[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):

🚡 Directiva de seguridad local			-		×
Archivo Acción Ver Ayuda					
Archivo Acción Ver Ayuda Archivo Acción Ver Ayuda Configuración de seguridad Directivas de cuenta Directivas locales Mindows Defender Firewall con segur Directivas de Administrador de listas (Directivas de clave pública Directivas de restricción de software Directivas de control de aplicaciones Directivas de seguridad IP en Equipo I Configuración de directiva de auditor	Nombre Directivas de cuenta Nombre	Descripción Directivas de bloqueo de cont Directivas de opciones de seg Windows Defender Firewall co Directivas de grupo de ubicac Directivas de control de aplica Administración del protocolo Configuración de directiva de	traseña uridad, on segu ión, ico aciones de seg	y cuenta derecho ridad ava no y nor uridad de ría avanz	s n e l ada
	Configuración de directiva de auditoría a	Configuración de directiva de	audito	ría avanz	ada

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

 Directiva de seguridad local Archivo Acción Ver Ayuda 				×
Archivo Acción Ver Ayuda				
 Configuración de seguridad Directivas de cuenta Directivas locales Directiva de auditoría Acceso a redes: modelo de seguridad y uso compartido para cuentas locales Clási Opciones de seguridad Windows Defender Firewall con segur Directivas de clave pública Directivas de clave pública Directivas de control de aplicaciones Directivas de seguridad IP en Equipol Configuración de directiva de auditori Acceso a redes: returas y class compartidos accesibles anónimamente No ec Directivas de seguridad IP en Equipol Acceso a redes: returas y subrutas del Registro accesibles remotamente Acceso a redes: returas y subrutas del Registro accesibles remotamente Acceso a redes: returas y subrutas del Registro accesibles remotamente Acceso a redes: returas y subrutas del Registro accesibles remotamente Acceso a redes: returas y subrutas del Registro accesibles remotamente Acceso a redes: rutas y subrutas del Registro accesibles remotamente Acceso a redes: rutas y subrutas del Registro accesibles remotamente Acceso a redes: rutas y subrutas del Registro accesibles remotamente Acceso a redes: rutas y subrutas del Registro accesibles remotamente Acceso a redes: rutas y subrutas del Registro accesibles remotamente Acceso a redes: rutas y subrutas del Registro accesibles remotamente Acceso a redes: rutas y subrutas del Registro accesibles remotamente Acceso a redes: rutas y subrutas del Registro accesibles remotamente Acceso a redes: rutas y subrutas del Registro accesibles remotamente Acceso a redes: rutas y subrutas del Registro accesibles remotamente Acceso a redes: rutas y subrutas del Registro accesibles remotamente	onfiguración de segu ásico: usuarios locale ishabilitada ishabilitada ishabilitada ishabilitada o está definido istem\CurrentContro o está definido ishabilitada ishabilitada ishabilitada ishabilitada ishabilitada ishabilitada ishabilitada ishabilitada ishabilitada ishabilitada ishabilitada ishabilitada ishabilitada	ridad 25 se aul ISet\Co ISet\Co	ntrol\	Pro Prir

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

🔡 Editor del Registro				-	\times
Archivo Edición Ver Favoritos Ayuda					
Equipo\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Cu	rrentVersion\Policies\System				
 MMDevices NcdAutoSetup NetCache NetworkServiceTriggers Notifications OEMInformation OneSettings OOBE OpenWith OpenWith OpenWith Operaulayout Parental Controls PerceptionSimulationExtensions Personalization PhotoPropertyHandler PlayReady Policies ActiveDesktop Attachments DataCollection Ext NonEnum Servicing System Audit UIPI PowerEfficiencyDiagnostics PrecisionTouchPad 	Nombre (Predeterminado) (ConsentPromptBehaviorAdmin ConsentPromptBehaviorUser dontdisplaylastusername DSCAutomationHostEnabled EnableCursorSuppression EnableFullTrustStartupTasks EnableIstallerDetection EnableSecureUIAPaths EnableUA EnableSecureUIAPaths EnableUADesktopToggle EnableUADesktopToggle EnableUVirtualization Elegalnoticecaption Elegalnoticetext PromptOnSecureDesktop SupportFullTrustStartupTasks SupportVupStartupTasks SupportVupStartupTasks SupportVupStartupTasks SupportVupStartupTasks SupportVupStartupTasks SupportVupStartupTasks SupportVupStartupTasks SupportVupStartupTasks SupportVupStartupTasks SupportVupStartupTasks SupportVupStartupTasks SupportVupStartupTasks	Tipo REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_SZ REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD	Datos (valor no establecido) 0x0000005 (5) 0x0000000 (0) 0x00000002 (2) 0x00000001 (1) 0x00000001 (1)		

