

## Re: exposing TS directly to Internet

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-10/0563.html>

---

**From:** Steven L Umbach (*n9rou\_at\_n0-spam-for-me-comcast.net*)

**Date:** 10/16/04

Date: Fri, 15 Oct 2004 23:41:01 GMT

OK. I had two servers set up for TS Remote administration over the internet – one at home and one at work. I never had a problem. I have not heard of any major vulnerabilities for port 3389 other than hack attacks that involve password guessing which is why using complex passwords and auditing of failed logon attempts are important. If you do find a users trying to password guess their way in, they usually will give up after a while and if your firewall logs their IP address you can add it to the blocked IP address list for port 3389 TCP. --- Steve

"michael" <admin@pcs.minsk.by> wrote in message  
news:94c65b3a.0410150324.29b8c7b5@posting.google.com...  
> "Steven L Umbach" <n9rou@n0-spam-for-me-comcast.net> wrote in message  
> news:<HOybd.182537\$wV.14835@attbi\_s54>...  
>> *Of course you can do that and a firewall to protect all other ports will*  
>> *go*  
>> *a long way to protect the computer. Be sure to do other normal securing*  
>> *procedures such as requiring the use of complex passwords, having an*  
>> *account*  
>> *lockout policy with a lockout threshold of no less than ten and a reset*  
>> *interval of around ten minutes to deter brut force password attacks,*  
>> *using*  
>> *antivirus, disabling unneeded services, and keeping current with critical*  
>> *updates. Since the built in administrator account can not be locked out*  
>> *and*  
>> *is the top target of attacks I would disable that account from logon*  
>> *through*  
>> *TS in it's account properties.*  
>>  
>> *It would increase security quite a bit if you could configure the*  
>> *firewall*  
>> *to only accept inbound port 3389 from authorized IP addresses of your*  
>> *users.*  
>> *That may not be possible if they roam or do not have static IP addresses.*  
>> *Also using a VPN to access the TS would increase security particularly if*  
>> *you can use l2tp that would require computer certificates for*  
>> *authentication*  
>> *to logon to the VPN. Users could then logon to the VPN and then access*  
>> *the*

>> *TS via it's LAN IP address and it would not have to be exposed to the*  
>> *internet. --- Steve*  
>  
>>  
>  
> *Well, Steve. Thanks. I understand that using VPN is the best choice to*  
> *secure data communication through the Internet. But let's suppose we*  
> *can't build a VPN. I'd like to collect information on any experience*  
> *in using MS 2003 directly connected to the Internet with respect to*  
> *its resistance to certain attacks on its 3389 port and RDP protocol.*