



Cyber Security Windows Security Event Log

By : Ammar Hakim Haris

Account Logon



[LinkedIn : Ammar Hakim Haris](#)

Subcategory	PID	Notes
1.1 Windows Credential Validation	4774	A Kerberos authentication ticket (TGT) was requested
	4775	An account could not be mapped for logon
	4776	The domain controller attempted to validate the credentials for an account
	4777	The domain controller failed to validate the credentials for an account
1.2 Kerberos Authentication Services	4768	A Kerberos authentication ticket (TGT) was requested
	4771	Kerberos pre-authentication failed
	4772	A Kerberos authentication ticket request failed
	4820	Kerberos Ticket-granting-ticket (TGT) was denied because the device does not meet the access control restrictions
1.3 Kerberos Services Ticket Operations	4769	A Kerberos service ticket was requested
	4770	A Kerberos service ticket was renewed
	4773	A Kerberos service ticket request failed

Account Management



Subcategory	PID	Notes
2.1 Application Group Management	4783	A basic application group was created
	4784	A basic application group was changed
	4785	A member was added to a basic application group
	4786	A member was removed from a basic application group
	4787	A non-member was added to a basic application group
	4788	non-member was removed from a basic application group
	4789	A basic application group was deleted
	4790	An LDAP query group was created
	4791	A basic application group was changed
	4792	An LDAP query group was deleted
2.2 Computer Account Management	4741	A computer account was created
	4742	A computer account was changed
	4743	A computer account was deleted
2.3 Distribution Group Management	4744	A security-disabled local group was created
	4745	A security-disabled local group was changed
	4746	A member was added to a security-disabled local group
	4747	A member was removed from a security-disabled local group
	4748	A security-disabled local group was deleted
	4749	A security-disabled global group was created
	4750	A security-disabled global group was changed
	4751	A member was added to a security-disabled global group
	4752	A member was removed from a security-disabled global group
	4753	A security-disabled global group was deleted
	4759	A security-disabled universal group was created
	4760	A security-disabled universal group was changed
	4761	A member was added to a security-disabled universal group
	4762	A member was removed from a security-disabled universal group
	4763	A security-disabled universal group was deleted
2.4 Other Account Management Events	4739	Domain Policy was changed
	4782	The password hash an account was accessed
	4793	The Password Policy Checking API was called



[LinkedIn : Ammar Hakim Haris](#)

Logon/Logoff



Subcategory	PID	Notes
4.1 Group Membership	4627	Group membership information.
4.2 IPsec Extended Mode	4978	During Extended Mode negotiation, IPsec received an invalid negotiation packet.
4.3 IPsec Main Mode	4646	IKE DoS-prevention mode started
	4650	An IPsec Main Mode security association was established
	4651	An IPsec Main Mode security association was established
	4652	An IPsec Main Mode negotiation failed
	4653	An IPsec Main Mode negotiation failed
	4655	An IPsec Main Mode security association ended
	4976	During Main Mode negotiation, IPsec received an invalid negotiation packet.
	4979	IPsec Main Mode and Extended Mode security associations were established.
	4980	IPsec Main Mode and Extended Mode security associations were established
	4981	IPsec Main Mode and Extended Mode security associations were established
	4982	IPsec Main Mode and Extended Mode security associations were established
	4983	An IPsec Extended Mode negotiation failed
4.4 IPsec Quick Mode	4984	An IPsec Extended Mode negotiation failed
	5453	An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service is not started
	4654	An IPsec Quick Mode negotiation failed
	4977	During Quick Mode negotiation, IPsec received an invalid negotiation packet.
4.5 LogOff	5451	An IPsec Quick Mode security association was established
	5452	An IPsec Quick Mode security association ended
	4634	An account was logged off
	4647	User initiated logoff



