The Sysadmin's Daily Grind: smap

FIND VOIP DEVICES

On a trip to Berlin, Charly discovers that the nmap port scanner has a new cousin who enjoys spying on phones – smap scans networks for VoIP devices.

BY CHARLY KÜHNAST

The CCC Congress has become one of my favorite events. I mainly visit the congress because of the excellent talks and workshops, but it's also a kind of community gathering where I might see people who I don't see for the rest of the year, although we regularly exchange email, chat on IRC, or even talk on the phone. Apart from that, it's a good thing to mingle with your own kind – sys admins, that is – from time to time.

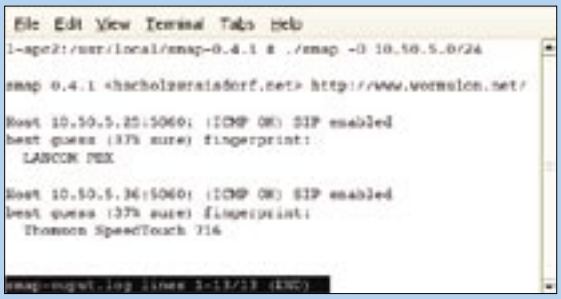

Figure 1: The smap scanner with the verbosity option -O guesses VoIP device names.

This year, I met Hendrik Scholz. Hendrik is an expert on anything that is remotely related to Voice-over-IP, including anything (in-)security related with respect to VoIP protocols and implementations. One thing in his box of tricks for the conference was smap [1]. Smap is a mix of nmap and sipsak [2]. It searches networks for VoIP devices and attempts to fingerprint them.

Being an inquisitive kind of person, I immediately jumped on the 30 KB tarball when I got back home. You can use *make* or *gmake* for the build.

Spot the Phone!

Admittedly, there are only two VoIP-compliant devices on my network at present, but smap immediately discovered them:

```
./smap 10.50.5.0/24
Host 10.50.5.25:5060: ➥
 (ICMP OK) SIP enabled
Host 10.50.5.36:5060: ➥
 (ICMP OK) SIP enabled
```

That's great, but now I wanted to know the device names. To find them, I enabled the fingerprinting option, which has two levels of verbosity: *-o* and *-O*. I select the latter for Figure 1. Teach mode, which you enable by setting the *-l* switch, lets you know all about the results of smap's individual fingerprinting tests shown in Listing 1.

If you need more detail, you can enable debug mode using the *-d* parameter. This gives you the details of the fingerprinting tests along with the normal results. As the version number of 0.4.1 would suggest, smap is still under development and shows some sign of instability at times. In particular, the number of known fingerprints is fairly small, but this is just teething trouble that I'm sure the developers will sort out in the near future. When that teething trouble is sorted out, smap will definitely have a spot in my toolbox. ■

Listing 1: ./smap -l 10.50.5.36

```
01 [...]
02 FINGERPRINT information:
03 newmethod=NR
04 allow_class=ignore
05 supported_class=ignore
06 hoe_class=16
07 options=400
08 brokenfromto=NR
09 prack=NR
10 ping=NR
11 invite=400
```

INFO

[1] Smap: *http://www.wormulon.net/files/pub*

[2] Sipsak: *http://sipsak.org*

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).