

Re: Intrusion attempts

Source: <http://unix.derkeiler.com/Newsgroups/comp.os.vms/2005-02/0366.html>

From: Peter Weaver (*WeaverConsultingServices_at_sympatico.ca*)

Date: 02/04/05

Date: Fri, 4 Feb 2005 13:33:32 -0500

Syltrem wrote:

>...
> *After 4 failed login attempts with 3 different usernames, and one ^Z*
> *(no username entered):*
>
> *In accounting I do not see the usernames used, and only one record*
> *with this message:*
> *%LOGIN-F-NOSUCHUSER, no such user*
> *There is another entry with this message (triggered by the ^Z):*
> *%LOGIN-F-CMDINPUT, error reading command input*
>
> *OTOH, the audit does not show anything for some reason*
> *I have the auditing enabled for loginfailures:*
> *System security audits currently enabled for:*
> *Logfailure:*
> *batch,dialup,local,remote,network,subprocess,detached,server*
> *but \$ anal/aud/ev=breakin sys\$manager:SECURITY.AUDIT\$JOURNAL/sin*
> *returns nothing.*
> ...

Take a look at your SYSGEN LGI parameters,

```
SYSGEN> SHOW /LGI
```

and see how many retries are permitted before the attempt is considered a breakin. I would guess that you are not yet hitting the breakin limit so ANA/AUD/EV=LOGFAIL is what you need rather than /EV=BREAKIN.

On the system I just tried (VAX/VMS 7.1) LGI_BRK_LIM is 5, so my 6th try showed up in the audit record as a breakin attempt with both the username and password showing. I do not have Auditing turned on for local login failures, but if I did the 1st to 5th attempts should have shown up with no password.

--

Peter Weaver
Weaver Consulting Services Inc.
Canadian VAR for CHARON-VAX
www.weaverconsulting.ca

Re: Intrusion attempts