

Rogue activity methodology (was: Tool to find hidden web proxy server)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2004-09/0144.html>

From: Chris Brenton (cbrenton_at_chrisbrenton.org)

Date: 09/05/04

To: Pen <pen-test@securityfocus.com>
Date: Sun, 05 Sep 2004 05:52:40 -0400

On Wed, 2004-09-01 at 13:44, Bénoni MARTIN wrote:

>

> *Well...*

> - *The easier way is to scan your whole network and see the machines which are up (nmap -sS xxx.xxx.xxx.0/24). Maybe, you will find a strange machine which can be your proxy.*

I have to say, I'm a bit surprised at how many people chimed in with "scan your whole network". This seems like a lot of work (and traffic) given the situation Vinay described. Just to go back over the "facts" he has given us:

- * Only certain IP's are permitted outbound HTTP access
- * Suspects one or more of these IP's have setup a rogue proxy
- * Unauthorized users may be accessing the Internet via the proxies
- * Suspects the proxies are on a non-standard ports (implies he might have already checked the standard ports)
- * No indication if the internal network is switched or repeated
- * No indication of the OS being used
- * No indication of whether he has admin access to these systems
- * No indication of how big the internal network may be
- * No indication of how many systems are permitted outbound HTTP access

So if he's running a class B, nmap is going to spend a whole lot of time saturating the wire. That and there is no guarantee that the systems in question will be "up" when nmap tries to hit their IP. Finally, nmap is probably going to produce a ton of data that needs to be sorted through. This will include a lot of false positives in the form of listening ports that are not the proxy servers in question. Bottom line, lots of work and no guarantee of resolving the problem.

Don't get me wrong, nmap is an awesome tool, but I guess I was trying to hit this from a methodology stand point. In other words, what's the easiest way to isolate the proxy traffic signature from "normal" traffic patterns? If you can do that, your false positives are minimal and thus the amount of "work" you have to do to resolve the problem is minimal.

SecurityFocus Penetration: Rogue activity methodology (was: Tool to find hidden web proxy server)

This is why myself and a few others chimed in with methods that would isolate proxy communications from normal traffic flow (look for "CONNECT" between local systems or "X-Forwarded-For" headed to the Internet, etc.). If you get a "hit", it is extremely unlikely to be a false positive. So by isolating what is unique about proxy communications you reduce the error rate as well as the amount of work that needs to be done to solve the problem.

Just wanted to throw the above out there for comment/discussion,
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.

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