

Report title: Account lockouts report

Description: The report is based on the 644 and 12294 events. The 644 event signals the fact that a user account has locked out because the number of sequential failed logon attempts is greater than the account lockout limit. The 12294 event indicates a possible brute force attack against the default Administrator account. Because this account does not lock out, the system event logs records SAM event 12294 instead. Investigate even a single occurrence of this event immediately, because this can also indicate the presence of an unauthorized operating system.

Generated on: 13-Sep-2006 16:28

Generated by: Calin

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

Event logs: Security, System

Other filters: event ID= 644 from Security log
and event ID= 12294 from System log with source 'SAM'

Reviewed by: _____

Reviewed date: _____

Signature: _____

Computer	User	Event ID	Description	Account	Logon Type	Time	Date
FSERVER	GFITEMASOFT\FSERVER\$	644	User Account Locked Out	Administrator	N/A	12:18:13AM	9/8/2006
FSERVER	GFITEMASOFT\FSERVER\$	644	User Account Locked Out	Administrator	N/A	1:32:41AM	9/8/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	12:01:42PM	9/8/2006
FSERVER	GFITEMASOFT\FSERVER\$	644	User Account Locked Out	pisu	N/A	2:26:04PM	9/8/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	3:34:59PM	9/8/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	3:35:44PM	9/8/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	5:01:09PM	9/8/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	5:08:33PM	9/8/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	5:14:54PM	9/8/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	5:47:21PM	9/8/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	5:50:54PM	9/8/2006
FSERVER	GFITEMASOFT\FSERVER\$	644	User Account Locked Out	Administrator	N/A	7:54:55PM	9/8/2006
FSERVER	GFITEMASOFT\FSERVER\$	644	User Account Locked Out	Administrator	N/A	12:18:13AM	9/12/2006
FSERVER	GFITEMASOFT\FSERVER\$	644	User Account Locked Out	Administrator	N/A	1:32:41AM	9/12/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	12:01:42PM	9/12/2006
FSERVER	GFITEMASOFT\FSERVER\$	644	User Account Locked Out	pisu	N/A	2:26:04PM	9/12/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	3:34:59PM	9/12/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	3:35:44PM	9/12/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	5:01:09PM	9/12/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	5:08:33PM	9/12/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	5:14:54PM	9/12/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	5:47:21PM	9/12/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	5:50:54PM	9/12/2006
FSERVER	GFITEMASOFT\FSERVER\$	644	User Account Locked Out	Administrator	N/A	7:54:55PM	9/12/2006
FSERVER	GFITEMASOFT\FSERVER\$	644	User Account Locked Out	Administrator	N/A	12:18:13AM	9/13/2006
FSERVER	GFITEMASOFT\FSERVER\$	644	User Account Locked Out	Administrator	N/A	1:32:41AM	9/13/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	12:01:42PM	9/13/2006
FSERVER	GFITEMASOFT\FSERVER\$	644	User Account Locked Out	pisu	N/A	2:26:04PM	9/13/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	3:34:59PM	9/13/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	3:35:44PM	9/13/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	5:01:09PM	9/13/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	5:08:33PM	9/13/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	5:14:54PM	9/13/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	5:47:21PM	9/13/2006
TESTSTATION	TESTING0\TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	5:50:54PM	9/13/2006
FSERVER	GFITEMASOFT\FSERVER\$	644	User Account Locked Out	Administrator	N/A	7:54:55PM	9/13/2006