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:

Propi	edades: Ex	amen		×	
General	Compartir	Seguridad	Versiones anteriores	Personalizar	
Nombre	e de objeto:	C:\Examen	I		
Nombre	s de grupos	o usuarios:			
SY See Sy See Ad See Us	Usuarios autentificados SYSTEM Administradores (MCBSW11\Administradores) Usuarios (MCBSW11\Usuarios)				
Para ca	Para cambiar los permisos, haga clic en Editar. Editar				
Permiso autentifi	is de Usuari icados	os	Permitir	Denegar	
Contr	rol total				
Modi	ficar		~		
Modi Lectu	ficar ura y ejecuci	ión	\sim		
Modi Lectu Most	ficar ura y ejecuc rar el conter	ión nido de la caŋ	v v peta		
Modi Lectu Most Lectu	ficar ura y ejecuci rar el conter ura	ión iido de la caŋ	peta		
Modi Lectu Mostr Lectu Escrit	ficar ura y ejecuc rar el conter ura tura	ión nido de la caŋ	peta		
Modi Lectu Most Lectu Escrit Para es configu en Opci	ficar ura y ejecuci ura ura tura pecificar pe raciones ava iones avanz	ión nido de la can misos especi anzadas, hag adas.	ales o Opcione	s avanzadas	

En dicha pestaña se presiona sobre el botón "Opciones Avanzadas" para que se muestre la siguiente ventana:

e clic en una entrada de p Acceso Control total Control total	permiso. Para modificar Heredada de C:\	una entrada de permiso, seleccione la Se aplica a Esta carpeta, subcarpetas y arc
Cambiar ivo clic en una entrada de p Acceso Control total Control total	permiso. Para modificar Heredada de C:\	una entrada de permiso, seleccione la Se aplica a Esta carpeta, subcarpetas y arc
Cambiar ivo e clic en una entrada de p Acceso Control total Control total	permiso. Para modificar Heredada de C:\	una entrada de permiso, seleccione la Se aplica a Esta carpeta, subcarpetas y arc
ivo e clic en una entrada de p Acceso Control total Control total	bermiso. Para modificar Heredada de C:\	una entrada de permiso, seleccione la Se aplica a Esta carpeta, subcarpetas y arc
c clic en una entrada de p Acceso Control total Control total	Heredada de	una entrada de permiso, seleccione la Se aplica a Esta carpeta, subcarpetas y arc
Control total Control total	C:\	Esta carpeta, subcarpetas y arc
Control total	C1	
	Cil	Esta carpeta, subcarpetas y arc
Lectura y ejecución	C:\	Esta carpeta, subcarpetas y arc
Modificar	C:\	Esta carpeta, subcarpetas y arc
e objetos secundarios po	or entradas de permisos	heredables de este objeto
	e objetos secundarios po	e objetos secundarios por entradas de permisos

Tras eso se presiona en el botón de agregar:

