Net Scanning for the Curious

by Remy

You may have heard about IP scanning before. You may have even done
it. Either way, this article is going to run over the basics to name, port, and service scanning. So, sit tight, droogies, and let's get ready for a bit of the old ultra-violence.

What we are doing:

If you're familiar with what a war dialer is, this isn't hard to understand. But, for the totally clueless...
A war dialer is a program that will call a set of numbers on a list you give it, and look for data ports. This can be very irritating if your phone is on the dial list. It is generally illegal to war dial, and you will get in deep trouble.
IP scanning follows the same principle, depending on which type of scanning we're doing. The three basic types:

- NAME SCANNING: Scan a list of IP addresses, and if they have domain
names that can be resolved, you will find them.

- PORT SCANNING: Scan a list of IP addresses for a certain port.

- SERVICE SCANNING: Scan ONE IP address, on a range of ports, to see
which ports accept connections.

Why should I do this? (aka, What's my motivation?):

IP scanning is invaluable in any manner. Name scanning can find you seperate hosts that you may be able to access the web server of. Name scan a major site (microsoft, apple, yahoo, cnn, etc) long enough, and you can see all sorts of lesser servers you never would know about other wise. Name scanning will also provide you with names for service scanning. Service scanning will let you see if, as the name implies, services are available. Find a machine with a domain name with a name scan, and you can see if you can telnet in with a service scan. Maybe there's a SMTP server, so you can relay mail through it. The possiblities are endless. Port scanning lets you do

service scanning for one port over multiple addresses. Find who on your ISP you can telnet into! See who's running a web server! All this, and more.

(Also, IP scanning is infinitely better than war dialing, because IP scanning isn't illegal.)

TOOLS:

I've found two different programs that can scan.
- AgNetTools 1.0 (http://www.aggroup.com/, also available on The Weasel's www site) - This is the greatest. You want this program. Not ONLY does it do 4 types of scans (the three mentioned before, and ping scanning, which is unuseful for the most part), but it ALSO can ping, trace route, finger, whois, do a throughput test, and do DNS and reverse DNS, and gives you some info about your system. The only things I've found wrong are a lack of saving lists, and limits on to how much you can scan. I would enclose it with the article, but it's 800+k.

- OTTool (Also available from The Weasel's www site) - Smaller (83k!), but also less useful than AgNetTools. Can ping, traceroute, dns and reverse, and name scan. Can also find system info (what sort of CPU, OS, etc an IP is running). Also gives you more info about your system than AGNetTools, but overall, not nearly as good.
Both programs require Open Transport, and are OS8 compatable.

*Editors note: OTTool (Open Transport Tool) is made by the same company (AG Group) that makes AgNetTools. OTTool is no longer supported because it was replaced by AgNetTools.

HOW TO DO IT:

1). Install/launch/register the program of your choosing. I'm going to go over all three scans, so I'll be doing this from an AGNetTools standpoint. OTTool people, glean what you can.

2). Pull open the "Name Lookup" tool. Punch in an address you feel like using. For this example, we'll use yahoo.com. Click "Lookup", and you'll get the IP address for Yahoo. 204.71.177.35, if you are keeping score at home.
(Why did we do this? Well, AGNT has problems with large scans. So, it's useful to have the IP so we can make scans without having to guess at what IP to have it stop at and get error messages for three hours.)

3) Now, open the "Name Scan" window. Fortunately, for name scanning, there is no limit for the range of IP addresses. So, put Yahoo!'s IP in the first slot, and 255.255.255.255 in the last one. Click Scan, and watch it fly. Stop it around 204.71.177.170.

What do we have here? A list of fun domain names we didn't know about before! bait, mutha, poppa, interpix2, fool...what on EARTH could these be?

Let's move on to a service scan. We'll stick with Yahoo.

1) Open the "Service Scan" window.

2) Punch the IP for Yahoo in the top box.
Now, Service Scans are limited by Ram, so what we want to do is not go all the way to 255.255.255.255, but instead we want to add to the IP address. Add 2 to the third digit. For those of you unable to do mental IP math... 204.71.177.35 + 0.0.2.0 = 204.71.179.35
3) Put 204.71.179.35 in the second box. Leave Port on 23 (for telnet) Scan away. Once again, let it run to about .170.
Personally, I haven't any idea what UDP is, so I just ignore that. Looking at the TCP column, however, I see three hosts that allow telnet connections. Mission accomplished.

(Editors Note: UDP stands for "User Datagram Protocol". It is just an alternative to TCP)

Finally, let's do a port scan. This time, we're going to use epix.net.

1) Open the "Port Scan" window.

2) Type "epix.net" in the box.

3) Leave the radio buttons on "TCP", unless you have use for UDP info.

4) Alter the port range however you want.

5) Start the scan! Port scans generally take a lot longer than the other types. Data will roll in slowly, but if you look, we can see that port 23 is good (so we can telnet). Port 25 is good, so we could relay our mail through there, assuming there's no blocking software installed. Port 22 is undefined by AGNT. Let's see what it is.

6) Open your favorite telnet program, and telnet to "epix.net:23".

7) Curse as the session will be auto closed by epix.
Still, you see the purpose, I hope. Find what ports are open, look into them. See what you can see. Find the back doors, and maybe you'll pull off a good hack.

- remy

(P.S. If you read a recent issue of 2600, there was an item in the news section about cyberpromo.com. Try a whois with AGNT for cyberpromo.com. anyone feel like making a phone call to the spammers?)