Fail2ban - savjeti i trikovi

Matko Kosmat | 31 ožujka, 2026

Brute-force i DDOS mrežni napadi na razne servise su svakodnevica svakog sistem-inženjera već dulji niz godina. Postoji niz rješenja koji pokušavaju riješiti taj problem, bilo hardverskim bilo softverskim putem. Fail2ban je softverski alat koji prati sumnjive unose u logovima, te nakon predefiniranog broja ilegalnih akcija jednostavno izolira napadača preko nekog od firewall mehanizama.

Fail2ban je dostupan i kao CARNet paket fail2ban-cn.

Slušajući zahtjeve kolega sistem-inženjera, u CARNetovu ponudu paketa uvrstili smo fail2ban-cn. Riječ je o jednostavnom i efikasnom sustavu zaštite koji prati logove i na određene učestale pojave blokira napadača.

Ovo čini uporabom iptables pravila, te tako blokira sve IP adrese s kojih dolaze napadi. Napadi najčešće dolaze od strane slabo upućenih korisnika, koji pokreću skripte i programe koje pronađu na Internetu (takozvani *script-kiddies*). Uspješnost provala preko ovih skripti je izuzetno niska, ali resurse utrošene s naše strane na ove napade, kao i mogućnost upada na sustav ne treba zanemariti.

Iako postoje drugi sustavi zaštite zasnovani na ovom principu, fail2ban je jedan od najjednostavnijih. On štiti odmah nakon instalacije, i ne traži više nikakvo konfiguriranje. Automatski štiti od SSH napada, iako je moguće zaštititi i druge servise bazirane na PAM-u.

Odmah ćemo se osvrnuti na mane fail2ban pristupa. Fail2ban je često kritiziran kao nepotreban servis, jer troši sistemske resurse (doduše, jako male), a ista se stvar može postići s recent mehanizmom ugrađenim preko modula ipt_recent (http://www.snowman.net/projects/ipt_recent) u iptablesima.

Najopasnije što se može dogoditi s fail2ban pristupom je da bilo tko na sustavu može uspješno zaustaviti rad bilo kojeg servisa krivotvorenjem unosa u logovima. Zapisati nesto u logove mogu i programski jezici, primjerice PHP, pa stoga treba pripaziti na to tko može pisati u logove. Možda bi bilo dobro zaštititi /dev/log device tako da se promijeni grupa, a sve servise potom upišemo u tu grupu.

Da ti napadi nisu rijetkost, pokazat će sljedeća naredba, odnosno niz naredbi:

Nakon instalacije, sustav automatski postaje aktivan i podrazumijevano je sustav zaštićen od SSH *brute force* napada. Pogledajmo te podrazumijevane vrijednosti, i lokacije konfiguracijskih datoteka.

Glavna konfiguracijska datoteka je /etc/fail2ban/fail2ban.conf. Ostale konfiguracijske datoteke se, kako je to već uobičajeno na Debianu, nalaze u conf.d direktorijima action.d, filter.d, te u dodatnoj konfiguracijskoj datoteci jail.conf. Ove konfiguracijske datoteke odražavaju interni način rada fail2ban-a:

filter - određuje što će izazvati "okidanje" akcije, uporabom regularnih izraza
action - određuje jednu ili više odgovora na "okidanje"
jail - skupina filtera i jedne (ili više) akcija

Navest ćemo primjer za SSH. U datoteci jail.conf se nalazi unos:

U datoteci action.d/sshd.conf možemo naići na unose poput ovoga:

I na kraju, u datotekama akcija (podsjetimo se, može ih biti više za jedan jail) možemo naći iptables pravila. Primjerice:

Iptables pravilima se nećemo u ovom članku baviti, samo ćemo reći da fail2ban prilikom starta

pokreće akciju "actionstart", prilikom gašenja "actionstop", a i ostalim akcijama samo ime govori prilikom čega se pokreću.

U prvom nastavku iz serije članaka o fail2ban sustavu zaštite uveli smo vas u osnovne postavke i način rada fail2ban sustava. U ovom nastavku ćemo malo više obratiti pažnju na ono što se zbiva “ispod haube”.

