

Što, gdje, kako

Da bismo nešto onemogućili, moramo se prvo uvjeriti da to postoji. Kako bismo se izvježbali u njihovom pronalaženju, moramo prvo kratko objasniti kako se zapravo svi ti servisi pokreću. Jedan dio njih se ne nalazi u nekoj *startup* skripti koja se izvršava pri pokretanju sustava, već postoji poseban globalni servis imena *inetd*. Njegov je princip da osluškuje na zadanim portovima i pokreće aplikacije kad se za njim ukaže potreba. Tako se smanjuje potreba za resursima ako se radi o rijetko korištenim programima jer oni ne moraju biti svi pokrenuti istodobno. Podaci o njima nalaze se u `/etc/inetd.conf`.

To neće raditi dobro ako su ti servisi često zahtijevani, jer ih onda servis svaki put mora ponovno pokretati, čekati dok završe, zaustaviti ih i tako u krug. Dulje se čeka da se neka aplikacija pokrene, troši više procesora i disk je opterećeniji. Zato se potrebne aplikacije pokrenu samo jednom na početku rada sustava. Nazivaju se *daemoni*, a najčešće kao zadnje slovo imena imaju "d" (*inetd*, *sshd*, *httpd*, *ftpd* itd.). Svi važniji servisi rade se kao *daemoni* pa njih često ni nećemo dirati, jer nam treba njihova funkcionalnost, odnosno bit su postojanja nekog servera. No to ipak nije slučaj sa svima, pa i njih moramo nekako locirati. Pogledamo li popis procesa na sustavu (`ps aux | less`), u desnom stupcu opaziti ćemo zavidan broj takvih. Neke od njih ne smijemo dirati iako im zadnje slovo imena odgovara našem kriteriju, poput *syslogd*, *klogd* i *kswapd*. Oni ne pružaju nikakve mrežne usluge, već su nužni za ispravan rad sustava (prvi se brine o logiranju, a druga dva su *kernel* procesi).

Ako nismo sigurni što koji proces radi, uvijek možemo naredbom "man program" pogledati njegovu *man* stranicu i tamo se informirati. No, nekad čak ni iz načina rada programa nije jasno li on sluša na mreži ili ne. Pritom mislimo na bazu MySQL, koja se (iako može slušati na portu ako joj dopustimo) za lokalne procese veže specijalnom *socket* datotekom i potpuno je nevidljiva izvana.

Skeniranje

No, samo će istrenirano oko uspjeti pohvatati sve procese na taj način, razlučiti mrežne od sistemskih, sjetiti se pogledati u `inetd.conf`, prepoznati koji je za što i odlučiti koji mu trebaju. Nama smrtnicima jednostavnije je direktno pogledati zauzeće portova, pa se zatim raspitivati što ih je to zauzelo. Za taj pregled možemo koristiti daleko najjači dostupni alat kodnog imena *nmap*. Sintaksa mu je u našem slučaju vrlo jednostavna i s "nmap localhost" dobivamo popis svih otvorenih portova TCP sloja mreže. Za UDP moramo dodati opciju "-sU". Razlike između ova dva sloja za naša su promatranja

```

screen - Shell - Konsole
Session Edit View Bookmarks Settings Help
PID TTY STAT TIME COMMAND
1 ? S 0:08 init [3]
2 ? SW 0:00 [keventd]
3 ? SW 0:02 [ksoftirqd_CPU0]
4 ? SW 0:00 [ksoftirqd_CPU1]
5 ? SW 0:03 [kswapd]
6 ? SW 0:00 [bdflush]
7 ? SW 1:11 [kupdated]
8 ? SW 0:00 [scsi_eh_0]
9 ? SW 0:00 [scsi_eh_1]
10 ? SW 0:00 [kreiserfsd]
19075 ? S 0:00 /sbin/rpc.portmap
8763 ? S 0:44 /usr/sbin/syslogd
27841 ? S 0:00 /usr/sbin/klogd -c 3 -x
10800 ? S 0:01 /usr/sbin/inetd
8549 ? S 0:00 /usr/sbin/sshd
1798 ? S 0:00 /usr/sbin/crond -l10
27579 ? S 0:35 sendmail: accepting connections
17312 ? S 0:00 sendmail: Queue runner@00:25:00 for /var/spool/clientmqueue
6813 ? S 0:01 proftpd (accepting connections)
31668 ? S 0:00 /bin/sh /usr/bin/mysqld_safe --user=mysql --pid-file=/var/lib/my
sql/www.pid --datadir=/var/lib/mysql -O max_connections=1000
30391 tty1 S 0:00 /sbin/agetty 38400 tty1 linux
9663 tty2 S 0:00 /sbin/agetty 38400 tty2 linux
23314 tty3 S 0:00 /sbin/agetty 38400 tty3 linux
6508 tty4 S 0:00 /sbin/agetty 38400 tty4 linux
30939 tty5 S 0:00 /sbin/agetty 38400 tty5 linux
14731 tty6 S 0:00 /sbin/agetty 38400 tty6 linux
24090 ? S 0:04 /usr/libexec/mysqld --basedir=/usr --datadir=/var/lib/mysql --us
er=mysql --pid-file=/var/lib/mysql/www.pid --skip-locking -O max_connections=1000
lines 1-28
02/08/04 01:22 0.03 0.03 0.00

