https://doi.org/10.37528/FTTE/9788673954752/POSTEL.2023.012

PROGNOZIRANJE INTENZITETA *BRUTE-FORCE* NAPADA U FUNKCIJI OPTIMIZACIJE NIVOA ZAŠTITE

Slobodan Mitrović, Valentina Radojičić, Goran Marković
University of Belgrade - Faculty of Transport and Traffic Engineering
s.mitrovic@sf.bg.ac.rs, valentin@sf.bg.ac.rs, g.markovic@sf.bg.ac.rs

Sadržaj: *Brute-force napadi predstavljaju opasnost za širok spektar online sistema i njihovih naloga što uključuje računare, mreže, servere i online servise. Fail2Ban kao adekvatan odgovor na ovu vrstu napada može postići različitu efikasnost zaštite u zavisnosti od primenjene bezbednosne polise. Stroga polisa zaštite u Fail2Ban-u može imati brojne implikacije, uključujući povećano opterećenje serverskih resursa i smanjenu dostupnost servisa ka korisnicima. Nasuprot tome, previše relaksirana polisa zaštite je "prijateljski nastrojena" ka korisnicima i smanjuje opterećenje resursa, ali utiče na povećanu verovatnoću kompromitovanja korisničkih akreditiva. Kao kompromis, nameće se izbor polisa zaštite koje pripadaju klasi tzv. balansiranih polisa. U ovom radu dat je akcenat na izbor balasirane bezbednosne polise, na osnovu prognoziranih vrednosti intenziteta brute-force napada primenom Holt-Winters metode. Eksperimentalni rezultati dobijeni su na osnovu podataka za nadzor rada serverskih sistema Saobraćajnog fakulteta.*

Ključne reči*: brute-force napadi, Fail2Ban servis, bezbednosna polisa, prognoziranje, Holt-Winters metoda*

1. Uvod

U digitalnom svetu, gde su kritične informacije i usluge permanentno dostupne putem interneta, bezbednost sistema predstavlja jedan od najznačajnijih izazova, bez obzira da li se digitalne aktivnosti odnose na savremeno poslovanje, ili su vezane za svakodnevni život. Bezbednost sistema može se posmatrati kao sposobnost sistema da aktivira adekvatan bezbednosni odgovor na pojavu različitih vrsta pretnji. U tom kontekstu, jedan od čestih oblika pretnji po bezbednost sistema je tzv. *brute-force* napad. Ova vrsta sajber napada bazira se na nameri napadača da dobije neovlašćeni pristup posmatranom sistemu ili nalogu metodom velikog broja uzastopnih pokušaja unosa kombinacija korisničkih imena i lozinki. Napadači mogu da koriste automatizovane alate da isprobaju hiljade ili čak milione različitih akreditiva za prijavu u veoma kratkom roku. Uprkos njihovoj naizgled jednostavnoj metodologiji, *brute-force* napadi predstavljaju efikasnu tehniku sajber napada, koja kao pojava u domenu sajber bezbednosti ima trajni karakter.

Da bi se zaštitili od ovakve vrste napada, administratori i stručnjaci za sajber bezbednost koriste različite alate i tehnike [1]. Među njima se nalazi se i *Fail2Ban* [2], softver za prevenciju upada otvorenog koda, koji je ocenjen kao efikasan odbrambeni mehanizam. *Fail2Ban* funkcioniše tako što u realnom vremenu nadgleda *log* datoteke, tragajući za obrascima aktivnosti koji ukazuju na ponovljene neuspele pokušaje prijavljivanja i potom preduzima mere za sprečavanje daljeg neovlašćenog pristupa blokiranjem IP adresa. Na taj način napadač se usporava u svojoj aktivnosti, što može dovesti do potencijalnog odustajanja od napada, kao i blagovremenog upozorenja administrativnog osoblja na pokušaje neovlašćenog pristupa kako bi se mogle preduzeti adekvatne zaštitne radnje [1] [3]. Efikasnost *Fail2Ban*-a zavisi od načina na koji je konfigurisan u konkretnom slučaju, kao i od smernica koje mrežni administratori postavljaju u slučaju pojedinačnih sistema.

