Event IDs

The list of possible Event IDs is extensive; however, here is a list of Event IDs that are most relevant:

Windows	513	Windows is shutting down
Windows	528	Successful Logon
Windows	529	Logon Failure - Unknown user name or bad password
Windows	530	Logon Failure - Account logon time restriction violation
Windows	531	Logon Failure - Account currently disabled
Windows	532	Logon Failure - The specified user account has expired
Windows	533	Logon Failure - User not allowed to logon at this computer
Windows	534	Logon Failure - The user has not been granted the requested logon type at this machine
Windows	535	Logon Failure - The specified account's password has expired
Windows	536	Logon Failure - The NetLogon component is not active
Windows	537	Logon failure - The logon attempt failed for other reasons.
Windows	539	Logon Failure - Account locked out
Windows	540	Successful Network Logon
Windows	552	Logon attempt using explicit credentials
Windows	577	Privileged Service Called
Windows	612	Audit Policy Change
Windows	636	Security Enabled Local Group Member Added
Windows	861	The Windows Firewall has detected an application listening for incoming traffic
Windows	1100	The event logging service has shut down
Windows	1102	The audit log was cleared
Windows	4609	Windows is shutting down
Windows	4624	An account was successfully logged on
Windows	4625	An account failed to log on
Windows	4657	A registry value was modified
Windows	4712	IPsec Services encountered a potentially serious failure
Windows	4732	A member was added to a security-enabled local group

Windows	4763	A security-disabled universal group was deleted
Windows	4950	A Windows Firewall setting has changed
Windows	5025	The Windows Firewall Service has been stopped
Windows	5031	The Windows Firewall Service blocked an application from accepting incoming connections on the network.
Windows	5050	An attempt to programmatically disable the Windows Firewall using a call to INetFwProfile.FirewallEnabled(FALSE)
Windows	5142	A network share object was added.
Windows	5145	A network share object was checked to see whether client can be granted desired access
Windows	5154	The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections

Recommended Internet Sites

- Windows Security Log Events:
  https://web.archive.org/web/20160726162033/https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/Default.aspx

Please contact the Course Coordinators if you are unable to access any of the Recommended Internet Sites.