Entidad de seguridad: Seleccionar una entidad de seguridad Tipo: Permitir Se aplica a: Esta carpeta, subcarpetas y archivos Permisos básicos: Mostrar permisos avant Ocntrol total Modificar Lectura y ejecución Mostrar el contenido de la carpeta Electura Escritura Permisos especiales Aplicar estos permisos solo a objetos y/o contenedores dentro de este contenedor	📒 Entrada de perm	iso para Examen	— D X
Tipo: Permitir Se aplica a: Esta carpeta, subcarpetas y archivos Permisos básicos: Mostrar permisos avanta Ontrol total Mostrar el contenido de la carpeta Ectura Escritura Escritura Permisos especiales Aplicar estos permisos solo a objetos y/o contenedores dentro de este contenedor	Entidad de seguri	dad: Seleccionar una entidad de seguridad	
Se aplica a: Esta carpeta, subcarpetas y archivos	Тіро:	Permitir \checkmark	
Permisos básicos: Mostrar permisos avant	Se aplica a:	Esta carpeta, subcarpetas y archivos $$	
Permisos básicos: Mostrar permisos avanta Ontrol total Modificar Electura y ejecución Mostrar el contenido de la carpeta Electura Escritura Permisos especiales Borrar toc Aplicar estos permisos solo a objetos y/o contenedores dentro de este contenedor Borrar toc			
 Control total Modificar Lectura y ejecución Mostrar el contenido de la carpeta Lectura Escritura Permisos especiales Aplicar estos permisos solo a objetos y/o contenedores dentro de este contenedor 	Permisos básicos:		Mostrar permisos avanzados
 Modificar Lectura y ejecución Mostrar el contenido de la carpeta Lectura Escritura Permisos especiales Aplicar estos permisos solo a objetos y/o contenedores dentro de este contenedor 	Co	ontrol total	
Mostrar el contenido de la carpeta Lectura Escritura Permisos especiales Aplicar estos permisos solo a objetos y/o contenedores dentro de este contenedor Borrar too	M	odificar	
Mostrar el contenido de la carpeta Lectura Permisos especiales Aplicar estos permisos solo a objetos y/o contenedores dentro de este contenedor Borrar toc	∠ Le	ctura y ejecucion	
Eccura Escritura Permisos especiales Aplicar estos permisos solo a objetos y/o contenedores dentro de este contenedor Borrar toc		ostrar el contenido de la carpeta	
Permisos especiales Aplicar estos permisos solo a objetos y/o contenedores dentro de este contenedor Borrar too	⊡ Es	ectura	
Aplicar estos permisos solo a objetos y/o contenedores dentro de este contenedor Borrar tod	- Pe	ernisos especiales	
Aplicar estos permisos solo a objetos y/o contenedores dentro de este contenedor Borrar toc	0.0		
	Aplicar estos po	ermisos solo a objetos y/o contenedores dentro de este contenedor	Borrar todo
Aceptar Can			Aceptar Cancelar

A continuación se presiona en el texto donde pone "Seleccionar una Entidad de Seguridad", en la ventana que se abre se introduce el nombre de usuario2, y se presiona en comprobar nombres, tras eso debería de aparecer el nombre del equipo seguido del de Usuario2 separados por una barra:

Seleccionar Usuario o Grupo	×
Seleccionar este tipo de objeto:	
Usuario, Grupo, o Entidad de seguridad integrada	Tipos de objeto
Desde esta ubicación:	
MCBSW11	Ubicaciones
Escriba el nombre de objeto para seleccionar (ejemplos):	
MCBSW11\usuario2	Comprobar nombres
Opciones avanzadas	Aceptar Cancelar

Tras eso se vuelve a la ventana anterior, donde ahora se pueden seleccionar los permisos, en este caso como el usuario solo puede realizar lectura, se retiran todos los permisos salvo el delectura:

Entrada de permis	so para Examen	— D X
Entidad de segurida	ad: usuario2 (MCBSW11\usuario2) Seleccionar una entidad de seguridad	
Тіро:	Permitir ~	
Se aplica a:	Esta carpeta, subcarpetas y archivos \checkmark	
Demaines hásisses		Matanania
	ntrol total	Mostrar permisos avanzados
	dificar	
Lec	tura y ejecución	
Mo:	strar el contenido de la carpeta	
🔽 Lec	tura	
Esci	ritura	
Peri	misos especiales	
Aplicar estos per	misos solo a objetos y/o contenedores dentro de este contenedor	Borrar todo
		Aceptar Cancelar