Predmet ovog rada je analiza uzoraka iz *log* datoteka, sa ciljem da se evidencija neuspelih pokušaja prijavljivanja, prepoznatih kao sajber-napadi, pretvori u validnu vremensku seriju, koja se nadalje koristi za prognoziranje intenziteta *brute-force* napada. Na osnovu dobijene prognoze, vrši se izbor adekvatne balansirane polise zaštite, sa ciljem da se pruži adekvatna zaštita posmatranog serverskog sistema za budući period.

Rad je struktuiran u pet poglavlja. Nakon uvodnog dela, objašnjena je priroda *brute-force* napada i *Fail2ban* servisa kao vida odbrane. Potom je analizirana efikasnost pojedinih strategija polisa zaštite. U trećem poglavlju opisana je *Holt-Winters* metoda za prognoziranje kao veoma pogodna za primenu kod nestabilnih vremenskih serija. Eksperimentalni rezultati prognoziranog intenziteta *brute-force* napada dati su u četvrtom poglavlju. Na kraju su predstavljena zaključna razmatranja.

2. *Brute-force* napadi i *Fail2ban* servis kao vid odbrane

Brute-force napadi su vrsta sajber napada u kojima napadač pokušava da dobije neovlašćeni pristup sistemu, koji se realizuje sistematskim isprobavanjem svake moguće kombinacije korisničkih imena i lozinki dok se ne otkriju ispravni akreditivi. Ovi napadi su uzastopni, metodični i obično su automatizovani. Oni ostaju značajna pretnja bezbednosti na mreži i pojavljuju se u nekoliko oblika, uključujući:

- napade „upotrebom rečnika“, u kojima napadač koristi listu najčešće korišćenih lozinki ili reči iz lingvističkog rečnika da bi sistematski testirao svaku od njih. Ovaj pristup može biti veoma efikasan ako je ciljana lozinka slaba ili se često koristi;
- napade „postojećim akreditivima“, u kojima napadači koriste prethodno ukradena korisnička imena i lozinke za pristup višestrukim nalozima na različitim internet lokacijama, oslanjajući se na činjenicu da mnogi pojedinci koriste iste akreditive u različitim servisima;
- napadi hibridno generisanim akreditivima, u kojima se primenjuju kombinacije tehnika, poput upotrebe „rečnika“ u kombinaciji sa dodavanjem brojeva ili specijalnih znakova, povećavajući verovatnoću uspeha.

Pretnja od *brute-force* napada ostala je konstantna u domenu sajber bezbednosti. Dok osnovni koncept sistematskog isprobavanja svih mogućih kombinacija korisničkih imena i lozinki ostaje nepromenjen, metode i alati koje koriste napadači značajno su evoluirali. Danas, savremeni napadači koriste napredni softver i hardver, u kombinaciji sa upotrebom *botneta* (distribuiranih mreža kompromitovanih računara), čime distribuiraju

opterećenje napada i održavaju anonimnost. *Brute-force* napadi ciljaju širok spektar sistema i korisničkih servisa, uključujući individualne korisničke naloge servisa poput elektronske pošte, socijalnih mreža ili bankovnih računa. Pored navedenog, ova vrsta napada može biti usmerena i na određene vrste mrežnih pristupa, koji zahtevaju upotrebu različitih protokola, poput SSH [4], FTP ili RDP. Cilj napada je dobijanje neovlašćenog pristupa serverima i računarima, kao i sistemima za upravljanje sadržajem (CMS) u slučaju različitih oblika web servisa, kao što su blog platforme ili platforme za e-trgovinu [5] [6]. Treba napomenuti da su ove vrste web lokacija posebno interesantne napadačima, jer one često skladište informacije o drugim klijentima (korisnička imena, email adresa i *hash* vrednosti njihovih lozinki) [7]. Ranjivosti koje olakšavaju *brute-force* napade uključuju slabe lozinke, nedostatak polisa za zaključavanje naloga, kao i nešifrovane procese autentifikacije u slučaju zastarelih servisa koji još uvek nisu ugašeni na Internetu.

