

Re: Scanning Class A network

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-10/0193.html>

From: Volker Tanger (vtlists_at_wyae.de)

Date: 10/24/05

Date: Mon, 24 Oct 2005 22:40:11 +0200

To: pen-test@securityfocus.com

Greetings!

On 24 Oct 2005 12:33:05 -0000

tarunthenut@gmail.com wrote:

- > *Recently I was given a task to carry out a port scan of an entire*
- > *valid*
- > *Class A range (Dont ask me what the huge pool of valid IP's was for*
- > *:)). The scan needed to be carried out externally, and not from*
- > *within the network to identify hosts and ports exposed to the*
- > *Internet.*
- > *The problem compounded cause of the following limitations :*
- > *1. ICMP was not allowed in the network*
- > *2. The IP range was to be scanned every month for the entire port*
- > *range from 1-65535 for TCP & UDP*

Okay, so you can't see wether a host is up and you have to scan all ports for all IPs.

2^{16} ports for each UDP and TCP = $2 * 2^{16} = 2^{17}$ tests for each host

Class A = 2^{24} hosts

Thus total IP+ports to test = packets to send:

2^{17} ports * 2^{24} hosts = 2^{41} tests

For simplicity's sake let's assume

60 bytes/packet = 480 bit/packet

To scan this within a month you'll need

2^{41} tests / month

= 2^{41} tests * 480 bits/test / month

= 1 Pbit/month

= 35 Tbit/day

= 1,5 Tbit/hour

= 24 Gbit/minute

SecurityFocus Penetration: Re: Scanning Class A network

= 407 Mbit/s in small packages, full duplex

= 848.389 tests/s = packets/s

So in best case (no collisions etc.) you'll saturate half an external GIGAbit/s line interface just for pen testing (give or take a small factor). And this only is for the outgoing port-knocking part...

...if you can test that at all. Depending on your gear and optimization you might not be able to sustain spewing out that many connections and track the responses. IPtables usually maxes out at roughly 300.000 packet/s, which is only a third of what you need.

For TCP connections RfC793 defines a limit of 268 new TCP sessions/second (54512 non-reusable source ports available, TCP timeout 4 minutes). So as long as you stay RfC-conform you're a bit more than factor 1500 too slow (unless you utilize 1500 parallelized PCs, of course). But you'll need to tweak Linux kernel settings e.g. for state tables anyway, so you might squeeze off a little bit from this, too.

So I'd say without being able to reliably check whether a host (IP) is up you won't have a realistic chance to meet your schedule. Even if the impact of that repeated scan onto network infrastructure is ... hm... quite a bit.

The network fabric (switches) and firewall (or whatever being used as external gateway) must be able to carry that load, too. We're talking about large-enterprise/carrier class firewalls here...

Are you sure your customer fully understood the impact and wants a scan that's saturating roughly half the a Gbit/s interface 24 hours a day, 7 days a week, 365+ days a year? Do you have the equipment capable of this? Does the customer have?

Good luck!

Volker

--

Volker Tanger <http://www.wvae.de/volker.tanger/>

vtlists@wvae.de PGP Fingerprint
378A 7DA7 4F20 C2F3 5BCC 8340 7424 6122 BB83 B8CB

Audit your website security with Acunetix Web Vulnerability Scanner:
Hackers are concentrating their efforts on attacking applications on your website. Up to 75% of cyber attacks are launched on shopping carts, forms, login pages, dynamic content etc. Firewalls, SSL and locked-down servers are futile against web application hacking. Check your website for vulnerabilities to SQL injection, Cross site scripting and other web attacks before hackers do!
Download Trial at:
http://www.securityfocus.com/sponsor/pen-test_050831

Re: Scanning Class A network