Finalmente se aplican los cambios y usuario2 quedará con los permisos establecidos:

Propiedades: Examen >
General Compartir Seguridad Versiones anteriores Personalizar
Nombre de objeto: C:\Examen
Nombres de grupos o usuarios:
👗 usuario2 (MCBSW11\usuario2)
Administradores (MCBSW11\Administradores)
Station (MCBSW11\Usuarios)
Para cambiar los permisos, haga clic en Editar. Editar
Permisos de usuario2 Permitir Denegar
Modificar
Lectura y ejecución
Mostrar el contenido de la carpeta
Lectura 🗸
Escritura
Escritura Permisos especiales
Escritura Permisos especiales Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas. Opciones avanzadas

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

Para aplicar esta configuración se siguen los pasos del anterior apartado y tras eso se procede a ir a las propiedades del archivo lectura1.txt, a la pestaña de seguridad:

Propiedades: lectura1.txt	×
General Seguridad Detalles Versiones anteriores	
Nombre de objeto: C:\Examen\lectura1.txt.txt	
Nombres de grupos o usuarios:	
Statisticados	
SYSTEM	
usuario2 (MCBSW11\usuario2)	
Administradores (MCBSW11\Administradores)	
Para cambiar los permisos, haga clic en Editar	
Persian de maria 2	
Permisos de usuano 2 Permitir Denegar	
Control total	
Modificar	
Lectura y ejecucion	
Locture d	
Lectura 🗸	
Lectura Escritura Permisos especiales	
Lectura Escritura Permisos especiales	
Lectura Escritura Permisos especiales Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas.)

Se selecciona el usuario2 y se establece el permiso de lectura desmarcando los demás.

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.

Se siguen los pasos de los anteriores apartados y tras eso se procede a modificar los permisos de la carpeta Examenes comenzando por cambiar los permisos de usuario2 presionando en mostrar permisos avanzados:

2025/08/12 16:47

9/12

Entrada de perr	niso para Examen		×
Entidad de segur	idad: usuario2 (MCBSW11\usuario2) Seleccionar una entida	id de seguridad	
Tipo:	Permitir		
Se aplica a:	Solo esta carpeta \sim		
Permisos básicos	s	Mostrar permisos avan	zados
	Control total		
	Aodificar		
	ectura y ejecución		
	Aostrar el contenido de la carpeta		
	ectura		
- E	scritura		
- P	ermisos especiales		
Aplicar estos p	permisos solo a objetos y/o contenedores dentro de este cont	enedor Borrar too	ob
0,	· · · · · · · · · · · · · · · · · · ·		
		Aceptar Can	celar

En "Se Aplica A" seleccionamos "Esta carpeta" y se procede a habilitar el permiso "Crear Carpetas / Anexar Datos":

Entrada de perr	miso para Examen		— D X
Entidad de segur	ridad: usuario2 (MCBSW11\usuario2) Selecc	onar una entidad de seguridad	
Тіро:	Permitir	\sim	
Se aplica a:	Solo esta carpeta	~	
Permisos avanza	idos:		Mostrar permisos básicos
	Control total	Escribir atributos	
<u> </u>	Atravesar carpeta / ejecutar archivo	🗌 Escribir atributos extendid	dos
N	Mostrar carpeta / leer datos	🗌 Eliminar subcarpetas y arc	chivos
🔽 L	eer atributos	🗌 Eliminar	
🔽 L	eer atributos extendidos	🔽 Permisos de lectura	
	Crear archivos / escribir datos	Cambiar permisos	
🔽 C	Crear carpetas / anexar datos	Tomar posesión	
Aplicar estos r	nermisos solo a obietos v/o contenedores de	tro de este contenedor	Borrar todo
- Aprical Catos p	permisos solo a objetos y/o contenedores del	to de este contenedor	
			Acentar Cancelar