LinkedIn : Ammar Hakim Haris

Logon/Logoff



Subcategory	PID	Notes
4.6 Logon	4624	An account was successfully logged on
	4625	An account failed to log on
	4626	User/Device claims information
	4648	A logon was attempted using explicit credentials
	4675	SIDs were filtered
4.7 Network Policy Server	6272	Network Policy Server granted access to a user
	6273	Network Policy Server denied access to a user
	6274	Network Policy Server discarded the request for a user
	6275	Network Policy Server discarded the accounting request for 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
	6278	Network Policy Server granted full access to a user because the host met the defined health policy
	6279	Network Policy Server locked the user account due to repeated failed authentication
4.9 Other Logon/Logoff Events	6280	Network Policy Server unlocked the user account
	4649	A replay attack was detected
	4778	A session was reconnected to a Window Station
	4779	A session was disconnected from a Window Station
	4800	The workstation was locked
	4801	The workstation was unlocked
	4802	The screen saver was invoked
	4803	The screen saver was dismissed
	5378	The requested credentials delegation was disallowed by policy
	5632	A request was made to authenticate to a wireless network
	5633	A request was made to authenticate to a wired network



LinkedIn : Ammar Hakim Haris

Logon/Logoff



Subcategory	PID	Notes
4.10 Special Logon	4672	Special privileges assigned to new logon
	4964	Special groups have been assigned to a new logon



LinkedIn : Ammar Hakim Haris

Non Audit (Event Log)



Subcategory	PID	Notes
5.1 Event processing	1101	Audit events have been dropped by the transport.
	1104	The security Log is now full
	1108	The event logging service encountered an error
5.2 Log automatic backup	1105	Event log automatic backup
5.3 Log clear	1102	The audit log was cleared
5.4 Service shutdown	1100	The event logging service has shut down



[LinkedIn : Ammar Hakim Haris](#)

Object Access



Subcategory	PID	Notes
6.1 Application Generated	4665	An attempt was made to create an application client context.
	4666	An application attempted an operation
	4667	An application client context was deleted
	4668	An application was initialized
6.2 Central Policy Staging	4818	Proposed Central Access Policy does not grant the same access permissions as the current Central Access Policy



[LinkedIn : Ammar Hakim Haris](#)

Subcategory	PID	Notes
6.3 Certification Services	4868	The certificate manager denied a pending certificate request
	4869	Certificate Services received a resubmitted certificate request
	4870	Certificate Services revoked a certificate
	4871	Certificate Services received a request to publish the certificate revocation list (CRL)
	4872	Certificate Services published the certificate revocation list (CRL)
	4873	A certificate request extension changed
	4874	One or more certificate request attributes changed.
	4875	Certificate Services received a request to shut down
	4876	Certificate Services backup started
	4877	Certificate Services backup completed
	4878	Certificate Services restore started
	4879	Certificate Services restore completed
	4880	Certificate Services started
	4881	Certificate Services stopped
	4882	The security permissions for Certificate Services changed
	4883	Certificate Services retrieved an archived key
	4884	Certificate Services imported a certificate into its database
	4885	The audit filter for Certificate Services changed
	4886	Certificate Services received a certificate request
	4887	Certificate Services approved a certificate request and issued a
	4888	Certificate Services denied a certificate request
	4889	Certificate Services set the status of a certificate request to pending
	4890	The certificate manager settings for Certificate Services changed.
	4891	A configuration entry changed in Certificate Services
	4892	A property of Certificate Services changed
	4893	Certificate Services archived a key
	4894	Certificate Services imported and archived a key
	4895	Certificate Services published the CA certificate to Active Directory Domain Services
	4896	One or more rows have been deleted from the certificate database
	4897	Role separation enabled
	4898	Certificate Services loaded a template
	4899	A Certificate Services template was updated
	4900	Certificate Services template security was updated
	5120	OCSP Responder Service Started

Object Access



Subcategory	PID	Notes
6.4 Detailed File Share	5145	A network share object was checked to see whether client can be granted desired access
6.5 File Share	5140	A network share object was accessed
	5142	A network share object was added.
	5143	A network share object was modified
	5144	A network share object was deleted.
	5168	Spn check for SMB/SMB2 fails.
6.6 File System	4656	A handle to an object was requested
	4658	The handle to an object was closed
	4659	A handle to an object was requested with intent to delete
	4660	An object was deleted
	4663	An attempt was made to access an object
	4664	An attempt was made to create a hard link
	4670	Permissions on an object were changed
	4985	The state of a transaction has changed
6.7 Filtering Platform Connection	5150	The Windows Filtering Platform has blocked a packet.
	5151	A more restrictive Windows Filtering Platform filter has blocked a packet.
	5154	The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections
	5155	The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections
	5156	The Windows Filtering Platform has allowed a connection
	5157	The Windows Filtering Platform has blocked a connection
	5158	The Windows Filtering Platform has permitted a bind to a local port
	5159	The Windows Filtering Platform has blocked a bind to a local port