2.1. *Fail2ban* servis

Fail2Ban je veoma popularan softver otvorenog koda za prevenciju napada, dizajniran da zaštiti sisteme i servise praćenjem aktivnosti zapisanih u *log* datotekama, kroz pretragu obrazaca koji ukazuju na ponovljene neuspele pokušaje prijave. Funkcionisanje ovog softverskog rešenja za zaštitu može se podeliti na nekoliko ključnih koraka:

- nadgledanje aktivnosti – *Fail2Ban* kontinuirano prati *log* datoteke za unapred određeni set servisa, kod kojih vrši pretragu sadržaja u potrazi za definisanim obrascima aktivnosti koji ukazuju na višestruke neuspele pokušaje prijave na posmatrani sistem;
- uparivanje šablona – kada *Fail2Ban* otkrije unapred definisani obrazac, beleži IP adresu odgovornu za neuspele pokušaje prijave;
- primena zabrane – kada se identifikuje unapred definisani broj neuspelih pokušaja po identifikovanom obrascu (a koji potiču sa iste IP adrese), tada se formira zabrana pristupa za posmatranu adresu, automatskim dodavanjem pravila u korespondentnom *firewall* modulu [8]. U slučaju operativnih sistema klase *Linux*, aktivira se pravilo na *firewall* modulu tipa „*iptables"* kako bi se blokirao pristup serveru ili mreži sa identifikovane IP adrese. Ova zabrana važi u toku unapred definisanog vremenskog perioda koje je u uskoj vezi sa unapred definisanim setovima pravila zaštite, poznatijim pod nazivom „bezbednosne polise".

Fail2Ban program ima širok spektar opcija za prilagođavanje bezbednosnih polisa specifičnim bezbednosnim potrebama. Ove opcije su podeljene u sledeće funkcionalne celine:

- filteri – pravila koja određuju koje linije u *log* datotekama treba uzeti u obzir da bi se mogao detektovati pokušaj neovlašćenog pristupa. Ove opcije se prilagođavaju u skladu sa specifičnim karakteristikama zapisa koje formira određeni operativni sistem, kao nosilac posmatranog servisa;
- pragovi – predstavljaju donju granicu vezanu za broj neuspelih pokušaja pristupa, iznad koje se taj pristup može okarakterisati kao neovlašćen ili maliciozan;
- akcije - odgovori koje *Fail2Ban* program treba da aktivira u slučaju aktivacije definisanog filtera. Akcije mogu uključivati zabranu IP adrese, slanje obaveštenja e-poštom ili izvršavanje prilagođenih skripti, kao specifičan vid odgovora na identifikovanu pretnju;

- trajanje zabrane - trajanje IP zabrana je opcija koja se može podesiti na način, takav da posmatrana akcija predstavlja odgovor koji je adekvatan u odnosu na ozbiljnost napada, kao i definisane sistemske smernice mrežnog servisa koji je predmet odbrane;
- „zatvori“ („*jails*“) predstavljaju kombinaciju filtera i jedne ili više akcija, na osnovu definisanog praga, čiji je cilj da se u potpunosti definiše postupanje sa IP adresom, kao identifikovanim izvorom napada u unapred definisanom periodu trajanja zabrane.

Iz navedenog se može primetiti da *Fail2Ban* može predstavljati adekvatan odgovor na pojavu *brute force* napada na posmatranom sistemu. Ovaj program funkcioniše kao samostalni serverski servis, kojim se može upravljati ručno, u poluautomatskom i/ili automatskom režimu rada.

