What are Windows privileges?

Windows privileges are named rights carried in a user's access token that allow specific powerful actions, separate from file permissions. Several are effectively a path to SYSTEM: SeImpersonate (impersonate tokens, used by Potato attacks), SeBackup/SeRestore (read or write any file, so dump the SAM and hives), SeDebug (open any process, including LSASS), SeTakeOwnership (take ownership of any object), and SeLoadDriver. The first check on a Windows host is `whoami /priv` to see which dangerous privileges the token holds.

HOW IT WORKS

01 The dangerous privileges and payload

The attacker lists token privileges and abuses any powerful one:

- List: `whoami /priv`
- SeImpersonatePrivilege: run a Potato attack to get SYSTEM.
- SeBackupPrivilege: read protected files, for example copy the SAM and SYSTEM hives, then dump hashes offline: `reg save HKLM\SAM sam.hive` and `reg save HKLM\SYSTEM system.hive` then `secretsdump.py -sam sam.hive -system system.hive LOCAL`.
- SeDebugPrivilege: open and dump LSASS to harvest credentials.
- SeRestore / SeTakeOwnership: overwrite or take ownership of protected files and binaries to plant code.

Documented techniques shown for defenders.

> **WHOAMI /PRIV FIRST**
>
> *On any Windows host,* `whoami /priv` *reveals the token's privileges. SeImpersonate, SeBackup, SeRestore, SeDebug, SeTakeOwnership, and SeLoadDriver are the ones that lead to SYSTEM.*

HOW TO DEFEND

- Grant powerful privileges only to accounts that genuinely need them, following least privilege.
- Review who holds SeImpersonate, SeBackup, SeRestore, SeDebug, SeTakeOwnership, and SeLoadDriver.
- Use managed/virtual service accounts with minimal rights.
- Protect LSASS (Credential Guard) so SeDebug abuse yields less.
- Audit token privileges across the estate and monitor for their use.

SOURCES

[1] MITRE ATT&CK: Privilege Escalation (TA0004)

[2] Microsoft: Privilege Constants (Windows)

[3] NIST SP 800-115 Technical Guide to Security Testing

Find the privilege-escalation paths before an attacker does.

securelayer7.net/learn/privilege-escalation/what-are-windows-privileges

Open online