

Re: too many logon/logoff events in security log

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2004-11/0271.html>

From: Anthony Yates (anthonyDINGyates_at_airDONGdesk.com)

Date: 11/26/04

Date: Fri, 26 Nov 2004 12:10:08 -0000

Logging Success events is impractical, unless you have a system to manage your event logs. Logging Failures should be enough,
Anthony

"Trevor" <news_register@yahoo.com.hk> wrote in message
news:evD0jRq0EHA.1296@TK2MSFTNGP10.phx.gbl...
> *I am using windows 2003 server, IIS 6 and sql 2000 server. fyi!*
>
> *"microsoft newsgroup" <news_register@yahoo.com.hk>*
> *¼¶¼g©ó¶¶¥ó·s»D:eN8sbIq0EHA.3808@tk2msftngp13.phx.gbl...*
> > *Hi, all,*
> >
> > *I turn on the audit policy to monitor the logon/logoff envents in*
security
> > *log. However, there is too many logon/logoff events, average 3 times per*
> > *minute. sometimes the logon/logoff by systems user, sometimes by*
> > *administrators. I have not idea to troubleshoot this event. I capture*
the
> > *logs detail as below:*
> >
> >
> > *User Logoff:*
> > *User Name: ITRA\$*
> > *Domain: ITRANET0*
> > *Logon ID: (0x0,0x105A389)*
> > *Logon Type: 3*
> >
> >
> > *Successful Network Logon:*
> > *User Name: ITRA\$*
> > *Domain: ITRANET0*
> > *Logon ID: (0x0,0xD3FD88)*
> > *Logon Type: 3*
> > *Logon Process: Kerberos*
> > *Authentication Package: Kerberos*
> > *Workstation Name:*
> > *Logon GUID: {d4e327c2-d024-f080-3e0b-1d7c89e9e484}*
> > *Caller User Name: -*

microsoft.public.windows.server.security: Re: too many logon/logoff events in security log

> > *Caller Domain:* –
> > *Caller Logon ID:* –
> > *Caller Process ID:* –
> > *Transited Services:* –
> > *Source Network Address:* 127.0.0.1
> > *Source Port:* 4644
> >
> > *Any idea or am I be hacked? why the source network address is the server
> > itself but the logon type is 3.*
> >
> > *Thanks you very much advance!*
> >
> > *Regards,*
> > *Trevor*
> >
>
>