Linux sigurnost

Potpuna kontrola (4)

Velik je broj programa za Linux pomoću kojih možemo nadzirati mrežu u očekivanju sigurnosnih problema. Neki (Snort) imaju popise tipičnih napada, pa onda osluškuju mrežni promet, dok drugi pregledavaju računalo u potrazi za problemima (Nessus)

Piše: Ivan Capan

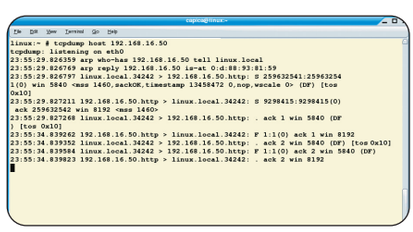
Nakon što smo u prethodnim nastavcima naučili osigurati umreženo računalo, poželjet ćemo da ono tako sigurno i ostane. Vrlo je bitno nadzirati stanje u mreži, budući da će iz tog smjera doći većina napada. Zlođudni mrežni paketi mogu biti namijenjeni istom tom računalu, ali se mogu zaputiti i prema nekom drugom. Ako je Linux na pola puta (tipični *firewall*), može ih zaustaviti prije odredišta. Nije li savršen osjećaj saznanje da Linux računalom možemo zaustaviti viruse klase W32.*, namijenjene računalima u mreži, koja se ponekad ne mogu sama braniti. Moć da pregledavamo promet dok prolazi kraj nas i da s njim činimo što nas je volja jako je dobro iskorištena raznim programima. U kontekstu sigurnosti to su programi za provjeru upada (*Intrusion detection*). Najpoznatiji takav je Snort. Često je korišten i portsentry kao protumjera skeniranju računala.

Trebamo li samo pasivno pratiti mrežni promet bez tumačenja sadržaja, tu su ngrep, referentni tcpdump, dotjeraniji Ethereal, svemoćni dsniff i interaktivni iptraf.

Bavimo li se zaštitom računala, stupanj njihove sigurnosti najbolje ćemo provjeriti programima koji već imaju bazu raznih sigurnosnih problema, kao i načine njihova testiranja. Tipičan predstavnik je Nessus, a pomoći će nam i nmap.

IDS - otkrivanje upada

Sustavi za provjeru upada - IDS - koriste se za nadzor aktivnosti u mreži. Promatraju pakete s podacima, formiraju neku informaciju te ju uspoređuju s vlastitom bazom. Iz toga mogu zaključiti je li taj promet možda zlonamjeran. Najvažnija je svrha takvog pristupa otkrivanje upada izvana. Tako možemo otkriti pokušaj neovlaštenog pristupa prije nego što je zahtjev uopće došao do ciljanog računala. Ono što IDS sustavi ne mogu napraviti, za razliku od *firewalla*, jest blokirati neovlašteni promet (iako ima dodataka i za to). Njihova je namjena isključivo nadzor, oni će trenutno upozoriti administratora da se nešto događa, pomoći u pronalaženju krivca, rekonstrukciji i dokumentiranju napada.



▲ **Tcpdump, osim što daje uvid u promet naše mreže, može poslužiti i kao edukacijski alat**

Razvoj IDS-a cijela je nauka, možda područje kojem se u sigurnosnoj problematici trenutno dodjeljuje najviše pozornosti. To je i razumljivo, budući da se kreće od pretpostavke da se problemi moraju prvo otkriti, kako bi se u idućem trenutku zaustavili. Iako se neprestano pojavljuju novi sigurnosni problemi, modularnost programa omogućuje njegovo ažuriranje.

Snort - njuškalo

Iako postoje vrlo skupa komercijalna rješenja, jedan od ponajboljih IDS programa dolazi iz Open Source svijeta - Snort. Iako ne previše trivijalan za instalaciju, koristi jasno definirana pravila za opis problema koje pronalazi, pa tako i korisnik ima priliku prilagoditi ga svojim potrebama. Neke od mogućnosti koje podržava su detekcija skrivenih skeniranja portova (nmap), preljeva *stacka* (*overflow*), CGI skriptnih napada, SMB i NetBIOS zahtjeva, raznih mrežnih problema i slično, pa čak i nekih tipova virusa za Windowse. Formati zapisa nisu baš previše čitljivi, no postoji ACID (*Analysis Console*) za pretraživanje i ispis podataka te statistika o napadima.

Sličan po filozofiji, no za red veličine manje funkcionalnosti, zgodan je programčić portsentry. Njegova namjena je otkrivanje skeniranja portova, te blokiranje računala izvora napada. Radi tako da osluškuje na nekim od definiranih portova i reagira kad na nekoliko njih slijedno stigne nepoznat zahtjev. Glavna mu je prednost lakoća konfiguriranja, jer radi dobro praktički odmah po instalaciji. Potrebno je jedino ukloniti oznaku komentara s prave naredbe za pokretanje u slučaju napada (iptables), koja će potpuno blokirati pristup udaljenom računalu.

Nadzor mreže

Ne mora sav promet u mreži biti zlođudan i kao takav objekt Snortove analize. Vrlo često moramo pratiti opće stanje u mreži, protok informacija, tip prometa, odredište i smjer kojim komunicira pojedino računalo. Takva situacija pojavljuje se u bilo kakvoj dijagnostici mreže, neovisno je li ona u prekidu ili neko od računala "divlja" prometom, a mi moramo saznati njegov identitet. Bilo kakav paket koji prođe kroz ili pokraj Linux servera može biti uhvaćen, analiziran i spremljen.

Klasičan alat za tu namjenu jest tcpdump. Pokreće se iz naredbenog retka, brz je, jednostavan i lak za korištenje. Osnovna namjena mu je "skidanje" zaglavlja paketa iz mrežnog