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

Para dar control total sobre la carpeta y sus componentes a Usuario 2 se selecciona el permiso control total:

	o para Examen	— O X
Entidad de segurida	ad: usuario2 (MCBSW11\usuario2) Seleccionar una entidad de seguridad	
Тіро:	Permitir ~	
Se aplica a:	Esta carpeta, subcarpetas y archivos \checkmark	
Permisos básicos:		Mostrar permisos avanzados
Cont	trol total	
Mod	dificar	
Lecto	tura y ejecución	
	strar el contenido de la carpeta	
Escri	itura	
Pern	nisos especiales	
Aplicar estos perr	misos solo a objetos y/o contenedores dentro de este contenedor	Borrar todo

e) CIFRADO: Solo pueden acceder al contenido de un archivo cifrado los propietarios y los agentes de recuperación por defecto

Para cifrar la carpeta, en propiedades, se presiona en "Opciones Avanzadas":

General Compartir	Seguridad	Versiones anteriores	Personalizar
	Examen		
Tipo:	Carpeta de	archivos	
Ubicación:	C:N		
Tamaño:	0 bytes		
Tamaño en disco:	0 bytes		
Contiene:	1 archivos, 0 carpetas		
Creado:	miérc <mark>o</mark> les, 3	10 de abril de 202	36:21
Creado: Atributos:	miércoles, 3 Solo lectura	10 de abril de 202 (17); (solo para archivos de la	36:21 a carpeta)
Creado: Atributos:	miércoles, 3 Solo lectura Oculto	0 de abril de 202 i 11: (solo para archivos de la Opciones a	36:21 a carpeta) avanzadas)
Creado: Atributos:	miércoles, 3 Solo lectura Oculto	0 de abril de 202 i 17: (solo para archivos de la Opciones a	36:21 a carpeta) avanzadas)
Creado: Atributos:	miércoles, 3 Solo lectura Oculto	0 de abril de 202 (17); (solo para archivos de la Opciones a	36:21 a carpeta) avanzadas)
Creado: Atributos:	miércoles, 3 Solo lectura Oculto	0 de abril de 202 (17); (solo para archivos de la Opciones a	36:21 a carpeta) avanzadas)

Aparecerá una ventana en la que se debe marca la casilla de "Cifrar contenido para proteger datos":

Atributos avanzados	×
Elija la configuración deseada para esta carpeta. Si hace clic en Aceptar o Aplicar en el diálogo Propiedades preguntará si desea también aplicar los cambios en todas subcarpetas.	s, se le las
Atributos de índice y archivación	
Carpeta lista para archivarse	
Permitir que los archivos de esta carpeta tengan indizado el contenido además de las propiedades de archivo	
Atributos de compresión y cifrado	
Comprimir contenido para ahorrar espacio en disco	
Cifrar contenido para proteger datos Deta	les
Aceptar Car	icelar

Tras eso se presiona en aceptar y aplicar para realizar el cifrado, en este caso se va a cifrar tanto la carpeta como archivos y subcarpetas.

f) PROHIBIDO: El usuario2 no tiene acceso a esta carpeta, tampoco de lectura

Para bloquear completamente el acceso y lectura de una carpeta a usuario2 se le retiran todos los permisos:

2	ridad: usuario2 (MCBSW11\usuario2) Seleccionar u	na entidad de seguridad	
Тіро:	Permitir	\checkmark	
Se aplica a:	Esta carpeta, subcarpetas y archivos	~	
^o ermisos avanza	ados:		Mostrar permisos básico
Control total		Escribir atributos	
Atravesar carpeta / ejecutar archivo		 Escribir atributos extendidos 	
Mostrar carpeta / leer datos		Eliminar subcarpetas y archivos	
Leer atributos		🗍 Eliminar	
	Leer atributos extendidos	Permisos de lectura	
	Crear archivos / escribir datos	Cambiar permisos	
	Crear carpetas / anexar datos	Tomar posesión	
Aplicar estos	permisos solo a obietos v/o contenedores dentro de	este contenedor	Borrar todo

