

Re: ~/.hosts patch

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/current/2006-06/msg00489.html>

- *From:* Harti Brandt <hartmut.brandt@xxxxxx>
 - *Date:* Wed, 21 Jun 2006 08:31:36 +0200 (CEST)
-

On Wed, 21 Jun 2006, Xin LI wrote:

```
XL>** 2006-06-21**** 01:54 -0400**Mike Jakubik*****
XL>> [snip]
XL>> > It's useful for cases where you want to add shortcuts to hosts as a user
XL>> > or do interesting ssh port forwarding tricks in some weird cases where
XL>> > you must connect to localhost:port as remotehost:port due to
XL>> > client/server protocol bugs.
XL>> >
XL>> > This patch appears to only support ~/.hosts for non-suid binaries which
XL>> > is the only real security issue. Any admin relying on host to IP
XL>> > mapping for security for ordinary users is an idiot so that case isn't
XL>> > worth worrying about. Doing this as a separate nss module probably
XL>> > makes sense, but I personally like the feature.
XL>>
XL>> Of course relying on /etc/hosts entries for security alone is indeed not
XL>> a good idea, however an Admin may choose to resolve and therefore route
XL>> specified hostnames via /etc/hosts. The user should not be able to
XL>> overwrite these, if this behavior is true, then it seems like a
XL>> reasonable change to me, otherwise it not only seems to be a security
XL>> problem, but also a breach of POLA.
XL>
XL>I think this would be better implemented with a nss module so that the
XL>administrator can choose whether to utilize the feature.
XL>
XL>BTW. I do not see much problem if the feature is not enabled for setuid
XL>binaries because if the user already knows some secret (run under his or
XL>her own credential), nor can the user trick others to utilize the
XL>~/.hosts if the program is a setuid binary. What's your concern about
XL>the "security problem", or could you please point how can we
XL>successfully exploit the ~/.hosts to get privilege escalation and/or
XL>information disclosure or something else, which could not happen without
XL>~/.hosts?
```

Wouldn't this enable the same kind of phishing attacks there are under windows? As far as I remember there are attacks where the hosts file (don't remember how its called under windows) is rewritten by a virus/java script/whatever to contain a different IP address for a given hostname?