Fail2ban rabi standardni način rada, putem *daemona* i klijentskog programa. S daemon programom ne bismo trebali imati nikakav direktan kontakt, jer se sve poruke daemonu mogu navesti preko klijenta. Daemon, ipak, kod starta prima određene opcije, pa ćemo ih navesti.

Kao što se može vidjeti, opcije su iskoristive praktički samo kod *debugiranja* i testiranja, pa se nećemo na njima zadržavati, jer je opis samorazumljiv. S druge strane, klijent prima sljedeće naredbe:

I ovdje možemo vidjeti da opcije prije svega služe za razna testiranja prije puštanja u produkciju. Najzanimljivije su opcije za smanjivanje i povećavanje razine zapisa u logovima (*verbosity*). Razina 1 je minimalna razina, a razina 4 se rabi samo u postupku eventualnog *debugiranja*.

No, najsnažnija karakteristika klijenta je direktna mogućnost konfiguriranja cijelog sustava, baš kao da smo rabili konfiguracijske datoteke. Naredbi je mnogo, pa ćemo opisati najkorisnije, a druge ćemo samo spomenuti. Za daljnje informacije pogledajte dokumentaciju na adresi http://www.fail2ban.org/wiki/index.php/MANUAL_0_8.

Naredbe koje fail2ban-client podržava:

Opcija iza get/set naredbi ima mnogo, primjerice *addignoreip*, *addlogpath*, *addfailregex*, *findtime* i tako dalje. No, vjerojatno je besmisleno na ovaj način učiti konfigurirati fail2ban, i držati se konfiguriranja preko standardnih konfiguracijskih datoteka. Ipak, neke naredbe bi bilo dobro znati, primjerice:

Dakle, trenutna razina je INFO (razina 3). Ostale razine su: ERROR (1), WARN (2) i DEBUG (4).

Fail2ban ima i interaktivni način, pa ćemo ostale opcije demonstarirati na taj način. Ulazak u interaktivni način je pomoću opcije "-i".

Dakle, ova naredba se isto mogla izvršiti i direktno iz naredbene linije, a prikazuje u koju datoteku se zapisuju logovi.

Slično kao i standardna naredba "ping" koja daje osnovnu informaciju je li mrežni uređaj aktivan, i ovdje ona samo daje potvrdu da je daemon "živ", bez dodatnih informacija.

Naredba "status" bez dodatnih opcija daje samo popis trenutno aktivnih zatvora.

Nešto izdašniji ispis daje naredba "status <JAIL>", gdje ćemo dobiti statističke podatke o tome koliko je adresa trenutno na "čekanju", te koliko ih je trenutno na crnoj listi. Adresa će na crnu listu doći kad prekorači zadane parametre.

Sa naredbom "stop" možemo određene zatvore zaustaviti, bilo radi dodatne konfiguracije, bilo radi pogrešnog rada, (pre)opeterećenja sustava i slično.

Kad smo se upoznali s osnovama i načinom rada, dalje je prilično jednostavno. Nakon instalacije paketa, automatski miate zaštitu od SSH i PAM napada (a autentikaciju preko PAM-a rabi većina servisa, primjerice login). Neki za autentikaciju ne rabe PAM, primjerice Apache može rabiti direktno LDAP, ili vlastiti htpasswd mehanizam. U tom slučaju, sve što trebate učiniti je uključiti odgovrajući zatvor u jail.conf:

Za uključivanje je dovoljno promijeniti prvi redak u:

Nakon toga samo treba napraviti *reload*:

i provjeriti je li zatvor uključen:

Od tog trenutka je aktivna i zaštita definirana s parametrom *failregex* unutar datoteke /etc/fail2ban/filter.d/apache-auth.conf.

Slična stvar je i sa drugim servisima, jedino kod mail servisa (kod nas je standardan Postfix), možda će trebati promijeniti putanju do logova:

u

U sljedećem, zadnjem, nastavku, pokazat ćemo vam kako prilagoditi fail2ban svojim potrebama, te napraviti vlastite filtere i akcije, u slučaju da ne postoje odgovarajuće u postojećoj distribuciji.

U prethodna dva nastavka smo vam pokazali način rada, te osnovnu konfiguraciju i uporabu programa **fail2ban**. U ovom nastavku zaokružit ćemo priču, i objasniti kako napraviti svoj, odnosno prilagoditi neki postojeći filter svojim potrebama.

