Bellator User Manual

1. INTRODUCCIÓN.

Bellator is an IT systems audit tool based on predefined security templates.

Therefore the *Bellator* intention is to check if the parameters included in the templates are applied and review its deployment status.

Bellator can be used to audit an IT system after apply the secure configuration or in a scheduled manner to know the secure configuration fulfillment and to find out if any no declared modification has occurred.

There are two types of templates:

- Security Local Policy, of which extension is .INF.
- Security Administrative Templates (within the Local Computer Directive, both the Computer Configuration and the User Configuration), of which extension is .POL.

The Security Local Policy template can be obtained in two ways:

- Through Microsoft, thanks to its secure configuration guides, the templates (.INF) to check can be downloaded.
- Exporting from a previously secure configured system, (secedit /export /cfg [*filename.inf*]), in this way it could be checked scheduled any modification in the initial configuration.

The Security Administrative Templates can be obtained from the secure configured system Group Policy folder.

In addition the information related to the previously exposed templates, the *Bellator* audit tool shows other interesting data as users, groups, operating system details, service packs, partitions, disk space and RAM memory.

2. USERS MANUAL

a. Requirements

To work properly *Bellator* require the Microsoft tool "<u>SubInACL.exe</u>" to obtain security information about files, registry keys, and services in <u>SDDL</u> (<u>Security Descriptor Definition Language</u>).

It is also essential to have the library msvcr70.dll in the audited system, which is a module which contains functions of the C standard library.

Both files are are integrated in the *Bellator* executable, if not, they should be included in the same folder.

Bellator requires as input the templates (INF and POL) which previously have been described. It is essential to rename the files as:

- **Template.inf**. As the Security Local Policy.
- **RegistryM.pol** and **RegistryU.pol**. As computer administrative configuration template and user administrative configuration template respectively.

Bellator has been tested in standalone computers which do not belong to any domain (Windows Server/Professional eng and spa, and Windows XP Professional eng and spa).

The most of the functions work properly over computers which belong to any domain, specifically those local related parameters. All the policies different to registry parameters could not work properly due to it has not been tested in domain computers.

Nowadays it is going tested correctly in Windows 2003.

b. Execution

After the configuration the *Bellator*.exe shall be executed.

Bellator will ask if the user wants a detailed report with the data obtained, in addition to the results report generated anyway.

Bellator v.1.5		×
Do you want a	detailed report (a	allResult.txt)?.
Yes	No	Cancel

When finish *Bellator* notify user the correct execution, as well as reports name.

Bellator v.1.5
Program finished. Results in file: "Bellator_22042010.txt" and "AllResult_Bellator_22042010.txt".
By Ricardo Ramos (rramosg@gmail.com)
ОК

c. Security Local Directive templates structure

Security template must have a specific format, grouping each audit module according to specific labels (i.e. [Application Log]):

```
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 3
AuditPrivilegeUse = 2
AuditPolicyChange = 1
[Service General Setting]
Alerter,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRR
C;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCLCSWLOCRRC;;;AU)S:(AU;FA;CC
DCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
CiSvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC
;;;IU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCLCSWLOCRRC;;;AU)S:(AU;FA;CCD
CLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
```

They are listed below:

• [System Log], [Security Log], [Application Log]: System, Security and application Events.

