

Re: get into the private campus server

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2006-11/msg00126.html>

- *From:* Andrew Schulman <andrex@xxxxxxxxxxxxx>
 - *Date:* Mon, 06 Nov 2006 19:38:53 GMT
-

Have your on-campus server act as an ssh client, connecting out to a cooperating ssh server. Once the ssh connection is established, you can tunnel any TCP traffic you like over it, in either direction. To maintain the connection over the long term, you can use e.g. autossh.

This is a well-known technique that I've used successfully for years. You can work out the details for yourself.

Of course if you then use that tunnel to move massive amounts of traffic across the campus firewall, then the admins will quickly catch on. Or, if you're not careful and the outside ssh server gets compromised, then the attackers will have a free ride into the campus network, and after they come in and wreck a few servers, the admins will trace the compromise to you and show up at your dorm room at 2 AM to take your computer away, right as you're in the middle of jacking off. Awkward, no? But see, the ssh tunnel circumvents all of their network controls and allows pretty much any traffic in or out, and you can bet that when they find out about it they'll be really pissed. Remember that they know about the technique, but have probably decided that the risk doesn't justify blocking all outbound ssh traffic. So now they'll kick you off of the network for sure, maybe out of the college, take your computer away and good luck getting it back, and maybe do something overreactive like cutting off all ssh access to the outside, while explaining to everyone who complains that it's because you compromised their network.

Have fun.
Andrew.

—

To reply by email, change "deadspam.com" to "alumni.utexas.net"

.