

Wednesday, February 28, 2007

Worm in the wild

Okay, when you still run a system without the patches for the telnetd vulnerability, when you still run a system with an activated telnetd, when you still run your system with access to telnet from the complete internet without a tcpwrapper or a packet filter okay ... that you really deserve that your system will be automatically owned by this worm. To reiterate it the millionth time: Don't use telnet, when you have to use it, patch your system and limit access to the the systems that really needs it.

Another suggestion: There is a good implementation of IPsec in Solaris. . You find the documentation in at docs.sun.com unter "How to Secure Traffic Between Two Systems With IPsec". You can kill two bird with one stone: Disallow all traffic to telnetd that didn't came from secured system and you circumvent the problem of the unencrypted nature auf telnetd. But: SSH would give you the same with less work. The above is only a solution when you really can't substitute telnet.

Posted by Joerg Moellenkamp at 20:07

For those who have always wanted to convert to SSH, but could not kick the telnet habit, have a look at my SSH Cheat Sheet - http://blogs.sun.com/timc/entry/ssh_cheat_sheet
Anonymous on Feb 28 2007, 23:26