

Re: PLINK and/or PuTTY -- Logon to Linux with no Privileges

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2006-03/msg00256.html>

- *From:* "Nico Kadel-Garcia" <nkadel@xxxxxxxxxxxx>
 - *Date:* Wed, 22 Mar 2006 08:13:30 -0500
-

Hal Vaughan wrote:

Nico Kadel-Garcia wrote:

"Hal Vaughan" <hal@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:ftSdnSyGnf_rF4LZnZ2dnUVZ_s6dnZ2d@xxxxxxxxxxxxxxxx

I need a forwarding application that people I'm working with can run from behind restrictive firewalls so VNC can be tunneled through it. I figured it would be possible to use putty or plink on port 443 so it would look like HTTPS to a firewall (is that right -- will the firewall think encrypted data from putty/plink is the same as HTTPS?).

There are firewalls that can detect this sort of thing, but not many that bother with that sort of smarts.

Now that I'm thinking about it -- and I don't know much about this -- I would think one type of encrypted data would look like any other. We've tried just regular VNC, with no luck, then tried it on port 80, with no luck. My best guess is that it's not only filtering based on ports, but on the type of data or packets. If so, from what I understand, encrypted data on port 443 will seem close enough to HTTPS that it should go through. That makes me wonder, though, if I could just run VNC normally on port 443 and it would likely go through. Is that likely? My guess on this is that it's hard to check encrypted data so not much checking would be done on that port anyway. Is that at all close to fact or is there any basis for that idea?

Re: PLINK and/or PuTTY -- Logon to Linux with no Privileges

Nope. SSH session traffic, for example, tends to be both ways as opposed to HTTPS, which is mostly download. And the beginning of both connections where keys are passed around and collected look rather different.

But running VNC on port 443 is feasible. Running services on ports below 1024, at least on Linux, requires root privilege. Perhaps 8080 is open? And less likely to be in use on the target machine?

Hmm. Does your network staff know you're doing this sort of stunt? Perhaps you can convince them to open up the standard VNC ports for you instead of trying to work around them, rather than having to sneak behind their backs and maybe cause them to get really cranky at you if they find you're drilling holes past their firewalls without their knowledge? Your desire is reasonable: I hope your network staff is reasonable and can help you get it done.

Actually, I'm dealing with admin people who have authority over IT people and basically would prefer me do this than change the firewall. In one case there's a Cisco router handling it and a history of having trouble finding anyone who knows IOS to program it, so the feeling is, "The firewall's working. Nobody's touching it. If you can find a way to work with it, great."

I detect weasel wording. Does the *IT* staff know you're doing this? They're the ones whose job it is to keep things running. If you leave something running that they don't even know about, or they're gathering information to plan an upgrade of the Cisco router to something more manageable, this is information that could help them avoid a problem down the road.

I never knew any of that was possible. Do you have Silverman's book title? I'm searching the local bookstores for it, in hopes I can get a copy today. I've been working on this for a few weeks and I really need to get it resolved before more work piles up. I've found one he co-authored, "SSH, the Secure Shell: The Definitive Guide". Is that it?

Yes, Richard responded on this. I highly recommend it.

I'm running Linux. Is there a way to set up a restricted login (even if I have to kill it with a kill command instead of them logging out) for putty or plink? Or is there a way to set up an account for others to log in to that has no rights except the ability to log out?

Re: PLINK and/or PuTTY -- Logon to Linux with no Privileges

Not.... trivially. It's theoretically possible, for example, to set up a restricted login binary to do just this, but a lot of "restricted shells" have just been badly written shell scripts that were easily broken out of because, well, they're shell scripts! And it can get complex if you are using a universal authentication method like LDAP to manage accounts, since the information about their login from LDAP can conflict with the setup you want to have them restricted to.

So what kind of search terms are best on this? Restricted shell? Restricted login? I can understand why a script would be bad. I figured this either had to be done by some special shell or something special with permissions and the group the user is in, but this is not an area I know much about. I do know enough to know that what you don't know in security can nail you, which is why I'm asking all of this.

Good man. *WISE* man. Somebody get this guy a cookie! We want to encourage sensible people to actually ask questions.

I like Richard's "use /bin/false as their shell and have the client do the port forwarding setup".