NMAP 5

I am generally loath to write anything about a specific version of a tool, simply because most tools change so quickly. But in this case I feel I have to make an exception. You see nmap (get it here) , the new version 5 of nmap is truly something worth writing about. For as long as I can remember nmap has been the way to do network scans, it is able to be tweaked, to be adapted to do whatever you wanted. So right now, why do I think it is worth writing about?

- *It runs everywhere*. It does not matter is you use OSX or Linux or Windows or BSD, nmap will run for you.
- *Visualization*. The zenmap application allows you to graphically represent your scans, used properly it is a very useful way of mapping out your network
- *Ndiff*. a nice simple tool to compare 2 different scans and output the difference. A very nice way to quickly report on changes which nmap finds.
- *Ncat*. A redone version of the venerable netcat utility. This alone deserves (and will get) its own write-up.
- *Services*. The ability for nmap to actually query and report useful information from open ports, not just the banner. And this is user extensible. Gotta love that.
- *Optimizations*. Pages upon pages of optimizations and tweaks, better OS detection, more options for live host discovery, and the list goes on.

But even with all of that, what does it look like? Well, if you have used nmap before then the layout is fairly simple, but even if you have or have not used it before, nmap now has the *-A* option to make it easier..

```
-A: Enables OS detection and Version detection, Script scanning and Traceroute
```

Yep, and it works great..

```
#nmap -A --reason localhost

Starting Nmap 5.00 ( http://nmap.org ) at 2009-09-04 04:39 BST
Interesting ports on localhost.localdomain (127.0.0.1):
Not shown: 999 closed ports
Reason: 999 resets
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 5.2 (protocol 2.0)
|  ssh-hostkey: 1024 dd:1f:55:e0:86:c3:5c:0b:10:dc:10:a6:49:e4:d6:f6 (DSA)
|_ 2048 b0:67:b3:b7:a8:5a:63:82:bf:92:98:34:43:d4:04:23 (RSA)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.15 - 2.6.27
Network Distance: 0 hops
```

Leaving aside any other options, with the new capabilities, speed-ups and reporting, using nmap to monitor your network is now exceptionally easy. Just schedule your scans across your network, use the *-oX* to store the results in XML and then use *ndiff* to see the differences. Personally I think that is great for monitoring a network baseline. And yes, there are many other ways to use it (for any number of hat colors) but I think this may be something everyone can benefit from. So go take a look, play around and be amazed.