

RE: Mapping Class A network (any easy trick?)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-02/0050.html>

robert_at_dyadsecurity.com

Date: 02/09/05

Date: Wed, 9 Feb 2005 10:14:49 -0800

To: pen-test@securityfocus.com

> *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)*

Because a network of that size will take some time to map, no matter what method/tool you're using, it's important to note exactly what information you're hoping to retrieve. Since you're not clearly saying what information you want, I'm assuming it's a list of live/interesting systems. You're also not saying if that network is local or remote to you, IE do you get routed to that network, or are they in the same broadcast domain as you.

There are dnsscanners out there that will let you specify a range of IP's to do in-addr.arpa lookups against. They can also take domain names and append host names from a word list to do a dictionary attack on host names. You could also do a true brute force for say, 1-4 characters in the host name. We wrote our own DNS scanning tool, but as long as you can find those features, you'll get what you want. We may be releasing our DNS scanner soon anyway. Remember to also do AXFR attempts for the SOA and other DNS servers listed. Also, you'll find additional DNS servers with the UDP Unicornscan command (below). Be sure to query those servers too.

As far as enumerating live systems, you may want to check out Unicornscan (<http://www.unicornscan.org>). Even though the current public release is pretty ghetto when compared to what will be the next release, I think it has enough functionality to provide you with a lot of help for systems enumeration. The website has an "accurate" description of the tool... but you can think about it as kind of like nmap (or scanrand), with some other features they don't have yet (nmap/scanrand also have features Unicornscan doesn't have, yet).

For a network of that size, you'll want to store the response data into a database. For the 0.4.2 version of Unicornscan, you could install Postgres SQL database (<http://www.postgresql.org/>). You'll also want to compile Unicornscan with the database output module. In the 0.4.2

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

(current public) release, you can see how to do that in the README.database file. You can find the SQL schema in unicornsca-0.4.2/src/output_modules/database/pgsql_schema.sql

Using Unicornscan on the most c