The Sysadmin's Daily Grind: Nmap 4

FYODOR'S DIET

Many tools keep growing with each new version, but Nmap 4.00 has lost weight thanks to the Diet-Nmap project. The latest incarnation of Nmap is not only quicker, it is also more frugal with memory.

BY CHARLY KÜHNAST

The Network Mapper tool, or Nmap [1], is my constant companion. Just recently, Nmap inventor Fyodor celebrated his brainchild's eighth birhtday, and the birthday present was a new diet of code with many useful new functions. One of the most exciting introductions is the addition of ARP scanning.

The operating system uses ARP requests to query MAC addresses on the target network. Nmap simply takes over this chore for the operating system, and as a result, the Nmap scanner generates a useful collection of reliable data on the number and type of active hosts on the network.

This feature totally removes the need for pinging or similar tricks. (Pinging is an imprecise technique, anyway, as there is no need for the host to respond). You don't even need to familiarize yourself with a new syntax. When you scan the local network, Nmap automatically chooses the more effective ARP scan, even if you specify *-sP* (Ping Scan) at the command line. According to the manpage, this only happens if you launch Nmap with root privileges. To tell the tool to keep its old behavior, you need to specify the *--send-ip* parameter.

Spoofer's Delight

The *--badsum* parameter is also new. It tells Nmap to send TCP or UDP packets with incorrect checksums to the target host. Almost any computer that receives a packet like this will drop it immediately, but if Nmap does receive a response, you can assume that the target to be a firewall or IDS that doesn't take the trouble of inspecting checksums. The tool can now easily spoof its own MAC address using the *--spoof-mac MAC address* command line option.

Nmap has supported operating system and version fingerprinting using the *-O* parameter for quite a while, but now fingerprinting is even more effective. For example, I scanned a router on my own lab network using the *nmap -O 10.0.0.50* command. I received the following output from Nmap 3.70 (reduced to the bare essentials):

```
MAC Address: 00:05:5E:96:3D:00
 (Cisco Systems)
No exact OS matches for host
```

Nmap 4.00 provides a far more accurate message:

```
Device type: router
Running: Cisco IOS 12.X
OS details: Cisco 2600
router running IOS 12.2(3),
Cisco router running IOS 12.1
```

The same applies to version fingerprinting. If I want to find out which version of the IMAP daemon is running on a server, I can type *nmap -sV 10.0.0.88 -p143* to get the results:

```
143/tcp  open    imap
UW imapd 2004.352
```

Nmap always has been a fantastic way of annoying people on your network, and wasting tons of paper, by scanning printers. Network printers often listen on port 9100, and more than a few printer models immediately convert any data sent to them on this port into hardcopy. The Nmap 4.00 developers have now introduced a smart paper-saving feature. When I entered *nmap -sV printer -p 9100*, I was first asked

```
9100/tcp open  jetdirect?
Excluded from version scan
```

which avoided the avalanche of paper. But this technique for saving paper doesn't mean that Fyodor is a spoilsport. If you decide you really want to waste paper after all, you can tell Fyodor's eight-year-old brainchild to scan *--allports*, thus extending the seven-year paper avalanche into the next generation. ■

INFO

[1] Nmap: *http://www.insecure.org/nmap/*

THE AUTHOR

Charly Kühnast is a Unix System Manager at the data-center in Moers, near Germany's famous River Rhine. His tasks include ensuring firewall security and availability and taking care of the DMZ (demilitarized zone).