

Re: testing for IP address space leakage in NAT systems

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-01/0072.html>

From: Chris Keladis (Chris.Keladis@cmc.cwo.net.au)

Date: 01/22/02

Date: Tue, 22 Jan 2002 10:40:38 +1100

To: R P G <inittab@itan.com>, <pen-test@securityfocus.com>

From: Chris Keladis <Chris.Keladis@cmc.cwo.net.au>

Hi Bob,

Alot of times misconfigured web servers return a "Content-Location" header which displays an internal IP..

Another good way is using things like epmapper, or BindViews rpctools, or AtStake's dctest to query a (Win32) DCE epmapper.

Sometimes, you find things when looking through the HTML code, comments, maybe even some code to speak to any back-end servers.

Then there is trying to talk SNMP to the NAT device, which may even return the exact mappings if your lucky! :)

Other techniques may involve firewalking depending on how the victim border routers/firewalls are configured.

And something that just popped into my head is getting a HTTP server to return an error. Alot of times the errors are overly verbose, giving up an IP.

HTH,

Chris.

At 12:02 PM 21/01/2002 -0500, R P G wrote:

*>I was wondering if anyone knows of a method to test a NAT system for
>address space leakage.*

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

- *Previous message:* [Joshua Wright: "RE: testing for IP address space leakage in NAT systems"](#)
- *Maybe in reply to:* [R P G: "testing for IP address space leakage in NAT systems"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)