

open source



Linux sigurnost

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 naučiti kako štiti 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 pažljivo 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 oslušuju 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

```

Session Edit View Bookmarks Settings Help
amlican@redhat ~$ cat /etc/passwd | grep :x:
#STD: These are standard services.
#time dgram udp wait root internal
#inetd stream tcp nowait root /usr/sbin/inetd /usr/sbin/inetd
#rcp rcp stream tcp nowait root /usr/sbin/rcpd /usr/sbin/rcpd
#rsh rsh stream tcp nowait root /usr/sbin/rshd /usr/sbin/rshd
#rlogin rlogin stream tcp nowait root /usr/sbin/rlogind /usr/sbin/rlogind
#talk dgram udp wait nobody tty /usr/sbin/in.talkd in.
#talkd dgram udp wait nobody tty /usr/sbin/in.talkd in.
#MAIL: Mail, news and uscp services.
#imap2 stream tcp nowait root /usr/sbin/tcpd /usr/sbin/imapd
#imap stream tcp nowait root /usr/sbin/tcpd /usr/sbin/imapd
#pop3 stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.qpoppe
#pop stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.qpoppe
#SMTP# smtp stream tcp nowait root /usr/sbin/sendmail sendmail -Am -bs
#coff# SMT stream tcp nowait root /usr/sbin/sendmail sendmail -Am -bs
#coff# smtps stream tcp nowait root /usr/sbin/sendmail sendmail -Am -bs
#INFO: Info services
#finger stream tcp nowait nobody /usr/sbin/tcpd /usr/sbin/i
#BOOT: Tftp service is provided primarily for booting. Most sites
# run this only on machines acting as "boot servers."
#RPC: RPC based services

```

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

ćemo biti zahvalniji ako nas sve već to čeka na računalo, 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 računalo. 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.

ASBIS on **IT4profit**
www.it4profit.com/asbis/hr

UVIJEK NAJPOVOLJNIJI

intel

Maxtor

Seagate

HITACHI
Inspire the Next

CANYON

CHAINTECH
COMPUTER CO.,LTD.

TOSHIBA

Kingston
TECHNOLOGY