

## Re: IRC-based Olympic Coverage

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2004-12/1196.html>

---

**From:** Lars M. Hansen (*badnews\_at\_hansenonline.net*)

**Date:** 12/27/04

Date: Sun, 26 Dec 2004 22:23:08 -0500

On Sun, 26 Dec 2004 14:45:50 -0800, Charles Newman spoketh

>>

>> *And yet again, you show exactly why we shouldn't trust an accountant*

>> *when it comes to network and computer security.*

>

> *Well, as I have said before, I do hope to be able to open*

> *my own observatory someday,. since astronomy is a*

> *hobby of mine, there are several for-profit privately run*

> *observatories in the USA now. I took a few course*

Well, I hope for your sake that you know a lot more about astrology than you do about computer and network security... But I'm not too confident that is the case. In the time that you've been frequenting this group, one would have thought that you would have picked up *\*something\**, but that doesn't seem to be the case.

It's understandable that you're not familiar with the "stroke" terminology with regards to subnets; it's really one of those things you need to be around for a while to wrap your head around.

But you continue to believe that you can do anything you want on a network, and bust through any firewall you want to watch TV, listen to music and bypass anything just because you read something about proxies and special applications that will magically do this for you. Yes, it probably could happen. I don't know who you work for (and I don't want to know), and it is possible that you could do what you say you can do there, but in the vast majority of medium to large sized companies today, you can't even fart in your office without it being logged on some computer somewhere.

With proper analysis of logfiles it's very easy to find who is doing something odd, even if it looks like normal traffic. First off, IRC is blocked by default everywhere except at home. Nobody corporate wants anything to do with IRC. With all these trojans that "calls home" to IRC servers, that's not likely to be an open port... Even if you use software that uses port 80 for this, if it doesn't actually look like http traffic, it may not pass through the firewall.

## comp.security.firewalls: Re: IRC-based Olympic Coverage

Now, lets say that it does pass the firewall, just because it could be done, and it makes for an interesting discussion. Let's say you could watch TV over IRC through port 80 on your company's network.

Now, just the regular run-of-the-mill web-browsing doesn't take up a whole lot of bandwidth at all. A couple of pages a minute perhaps, shouldn't be more than a few hundred KB's per page, even less if some of the elements are cached. Considering that you should be working, you won't be browsing the web all that, so it won't really add up to much. Looking at what experience have told me, regular web browsing at work doesn't come up high on the list (viewed by individual source IP). E-Mail will probably top the list (total bandwidth over 24 hours, total bandwidth to & from a single IP address). Next on the list there would be IT people. Then comes the regular people with their regular web browsing.

Since video broadcasts actually takes up quite a but of bandwidth, and usually lasts for a while, the accumulated additional bandwidth of you watching Olympic figuraskating over the internet would skyrocket your ranking on the "bandwidth-hog" from way down on the list to the top spot! 2 hours of TV at 160Kbps would mean a whopping 140MegaBYTES of data.

The first thing I did in my old job when I got into work, was load up a web-browser and load the nice pages made by the handy-dandy free log-file analyzer software package I had installed on a spare server. 140MB would stand out like a puritan in a whore-house, and there would definitely be some searching in the log files to find out just where the heck those 140MB where and were they came from...

Oh, and porn surfers get spotted easily too. Since there's a lot of pictures, the total bandwidth used are often higher, so they tend to be high on the list of "regular" web-traffic users. Of course, if you come in on the weekends to "work" and download some dirty pictures, don't be surprised if those web sites won't work next time you try it...

Any which way you try it, Charles, the traffic gets logged. Logged traffic are often passed through analyzers, and someone suddenly downloading hundreds of megs of data are sure to be spotted...

So, if you want to do some weird stuff, do it at home. Watching TV on company time is not only unethical and disrespectful to those who pay your salary, if you're attempting to avoid detection using any type of "funky" software, you are probably violating company policy, and it could get you fired. If you want to watch an event that bad, take a day off, or better yet, buy a ReplayTV and record it, then you can view it commercial free when you get home...

Lars M. Hansen

<http://www.hansenonline.net>

(replace 'badnews' with 'news' in e-mail address)

Re: IRC-based Olympic Coverage