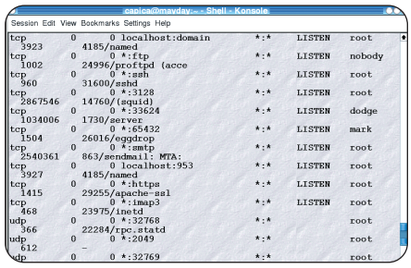


▲ Procesima koji zauzimaju mrežne resurse lako možemo saznati ime i vlasnika naredbom netstat

spomenuli, *inetda*. Prvi nam je korak izmjena njegove konfiguracijske datoteke inetd.conf u kojoj ćemo komentirati (znakom # koji je standardni Linuxov simbol za komentare) retke zaslužne za pokretanje neželjenih servisa. Nakon toga, trebamo samo *restartati inetd* pomoću "kill -HUP `pidof inetd`" (čudan znak nije jednostruki navodnik već tzv. *backtick* - znak dobiven tipkom iznad tipke *Tab* na engleskoj tipkovnici). Isprobamo li sad naredbu nmap, vidjet ćemo osjetno manji broj redaka ispisa. Dakle, pola puta smo prešli.

Sad ćemo zaustaviti i *daemone* koji ne ovise o inetdu. Način na koji ćemo to napraviti ovisi o distribuciji pa nećemo moći dati univerzalan recept. Neke imaju grafička sučelja u kojima se te stvari mijenjaju, a negdje (Debian) postoje skripte koje se pokreću u tu svrhu. U Debianu ćemo prvo zaustaviti servis pomoću "/etc/init.d/imeservisa stop", a za sprečavanje pokretanja: "update-rc.d -f imeservisa remove". Red Hat ima sličnu strukturu direktorija (/etc/rc.d/inet.d) i naredbu chkconfig, ali i intuitivno grafičko sučelje. SuSE to radi preko YaST-a.

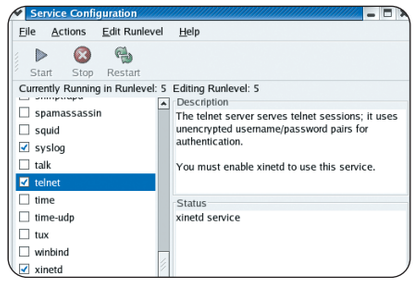
Naravno, cijelu proceduru trebalo bi ponoviti s vremena na vrijeme. Ako se naknadnom provjerom otvorenih portova pojavi neki novi servis na bezveznom portu za koji nismo nikad čuli niti ga prije vidjeli, prvo moramo provjeriti što on predstavlja (opisanom netstat naredbom). Ako nam je išta sumnjivo (program se primjerice nalazi u /tmp direktoriju i ima čudno ime), to je sigurna smjernica da je nešto pošlo po zlu. Radi li se o lokalnom računalu, preporučamo trenutno izvlačenje mrežnog kabela iz kartice, spremanje *log* datoteka na sigurno, ubijanje tog procesa, te forenziku: tko, na koji način, kada, otkuda, zašto i kolika je šteta. Nekad je najsigurnije ponovno napraviti instalaciju jer ne možemo biti sigurni što je na sustavu mijenjano.

