

Re: tcp-md5 check for incoming connection

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2008-01/msg00302.html>

- *From:* Andre Oppermann <andre@xxxxxxxxxxxx>
 - *Date:* Thu, 31 Jan 2008 11:02:42 +0100
-

Ingo Flaschberger wrote:

Dear Bjoern, Bruce,

Looking trough linux, netbsd and Bruce old patch
(which works with minimal modification at my freebsd 6.2)
I have 3 ideas how md5 could be integrated.

1) netbsd method:

http://cvsweb.netbsd.org/bsdweb.cgi/src/sys/netinet/tcp_input.c?rev=1.277&content-type=text/x-cvsweb-man

Look for TCP_SIGNATURE.

The main-code part is handled in tcp_dooptions
The have modified the return value of tcp_dooptions from void to
int. If md5 fails, -1 is returned (ony md5 use this return
feature) and in the tcp_input the return value of
tcp_dooptions is checked and handled.
-> for freebsd: change the retutn value of tcp_dooptions and
add little logic to tcp_input function.

Please do not use this method. tcp_dooptions should not have any side-
effects other than parsing the tcp options. It sets a flag if TCPOPT_SIGNATURE
was detected and give you the pointer to the hash in to_signature.

2) linux method:

Look for CONFIG_TCP_MD5SIG in linux-2.6.24/net/ipv4/tcp_ipv4.c
(sorry no weblink..)

They check and block md5-packets early in tcp_v4_do_rcv.
afinet.c -> tcp_v4_rcv -> tcp_v4_do_rcv
-> for Freebsd: place some logic early in tcp_input function
and call a new function to check md5.

IMHO calling a special function that does the check (like in tcp_output)
is the way to go. This function should be run as late as possible after
the other segment validity checks to prevent easy cpu exhaustion attacks
with packets that only get the port numbers right.

Re: tcp-md5 check for incoming connection

In tcp_new there is a natural place to perform the check. tcp_input will show up this weekend. This doesn't prevent your work on the current code at all as tcp_new won't show up in -current for a long time and when it does it will not get MFC'd.

3) Bruce extended method:

<http://lists.freebsd.org/pipermail/freebsd-net/2004-April/003761.html>

Use his code and add at several places in tcp_input function similar checks.

Options:

*) enable/disable it via sysctl

*) count total, good and bad packets via sysctl

This belongs into struct tcpstat, not a new sysctl.

--

Andre

freebsd-net@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-net>

To unsubscribe, send any mail to "freebsd-net-unsubscribe@xxxxxxxxxxx"