

[FORT] Práctica 10: NTFS y APPLOCKER

1. ¿Es posible customizar la seguridad de UAC de una manera más precisa?

Si, se puede customizar con mayor precisión mediante el uso de Directivas de Seguridad Local (secpol.msc):

Nombre	Descripción
Directivas de cuenta	Directivas de bloqueo de contraseña y cuenta
Directivas locales	Directivas de opciones de seguridad, derechos ...
Windows Defender Firewall con seguridad avanzada	Windows Defender Firewall con seguridad avanzada
Directivas de Administrador de listas de reproducción	Directivas de grupo de ubicación, ícono y nom...
Directivas de clave pública	
Directivas de restricción de software	
Directivas de control de aplicaciones	Directivas de control de aplicaciones
Directivas de seguridad IP en Equipo local	Administración del protocolo de seguridad de l...
Configuración de directiva de auditoría avanzada	Configuración de directiva de auditoría avanzada

Con estas directivas se pueden realizar ajustes en las políticas como las de opciones de seguridad:

The screenshot shows the Windows Security Policy Editor window. On the left, there's a tree view of security policies under 'Configuración de seguridad'. The 'Opciones de seguridad' node is expanded. On the right, a table lists various security settings with their descriptions and current status (Classic, Enabled, Disabled, Not defined). Some settings like 'Apagado: permitir traducción SID/nombre anónima' and 'Apagado: permitir apagar el sistema sin tener que iniciar sesión' are explicitly marked as disabled.

Directiva	Configuración de seguridad
Acceso a redes: canalizaciones con nombre accesibles anónimamente	Clásico: usuarios locales se autentican en la red
Acceso a redes: modelo de seguridad y uso compartido para cuentas locales	Deshabilitada
Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación en la red	Habilitada
Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM	Deshabilitada
Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM	Deshabilitada
Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos	No está definido
Acceso a redes: recursos compartidos accesibles anónimamente	Habilitada
Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos	System\CurrentControlSet\Control\Pro
Acceso a redes: rutas del Registro accesibles remotamente	System\CurrentControlSet\Control\Priv
Acceso a redes: rutas y subtareas del Registro accesibles remotamente	No está definido
Acceso de red: evitar que clientes con permiso realicen llamadas remotas a SAM	Habilitada
Acceso de red: permitir traducción SID/nombre anónima	Deshabilitada
Apagado: borrar el archivo de paginación de la memoria virtual	Deshabilitada
Apagado: permitir apagar el sistema sin tener que iniciar sesión	Habilitada
Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad	Deshabilitada
Auditoría: auditar el acceso de objetos globales del sistema	Deshabilitada
Auditoría: auditar el uso del privilegio de copias de seguridad y restauración	Deshabilitada
Auditoría: forzar la configuración de subcategorías de la directiva de auditoría (Windows Vista o posterior)	No está definido
Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitada
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitada
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Deshabilitada
Configuración del sistema: subsistemas opcionales	

También se puede utilizar el registro (regedit) en "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" para customizar algunos parámetros de UAC:

