|  |  |  |
| --- | --- | --- |
|  | 1100 | The event logging service has shut down. |
|  | 1102 | Audit log was cleared. This can relate to a potential attack |
|  | 1108 | The event logging service encountered an error while processing an incoming event |
|  | 4616 | System time was changed |
|  | 4618 | A monitored security event pattern has occurred. |
|  | 4621 | Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded. |
|  | 4624 | Successful account log on |
|  | 4625 | Failed account log on |
|  | 4634 | An account logged off |
|  | 4648 | A logon attempt was made with explicit credentials |
|  | 4649 | A replay attack was detected. May be a harmless false positive due to a misconfiguration error. |
|  | 4657 | A registry value was changed |
|  | 4697 | An attempt was made to install a service |
|  | 4698 | A scheduled task was created |
|  | 4699 | A scheduled task was deleted |
|  | 4700 | A scheduled task was enabled |
|  | 4701 | A scheduled task was disabled |
|  | 4719 | System audit policy was changed. |
|  | 4720 | A user account was created |
|  | 4722 | A user account was enabled |
|  | 4723 | An attempt was made to change the password of an account |
|  | 4724 | An attempt was made to reset an account's password. |
|  | 4725 | A user account was disabled |
|  | 4726 | A user account was deleted |
|  | 4728 | A user was added to a privileged global group |
|  | 4732 | A user was added to a privileged local group |
|  | 4735 | A privileged local group was modified |
|  | 4737 | A privileged global group was modified |
|  | 4738 | A user account was changed |
|  | 4740 | A user account was locked out |
|  | 4755 | A privileged universal group was modified |
|  | 4756 | A user was added to a privileged universal group |
|  | 4765 | SID History was added to an account. |
|  | 4766 | An attempt to add SID History to an account failed. |
|  | 4767 | A user account was unlocked |
|  | 4772 | A Kerberos authentication ticket request failed |
|  | 4777 | The domain controller failed to validate the credentials of an account. |
|  | 4782 | The password hash of an account was accessed |
|  | 4794 | An attempt was made to set the Directory Services Restore Mode. |
|  | 4896 | One or more rows have been deleted from the certificate database. |
|  | 4946 | A rule was added to the Windows Firewall exception list |
|  | 4947 | A rule was modified in the Windows Firewall exception list |
|  | 4950 | A setting was changed in Windows Firewall |
|  | 4954 | Group Policy settings for Windows Firewall has changed |
|  | 4964 | A special group has been assigned to a new log on |
|  | 5025 | The Windows Firewall service has been stopped |
|  | 5030 | The Windows Firewall Service failed to start. |
|  | 5031 | Windows Firewall blocked an application from accepting incoming traffic |
|  | 5035 | The Windows Firewall Driver failed to start. |
|  | 5037 | The Windows Firewall Driver detected critical runtime error. Terminating. |
|  | 5124 | A security setting was updated on OCSP Responder Service. |
|  | 5152 | The Windows Filtering Platform blocked a packet |
|  | 5153 | A more restrictive Windows Filtering Platform filter has blocked a packet |
|  | 5155 | Windows Filtering Platform blocked an application or service from listening on a port |
|  | 5157 | Windows Filtering Platform blocked a connection |
|  | 5447 | A Windows Filtering Platform filter was changed |
|  | 6273 | Network Policy Server denied access to a user. |
|  | 6276 | Network Policy Server quarantined a user. |
|  | 6277 | Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy. |
|  | 6279 | Network Policy Server locked the user account due to repeated failed authentication attempts. |