Acción Ver 🛛 🗢 🔿 🖻	1 🖬 😭 🔂	l 😫						
rbol	Security Log	91.548 sucesos						
Visor de sucesos (local)	Тіро	Fecha	Hora	Origen	Categoría	Suceso	Usuario	E
Application Log	😽 Aciertos	20/04/2010	16:56:58	Security	Seguimie	593	Admin	E
🕖 Security Log	😽 Aciertos	20/04/2010	16:56:58	Security	Seguimie	592	Admin	E
System Log	😽 Aciertos	20/04/2010	16:56:53	Security	Seguimie	593	Admin	E
	😽 Aciertos	20/04/2010	16:56:53	Security	Seguimie	592	Admin	E
	😽 Aciertos	20/04/2010	16:56:48	Security	Seguimie	593	Admin	E
	😽 Aciertos	20/04/2010	16:56:47	Security	Seguimie	592	Admin	E
	😽 Aciertos	20/04/2010	16:56:42	Security	Seguimie	593	Admin	E
	😽 Aciertos	20/04/2010	16:56:42	Security	Seguimie	592	Admin	E
	😽 Aciertos	20/04/2010	16:56:37	Security	Seguimie	593	Admin	E
	😽 Aciertos	20/04/2010	16:56:36	Security	Seguimie	592	Admin	E
	😽 Aciertos	20/04/2010	16:56:31	Security	Seguimie	593	Admin	E
	😽 Aciertos	20/04/2010	16:56:31	Security	Seguimie	592	Admin	E
	😽 Aciertos	20/04/2010	16:56:26	Security	Seguimie	593	Admin	E
	dciertos	20/04/2010	16:56:26	Security	Seguimie	592	Admin	E
	😽 Aciertos	20/04/2010	16:56:21	Security	Seguimie	593	Admin	E
	Aciertos	20/04/2010	16:56:21	Security	Seguimie	592	Admin	E
	💰 Aciertos	20/04/2010	16:56:16	Security	Seguimie	593	Admin	E
	😽 Aciertos	20/04/2010	16:56:16	Security	Seguimie	592	Admin	E
	Aciertos	20/04/2010	16:56:10	Security	Seguimie	593	Admin	E
	•							۱.

• [Event Audit]: Audit directive.

📑 Local Security Settings			<u>-0×</u>
$ $ Acción Ver $ \Leftarrow \Rightarrow $ \textcircled{E} $\boxed{\blacksquare} \times \textcircled{E} $			
Árbol	Directiva 🔺	Configuración local	Configuración vigente
Configuración de seguridad	Auditar el acceso a objetos	Correcto, Erróneo	Sin auditoría
🖻 📴 Directivas de cuenta	Auditar el acceso del servicio de di	Sin auditoría	Sin auditoría
😟 📴 Directiva de contraseñas	👸 Auditar el cambio de directivas	Sin auditoría	Correcto, Erróneo
😥 🧰 Directiva de bloqueo de cuentas	Auditar el seguimiento de procesos	Sin auditoría	Correcto, Erróneo
🖻 记 Directivas locales	Auditar el uso de privilegios	Sin auditoría	Sin auditoría
🕀 🧰 Directiva de auditoría	🔀 Auditar la administración de cuentas	Sin auditoría	Correcto, Erróneo
🕀 📴 Asignación de derechos de usuario	👸 Auditar sucesos de inicio de sesión	Sin auditoría	Correcto, Erróneo
庄 📴 Opciones de seguridad	Auditar sucesos de inicio de sesión	Sin auditoría	Correcto, Erróneo
😟 💼 Directivas de claves públicas	👸 Auditar sucesos del sistema	Sin auditoría	Correcto, Erróneo
🗄 🗏 Directivas de seguridad IP en Máquina local			
	•		
, 			
		1	J

• [Service General Setting]: Security information about the system services.

🚡 Consola1 - [Raíz de la cor	nsola\Configuración y análisis	de seguridad\!	Servicios del sisten	na]		
🛛 🚡 Consola Ventana Ayy	īda] 🗅 🖻 🖬	🗉 💷 🗵
<u>A</u> cción <u>V</u> er <u>F</u> avoritos	⇔ → € 🖪 × 🖳	E ²				
Árbol Favoritos	Nombre de servicio 🛛 🛆	Inicio	Permiso			
Configuración y análisis Configuración y análisis Directivas de cuent Directivas locales Configuración y análisis Configuración y análisis Directivas locales Configuración y análisis Configuración y análisis	 Actualizaciones automáticas AgentInstallationService Alerter Application Management ASP.NET State Service Background Intelligent Tran ClipBook COM+ Event System Computer Browser Coordinador de transaccion DHCP Client Distributed Link Tracking Client DISC Client Event Log Fax Service IBM Trace Facility Internet Connection Sharing IPSEC Policy Agent Logical Disk Manager Logical Disk Manager McAfee McShield McAfee Task Manager Messenger 	No está def No está def Aceptar No está def Aceptar No está def Aceptar No está def Aceptar Aceptar Aceptar Aceptar No está def No está def	No está def No está def Aceptar No está def Aceptar No está def Aceptar No está def Aceptar Aceptar Aceptar No está def No está def No está def Aceptar No está def Aceptar No está def Aceptar No está def No está def No está def No está def No está def No está def			
۲	Microsoft Telnet Service	No está def	No está def			-
	** **					

