Windows Privileges

- **SeAssignPrimaryTokenPrivilege** — Replace a process-level token. — With this privilege, the user can initiate a process to replace the default token associated with a started subprocess.
- **SeCreateSymbolicLinkPrivilege** — Create symbolic links. — Can reveal security flaws in programmes that are not built to handle symbolic connections.
- **SeIncreaseWorkingSetPrivilege** — Increase a process working set. — To raise the minimal working set, SetProcessWorkingSetSize must be called.
- **SeProfileSingleProcessPrivilege** — Profile single process. — When using NtQuerySystemInformation to obtain information for a specific process, Superfetch and the prefetcher check this value.
- **SeShutdownPrivilege** — Shutdown the system. — NtShutdownSystem and NtRaiseHardError, which display a system error dialogue box on the interactive terminal, are used to check for problems.
- **SeTrustedCredManAccessPrivilege** — Access Credential Manager as a trusted caller. — The Credential Management checks to see if it can trust the caller with unencrypted access to credentials.
- **SeAuditPrivilege** — Generate security audit. — With this privilege, the user can add entries to the security log.
- **SeCreateTokenPrivilege** — Create a token object. — Allows a process to create a token which it can then use to get access to any local resources when the process uses NtCreateToken() or other token-creation APIs.
- **SeLoadDriverPrivilege** — Load and unload device drivers. — This privilege causes the system to grant all write access control to any file, regardless of the ACL specified for the file. Any access request other than write is still evaluated with the ACL.
- **SeDebugPrivilege** — Debug programs. — Required to debug and adjust the memory of a process owned by another account.
- **SeSecurityPrivilege** — Manage auditing and security log. — With this privilege, the user can specify object access auditing options for individual resources, such as files, Active Directory objects, and registry keys.
- **SeTcbPrivilege** — Act as part of the operating system. — This user right allows a process to impersonate any user without authentication. The process can therefore gain access to the same local resources as that user.
- **SeBackupPrivilege** — Backup file and directories. — With this privilege, the user can bypass file and directory, registry, and other persistent object permissions for the purposes of backing up the system.
- **SeManageVolumePrivilege** — Perform volume maintenance tasks. — Enforced by file system drivers during a volume open operation, which is required to perform disk-checking.
- **SeRestorePrivilege** — Restore files and directories. — Grant access to any file or directory, regardless of the security descriptor that's present: WRITE_DAC, WRITE_OWNER, ACCESS_SYSTEM_SECURITY, FILE_GENERIC_WRITE, FILE_ADD_FILE, FILE_ADD_SUBDIRECTORY and DELETE.
- **SeTimeZonePrivilege** — Change the time zone. — Required to change the time zone.
- **SeChangeNotifyPrivilege** — Bypass traverse checking. — Avoid checking permissions on intermediate directories of a multilevel directory lookup.
- **SeEnableDelegationPrivilege** — Enable computer and user accounts to be trusted for delegation. — With this privilege, the user can set the Trusted for Delegation setting on a user or computer object.
- **SeSyncAgentPrivilege** — Synchronize directory service data. — Required to use the LDAP directory synchronization services. It allows the holder to read all objects and properties in the directory.
- **SeTakeOwnershipPrivilege** — Take ownership of files and other objects. — his privilege allows the owner value to be set only to those values that the holder may legitimately assign as the owner of an object.
- **SeImpersonatePrivilege** — Impersonate a client after authentication. — With this privilege, the user can impersonate other accounts.
- **SeSystemEnvironmentPrivilege** — Modify firmware environment variables. — Required to modify the nonvolatile RAM of systems that use this type of memory to store configuration information.
- **SeUndockPrivilege** — Remove computer from a docking station. — Checked by the user-mode Plug and Play manager when a computer undock is initiated.

- **SeCreatePagefilePrivilege** — Create a pagefile. — Checked by NtCreatePagingFile, which is the function used to create a new paging file.
- **SeIncreaseBasePriorityPrivilege** — Increase scheduling priority. — Checked by the process manager and is required to raise the priority of a process.
- **SeLockMemoryPrivilege** — Lock pages in memory. — Checked by NtLockVirtualMemory, the kernel implementation of VirtualLock.
- **SeRelabelPrivilege** — Modify an object label. — Checked by the SRM when raising the integrity level of an object owned by another user.
- **SeSystemProfilePrivilege** — Profile system performance. — Checked by NtCreateProfile, the function used to perform profiling of the system. This is used by the Kernprof tool, for example.
- **SeCreatePermanentPrivilege** — Create permanent shared objects. — Checked by the object manager when creating a permanent object.
- **SeIncreaseQuotaPrivilege** — Adjust memory quotas for a process. — Enforced when changing a process' s working set thresholds, a process' s paged and nonpaged pool quotas, and a process' s CPU rate quota.
- **SeMachineAccountPrivilege** — Add workstations to the domain. — Checked by the SAM on a domain controller when creating a machine account in a domain.
- **SeRemoteShutdownPrivilege** — Force shutdown from a remote system. — Winlogon checks that remote callers of the InitiateSystemShutdown function have this privilege.
- **SeSystemtimePrivilege** — Change the system time. — Required to change the time or date.
- **SeNetworkLogonRight** — Access this computer from the network — Determines which users can connect to the device from the network
- **SeInteractiveLogonRight** — Allow log on locally — This policy setting determines which users can start an interactive session on the device
- **SeRemoteInteractiveLogonRight** — Allow log on through Remote Desktop Services — This policy setting determines which users or groups can access the sign-in screen of a remote device through a Remote Desktop Services connection.
- **SeCreateGlobalPrivilege** — Create global objects — This policy setting determines which users can create global objects that are available to all sessions
- **SeDenyNetworkLogonRight** — Deny access to this computer from the network — This security setting determines which users are prevented from accessing a device over the network
- **SeDenyBatchLogonRight** — Deny log on as a batch job — This policy setting determines which accounts are prevented from logging on by using a batch-queue tool to schedule and start jobs automatically in the future
- **SeDenyServiceLogonRight** — Deny log on as a service — This policy setting determines which users are prevented from logging on to the service applications on a device
- **SeDenyInteractiveLogonRight** — Deny log on locally — This policy setting determines which users are prevented from logging on directly at the device's console
- **SeDenyRemoteInteractiveLogonRight** — Deny log on through Remote Desktop Services — This policy setting determines which users are prevented from logging on to the device through a Remote Desktop connection through Remote Desktop Services
- **SeBatchLogonRight** — Log on as a batch job — This policy setting determines which accounts can sign in by using a batch-queue tool such as the Task Scheduler service
- **SeServiceLogonRight** — Log on as a service — This policy setting determines which service accounts can register a process as a service
- **SeDelegateSessionUserImpersonatePrivilege** — Obtain an impersonation token for another user in the same session — This policy setting determines which programs are allowed to impersonate a user or another specified account and act on behalf of the user