metodom isprobavanja svake riječi (*brute-force*) iz višejezičnih rječnika pokušavaju pogoditi ispravnu. Nerijetko i uspiju. Administratori bi također trebali pokretati te programe, kako bi ih preduhitrili i natjerali korisnike da ih mijenjaju. Primjeri takvih programa su *Crack* ili *John the Ripper*.

Još jedna od metoda prikupljanja lozinki je *sniffing* ili prisluškivanje mrežnog prometa. Lozinke kroz mrežu putuju nekriptirane i netko na pola puta (najčešće posebno računalo) uz vrlo malo truda može skupiti zavidnu količinu informacija o sustavu. Servisi poput telneta, običnog FTP-a, POP3 *maila* imaju tu neugodnu osobinu da primaju nezaštićenu lozinku (*plain text*). To se donekle može riješiti zamjenama protokola za komunikaciju. SSH kao zamjena za telnet kriptira sav promet kroz mrežu garantirajući privatnost i sigurnost. On je apsolutno nužan kod bilo kakve udaljene administracije, jer bi inače bilo kakvo upisivanje *root* lozinke preko mreže rezultiralo ozbiljnim problemima.

Dobra je praksa ograničavanje spajanja (*firewallom* ili u konfiguraciji servisa) samo s dozvoljenih IP adresa. Tako bi, primjerice, zaposlenici neke tvrtke svim servisima pristupali samo iz lokalne mreže, dok s Interneta imaju dozvoljen samo POP3.

Zaštita direktorija

Na višekorisničko računalo treba obratiti posebnu pažnju. Korisnicima je potrebno u početku dodijeliti najmanja prava, a kasnije ih prema potrebama proširivati. Treba izbjegavati omogućivanje pokretanja ljuske (*shell*), tj. naredbenog retka, jer to često nije potrebno. Korisnicima-početnicima se obično dodijeli lažna ljuska (/bin/false).

Bitan dio sustava su direktoriji i datoteke. Treba biti siguran da korisnici ne smiju pisati na mjestima gdje to nije predviđeno (izvan direktorija /home i /tmp) i da ne smiju pregledavati datoteke koje sadrže osjetljive informacije. Sam Linux bi se trebao brinuti o tome, no nije loše automatiziranim skriptama ponekad to provjeriti. Isto tako bi trebalo definirati kvote (količina datoteka koja se može držati), dovoljno velike da korisnicima ne smetaju, a opet dovoljno male da netko ne popuni cijelu particiju onemogućujući rad svima. Prilikom instalacije dobro je definirati dovoljno particija (*home, var, usr, tmp, root*) budući da svaka ima drugačiju namjenu i trebala bi biti odvojena. Particije po kojima svi mogu pisati (/tmp i /var/tmp) trebaju se montirati s opcijama “nosuid” i “noexec” u /etc/fstab kako korisnici ne bi mogli ništa pokretati iz njih, niti koristiti *setuid* programe. To su obični programi kojima je dodana opcija da se pokreću s pravima vlasnika datoteke. Primjerice, ako se *setuid* prava dodijele naredbi “ls” koja je u *root* vlasništvu, bilo tko će moći izlistavati i zaštićene direktorije. Korisnicima se mogu dodijeliti povećana, ali ne i potpuna administratorska prava putem programa *sudo*, koji može definirati listu programa što se pokreću “kao *root*”.

Backup podataka štiti kako od hakera, tako i od fizičkih kvarova i apsolutno je nužan. Spremaju se korisnički podaci (/home) i postavke sustava (/etc) i promjenjive datoteke (/var). Naravno, i same medije za *backup* treba čuvati na sigurnom mjestu.

▲ linuxsecurity.com vodeći je portal o sigurnosti, s ažurnim vijestima i kvalitetnim uputama

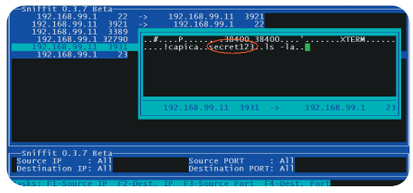
Od neovlaštenog mijenjanja datoteka štite nas IDS (Intrusion detection) sustavi (Tripwire, AIDE) koji prođu kroz sve datoteke na sustavu, generiraju *checksum* datotke (*md5sum*) i spreme ih na *read-only* medij (disketa, CD) kako ih ne bi netko naknadno mijenjao. Njime možemo otkriti je li netko promijenio postojeću izvršnu datoteku pretvorivši je u *trojana* - podmetnutu datoteku, skrivenu iza lažnog imena - i vratiti originalnu.