Tipični servisi i njihov port

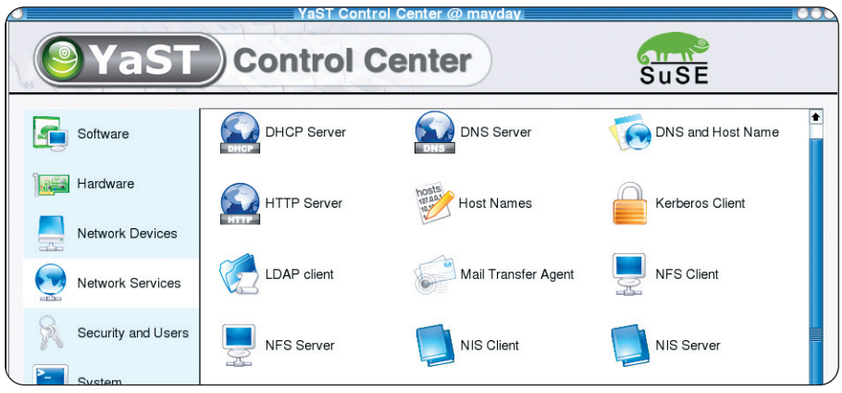
ftp	21/tcp	nekriptiran prijenos datoteka
ssh	22/tcp	kriptirano spajanje
telnet	23/tcp	nezaštićeno spajanje
smtp	25/tcp	*mail* server
domain	53/udp	DNS upiti
finger	79/tcp	podaci o korisnicima
www	80/tcp	web server
pop3	110/tcp	čitanje *maila*
sunrpc	111/tcp	izvršavanje udaljenih procedura
auth	113/tcp	podaci o *loginu* korisnika
nntp	119/tcp	Usenet *news* server
ntp	123/tcp	Network Time Protocol
netbios-ns	137/tcp	Netbios komunikacija
netbios-ns	137/udp	komunikacija s Windowsima
netbios-dgm	138/tcp	
netbios-dgm	138/udp	
netbios-ssn	139/tcp	
netbios-ssn	139/udp	
imap2	143/tcp	čitanje *maila*
imap3	220/tcp	
https	443/tcp	kriptiran web server
printer	515/tcp	
talk	517/udp	
rsync	873/tcp	prijenos datoteka
mysql	3306/tcp	baza podataka
postgres	5432/tcp	baza podataka
x11	6000/tcp	X Window System
ircd	6667/tcp	IRC server

Treba imati mjeru

Postupkom zatvaranja servisa možemo se i zanijeti toliko da ih sve onemogućimo. To onda predstavlja vrhunski siguran (iz mrežne perspektive) ali i potpuno beskoristan stroj. Javno potrebne programe (web, *mail*) nema smisla ograničavati, ali to ćemo učiniti s programima potrebnim užem krugu ljudi (ako što je ssh) i točno određenim IP adresama. Bilo koja druga neće moći ni blizu. Nekoliko je načina kako to postići. Često već i sam program u svojoj konfiguraciji podržava pristupne liste. Ta metoda nije toliko pouzdana budući da *bugovi* u samom programu još uvijek mogu doći do izražaja. Nešto su nižeg stupnja TCP *wrapperi* koji kontroliraju *inetd* servise ili ostale koji ih podržavaju. Oni slušaju zahtjeve i pokreću neki servis samo ako je klijent dozvoljen. Pokušaji spajanja se bilježe. Sintaksa konfiguracijske datoteke dosta je jednostavna, mogućnosti velike, no ipak se TCP *wrapperi* u posljednje vrijeme sve manje koriste. Današnji hit su *firewallovi* koji na najnižoj, jezgrinoj, razini mogu izvesti bilo kakvo ograničenje u umreženom okružju pa se zato i najčešće upotrebljavaju. Naravno, sve te metode možemo i kombinirati, ali bez nekog osobitog dobitka.



▲ Red Hat ima odlično riješen alat za pokretanje i zaustavljanje servisa; s opisima, no ne i konfiguracijom



▲ Suse ima YaST, centar za konfiguraciju važnijih servisa

Koristeći sve ove principe, kao i one navedene u prijašnjim tekstovima, Linux računalo smo podigli na jednu novu razinu sigurnosti. Naravno, nije bilo dovoljno prostora za detaljno opisivanje procedura, ali najbitnije koncepte smo - nadamo se - uspjeli nabrojati. U sljedećim tekstovima pokušat ćemo pobliže opisati neke od sigurnosnih programa koje smo prije tek spomenuli, a dovoljno su bitni da bi ih trebali poznavati u dušu.