Windows-Sicherheitsmechanismen

Systemprivilegien / Benutzerrechte

Im Access-Token ist festgelegt, welche Systemprivilegien ein Benutzer hat
(z.B. `SeSystemtimePrivilege` = „Ändern der Systemzeit“)

Tools

- **`whoami /priv`**
- Gruppenrichtlinien → Computerkonfiguration → Windows-Einstellungen → Sicherheitseinstellungen → Lokale Richtlinien → Zuweisen von Benutzerrechten

NTFS-Berechtigungen

Jeder Ordner und jede Datei auf einer NTFS-Partition hat einen Security Descriptor (SD),
in dem festgelegt ist,
welche Benutzer und Gruppen wie zugreifen können (DACL – Discretionary Access Control List)
und welche Zugriffe mitprotokolliert werden (SACL – System Access Control List).

Tools

- Windows-Explorer
- **`icacls`**

UAC (User Account Control / Benutzerkontensteuerung)

Mitglieder der Gruppe „Administratoren“ erhalten ein „Split-Token“

Standard-Token

- Es gelten für die Gruppe Administratoren nur die NTFS-Rechte „Verweigern“
- nur eingeschränkte Systemprivilegien
- Integritätslevel: Mittel

Elevated-Token

- Es gelten alle NTFS-Rechte für die Gruppe Administratoren
- mehr Systemprivilegien
- Integritätslevel: Hoch

Tools

- **`whoami /all`**

MIC (Mandatory Integrity Control / Integritätslevel)

Ein Prozess mit einem kleineren Integritätslevel kann nicht schreibend auf ein Objekt mit einem größeren Integritätslevel zugreifen.

Integritätslevel

- untrusted
- low (z.B. IE protected mode)
- medium (Standard, z.B. normale Datei)
- medium plus
- high (z.B. Administratoren)
- system (z.B. SYSTEM)
- protected process
- secure process

Tools

- **`whoami /groups`**
- **`icacls`**
- ProcessExplorer