Nadzor i logiranje

Pravi administrator mora u svakom trenutku imati uvid u sve što se događa na sustavu. Kako čak i on ponekad mora spavati, za to vrijeme sam sustav na za to predviđena mjesta marljivo bilježi što su programi, pa čak i korisnici, radili. Prije nego što pomislimo kako je ovo napad na nečiju privatnost, recimo da se bilježe samo imena naredbi koje su korisnici pokretali. Ostali *logovi* bilježe zapise od programa kojima je to centralizirano mjesto za čuvanje podataka (/var/log). Tako, primjerice, web server skuplja zapise o pristupanim web stranicama, *mail* server bilježi svaki *e-mail* koji je prešao preko njega, sigurnosne se informacije također čuvaju kako bi kasnije poslužile, ako nastanu problemi, da se vidi što se dogodilo. Bitno je da računalo ima točno vrijeme (održava se programom ntpd) radi lakšeg praćenja tragova.

Na opterećenim serverima te se datoteke povećavaju velikom brzinom i nužno je složiti mehanizme (skripta *logrotate*) koji ih jednom dnevno komprimiraju, a nakon nekog vremena brišu ili snime na CD. Jedna od metoda zaštite tih datoteka (kod provale hakeri ih gotovo uvijek mijenjaju kako bi prikrili tragove) je i njihovo kopiranje na udaljeno računalo, a za najparanoičnije ispis na igličnom pisaču.

▲ Skripta Logcheck periodički administratoru šalje *mail* s važnijim detaljima iz log datoteke



▲ Program sniffit može hvatati bilo kakvu lozinku koja nekriptirana putuje mrežom

Kod velikih količina podataka vrlo je teško čitati silne megabajte teksta. Za tu svrhu razvijeni su *logwatch* i *logcheck*, programi koji će periodički pregledavati *log* datoteke i *mailom* administratoru slati dijelove koje smatraju sigurnosnim problemima.

Zaštita jezgre - grsecurity

U posljednje se vrijeme pojavilo nekoliko sigurnosnih rupa u 2.4. seriji *kernela*, kojima se moglo dobiti administratorska prava na računalu. Zbog toga je potrebno pratiti razne sigurnosne *mailing* liste (ili vijesti na portalu linuxsecurity.com) i brzo reagirati kad se takvo nešto pojavi, te instalirati novi *kernel* ili zakrpu (*patch*). Osim toga, *kernel* može poslužiti kao dodatni stupanj zaštite jer može onemogućiti brojne pa i tek otkrivene sigurnosne rupe. Naime, većina problema u programima rezultat je prepunjenosti stoga (*stack*), privremene lokacije u memoriji koju programi koriste za podatke. Slanjem previše podataka oni se počnu zapisivati na mjestima koja za to nisu predviđena i mogu program dovesti do rušenja, ili - ako su u pitanju posebno pripremljeni podaci - do izvršavanja bilo kakvog programskog koda. Takve su metode baza većine rupa (*exploit*) u bilo kojem operacijskom sustavu.

Instalacijom posebnih zakrpa *kernel* može spriječiti izvršavanje takvog koda i time onemogućiti mnogobrojne rupe, pa i one koje tek trebaju nastati. Najpoznatija zakrpa te vrste je Grsecurity (grsecurity.net). Ona također štiti i od “fork bombi” - programa koji zauzmu svu raspoloživu memoriju, štiti /proc direktorij kako napadač ne bi mogao saznati detalje sustava, može štititi datoteke od neovlaštenog mijenjanja, bez obzira na prava korisnika i brojna druga poboljšanja. Zbog brojnih opcija, nije ju jednostavno složiti, a i neki legitimni programi uz nju neće raditi kako treba. No, zbog dobitaka koje pruža, svakako je preporučujemo.