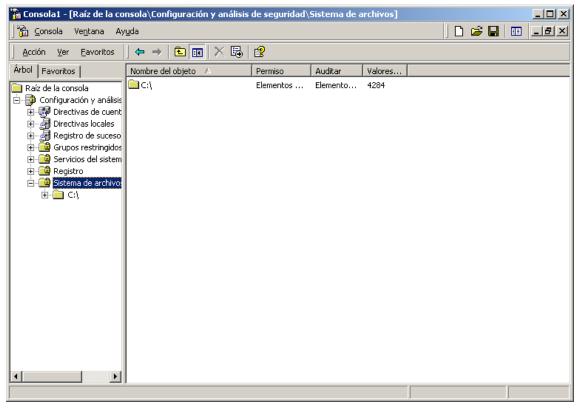
• [Privilege Rights]: User Privilege Rights.

Local Security Settings Acción ⊻er 🗢 → 🗈 📧 🗙 🚱 🔮			
rbol	Directiva 🛆	Configuración local	Configuración vigente
Configuración de seguridad	Act as part of the operating system	*S-1-5-21-1248158	*S-1-5-21-1248158
Directivas de cuenta	👸 Add workstations to domain		
🗄 🛄 Directiva de contraseñas	Back up files and directories	Backup Operators,	Backup Operators,
🗄 💼 Directiva de bloqueo de cuentas	Bypass traverse checking	Backup Operators,P	Backup Operators,P
🗆 🧰 Directivas locales	👸 Change the system time	Power Users, Admini	Power Users, Admini
🕂 🧰 Directiva de auditoría	👪 Create a pagefile	Administrators	Administrators
🕂 🧰 Asignación de derechos de usuario	📖 Create a token object		
🗄 🧰 Opciones de seguridad	📖 Create global objects	SERVICE, Administra	SERVICE, Administra
Directivas de claves públicas	Create permanent shared objects		
🖂 🛃 Directivas de seguridad IP en Máquina local	B Debug programs	Administrators	Administrators
	Denegar el acceso desde la red a		
	BDenegar el inicio de sesión como s		
	Denegar el inicio de sesión como tr		
	Denegar el inicio de sesión localme	ECD15302\ASPNET	ECD15302\ASPNET
	Enable computer and user account		
	Force shutdown from a remote sy	Administrators	Administrators
	Generate security audits		
	Impersonate a client after authent	Administrators, SER	Administrators, SER
	Increase quotas	*5-1-5-21-1248158	*5-1-5-21-1248158
	Increase scheduling priority	Administrators	Administrators
	Iniciar sesión como proceso por lotes	SYSTEM.ECD15302\	SYSTEM, ECD15302\
	Iniciar sesión como servicio	*5-1-5-21-1248158	*5-1-5-21-1248158
	Inicio de sesión local	*5-1-5-21-1248158	*5-1-5-21-1133456
	Load and unload device drivers	Power Users, Admini	Power Users, Admini
	ELOCK pages in memory		
	Manage auditing and security log	Administrators	Administrators
	Modify firmware environment values		Administrators
	Profile single process	Power Users, Admini	Power Users.Admini
	Profile system performance	Administrators	Administrators
	Remove computer from docking st		Power Users, Users,
	Replace a process level token	*5-1-5-21-1248158	*5-1-5-21-1248158

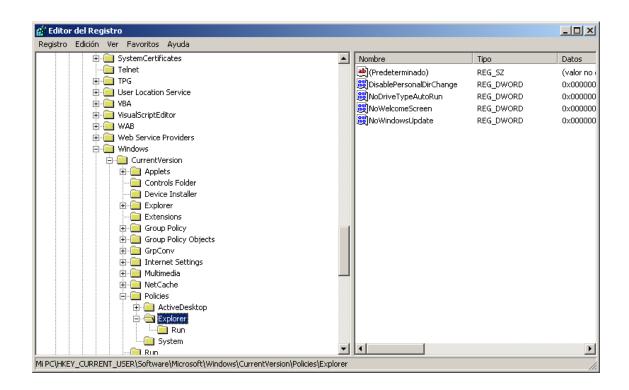
• [Registry Keys]: Rights over system registry keys.