[LinkedIn : Ammar Hakim Haris](#)

Object Access



Subcategory	PID	Notes
6.8 Filtering Platform Connection	5150	The Windows Filtering Platform has blocked a packet.
	5151	A more restrictive Windows Filtering Platform filter has blocked a packet.
	5154	listen on a port for incoming connections
	5155	listening on a port for incoming connections
	5156	The Windows Filtering Platform has allowed a connection
	5157	The Windows Filtering Platform has blocked a connection
	5158	The Windows Filtering Platform has permitted a bind to a local port
	5159	The Windows Filtering Platform has blocked a bind to a local port
6.9 Filtering Platform Packet Drop	5031	The Windows Firewall Service blocked an application from accepting incoming connections on the network.
	5152	The Windows Filtering Platform blocked a packet
	5153	A more restrictive Windows Filtering Platform filter has blocked a packet
6.10 Handle Manipulation	4656	A handle to an object was requested
	4658	The handle to an object was closed
	4690	An attempt was made to duplicate a handle to an object
6.11 Kernel Object	4658	The handle to an object was closed
	4660	An object was deleted
	4661	A handle to an object was requested
	4663	An attempt was made to access an object



[LinkedIn : Ammar Hakim Haris](#)

Object Access



Subcategory	PID	Notes
6.8 Filtering Platform Connection	5150	The Windows Filtering Platform has blocked a packet.
	5151	A more restrictive Windows Filtering Platform filter has blocked a packet.
	5154	listen on a port for incoming connections
	5155	listening on a port for incoming connections
	5156	The Windows Filtering Platform has allowed a connection
	5157	The Windows Filtering Platform has blocked a connection
	5158	The Windows Filtering Platform has permitted a bind to a local port
	5159	The Windows Filtering Platform has blocked a bind to a local port
6.9 Filtering Platform Packet Drop	5031	The Windows Firewall Service blocked an application from accepting incoming connections on the network.
	5152	The Windows Filtering Platform blocked a packet
	5153	A more restrictive Windows Filtering Platform filter has blocked a packet
6.10 Handle Manipulation	4656	A handle to an object was requested
	4658	The handle to an object was closed
	4690	An attempt was made to duplicate a handle to an object
6.11 Kernel Object	4658	The handle to an object was closed
	4660	An object was deleted
	4661	A handle to an object was requested
	4663	An attempt was made to access an object



[LinkedIn : Ammar Hakim Haris](#)

Policy Change



LinkedIn : Ammar Hakim Haris

Subcategory	PID	Notes
7.1 Audit Policy Change	4715	The audit policy (SACL) on an object was changed
	4719	System audit policy was changed
	4817	Auditing settings on object were changed.
	4902	The Per-user audit policy table was created
	4904	An attempt was made to register a security event source
	4905	An attempt was made to unregister a security event source
	4906	The CrashOnAuditFail value has changed
	4907	Auditing settings on object were changed
	4908	Special Groups Logon table modified
	4912	Per User Audit Policy was changed
7.2 Authentication Policy Change	4706	A new trust was created to a domain
	4707	A trust to a domain was removed
	4713	Kerberos policy was changed
	4716	Trusted domain information was modified
	4717	System security access was granted to an account
	4718	System security access was removed from an account
	4865	A trusted forest information entry was added
	4866	A trusted forest information entry was removed
7.3 Authorization Policy Change	4867	A trusted forest information entry was modified
	4670	Permissions on an object were changed
	4703	A token right was adjusted
	4704	A user right was assigned
	4705	A user right was removed
	4714	Encrypted data recovery policy was changed
	4911	Resource attributes of the object were changed
	4913	Central Access Policy on the object was changed



