

Report title: System access granted/removed

Description: The report is based on the 621 and 622 events. The events signal the fact that a user was granted access to a system or user system access was removed. Check User Name and Account Modified, particularly if access permission is interactive. Event 622 might indicate that an attacker removed evidence of event 621 (system access granted to user account) in order to cover the trails, or is attempting to deny service to some other account(s).

Generated on: 13-Sep-2006 16:32

Generated by: Calin

Date filter: 9/7/2006 12:00:00AM to 9/13/2006 11:59:59PM

Event logs: Security

Other filters: event ID= 621 from Security log
and event ID= 622 from Security log

Reviewed by: _____

Reviewed date: _____

Signature: _____

Account modified	By User	Event Description	Time	Date
GFITEMASOFT\pisu	GFITEMASOFT\FSERVER\$	System Access was granted to account	1:49:29PM	9/8/2006
GFITEMASOFT\calin	GFITEMASOFT\calin	System Access was granted to account	2:10:38PM	9/8/2006
GFITEMASOFT\calin	GFITEMASOFT\FSERVER\$	System Access was granted to account	2:31:50PM	9/8/2006
GFITEMASOFT\IUSR_FSERVER	GFITEMASOFT\administrator	System Access was granted to account	2:51:27PM	9/8/2006
GFITEMASOFT\IUSR_FSERVER	GFITEMASOFT\administrator	System Access was granted to account	2:51:28PM	9/8/2006
GFITEMASOFT\IWAM_FSERVER	GFITEMASOFT\administrator	System Access was granted to account	2:51:42PM	9/8/2006
GFITEMASOFT\IWAM_FSERVER	GFITEMASOFT\administrator	System Access was granted to account	2:51:43PM	9/8/2006
GFITEMASOFT\IIS_WPG	GFITEMASOFT\administrator	System Access was granted to account	2:51:55PM	9/8/2006
GFITEMASOFT\IUSR_FSERVER	GFITEMASOFT\FSERVER\$	System Access was granted to account	3:13:31PM	9/8/2006
GFITEMASOFT\pisu	GFITEMASOFT\FSERVER\$	System Access was removed for account	11:45:14PM	9/8/2006
GFITEMASOFT\pisu	GFITEMASOFT\FSERVER\$	System Access was granted to account	1:49:29PM	9/12/2006
GFITEMASOFT\calin	GFITEMASOFT\calin	System Access was granted to account	2:10:38PM	9/12/2006
GFITEMASOFT\calin	GFITEMASOFT\FSERVER\$	System Access was granted to account	2:31:50PM	9/12/2006
GFITEMASOFT\IUSR_FSERVER	GFITEMASOFT\administrator	System Access was granted to account	2:51:27PM	9/12/2006
GFITEMASOFT\IUSR_FSERVER	GFITEMASOFT\administrator	System Access was granted to account	2:51:28PM	9/12/2006
GFITEMASOFT\IWAM_FSERVER	GFITEMASOFT\administrator	System Access was granted to account	2:51:42PM	9/12/2006
GFITEMASOFT\IWAM_FSERVER	GFITEMASOFT\administrator	System Access was granted to account	2:51:43PM	9/12/2006
GFITEMASOFT\IIS_WPG	GFITEMASOFT\administrator	System Access was granted to account	2:51:55PM	9/12/2006
GFITEMASOFT\IUSR_FSERVER	GFITEMASOFT\FSERVER\$	System Access was granted to account	3:13:31PM	9/12/2006
GFITEMASOFT\pisu	GFITEMASOFT\FSERVER\$	System Access was removed for account	11:45:14PM	9/12/2006
GFITEMASOFT\pisu	GFITEMASOFT\FSERVER\$	System Access was granted to account	1:49:29PM	9/13/2006
GFITEMASOFT\calin	GFITEMASOFT\calin	System Access was granted to account	2:10:38PM	9/13/2006
GFITEMASOFT\calin	GFITEMASOFT\FSERVER\$	System Access was granted to account	2:31:50PM	9/13/2006
GFITEMASOFT\IUSR_FSERVER	GFITEMASOFT\administrator	System Access was granted to account	2:51:27PM	9/13/2006
GFITEMASOFT\IUSR_FSERVER	GFITEMASOFT\administrator	System Access was granted to account	2:51:28PM	9/13/2006
GFITEMASOFT\IWAM_FSERVER	GFITEMASOFT\administrator	System Access was granted to account	2:51:42PM	9/13/2006
GFITEMASOFT\IWAM_FSERVER	GFITEMASOFT\administrator	System Access was granted to account	2:51:43PM	9/13/2006
GFITEMASOFT\IIS_WPG	GFITEMASOFT\administrator	System Access was granted to account	2:51:55PM	9/13/2006
GFITEMASOFT\IUSR_FSERVER	GFITEMASOFT\FSERVER\$	System Access was granted to account	3:13:31PM	9/13/2006
GFITEMASOFT\pisu	GFITEMASOFT\FSERVER\$	System Access was removed for account	11:45:14PM	9/13/2006