

can Hopster traffic be blocked?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2004-08/0001.html>

From: Prakash Purushotham (prakashp_at_bigfoot.com)

Date: 08/04/04

To: focus-linux@securityfocus.com

Date: Wed, 04 Aug 2004 10:35:04 +0530

Current setup:

RH9 all patches current
iptables set to deny all direct traffic out except to a select few
squid with acls to allow only http(s)/ftp, more acls to allow access to
msn/yahoo.

Problem:

Some users have installed hopster and are able to connect to messenger
servers even if they are not listed under the "chat access" acls.

The following site has some information on hopster and similar software.

<http://www.hackingspirits.com/eth-hac/prf-of-conc/bypass-fw/PoF01/bypass-fw-sock.html>

I have tried in vain to block traffic using iptables. I tried INPUT
filter on traffic coming in from port 1863 (for example), under the
assumption that the messenger server has to reply to hopster requests. I
have tried blocking FORWARDS again, based on source port 1863 on the
external interface.

My last resort (administrative) is to invoke the rule that no
unauthorized software be installed on the systems.

Any suggestions on how I can block hopster (and other similar socks
based tunneling applications) from tunnelling out.