LinkedIn : Ammar Hakim Haris

Subcategory	PID	Notes
7.4 Filtering Platform Policy Change	4709	IPsec Services was started
	4710	IPsec Services was disabled
	4711	PAStore Engine (1%)
	4712	IPsec Services encountered a potentially serious failure
	5440	The following callout was present when the Windows Filtering Platform Base Filtering Engine started
	5441	The following filter was present when the Windows Filtering Platform Base Filtering Engine started
	5442	The following provider was present when the Windows Filtering Platform Base Filtering Engine started
	5443	The following provider context was present when the Windows Filtering Platform Base Filtering Engine started
	5444	The following sub-layer was present when the Windows Filtering Platform Base Filtering Engine started
	5446	A Windows Filtering Platform callout has been changed
	5448	A Windows Filtering Platform provider has been changed
	5449	A Windows Filtering Platform provider context has been changed
	5450	A Windows Filtering Platform sub-layer has been changed
	5456	PAStore Engine applied Active Directory storage IPsec policy on the computer
	5457	PAStore Engine failed to apply Active Directory storage IPsec policy on the computer
	5458	PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer
	5459	PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer
	5460	PAStore Engine applied local registry storage IPsec policy on the computer
	5461	PAStore Engine failed to apply local registry storage IPsec policy on the computer
	5462	PAStore Engine failed to apply some rules of the active IPsec policy on the computer
	5463	PAStore Engine polled for changes to the active IPsec policy and detected no changes
	5464	PAStore Engine polled for changes to the active IPsec policy, detected changes, and applied them to IPsec Services
	5465	PAStore Engine received a control for forced reloading of IPsec policy and processed the control successfully
	5466	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory cannot be reached, and will use the cached copy of the Active Directory IPsec policy instead
	5467	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, and found no changes to the policy
	5468	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, found changes to the policy, and applied those changes
	5471	PAStore Engine loaded local storage IPsec policy on the computer
	5472	PAStore Engine failed to load local storage IPsec policy on the computer
	5473	PAStore Engine loaded directory storage IPsec policy on the computer
	5474	PAStore Engine failed to load directory storage IPsec policy on the computer
	5477	PAStore Engine failed to add quick mode filter



LinkedIn : Ammar Hakim Haris

Policy Change



Subcategory	PID	Notes
7.5 MPSSVC Rule-Level Policy Change	4944	The following policy was active when the Windows Firewall started
	4945	A rule was listed when the Windows Firewall started
	4946	A change has been made to Windows Firewall exception list. A rule was added
	4947	A change has been made to Windows Firewall exception list. A rule was modified
	4948	A change has been made to Windows Firewall exception list. A rule was deleted
	4949	Windows Firewall settings were restored to the default values
	4950	A Windows Firewall setting has changed
	4951	Windows Firewall
	4952	Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall
	4954	Windows Firewall Group Policy settings has changed. The new settings have been
	4956	Windows Firewall has changed the active profile
	4957	Windows Firewall did not apply the following rule
	4958	Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer
7.6 Other Policy Change Events	4819	Central Access Policies on the machine have been changed
	4826	Boot Configuration Data loaded
	5063	A cryptographic provider operation was attempted
	5064	A cryptographic context operation was attempted
	5065	A cryptographic context modification was attempted
	5066	A cryptographic function operation was attempted
	5067	A cryptographic function modification was attempted
	5068	A cryptographic function provider operation was attempted
	5069	A cryptographic function property operation was attempted
	5070	A cryptographic function property operation was attempted
	5447	A Windows Filtering Platform filter has been changed
	6144	Security policy in the group policy objects has been applied successfully
	6145	One or more errors occurred while processing security policy in the group policy objects

Privilege Use



Subcategory	PID	Notes
9.1 Sensitive Privilege Use	4673	A privileged service was called
	4674	An operation was attempted on a privileged object



[LinkedIn : Ammar Hakim Haris](#)



System



Subcategory	PID	Notes
10.1 IPsec Driver	5478	IPsec Services has started successfully
	5479	IPsec Services has been shut down successfully
	5480	IPsec Services failed to get the complete list of network interfaces on the computer
	5483	IPsec Services failed to initialize RPC server. IPsec Services could not be started
	5484	IPsec Services has experienced a critical failure and has been shut down
	5485	IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces



[LinkedIn : Ammar Hakim Haris](#)



