

Re: telnet replacement – not ssh?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-01/0142.html>

From: those who know me have no need of my name (not-a-real-address@usa.net)

Date: 01/09/03

From: those who know me have no need of my name <not-a-real-address@usa.net>

Date: 09 Jan 2003 18:28:11 GMT

[fu-t set]

in comp.unix.questions i read:

>*This is why I'm concentrating on a technical solution. So far, OPIE is
>looking good...*

i've mentioned some possibilities, but i haven't seen them discussed so perhaps the articles have been lost or i'm it's due to me followup-to setting a group you don't normally use (because i feel it's a non-unix security issue, and which i've done again, sorry), so i'll reiterate:

there's some information on the topic in the kermit security reference.

telnet in combination with kerberos, s/key or srp ought to do as you ask. since part of the traffic is via the internet an unencrypted transport means the potential for disclosing secret information, including but not limited to: hostnames, configurations, high privilege account credentials, or company memos. kerberos with ticket forwarding solves the credentials issue, but only if it is consistently used. so ...

can the security group be convinced that it would be better (safer for the company) for the public portion of the link to be encrypted, just so long as the internal traffic is not? if so then perhaps the firewall has a telnet proxy that can be enabled and configured in such a manner, or a secured ssh-to-telnet server can be installed and tied down (you can connect to it via ssh from outside via the firewall but nothing but telnet can leave it), or perhaps the firewall supports vpn's which would be encrypted across the internet then you would use unencrypted telnet to access the `internal' (but `on' your own network) hosts.

at the edge of insubordination (perhaps over): install a few encrypted http tunnels (so that you always have at least one available) on internal hosts with the other end being your (home?) machine. you can use the tunnel to enter the company's network securely then telnet to the system you need to work on. you'd need to ensure that you never do anything other than launch

comp.security.misc: Re: telnet replacement – not ssh?

telnet from the tunnel terminus, so if work needs to be done on the terminus you need to telnet to it even though you are `already there'. as you can see this is perilous because you will be willfully penetrating the firewall in what is almost certain to be an unapproved way.

--
bringing you boring signatures for 17 years