WINDOWS PRIVILEGES

T.me/Library_Se

 Commonly abused privileges

🐦 @FR0GGER_
THOMAS ROCCIA

SeAssignPrimaryTokenPrivilege
Replace a process-level token.

Checked by various components, such as NtSetInformationJobObject, that set a process's token.

SeAuditPrivilege
Generate security audit.

Required to generate events for the Security event log with the ReportEvent API.

🐛 SeBackupPrivilege
Backup file and directories.

Grant the following access to any file or directory: READ_CONTROL, ACCESS_SYSTEM_SECURITY, FILE_GENERIC_READ, FILE_TRAVERSE.

SeChangeNotifyPrivilege
Bypass traverse checking.

Avoid checking permissions on intermediate directories of a multilevel directory lookup.

SePrivilege
Create global objects.

Required for a process to create section and symbolic link objects in the directories of the object manager namespace.

SeCreatePagefilePrivilege
Create a pagefile.

Checked by NtCreatePagingFile, which is the function used to create a new paging file.

SeCreatePermanentPrivilege
Create permanent shared objects.

Checked by the object manager when creating a permanent object.

SeCreateSymbolicLinkPrivilege
Create symbolic links.

Checked by NTFS when creating symbolic links with the CreateSymbolicLink API

🐛 SeCreateTokenPrivilege
Create a token object.

Checked by NtCreateToken to create a token object.

🐛 SeManageVolumePrivilege
Perform volume maintenance tasks.

Enforced by file system drivers during a volume open operation, which is required to perform disk-checking.

SeEnableDelegationPrivilege
Enable computer and user accounts to be trusted for delegation.

Used by Active Directory services to delegate authenticated credentials.

🐛 SeImpersonatePrivilege
Impersonate a client after authentication.

Process manager checks for this when a thread wants to use a token for impersonation.

SeIncreaseBasePriorityPrivilege
Increase scheduling priority.

Checked by the process manager and is required to raise the priority of a process.

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.

SeIncreaseWorkingSetPrivilege
Increase a process working set.

Required to call SetProcessWorkingSetSize to increase the minimum working set.

🐛 SeLoadDriverPrivilege
Load and unload device drivers.

Checked by NtLoadDriver and NtUnloadDriver driver functions.

SeLockMemoryPrivilege
Lock pages in memory.

Checked by NtLockVirtualMemory, the kernel implementation of VirtualLock.

SeMachineAccountPrivilege
Add workstations to the domain.

Checked by the SAM on a domain controller when creating a machine account in a domain.

SeProfileSingleProcessPrivilege
Profile single process.

Checked by Superfetch and the prefetcher when requesting information for an individual process through NtQuerySystemInformation.

🐛 SeDebugPrivilege
Debug programs.

If the caller has this privilege enabled, the process manager allows access to any process or thread using NtOpenProcess or NtOpenThread, regardless the security descriptor.

SeRelabelPrivilege
Modify an object label.

Checked by the SRM when raising the integrity level of an object owned by another user.

SeRemoteShutdownPrivilege
Force shutdown from a remote system.

Winlogon checks that remote callers of the InitiateSystemShutdown function have this privilege.

SeShutdownPrivilege
Shutdown the system.

Checked by NtShutdownSystem and NtRaiseHardError, which presents a system error dialog box on the interactive console.

SeSecurityPrivilege
Manage auditing and security log.

Required to access the SACL of a security descriptor and to read and clear the security event log.

🐛 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

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.

SeSystemEnvironmentPrivilege
Modify firmware environment variables.

Required by NtSetSystemEnvironmentValue and NtQuerySystemEnvironmentValue to modify and read firmware environment variables using the HAL

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.

SeSystemtimePrivilege
Change the system time.

Required to change the time or date.

SeTrustedCredManAccessPrivilege
Access Credential Manager as a trusted caller.

Checked by the Credential Manager to verify that it should trust the caller with credential information that can be queried in plaintext.

🐛 SeTcbPrivilege
Act as part of the operating system.

Checked by the SRM when the session ID is set in a token, by the Plug and Play manager for Plug and Play event creation and management.

SeTimeZonePrivilege
Change the time zone.

Required to change the time zone.

🐛 SeTakeOwnershipPrivilege
Take ownership of files and other objects.

Required to take ownership of an object without being granted discretionary access.

SeUndockPrivilege
Remove computer from a docking station.

Checked by the user-mode Plug and Play manager when a computer undock is initiated.

SeUnsolicitedInputPrivilege
Receive unsolicited data from a terminal device.

This privilege is not currently used by Windows.