PRÁCTICA 7

H- Verifica la auditoria de control de acceso "Visor de sucesos" de dicho usuario en Windows y Linux.

Windows ۲

Si un controlador no funciona o lo hace de forma defectuosa Windows incorpora el Visor de sucesos, que nos permite analizar qué es lo que ha ocurrido con el controlador que está causando problemas.

Si un controlador no funciona y quieres saber que ha pasado abre el visor de sucesos de la siguiente forma:

🕒 🔍 💌 💷 🕨 Panel de control 🕨 Todos los elementos de Panel de control 🕨 ▼ 4→ Buscar en el Panel de control <u>A</u>rchivo <u>E</u>dición <u>V</u>er <u>H</u>erramientas Ay<u>u</u>da Ajustar la configuración del equipo Ver por: Iconos pequeños 🔻
 Image: Second State State
 Image: Second State
 Administración del color Barra de tareas y menú Inicio Concession de KemoteApp y Escritorio
Concession de KemoteApp y Escrit Administrator de cloior
Administrator de catessis
Administrator de accesibilidad
Centro de accesibilidad
Centro de accesibilidad
Centro de accesibilidad
Conesón de RemoteApp y Escritorio
Configuración regional y de idiona
Gortor De parental
Copias de asguidad y restauración
Ocoreo
Coneco
Contro de RemoteApp y Escritorio
Contro de acusia

Haz clic sobre el botón Inicio y a continuación sobre Panel de Control.

Ahora debes hacer doble clic sobre el icono de Herramientas Administrativas y luego nuevamente doble clic sobre el icono Visor de Sucesos.

hivo <u>E</u> dición ⊻er	<u>H</u> erramientas Ay <u>u</u> da				
rganizar 👻 🔳 Abri	r				H • 🔟 🌔
Favoritos	Nombre	Fecha de modifica	Тіро	Tamaño	
🗼 Descargas	Administración de equipos	14/07/2009 6:41	Acceso directo	2 KB	
📃 Escritorio	Administración de impresión	21/08/2010 17:50	Acceso directo	2 KB	
Sitios recientes	🐻 Configuración del sistema	14/07/2009 6:41	Acceso directo	2 KB	
	📷 Diagnóstico de memoria de Windows	14/07/2009 6:41	Acceso directo	2 KB	
Bibliotecas	🗟 Directiva de seguridad local	21/08/2010 17:50	Acceso directo	2 KB	
Documentos	🔊 Firewall de Windows con seguridad avan	14/07/2009 6:41	Acceso directo	2 KB	
📔 Imágenes	🙈 Iniciador iSCSI	14/07/2009 6:41	Acceso directo	2 KB	
👌 Música	Monitor de rendimiento	14/07/2009 6:41	Acceso directo	2 KB	
🚼 Videos	🔊 Orígenes de datos ODBC	14/07/2009 6:41	Acceso directo	2 KB	
	😥 Programador de tareas	14/07/2009 6:42	Acceso directo	2 KB	
🝓 Grupo en el hogar	Servicios de componentes	14/07/2009 6:46	Acceso directo	2 KB	
	Servicios	14/07/2009 6:41	Acceso directo	2 KB	
Equipo	🛃 Visor de eventos	14/07/2009 6:42	Acceso directo	2 KB	
🛍 Disco local (C:)	😿 Windows PowerShell Modules	14/07/2009 6:52	Acceso directo	3 KB	
Red					

A continuación verás una ventana en la se registran todos los sucesos de Windows, y también verás si alguno de ellos está fallando.

Ahora si haces doble clic sobre el controlador que marca el error, accederás a otra ventana en la muestra la causa del error.

