open source

Arthur - Transfer the funds from the corporate account tonight

Mrežna zaštita (3)

Linux moramo osigurati i od napada preko mreže. Nakon što pronađemo i uklonimo sve programe koji bi mogli biti zloupotrijebljeni za napade, gotovo smo dostigli ideal sigurnog računala

Piše: Ivan Capan

Dosad smo uspjeli naučili kako štititi Linux računalo od problema koji bi se mogli pojaviti kad ono nije umreženo. Jasno je da je takvo računalo samo iluzija, pa ima li većeg izazova od 24-satnog priključka na Internet putem javno dostupne adrese? Upravo zato moramo biti posebno pripremljeni kad se jednom odlučimo priključiti taj kabel i kad paketi počnu teći, jer u tom trenutku sva paranoja postaje potpuno opravdana. Upravo tad počinje stalno nadmudrivanje s udaljenim hakerima i ništa se ne smije prepustiti slučaju. Neposredno prije priključivanja treba napraviti *backup* i *snapshot* sustava (da, ponavljamo se) nekim od prije spomenutih alata i početi pozorno pratiti neku sigurnosnu *mailing* listu (najbolje onu svoje distribucije). No, možda najbitnije je da osiguramo sustav zaustavljanjem nepotrebnih servisa.

Manje je bolje

Današnje distribucije, neposredno nakon instalacije, pokreću jednostavno previše raznih vrsta servisa. To su programi koji osluškuju dolazeće zahtjeve i izvršavaju neku funkciju - web server je servis koji sluša na portu 80 i na zahtjev šalje HTML kôd klijentu. Odaberemo li serversku instalaciju pogotovo u nekih *user-friendly* distribucija, broj pokrenutih servisa daleko prelazi broj onih koji su nam stvarno tada, pa i ikad potrebni. Jasno, distribucije ne mogu pogoditi naše želje i očito se nadaju da

▲ Inetd je glavni servis koji može pokretati ostale programe ako se za njima ukaže potreba

ćemo biti zahvalniji ako nas sve već to čeka na računalu, ali u današnjem nesigurnom svijetu vrijedi ona - manje je bolje. Za dio njih možda nismo nikad ni čuli, pa što će nam onda? Neki servisi mogu sadržavati - sad ili u budućnosti - sigurnosne pogreške koje bi mogle ugroziti sigurnost podataka ili cijelog računala. Neki, iako sigurni, mogu odavati previše informacija o računalu. Najbolji primjer za to je *finger*. On pruža informacije o trenutno aktivnim korisnicima na sustavu i - osim zaštite privatnosti - može napadaču dati vrijedne informacije. *Finger* je zaostatak iz prošlih dana Interneta kad smo se mogli pouzdati jedni u druge, a kad je naglasak bio na pružanju informacija, a ne njihovoj zaštiti.

Zbog svega toga vrijedi pravilo: zaustavimo li servis, više se njime ne moramo zamarati i on ne predstavlja prijetnju. Mogli bi ga i ukloniti, jer ga možemo nekad slučajno pokrenuti kod *restarta*, ali moramo se pobrinuti i za to. Naše napore ćemo okrenuti prema detekciji i zaustavljanju pokrenutih servisa, odnosno otežavanju pristupa do njih.