```

▲ Popis procesa na sustavu otkriva velik broj *daemoni* od kojih su neki ključni za rad sustava

previše suptilne i izlaze iz okvira teksta, no recimo da je moguće u računalo upasti putem bilo kojeg, ako ga servis koristi. TCP je nešto češći u klasičnoj internetskoj komunikaciji, dok je UDP češći u *streaming* prometu, gdje nije previše bitan minimalni gubitak informacija, već njihova pravovremena isporuka.

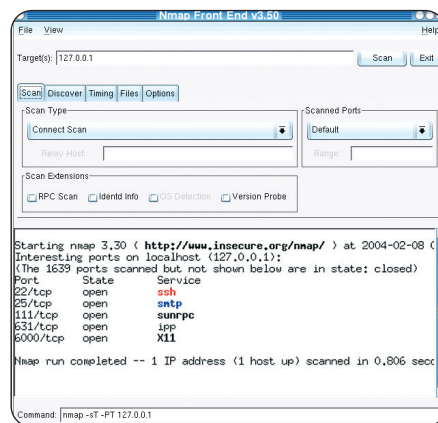
Nakon što smo se nekako dočepali popisa, čudom se čudimo svim tim kriptičnim skraćenicama, za koje nam nije baš jasno što znače. Da bismo se malo bliže upoznali s njima (želimo saznati ime programa i korisnika), koristit ćemo "netstat -tuple" koji će nam u pomalo opskurnoj formi vratiti tražene podatke. Inače, vrlo je korisno pobliže se upoznati s kombinacijama port/servis, a neke češće smo naveli u tablici (cjelovit popis nalazi se u `/etc/services`). Koji od njih nam smeta, neće biti uvijek lako odrediti, no ako zaustavimo krivi i nešto se potrga, uvijek ga možemo ponovno pokrenuti.

```

screen - Shell - Konsole
Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Warning: You are not root == using TCP pingcan rather than ICMP
Interesting ports on localhost (127.0.0.1):
(The 1538 ports scanned but not shown below are in state: closed)
Port      State  Service
21/tcp    open   ftp
22/tcp    open   ssh
25/tcp    open   smtp
53/tcp    open   domain
80/tcp    open   http
110/tcp   open   pop3
111/tcp   open   sunrpc
139/tcp   open   netbios-ssn
220/tcp   open   imap2
443/tcp   open   https
515/tcp   open   printer
587/tcp   open   submission
783/tcp   open   hp-alarm-mgr
953/tcp   open   rndc
2401/tcp  open   cvspserver
3128/tcp  open   squid-http
Nmap run completed -- 1 IP address (1 host up) scanned in 0 seconds

```

▲ Popis svih otvorenih portova na sustavu lako se dobiva programom *Nmap*



▲ Grafičko sučelje programa *Nmap* jednostavno je za korištenje

Često su kao nesigurni servisi označeni oni koji na neki način primaju nekriptiranu lozinku, pa bi tako bilo poželjno izbjegavati *telnet*, *ftp*, neke starije (*rsh*, *rlogin*) pa čak i *pop3* za *mail*. Svi - pa makar sami po sebi bili najsigurniji na svijetu - mogu otkriti lozinku bilo kojeg korisnika i to bi haker uz vrlo malo truda mogao iskoristiti za spajanje.

Istjerajmo demone iz pingvina

Sad dolazi najkorisniji dio posla. Sve te suviše programe trebamo locirati, zaustaviti i onemogućiti im pokretanje kod *restarta* sustava. Počnimo od stvari koju smo prvu

UVJETI U DISTRIBUCIJI KOMPONENATA

POI

ALPS

Gadaptec

MMORE

Prestigio

TEAC

LITEON

NEC

iomega