

Report title: Failed attempts to access files and registry keys

Description: The report is based on events 560 and 565 with type failure audit. These events show when an object has rejected access to a request, such as list, read, create, and delete. The reports shows failed attempts to access files or registry and does not include normal system activity. Note that for best results, file auditing is required to be enabled on the files and registry values of interest. Use the report to identify users who are trying to access resources they are not granted access to.

Generated on: 13-Sep-2006 16:33

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= 560 from Security log and type= 'audit failure'
and event ID= 567 from Security log and type= 'audit failure'
,User Name not equal to NT AUTHORITY\SYSTEM

Reviewed by: _____

Reviewed date: _____

Signature: _____

Computer	User	Event ID	Description	Object Name	Object Type	Time	Date
FSERVER	GFITEMASOFT\pisu	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	3:05:00PM	9/8/2006
FSERVER	GFITEMASOFT\pisu	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	3:05:00PM	9/12/2006
FSERVER	GFITEMASOFT\pisu	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	3:05:00PM	9/13/2006