

Re: Writing to Windows Security Log

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-12/0033.html>

From: Adrien de Beaupre (adrien.debeaupre@elytra.com)

Date: 12/07/01

From: "Adrien de Beaupre" <adrien.debeaupre@elytra.com>

To: <pen-test@securityfocus.com>

Date: Fri, 7 Dec 2001 16:35:22 -0500

While not exactly what you are looking for this tool can selectively remove entries from the NT/2K event log. Does not work remotely and requires admin access.

<http://www.ntsecurity.nu/toolbox/winzapper/>

From his FAQ:

Q: Is it possible to add your own "made up" event records to the log?

A: Yes, that's possible, but I haven't added that feature because I think it's too nasty. ;-)

You could insert completely "made up" records anywhere in the log.

Adrien

----- Original Message -----

From: "Tina Bird" <tbird@precision-guesswork.com>

To: "Mr Rufus Faloofus" <foofus@foofus.net>

Cc: <pen-test@securityfocus.com>; <jon.bull@knowledgelinks.com>; <marvin.marin@eds.com>; <tbird@precision-guesswork.com>

Sent: Wednesday, December 05, 2001 4:16 PM

Subject: Re: Writing to Windows Security Log

> *Let me provide more details.*

>

> *We all understand that one of the big problems with*
> *UNIX syslog—the-network-protocol is that it's UDP –*
> *not authenticated, not reliable. An evildoer who*
> *wants to make my logs less trustworthy can easily*
> *send bogus data to my central loghost, at a minimum*
> *introducing nonsense into my audit stream, and at*
> *a maximum, knocking the loghost off line.*

>

> *As explained below, a Windows application or service*
> *that registers itself with the Event Log service can*
> *write messages to the Windows System and Application*
> *Logs. So one way for me to introduce a roughly*

SecurityFocus Penetration: Re: Writing to Windows Security Log

> equivalent source of bogus data into an Event Log stream
> is to register an illegitimate application with
> associated DLL with the Event Log service. I expect
> that's a relatively straightforward thing to do, given
> how easy it is to install back doors on Windows boxes --
> although one doesn't typically write back doors with lots
> of logging capabilities, it might make sense to create
> a program that muddied up the logs.
>
> However, the only things on a Windows box that can write
> to the >Security< Event Log are the LSA and the Event
> Log service itself, which have the SeAuditPrivilege.
> This suggests that the Security Event Log has a much
> higher level of assurance than anything in the off-the-shelf
> UNIX world.
>
> This conclusion startled me ;-) so I figured I'd ask this
> group if anyone knew of a tool that would get around
> this access restriction. Does that clarify what I'm
> after?
>
> thanks -- tbird
>
> On Wed, 5 Dec 2001, Mr Rufus Faloofus wrote:
>
>> At 07:26 PM 12/4/01 -0600, Tina Bird wrote:
>>> >Anyone out there have a tool that allows me to
>>> >forge Windows Security Event Log data?
>>
>> Depends what you mean by "forge," and what kind of access
>> you have to the machine. To log an event, the Right Way is
>> to register a DLL with your messages in it. It's not hard
>> (see LOGEVENT.EXE from the resource kit, or section 15.2 in
>> Marshall Brain's Win32 SYSTEM SERVICES: The Heart of Windows
>> 95 and Windows NT [Prentice Hall PTR: NJ]: 1996), and you
>> can roll your own.
>>
>> But these don't "forge" events, in the sense that the
>> events they record are legitimate messages, and don't appear
>> to come from bogus sources. So, for example, if you want
>> to insert an apparent IIS message into a log (not using
>> IIS), this would be hard. Also, we're assuming, so far,
>> that you have NetBIOS access to the machine in question.
>>
>> If you want to insert arbitrary false messages into the
>> files, that's complicated: the logging API doesn't permit
>> it, and you'd be relegated (I think) to either finding a
>> flaw in it-- like the recent discussions involving URLs
>> with special characters embedded in them (but related to
>> the security log, instead of the application log), or to
>> programmatically editing the log files (which also is

SecurityFocus Penetration: Re: Writing to Windows Security Log

> > *tricky, I bet).*
> >
> > *Does this help at all?*
> >
> > *--Foofus.*
> >
> >
>
>
>
>
>
>
>

--
> This list is provided by the SecurityFocus Security Intelligence Alert
> (SIA)
> Service. For more information on SecurityFocus' SIA service which
> automatically alerts you to the latest security vulnerabilities please
> see:
> <https://alerts.securityfocus.com/>
>
>

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

- ***Previous message:*** [Erik Parker: "Re: Raptor Firewall"](#)
- ***In reply to:*** [Tina Bird: "Re: Writing to Windows Security Log"](#)
- ***Next in thread:*** [Stuart: "Stunnel Problems"](#)
- ***Messages sorted by:*** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)