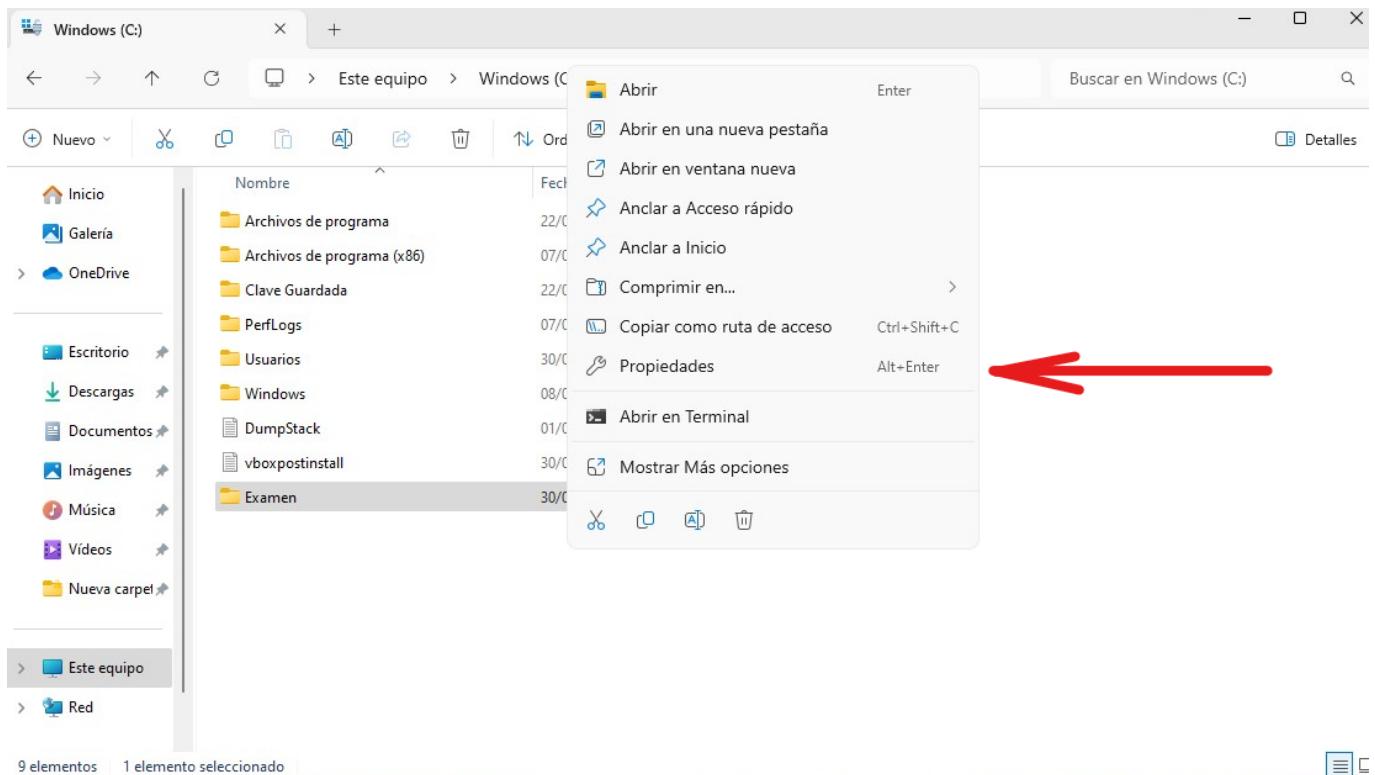
The screenshot shows the Windows Registry Editor window. The left pane shows the registry tree under 'Equipo\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System'. The right pane displays a table of registry keys with their names, types, and values. Several keys are highlighted in yellow, indicating they are being edited or selected. These include 'ConsentPromptBehaviorAdmin', 'ConsentPromptBehaviorUser', 'DontDisplayLastUsername', 'DSCAutomationHostEnabled', 'EnableCursorSuppression', 'EnableFullTrustStartupTasks', 'EnableInstallerDetection', 'EnableLUA', 'EnableSecureUIAPaths', 'EnableUIADesktopToggle', 'EnableUwpStartupTasks', 'EnableVirtualization', 'LegalNoticeCaption', 'LegalNoticeText', 'PromptOnSecureDesktop', 'Sforceoption', 'ShutdownWithoutLogon', 'SupportFullTrustStartupTasks', 'SupportUwpStartupTasks', 'UndockWithoutLogon', and 'ValidateAdminCodeSignatures'.

Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
ConsentPromptBehaviorAdmin	REG_DWORD	0x00000005 (5)
ConsentPromptBehaviorUser	REG_DWORD	0x00000003 (3)
DontDisplayLastUsername	REG_DWORD	0x00000000 (0)
DSCAutomationHostEnabled	REG_DWORD	0x00000002 (2)
EnableCursorSuppression	REG_DWORD	0x00000001 (1)
EnableFullTrustStartupTasks	REG_DWORD	0x00000002 (2)
EnableInstallerDetection	REG_DWORD	0x00000001 (1)
EnableLUA	REG_DWORD	0x00000001 (1)
EnableSecureUIAPaths	REG_DWORD	0x00000001 (1)
EnableUIADesktopToggle	REG_DWORD	0x00000000 (0)
EnableUwpStartupTasks	REG_DWORD	0x00000002 (2)
EnableVirtualization	REG_DWORD	0x00000001 (1)
LegalNoticeCaption	REG_SZ	
LegalNoticeText	REG_SZ	
PromptOnSecureDesktop	REG_DWORD	0x00000001 (1)
Sforceoption	REG_DWORD	0x00000000 (0)
ShutdownWithoutLogon	REG_DWORD	0x00000001 (1)
SupportFullTrustStartupTasks	REG_DWORD	0x00000001 (1)
SupportUwpStartupTasks	REG_DWORD	0x00000001 (1)
UndockWithoutLogon	REG_DWORD	0x00000001 (1)
ValidateAdminCodeSignatures	REG_DWORD	0x00000000 (0)

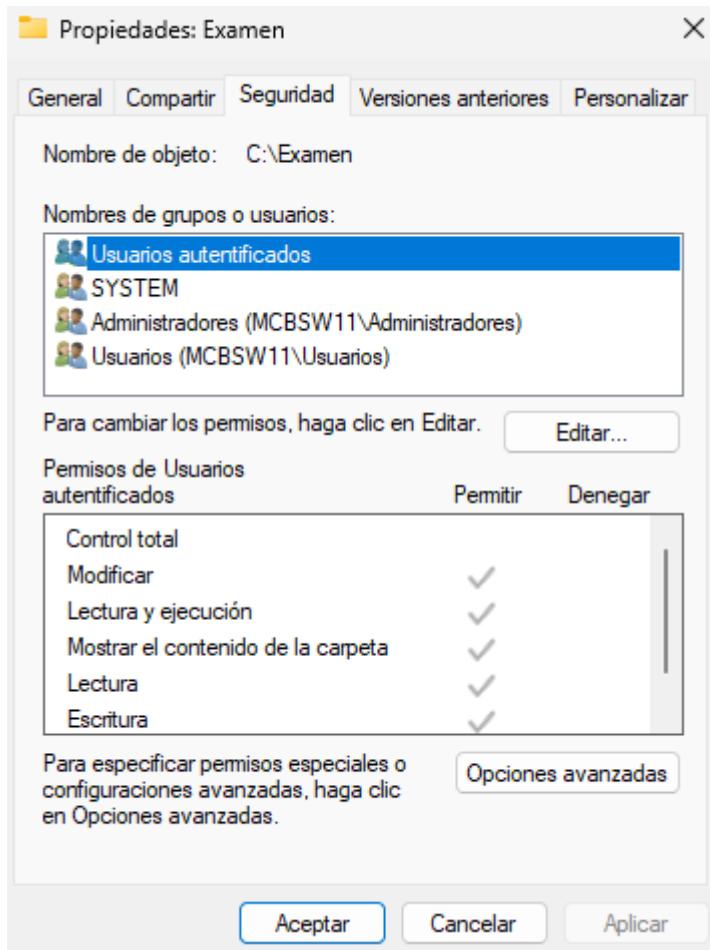
Sobre una carpeta “Examen” creada en “C:\” se van a realizar las siguientes configuraciones de UAC:

a) LECTURA: El usuario2 puede leer contenido pero no eliminar o crear carpetas/archivos

Para realizar esta configuración primero hay que dirigirse a las propiedades de la carpeta Examen:



En la ventana que saldrá hay que dirigirse a la pestaña de seguridad:



b) SOLO LECTURA: El usuario 2 Solo puede leer el contenido de la carpeta y del archivo lectura1.txt

c) LECTURA + AÑADIR: El usuario2 solo puede leer el contenido de la carpeta y del archivo añadir.txt. Puede crear carpetas y dentro de estas puede crear archivos.

d) ACCESO TOTAL: El usuario 2 tiene el control total sobre la carpeta y componentes

From:
<https://knoppia.net/> - Knoppia

Permanent link:
https://knoppia.net/doku.php?id=master_cs:fortificacion:p10&rev=1746027619

Last update: 2025/04/30 15:40

