

Übung: MIC (Mandatory Integrity Control) - Integritätslevel, UAC (User Account Control) - Benutzerkontensteuerung

1. Normaler Benutzer

a) Erstellen Sie mit dem mmc-Snap-In **Lokale Benutzer und Gruppen** einen Benutzer **normal**.

In welcher Gruppe ist **normal** laut mmc Mitglied? _____

b) Melden Sie sich als **normal** an und lassen Sie sich mit dem Befehl `whoami /user` Ihre SID anzeigen.

Wie lauten die letzten vier Ziffern der SID von **normal**? `S-1-5-21-ComputerId-`_____

c) Lassen Sie sich mit dem Befehl `whoami /groups` anzeigen, in welchen Gruppen der Benutzer **normal** Mitglied ist.

Welches Integritätslevel (Verbindlichkeitsstufe) hat **normal** (das Integritätslevel wird auch als Gruppe angezeigt)?

d) Lassen Sie sich mit dem Befehl `whoami /priv` anzeigen, welche Privilegien (Berechtigungen) **normal** hat.

e) Vergleichen Sie die Privilegien mit den Einstellungen in den Gruppenrichtlinien („**Zuweisen von Benutzerrechten**“).

Wo befinden sich diese?

f) Geben Sie dem Benutzer **normal** das Privileg, die Systemzeit zu ändern.

g) Melden Sie sich wieder als **normal** an und geben Sie nochmal den Befehl `whoami /priv` ein.

Wie lautet der Berechtigungsname des Privilegs **Systemzeit ändern**?

2. Mitglied der Gruppe Administratoren

a) Erstellen Sie einen Benutzer **admin2** und machen Sie ihn zum Mitglied der Gruppe **Administratoren**.

In welchen Gruppen ist **admin2** laut mmc Mitglied? _____

b) Melden Sie sich als **admin2** an.

Wie lauten die letzten vier Ziffern der SID von **admin2**? s-1-5-21-ComputerId-_____

Wie lautet der Wert für „**Attribute**“ der Gruppe **Administratoren**?

Welches Integritätslevel (Verbindlichkeitsstufe) hat **admin2** ?

Hat **admin2** mehr Privilegien als **normal**?

c) Starten Sie die Eingabeaufforderung per Rechtsklick mit „**Als Administrator ausführen**“.

Wie lautet nun der Wert für „**Attribute**“ der Gruppe **Administratoren**?

Welches Integritätslevel (Verbindlichkeitsstufe) hat **admin2** jetzt?

Hat **admin2** nun mehr Privilegien als **normal**?

3. Prozesse

a) Starten Sie als **admin2** zweimal **Paint**: einmal normal und einmal als Administrator.

Starten Sie den **ProcessExplorer** als Administrator.

Welche Integritätslevel haben die beiden Paint-Prozesse?

Integritätslevel von Paint normal gestartet: _____

Integritätslevel von Paint als Administrator gestartet: _____

Welcher laufende Prozess hat die kleinste Prozess-ID?
