

Fw: Re: Mapping Class A network (any easy trick?)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-02/0045.html>

From: Volker Tanger (vtlists_at_wyae.de)

Date: 02/09/05

Date: Wed, 9 Feb 2005 00:01:50 +0100

To: pen-test@securityfocus.com

Greetings!

On 8 Feb 2005 16:41:33 -0000

John Thomas <mjohn2000_99@yahoo.com> wrote:

>

> *I am about to do a penetration testing on a "Class A
> network" and wondering how I can map the network
> without pinging 17 million IPs.(nmap -Sp 10.0.0.0/8)*

If you assume that such a "big" net is generously divided into class-C (8 or bigger) networks, then it should be sufficient to ping the usual suspects: .1 and .254 – where usually routers have their base within the net. If you want you could add a class-C broadcast just to make sure.

With this you save a factor 100 off your share and usually find out populated subnets of the class-A one. Then proceed with fine-grained inspection of the class-C ones found.

Beware: this only works on the assumption that "border" addresses are usually populated – which may not always hold true.

A full class-A pingrun will take the better half a year if done on-per-second, two days if done 100 per second, etc.

A 10Mbit/s line will max out somewhere below 10.000 pings per second, or 100k resp. 1M-Pings on 100Mbit/1Gbit LANs. So if you (are allowed to) saturate the LAN you might theoretically be able scan the net within 20 seconds or a few minutes. Theoretically.

In practice that probably will be a few hours on a LAN-only net. This is do-able but will quite probably not go undetected even if there is no IDS running, especially not via (usually) congested WAN lines.

Another option (more time-consuming yet way less intrusive) is to let ARPWATCH run and map the addresses in action – only within the local

SecurityFocus Penetration: Fw: Re: Mapping Class A network (any easy trick?)

network, that is.

The choice is depending on wether you want to save time or publicity...

;:-)

Bye

Volker

--

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

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