

Re: Find out the subnetting of a company

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2004-08/0009.html>

From: Miles Stevenson (miles_at_mstevenson.org)

Date: 08/04/04

To: pen-test@securityfocus.com

Date: Tue, 3 Aug 2004 18:23:03 -0400

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Don't mean to re-hash old stuff, but it took me a while to get around to doing some testing. After a bit of playtime, it seems to me that the ICMP type 18 request is a very unreliable method to discover IP subnetting, as almost all modern IP stacks will simply ignore these requests.

This was tested by installing multiple OS's under vmware, and using both hping2 and thcrut (thanks to Jerry Shenk for posting a link that works!) to test sending ICMP type 18 requests (address mask request) against each system. I tested the following systems:

Windows 2000 SP1

Windows XP SP1

Windows NT 4 SP1

Windows NT 4 SP6

Linux 2.4

Linux 2.6

Please note that I have NOT tested any of the BSD's or Solaris. The only system in the above list that actually responded with its subnet was the NT 4.0 SP1 system. However, after installing SP6a, the system ceased to respond.

I saw one suggestion to look for some SNMP enabled routers that you can grab the info from, but this is also less likely to be available these days. So far, the most reliable method that I have found for mapping out the subnetting of a network, is to look for broadcast addresses.

The only theoretical problem with this approach, as pointed out by J.A. Terranson in a previous post to this thread, is that some older systems will also treat the network address as a broadcast, and respond to both ends. I have yet to actually see this kind of behavior, nor have I any systems to actively test this on, but I if this is true, it wouldn't be hard to work around.

SecurityFocus Penetration: Re: Find out the subnetting of a company

It would be a simple matter to notice the same system responding on two supposedly different broadcast addresses, and assume the lower of the two is a network address. Combine this with some OS fingerprinting to reinforce those findings. I would also imagine that a system this old would most likely give a response to an ICMP 18 request. Hence, searching for broadcast addresses will still provide a reliable way to map subnetting as long as you keep the previous issue in mind.

I would also like to point out to any beginners out there who might be afraid to ask, that network discovery (finding all of the devices connected to a network) is extremely unreliable and almost NEVER finds everything. This is especially true when you are attempting the discovery from a system that is not on the local network. Remember that there could be a number of devices that are in "stealth" mode, such as NIDS (although there have been some techniques developed to detect devices in promisc mode, with varying success). This doesn't count any devices operating at layer 2, such as bridges, hubs, switches, etc. A good pen-tester that is attempting to discover as many network devices as possible will not rely on network scanning alone, but will also use different channels, such as data-mining and social engineering.

Regards,

Miles Stevenson

miles@mstevenson.org

PGP FP: 035F 7D40 44A9 28FA 7453 BDF4 329F 889D 767D 2F63

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.3 (GNU/Linux)

iD8DBQFBEBBKMp+InXZ9L2MRAIPDAKCVRwmUyQ3jeoexp1Bex8InoTq6VACeO3aT
t9R0q5Dk6s2WOp24q/lueK4=
=155u

-----END PGP SIGNATURE-----