Kako sam fail2ban donosi filtere za većinu servisa koji će vam ikada trebati, bio nam je problem osmisliti neki novi filter. No, ipak smo se dosjetili jedne svima poznate pojave u apache logovima: tragovi potrage za bugovitim skriptama na sustavu.

Obično se traže stare inačice PHP skripti, a najčešće je to phpmyadmin. PhpMyAdmin je PHP skripta za jednostavan rad s MySql bazama podataka na vašem sustavu, ali je poznat po mnogobrojnim sigurnosnim rupama.

U vašim logovim često možete vidjeti unose slične ovima:

Napadači žele "ispipati" imate li PhpMyAdmin, i koje je inačice. Naravno, obično se radi o *script-kiddies* korisnicima, ali koji ipak uz pomoć određenih programa mogu upasti na vaš stroj. Iz tog razloga je najbolje preventivno onemogućiti napadačevu IP adresu. Pa, krenimo redom.

U direktoriju /etc/fail2ban/filter.d napravimo novu datoteku apache-php.conf (izostavili smo komentare radi kratkoće, vi ih slobodno ostavite):

Umjesto XX i YY upišite IP adrese i adrese mreže svog LAN-a, i adrese vaših suradnika koji trebaju pristu PhpMyAdminu. Slično možete i za bilo koji dio IP adrese, s napomenom da oznaka '\d' označava regex klasu '[0-9]', dakle obuhvaća sve brojeve od 0 do 9. Ovu sintaksu, među ostalim, rabi programski jezik Python u kojem je napisan fail2ban.

U datoteku jail.conf dodamo retke:

i napravimo

Što smo ovime napravili? Rezultat će biti zabrana pristupa bilo kojem klijentu (koji nije u varijabli ignoreregex), a koji pokuša više od 5 puta pristupiti PhpMyAdmin programu. Ovo će odraditi iptables.conf, no vi možete birati i između nekoliko drugih načina zaštite (primjerice preko tcp_wrappera).

Sami regularni izrazi su *case-sensitive*, i morat ćete pripaziti na velika i mala slova, što uopće nije loše kako slučajno ne bi onemogućili previše stvari odjednom.

Umjesto zabrane, možete jednostavno poslati mail sebi ili drugim kolegama da se nešto događa. U iptables.conf upišite:

Uz zabranu, fail2ban će poslati mail s osnovnim informacijama na neku adresu. Oprezno s ovom funkcijom, kako pretjerani broj mailova ne bi napravio DDoS sam po sebi!

Na kraju, samo ćemo navesti konfigurabilne parametre koje možete rabiti u svojim "zatvorima". Iako su im imena samoobjašnjiva, radi potpunosti navest ćemo ih, zajedno s pretpostavljenim vrijednostima:

Broj pokušaja, točnije, broj puta kada je neki redak u logovima odgovorao regexu koji smo postavili. Radi se o
individualnim brojevima za svaku IP adresu.

Filter se nalazi u direktoriju /etc/fail2ban/filters.d, u našem slučaju bi to bio apache-php.conf. Vrijedi napomenuti da svako pravilo unutar filtera povećava brojač (maxretry) za jedan, naravno ukoliko se redak u logu poklapa sa zadanim regularnim izrazima.

Brojač će se vratiti na nulu, ukoliko unutar ovog vremena s iste adrese ne bude nikakve dodatne aktivnosti. Neki programi pokušavaju proći "ispod radara" i svoje pokušaje smanjuju na jedva primjetnu razinu. Neke pak treba što prije detektirati i onemogućiti, pa je namještanje ove vrijednosti individualna potreba svakog sistemca i stroja.

Vremenski period koliko će određena IP adresa biti zabranjena.

Jednostavno, putanja do log datoteku koju ćemo nadzirati. Može biti /var/log/syslog, ili bilo što drugo, pa čak i izvan /var/log.

Obavezno istestirajte nova pravila prvo na neprodukcijskom stroju, a ukoliko zapnete konzultirajte Wiki dokumentaciju na http://www.fail2ban.com/wiki, a pomoć za Python regularne izraze možete naći na http://docs.python.org/dev/howto/regex.html.

Za općenite regularne izraze, jako dobar izvor informacija je web sjedište http://www.regular-expressions.info/.

Sretno u uporabi fail2ban sustava!