2.2 Efikasnost *Fail2Ban* servisa i uloga bezbednosnih polisa

Efikasnost *Fail2Ban* programa u najvećoj meri zavisi od načina na koji je definisana bezbednosna polisa za posmatrani mrežni servis. U navedenom kontekstu, bezbednosne polise se mogu definisati u opsegu od tzv. „rigidnih“, pa sve do tzv. „relaksiranih“ polisa.

„Rigidna“ *Fail2Ban* polisa predstavlja set bezbednosnih smernica koje karakterišu strogo definisani pragovi, dugo trajanje zabrane i brza reakcija čak i na mali broj neuspešnih pokušaja prijave. Ova vrsta polise može biti efikasna u brzom reagovanju na *brute-force* napade, gde čak i nekoliko neuspešnih pokušaja prijave može da izazove blokadu određene IP adrese (tzv. IP ban), sprečavajući napadače da učine dalje pokušaje sa tog adresnog izvora. Na taj način se minimizira tzv. „prozor mogućnosti“ za napadače. Međutim, preterano rigidne smernice mogu nenamerno da iscrpe sistemske resurse tako što će zabraniti previše IP adresa u određenom vremenskom periodu. Na taj način, odziv sistema se smanjuje na način sličan kao u slučaju *Denial of Service* (DoS) napada. Pored navedenog, rigidne smernice mogu da ometaju i korisnike, koji pogrešno ukucaju lozinke ili naiđu na privremene probleme sa autentifikacijom. To ima za rezultat povećane operativne troškove (tzv. „administratorsko opterećenje“), imajući u vidu potrebu za stalnim nadgledanjem kao i učestalim administrativnim poslovima deblokade legitimnih korisnika u slučaju servisa sa masovnom upotrebom.

Sa druge strane, tzv „relaksirana“ *Fail2Ban* polisa uključuje blaže pragove reakcije, kraće trajanje zabrane i „više prijateljski“ odnos prema neuspelim pokušajima prijave. Prednost primene relaksirane bezbednosne polise se ogleda u tome da se one karakterišu kao „prilagođene korisničkim potrebama“, imajući u vidu da umanjuju verovatnoću smetnje korisnicima sa stvarnim problemima sa prijavljivanjem. Na taj način je smanjeno „administrativno opterećenje“ odnosno umanjene potrebe za intervencijama, čime se smanjuju i operativni troškovi u slučaju masovnih servisa. Pored navedenog, manja je i verovatnoća da će relaksirana polisa dovesti do iscrpljivanja serverskih resursa zabranom manjeg broja IP adresa. Ipak, „relaksirana“ polisa pruža napadačima veći „prozor mogućnosti“, pružajući im mogućnost da održe kontinuitet *brute force* napada, kroz frekventniju ponovnu upotrebu istog IP adresnog opsega koji im stoji na raspolaganju, uvećavajući na taj način verovatnoću uspešne realizacije neovlašćenog pristupa.

Balansirana konfiguracija *Fail2Ban* smernica, odnosno balansirana bezbednosna polisa ima za cilj da uspostavi ravnotežu između bezbednosti i upotrebljivosti. Ovakva konfiguracija zavisi od specifičnih zahteva sistema, razvoja pretnji i tolerancije na lažne

pozitivne rezultate. U praksi, mnogi sistemi se opredeljuju za primenu umerenih polisa koje nisu ni preterano rigidne, niti previše relaksirane. Ovakve polise se dobijaju uzimanjem u obzir potreba korisnika, potencijalni uticaj na sistemske resurse i potreban nivo zaštite. Pored toga, redovno praćenje i prilagođavanje polisa imaju ključnu važnost u procesu održavanja ravnoteže između navedenih potreba. Promenom različitih pripadajućih parametara, dobija se čitav niz različitih polisa, koje predstavljaju gradaciju između balansiranih i rigidnih polisa.