Visor de eventos		-		Contractory of			Hind M. specification. 1 Tree & second satisfies. 1 Washington advances of	and the second second	tage fragment fragment in the Contract	х	
Archivo Acción Yer Ayyda											
(n n n n n n n n n n n n n n n n n n n											
Visor de eventos (local)	Visor de eventos (local)		Acciones								
Vistas personalizadas			Visor de eventos (local)								
Registros de Windows	introduccion y resu	men					Ultima actualización: 08/11/2011 23/s	5.50	Abrir registro guardado	_	
Suscripciones	Introducción		Crear vista nersonalizada								
	Para ver los eventos	Para ver los eventos que se produjeron en el equipo, seleccione el nodo adecuado de vista personalizada, registro u origen en el árbol de la consola. La vista personalizada Eventos administrativos contiene todos los eventos administrativos,									
	independientement	independientemente del origen. A continuación, se muestra una vista agregada de todos los registros.									
			Conectarise a outo equipo	-							
	Resumen de eventos admini-		ver								
			G Actualizar								
	Tipo de evento Id. del	e Origen	Registro	Última hora	24 horas	7 dias			Ayuda	•	
	E Critico -			0	1	1					
	EE Error -			0	5	13					
	Advertencia -			0	11	33					
	Información -			9	440	1.020					
	Ut Auditoria cor			0	109	386					
	tti Error de audit			0	1	1					
								- 1			
	Nodor vistor regisotemente		-								
	House have recenterion	-									
	Nombre	Descripción	Modificado	Creado				1			
								112			
								112			
								112			
								112			
								112			
								- 11 2			
								- 11 2			
								<u> </u>			
	Kesumen de registro										
	Nombre de registro	Tamaño (Modificado	Habilitado	Directiva d	e retención		-			
	Aplicación	8.07 MB/2	08/11/2011 15:45-25	Habilitado	Sobrescelle	ir eventos si f			1		
	Eventos de hardware	68 KB/20	21/08/2010 17:50:41	Habilitado	Sobrescrib	ir eventos si f.		6 H Z			
	Internet Explorer	68 KB/1.0	21/08/2010 17:50:41	Habilitado	Sobrescrib	ir eventos și f.					
	Key Management Service	68 KB/20	21/08/2010 17:50:41	Habilitado	Sobrescrib	ir eventos si f.					
	Media Center	68 KB/8 MB	21/08/2010 17:50:41	Habilitado	Sobrescrib	ir eventos si f.					
	Microsoft Office Diagnos.	68 KB/16	21/08/2010 23:06:16	Habilitado	Sobrescrib	ir eventos si f.					
	Microsoft Office Sessions	1,07 M8/1	08/11/2011 15:49:39	Habilitado	Sobrescrib	ir eventos si f.					
	Seguridad	20,00 MB/	08/11/2011 15:45:24	Habilitado	Sobrescrib	ir eventos si f.					
	Sistema	20,00 MB/	08/11/2011 15:45:24	Habilitado	Sobrescrib	ir eventos si f.					
								- 1			
×									1		

Por ejemplo si un usuario intenta tener acceso a una unidad de red y se produce un error, ese intento se registra como Acceso Erróneo Auditado.

Visor de eventos	_	_			_	_	_	rannahorent Manthedran. Som ales out. Boards fann tel		
Archivo Acción Yer Ayyda										
4 4 🖂 🖬 🖬										
Visor de eventos (local)	Visor de eventos Bocal		Acciones							
> 📑 Vistas personalizadas	Introducción v resumen									Visor de eventos (local)
Registros de Windows	Utima estadoreiro 00/1/2012253-07									Abrir registro guardado
Suscipciones	Introducción .								11	Crear vista personalizada
	Para ver los exentos que se produjeron en el equipo, seleccione el nodo adecuado de vista personalizada, registro u origen en el ábol de la consola. La vista personalizada Eventos administrativos contienes todos los eventos administrativos, independientemente del origen. A continuación, se muestra una vista agregada de todos los registros.									Importar vista personalizada
										Conectanie a otro equipo
										Ver b
	Resumen de evertos administrativos .									Actualizar
	Terrelevante Melder Merre Barley (Merrelevan Merrel 7 Mer									handa h
	Tipo de evento	all del e	Orgen	Kegetro	Ottema hora	24 horas	7 dias		14	L Ayou F
	Efror				0	5	13			Error 🔺
		3	Windows Activ	Aplicación	0	0	1	1		Ver todas las instancias de este evento
		13	VSS	Aplicación	0	1	1			Ayuda
		35	volsnap	Sistema	0	0	1			
		1002	Dhop-Client	Microsoft	0	ő	î			
		4103	Winlogon	Aplicación	0	1	1			
		6008	EventLog	Sistema	0	1	1			
	Nodos vistos recientemente +									
	Nombre Descripción Medificado Creado									
	Barris de contrar									
	Navannen de registro								4	
	Nombre de registro	Tar	meño (Modifi	icado	Habilitade	Directiva d	e retención	8		
	Aplicación	8,0	7 MB/2 08/11/	2011 15:45:25	Habilitade	Sobrescrib	r eventos si f			
	Eventos de hardwar	re 68	KB/20 21/08/	2010 17:50:41	Habilitade	Sobrescrib	r eventos si f			
	atternet Explorer	68 (anica 68)	NB/1/0 21/08/ NB/20 21/08/	2010175041	Habilitade	Sotrescrib	r eventos sit			
	Media Center	68	KB/8 MB 21/08/	2010 17:50:41	Habilitade	Sobreacrib	eventos si f			
	Microsoft Office Di	agnos 68	KB/16 21/08/	2010 23:06:16	Habilitade	Sobrescrib	r eventos si f			
	Microsoft Office Se	ssions 1,0	7 MB/1 08/11/	2011 15:49:39	Habilitade	Sobrescrib	r eventos si f			
	Segurided	20)	00 MB/ 08/11/	2011 15:45:24	Habilitade	Sobrescrib	r eventos si f			
	osterná	20)	00 MB/ 08/11/	2011 15:85:24	HISTORIA	sourcescrib	evensos si t			
* * *										

• <u>Ubuntu</u>

Para acceder al visor de sucesos en Ubuntu, nos situamos en Administración, Visor de archivos de sucesos.



En **auth.log1** podemos ver los accesos de los usuarios en diferentes días, con esta técnica podemos controlar todo tipo de accesos y posibles ataques a nuestro sistema de gente que no teníamos prevista su acceso.

