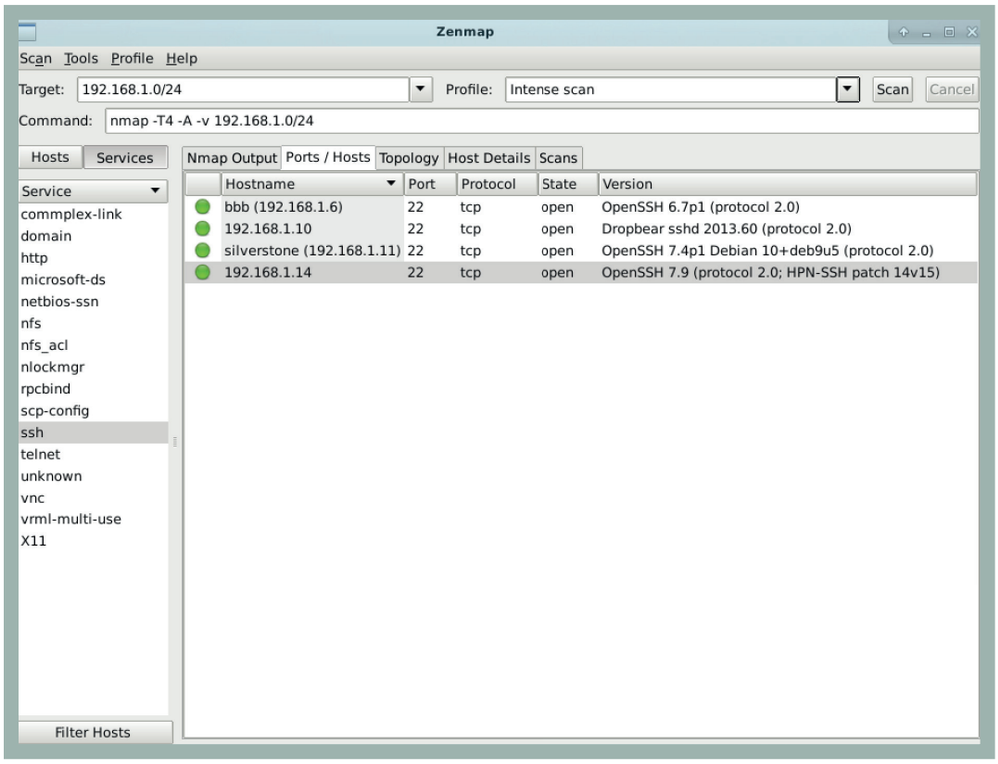
# Analyseer je netwerk

## DE BESTE APPS OM JE NETWERK BETER TE LEREN KENNEN

Linux bevat erg krachtige tools om netwerkverbindingen te analyseren. De meeste tools bestaan enkel voor de commandline, maar gelukkig zijn er ook uitzonderingen. We stellen hier kort drie verschillende tools voor met een grafische interface: Zenmap, EtherApe en Wireshark. **Filip Vervloesem**

Commandline tools hebben de reputatie dat ze moeilijk te gebruiken zijn. Voor beginners zijn ze over het algemeen inderdaad minder toegankelijk. Dat betekent echter niet dat grafische tools per definitie veel gemakkelijker zijn. Je hoeft niet de precieze syntax uit te zoeken voordat je aan de slag gaat, maar lukraak klikken in de gui brengt ook niet veel op. Je hebt nog steeds enige kennis nodig van de tool in kwestie en netwerken in het algemeen. Voor deze test bekeken we drie populaire tools met elk hun eigen toepassingsgebied. Zie ze dus niet als concurrenten van elkaar, maar eerder als verschillende troubleshooting tools voor andere problemen.




Zenmap is een overzichtelijke gui voor de nmap netwerkscanner.

### ZENMAP

Op de laatste pagina van dit blad maak je kennis met nmap, een populaire netwerkscanner voor de commandline. Zenmap is een gui die nmap iets toegankelijker hoopt te maken. Bij het opstarten, krijg je meteen de melding dat je nmap best als root opstart. Als gewone gebruiker krijg je immers niet alle mogelijkheden. (Dat geldt in feite voor alle tools die we hier bespreken.) De meeste distributies voorzien een extra menu-item om Zenmap als root te starten. Je hoeft slechts twee zaken in te vullen om een scan te starten:

- het doel, zoals één host (bijvoorbeeld 192.168.1.6) of een volledig netwerk (bijvoorbeeld 192.168.1.0/24);
- het scanprofiel.

Zenmap bevat standaard een tiental verschillende profielen, variërend van een snelle ping scan tot een grondige scan van alle poorten. Handig is dat je bij elk profiel de gebruikte nmap-opties ziet. Wil je exact weten wat Zenmap doet, zoek dan even die opties op in de nmap manpage. Voor meer uitleg over de verschillende types scans verwijzen we je naar de commandline tips verder in dit blad. Het is mogelijk om de nmap-opties van de profielen aan te passen of je eigen profielen aan te maken. De Profile Editor bevat een korte beschrijving van de meeste opties. Wil je een nmap-optie toevoegen die je niet in de Editor vindt? Dat kan via 'Extra options defined by user' onder het Other-tabblad.

### OVERZICHTELIJKE UITVOER

Heb je eenmaal een scan uitgevoerd, dan toont Zenmap nmaps tekstuitvoer in het rechtervenster. Gelukkig zijn er verschillende mogelijkheden om die uitvoer in een meer leesbare vorm te bekijken. In het linkervenster zie je meteen een lijst van alle gevonden hosts, inclusief een icoontje dat het besturingssysteem aangeeft. Selecteer nu een host en ga naar de tabbladen 'Ports / Hosts' en 'Host Details' voor meer informatie over die host. In dat eerste tabblad zie je welke services er op welke poorten draaien, eventueel voorzien van versie-informatie. In het tweede tabblad krijg je informatie over het besturingssysteem van de host (als nmap dat kon detecteren) en het aantal gescande poorten. Klik in het linker venster op 'Services' in plaats van 'Hosts' om te resultaten te groeperen via de gevonden services. Zo zie je meteen welke hosts bijvoorbeeld Samba of ssh draaien. Wat ons betreft, is Zenmap een mooie aanvulling op nmap om de resultaten eenvoudiger te doorzoeken.

### ETHERAPE

Vraag je je ook wel eens af welke netwerkverbindingen momenteel actief zijn op jouw PC? Dan moet je zeker EtherApe eens proberen.