LinkedIn : Ammar Hakim Haris

Subcategory	PID	Notes
10.2 Other System Events	4821	A Kerberos service ticket was denied because the user, device, or both does not meet the access control restrictions
	4822	NTLM authentication failed because the account was a member of the Protected User group
	4823	NTLM authentication failed because access control restrictions are required
	4824	Kerberos preauthentication by using DES or RC4 failed because the account was a member of the Protected User group
	4825	A user was denied the access to Remote Desktop. By default, users are allowed to connect only if they are members of the Remote Desktop Users group or Administrators group
	4830	SID History was removed from an account
	5024	The Windows Firewall Service has started successfully
	5025	The Windows Firewall Service has been stopped
	5027	The Windows Firewall Service was unable to retrieve the security policy from the local storage
	5028	The Windows Firewall Service was unable to parse the new security policy.
	5029	The Windows Firewall Service failed to initialize the driver
	5030	The Windows Firewall Service failed to start
	5032	Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network
	5033	The Windows Firewall Driver has started successfully
	5034	The Windows Firewall Driver has been stopped
	5035	The Windows Firewall Driver failed to start
	5037	The Windows Firewall Driver detected critical runtime error. Terminating
	5058	Key file operation
	5059	Key migration operation
	5071	Key access denied by Microsoft key distribution service



LinkedIn : Ammar Hakim Haris

Subcategory	PID	Notes
10.3 Security State Change	4608	Windows is starting up
	4609	Windows is shutting down
	4616	The system time was changed.
	4621	Administrator recovered system from CrashOnAuditFail
10.4 Security System Extension	4610	An authentication package has been loaded by the Local Security Authority
	4611	A trusted logon process has been registered with the Local Security Authority
	4614	A notification package has been loaded by the Security Account Manager.
	4622	A security package has been loaded by the Local Security Authority.
	4697	A service was installed in the system
10.5 System Integrity	4612	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
	4615	Invalid use of LPC port
	4618	A monitored security event pattern has occurred
	5038	Code integrity determined that the image hash of a file is not valid
	5056	A cryptographic self test was performed
	5061	Cryptographic operation
	5890	An object was added to the COM+ Catalog
	6281	Code Integrity determined that the page hashes of an image file are not valid...
	6410	load into a process. This could be due to the use of shared sections or other

Uncategorized



Subcategory	PID	Notes
11.1 Subcategory could not be determined	4864	A namespace collision was detected
	4909	The local policy settings for the TBS were changed
	4910	The group policy settings for the TBS were changed
	4953	A rule has been ignored by Windows Firewall because it could not parse the rule
	4960	IPsec dropped an inbound packet that failed an integrity check
	4961	IPsec dropped an inbound packet that failed a replay check
	4962	IPsec dropped an inbound packet that failed a replay check
	4963	IPsec dropped an inbound clear text packet that should have been secured
	4965	IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI).
	5039	A registry key was virtualized.
	5040	A change has been made to IPsec settings. An Authentication Set was added.
	5041	A change has been made to IPsec settings. An Authentication Set was modified
	5042	A change has been made to IPsec settings. An Authentication Set was deleted
	5043	A change has been made to IPsec settings. A Connection Security Rule was added
	5044	A change has been made to IPsec settings. A Connection Security Rule was modified
	5045	A change has been made to IPsec settings. A Connection Security Rule was deleted
	5046	A change has been made to IPsec settings. A Crypto Set was added
	5047	A change has been made to IPsec settings. A Crypto Set was modified
	5048	A change has been made to IPsec settings. A Crypto Set was deleted
	5049	An IPsec Security Association was deleted
	5050	An attempt to programmatically disable the Windows Firewall using a call to
	5051	A file was virtualized
	5057	A cryptographic primitive operation failed
	5060	Verification operation failed
	5062	A kernel-mode cryptographic self test was performed
	5121	OCSP Responder Service Stopped
	5122	A Configuration entry changed in the OCSP Responder Service
	5123	A configuration entry changed in the OCSP Responder Service
	5124	A security setting was updated on OCSP Responder Service
	5125	A request was submitted to OCSP Responder Service
	5126	Signing Certificate was automatically updated by the OCSP Responder Service
	5127	The OCSP Revocation Provider successfully updated the revocation information



LinkedIn : Ammar Hakim Haris



[LinkedIn : Ammar Hakim Haris](#)

THANK YOU