

Re: Tool to find hidden web proxy server

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2004-09/0062.html>

From: Chris Brenton (cbrenton_at_chrisbrenton.org)

Date: 09/02/04

To: vinay mangal <vinay.mangal@eil.co.in>

Date: Thu, 02 Sep 2004 14:06:22 -0400

On Wed, 2004-09-01 at 23:36, vinay mangal wrote:

>

> *Few smart guys have installed free proxy server running on non
> default ports and distributed the internet access to their friends. The
> firewall sees the traffic coming from the authorized IP and does not stop
> them. We want to know who has installed proxy on there machine.*

This will be easy or hard, depending on just how smart the "smart guys" are. ;-)

Someone else posted saying to use ngrep. Its still your friend in this case. Most proxies stamp an "X-Forwarded-For" field into the payload so you can use ngrep to key in on that. Something like:

```
ngrep -q 'X-Forwarded-For' port 80
```

in the path of the firewall will do the trick. Now for the bad news, most proxies also let you remove that "X-Forwarded-For" field, so if they are **really** smart and have done this you will not catch it.

BTW, if you catch one box, do a full TCP port scan of that IP to find the proxy server, and then start checking all your internal IP's for that same open port. When I've seen this before one bad apple starts the whole thing and then others just copy their config.

HTH!

Chris

Ethical Hacking at the InfoSec Institute. All of our class sizes are guaranteed to be 12 students or less to facilitate one-on-one interaction with one of our expert instructors. Check out our Advanced Hacking course, learn to write exploits and attack security infrastructure. Attend a course taught by an expert instructor with years of in-the-field pen testing experience in our state of the art hacking lab. Master the skills of an Ethical Hacker to better assess the security of your organization.

SecurityFocus Penetration: Re: Tool to find hidden web proxy server

http://www.infosecinstitute.com/courses/ethical_hacking_training.html