🚡 <u>C</u> onsola Ve <u>n</u> tana Ay <u>u</u> da				🗋 🖬	ê 🔒 🔲 💷
Acción Ver Eavoritos $4 \Leftrightarrow \Rightarrow 1$	🔲 🛛 🕹 🔒				
rbol Favoritos	Nombre del objeto 🛛 🛆	Permiso	Auditar	Valores	
Raíz de la consola	1 😥 Arbiters	Aceptar	Aceptar	0	
🕞 Configuración y análisis de seguridad 🦷	👔 😥 BackupRestore	Aceptar	Aceptar	0	
🗄 🗊 Directivas de cuenta	Biosinfo	Aceptar	Aceptar	0	
🗄 📲 Directivas locales	BootVerificationProgram	Aceptar	Aceptar	0	
🗄 🛃 Registro de sucesos	Class	Aceptar	Aceptar	0	
🗄 🔂 Grupos restringidos	CoDeviceInstallers	Aceptar	Aceptar	0	
🗄 🔂 Servicios del sistema	COM Name Arbiter	Aceptar	Aceptar	0	
🛱 📴 Registro	ComputerName	Aceptar	Aceptar	0	
E 🔐 🙀 CLASSES_ROOT	ContentIndex	Aceptar	Aceptar	0	
	ContentIndexCommon	Aceptar	Aceptar	0	
🕀 🎬 HARDWARE	CrashControl	Aceptar	Aceptar	0	
🗄 🎬 SAM	CriticalDeviceDatabase	Aceptar	Aceptar	0	
SECURITY	DeviceClasses	Aceptar	Aceptar	0	
	FileSystem	Aceptar	Aceptar	0	
⊡- 📸 SYSTEM ⊡- ử ControlSet001	GraphicsDrivers	Aceptar	Aceptar	0	
ControlSet001 ControlSet002	GroupOrderList	Aceptar	Aceptar	0	
E A ControlSet002	HAL .	Aceptar	Aceptar	0	
	📸 hivelist	Aceptar	Aceptar	0	
		Aceptar	Aceptar	0	
Enum	Keyboard Layout	Aceptar	Aceptar	0	
	Keyboard Layouts	Aceptar	Aceptar	0 0	
⊕ 💮 Services	Color Color Color Color	Aceptar	Aceptar	4	
	MediaCategories	Aceptar	Aceptar	0	
🕀 📸 Select 📃	MediaInterfaces	Aceptar	Aceptar	0	

• [File Security]: System file security rights.



• [Registry Values]: System Registry Keys values. It is related to security options from the configuration guide.



For the moment *Bellator* do not cover the [System Access] Account Directives.

d. Security Administrative Templates Structure

The RegistryM.pol and RegistryU.pol must fulfill the <u>ABNF</u> format. It must not be modified with a text editor due to it is in a hexadecimal format and could contains special characters.

3. COLLABORATIONS

Bellator is a project started time ago and it is the result of the effort realized by its author, but it counts with collaborations in the different parts of the projects, people who the author wants to thank for their altruist support.

They are:

Manuel Rodríguez. In charge of coordinate the *Bellator* test over different systems and environments.

Serg. For his contributions and his *commercial actions*.

Yago Molina. For his invaluable help, helping to start in the Windows programming world.

Any other partner/friend/colleague by its ideas and something more.

4. CONTACT

For any suggestion, error, criticism (constructive) or simply for any question related to *Bellator*, you can use the e-mail address <u>Bellator.audit@gmail.com</u>.

Thanks a lot. Ricardo.