

RE: Audit Explanations

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-sun/2001-08/0062.html>

From: Darren Moffat (Darren.Moffat@eng.sun.com)

Date: 08/14/01

Message-Id: <200108142123.f7ELN8B246379@jurassic.eng.sun.com>
Date: Tue, 14 Aug 2001 14:22:32 -0700 (PDT)
From: Darren Moffat <Darren.Moffat@eng.sun.com>
Subject: RE: Audit Explanations
To: Jeff.Leckemby@sptrm.com, jeffrey.leckemby@langley.af.mil

Using the example you gave (properly formatted where \ is a continuation on the same line).

```
header,148,2,open(2) - write,creat,trunc,,Fri Jun 08 13:50:23 2001 \  
+979998030 msec  
path,/export/home/someuser/.Xauthority-n  
attribute,100600,someuser,staff,136,16540,0  
subject,someuser,someuser,staff,someuser,staff,313,312,0 0 someputer  
return,success,4
```

In prose the says:

On Fri Jun 08 @ 13:50:23 process 313 on host someputer, operating on behalf of user someuser of group staff, opened the file /export/home/someuser/.Xauthority-n as file descriptor 4 for writing. Creating it with mode 600 if doesn't exist or truncating it if was already there. The file was found at inode 16540, the operation was successful. No additional privilege was used to complete this operation.

>Per your reply "What parts of the audit records you listed do you not understand ?

>

> What is: 148,2,

[http://docs.sun.com:80/ab2/coll.47.11/SHIELD/@Ab2PageView/idmatch\(APARECORD-920\)?Ab2Lang=C&Ab2Enc=iso-8859-1#APARECORD-920](http://docs.sun.com:80/ab2/coll.47.11/SHIELD/@Ab2PageView/idmatch(APARECORD-920)?Ab2Lang=C&Ab2Enc=iso-8859-1#APARECORD-920)

148 is the number of bytes in the record, 2 is the version number.

> and: .Xauthority-n
attribute,100600

path is the path token to this is the file that open(2) was passed.

SecurityFocus SUN: RE: Audit Explanations

attribute is on a new line and is the attr token which describes the vnode that open(2) was operating on.

[http://docs.sun.com:80/ab2/coll.47.11/SHIELD/@Ab2PageView/idmatch\(APARECORD-908\)?Ab2Lang=C&Ab2Enc=iso-8859-1#APARECORD-908](http://docs.sun.com:80/ab2/coll.47.11/SHIELD/@Ab2PageView/idmatch(APARECORD-908)?Ab2Lang=C&Ab2Enc=iso-8859-1#APARECORD-908)

100600 is the mode.

> *and: 313,312,0 0*

These are part of the subject token which is described in:

<http://docs.sun.com:80/ab2/coll.47.11/SHIELD/@Ab2PageView/7410?Ab2Lang=C&c=iso-8859-1>

313 == process id

312 == session id

0, 0 someputer is all the terminal id.

0 is the device

0 is the port

Since both of these are 0 this was on the local host and not a remote connection.

> *and: return,success,4*

<http://docs.sun.com:80/ab2/coll.47.11/SHIELD/@Ab2PageView/7288?Ab2Lang=C&c=iso-8859-1>

The return token. success means open(2) returned a non error value (ie != -1) and 4 is the return value so in this it is the file descriptor.

--

Darren J Moffat

-
- ***Previous message:*** [Jan-Philip Velders: "Re: NFS Security Question"](#)
 - ***Maybe in reply to:*** [Jeff Leckemby: "Audit Explanations"](#)
 - ***Next in thread:*** [Leckemby Jeffrey M Contr ACC/INSC \(SPECTRUM\): "RE: Audit Explanations"](#)
 - ***Messages sorted by:*** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)