTokenPrivilege

4697 Service installed:
- **Driver type**
  - 0x1 - kernel driver
  - 0x2 - file system driver
  - 0x4 - service adapter
  - 0x8 - recognizer driver
  - 0x10 - service that runs its own process
  - 0x20 - service that shares process with other service(s)
  - 0x110 - same as 10 but allows desktop interaction
  - 0x220 - same as 20 but allows desktop interaction
- **Startup type**
  - 0 - driver started by system loader
  - 1 - driver started by IoInitSystem
  - 2 - automatic
  - 3 - manual
  - 4 - disabled

Kerberos weak encryption:
- Ticket encryption
  - 0x1 - des-cbc-crc
  - 0x2 - des-cbc-md4
  - 0x3 - des-cbc-md5
  - 0x4 - des-cbc-raw
  - 0x5 - des3-cbc-md5
  - 0x6 - des3-cbc-raw
  - 0x17 - rc4-hmac
  - 0x18 - rc4-hmac-exp