Packages - Bug #1274

[openssh-knock] is ignoring TCPStealthSecret and always accept the connection even if secret are different

2017-04-02 12:47 PM - belette

Status:	fixed	**% Done:**	100%
Priority:	bug		
Assignee:			
Category:			

Description

I have tested different TCPStealthSecret on server and client side but it ignores it and always accept to connect.
To confirm I don't have an issue on my kernel (I am using linux-libre-grsec-knock) I have use the simple program Gnunet proposed on their website (https://gnunet.org/sites/default/files/examples.tar.gz) and it is working as expected (different secrets makes the connection fails, same secret validate the connection).

History

#1 - 2017-04-05 02:12 PM - belette

Doing further analysis, the patch doesn't seems to define TCP_STEALTH_SECRET on the right place.

The sample program from Gnunet gives 0x1e for setsockopt:
setsockopt(3, SOL_TCP, 0x1e /* TCP_??? */,"thisismysecret\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0"..., 64) = 0
and the knock process is working correctly.

The same setsockopt from the openssh-knock is doing:
setsockopt(3, SOL_TCP, TCP_NOTSENT_LOWAT,"thisismysecret\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0"..., 64) = 0
and the knock process is not working (ssh always accept connection even if secret are not the same between client and server)

#2 - 2017-04-08 03:48 PM - Anonymous

- Assignee set to Anonymous

#3 - 2017-04-11 10:37 PM - korobkov

I confirm this behavior. It was so for a long time already.

#4 - 2017-04-12 04:02 PM - Anonymous

- % Done changed from 0 to 100

- Status changed from open to fixed

#5 - 2017-04-12 04:18 PM - belette

Yep I confirmed it is fixed
many thanks @Emulatorman for your quick fix :)