

Re: Port 135 Probes Continue

Source: <http://www.derkeiler.com/Newsgroups/comp.security.unix/2004-01/0019.html>

From: Nico Kadel-Garcia (nkadel_at_comcast.net)

Date: 01/11/04

Date: Sun, 11 Jan 2004 17:29:17 -0500

"Walter Roberson" <roberson@ibd.nrc-cnrc.gc.ca> wrote in message
news:bsqo5i\$88u\$1@canopus.cc.umanitoba.ca...

> *In article <MPG.1a5a8cc8a0b9bf9698a011@news-server.columbus.rr.com>,*

> *Leythos <void@nowhere.com> wrote:*

> *:If you are using MS Exchange over an open connection you need to fire*

> *:the IT staff or get a new hosting company. You should be using ANY form*

> *:of VPN connection in place of an open Exchange connector.*

>

> *You assume, Leythos, that the IT staff have the budget and authority*

> *to purchase appropriate VPN equipment and deploy it.*

Authority, yes. Budget? The only budget item is manpower for the project.

Take a careful look at FreeSwan if you prefer IPsec, or at www.poptop.org
for the UNIX/Linux based PPTP server that handles Microsoft's built-in VPN
clients without pain. They can be hosted on quite a low end little machine,
including a discarded old laptop, and even run from CD instead of from disk
for security reasons.

> *I have the authority to deploy VPN equipment locally, but not the*

> *budget to purchase it. Fortunately, a few years ago I was able to get*

> *some equipment covered under a grant for joint work with an*

> *organization required by law to protect its data; if the grant*

> *committee had thought there was a legal option not to use the*

> *equipment, then they could have done a line-item veto of it.*

Yeah, leverage to create a new service can be quite hard.

> *I have no authority or budget to deploy VPN equipment at HQ,*

> *and no travel authority to go to HQ to deploy even if appropriate*

> *equipment were to "fall off the truck" into my hands.*

>

> *The Exchange people at HQ have no authority or budget to deploy*

> *networking equipment beyond their office.*

Then they have not the authority or budget to use those services outside of
their own local network. Period, end of discussion.

- > *The networking people at HQ have no authority or budget to deploy*
- > *security-related networking equipment -- in particular they have*
- > *no authority to install security-related equipment at the regional*
- > *sites.*

They don't have to install a single piece of hardware remotely. The capability of using a VPN is already built into the Win2K and WinXP clients. They may need to get the remote clients admins to open a firewall hole to allow GRE packets to HQ, but that's amazingly vastly superior to insisting that they keep the file-sharing or RPC ports open.

- > *The security people at HQ have the authority to hold consultations with*
- > *the affected parties and recommend a policy change that would give them*
- > *authority to deploy security-related equipment at the regional sites.*
- > *But they don't have any budget and they don't have the human resources.*

Human resources, I can believe. They probably have to waste a lot of man-hours cleaning up after the debris caused by leaving such services open: it's penny-wise, pound-foolish, and a decent VPN setup would provide vastly safer access for their own authorized staff in the field, to any services they wish to allow.

- > *They did make the appropriate internal applications for the funds, but*
- > *the budget committee turned them down this year; they are hoping they*
- > *will be able to roll out VPN services by this time next year, if they*
- > *are able to get the funding.*

Have them come talk to us if you need help explaining the facts of life: it sounds like you've got a lot of "process" going on there, at the expense of basic support or engineering, and reading between the lines I suspect you're frustrated with it yourself.