Shodno navedenom, operativni pristup koji ima za cilj postizanje ravnoteže između bezbednosti i upotrebljivosti prilikom konfigurisanja *Fail2Ban* smernica zahteva pažljivo posmatranje rada datog servisa, kao i kontinuiranu primenu adekvatnih mera, zasnovanu na kontinuiranoj proceni efikasnosti uvedenih polisa. Ove mere se odnose na podešavanje pragova i trajanja odgovarajućih zabrana, kao i na druga podešavanja koja treba primeniti po potrebi. Ovi koraci se zasnivaju na analizi tipičnih obrazaca prijavljivanja i ponašanja korisnika, sa ciljem uočavanja eventualno novih metoda koje se javljaju u pokušajima neovlašćenog pristupa, kao i zbog potreba minimizacije lažnih pozitivnih rezultata sa druge strane. Na osnovu toga vrši se fino podešavanje parametara „*jails*“ sekcije *Fail2Ban* programa. Naknadna provera upotrebljivosti rekonfigurisanog sistema vrši se u komunikaciji sa krajnjim korisnicima, prikupljanjem povratnih podataka.

Dodatni procesi automatizacije servisa mogu se postići kroz kontinuirano praćenje *log* datoteka, primenom automatskih alata za analizu, zatim implementacijom sistema upozorenja, kojim se obaveštavaju administratori o neuobičajenim visokim nivoima neuspešnog prijavljivanja, kao i naknadnim analizama uzroka ovakvih pojava.

Pored navedenog treba uvek imati u vidu da primena bezbednosnih programa poput *Fail2Ban* nije dovoljna za potupunu zaštitu od *brute force* napada, koja se značajno može uvećati i primenom sistema za multi-faktorsku autentifikaciju (*Multi-factor authentication*, MFA), sistema za detekciju intruzija (*Intrusion Detection System*, IDS), sistema za naprednu detekciju anomalija, poput sistema za multivarijantno statističko praćenje mreže (*Multivariate Statistical Network Monitoring,* MSNM) [9] kao i primenom metoda prevencije, koja se ogleda u podsticanju korisnika u sprovođenju redovne zamene lozinki, kao i redovnim informisanjem korisnika o najboljim praksama u sajber bezbednosti.

3. Primena *Holt-Winters* metode za prognoziranje *brute-force* napada

Holt-Winters (HW) metoda spada u kratkoročne metode prognoziranja nestabilnih vremenskih serija ulaznih podataka. Primenjuje se kada postoji izražen trend, kao i sezonska komponenta [10] [11]. Pripada grupi *ad hoc* procedura prognoziranja. Predstavlja preteču modernih strukturnih modela za koje je utvrđeno da se baziraju na statističkoj teoriji a mogu se smatrati posebnim slučajevima opšte klase modela strukturnih vremenskih serija koji su nastali proširenjem Eksponencijalnog izglađivanja (*Exponential Smoothing*) i ARIMA (*Auto Regressive Integrated Moving Average*) modela [12] [13]. Postoje dva osnovna oblika primene *Holt-Winters* metode: Aditivna *Holt-Winters* metoda i Multiplikativna *Holt-Winters* metoda.

Multiplikativna *Holt-Winters* metoda se bazira na tri jednačine izglađivanja. Prvom jednačinom se izglađuje nivo posmatrane veličine, drugom trend, a trećom sezonske varijacije.

Nivo vremenske serije podataka, l_T, može se definisati sledećom jednačinom:

$$l_t = \alpha\left(\frac{y_t}{S_{t-s}}\right) + (1-\alpha)(l_{t-1} + b_{t-1}) \quad (1)$$

Stepen rasta ili trend, b_t, definiše se jednačinom:

$$b_t = \gamma(l_t - l_{t-1}) + (1-\gamma)b_{t-1} \quad (2)$$

Nakon određivanja nivoa i trenda, odredjuje se sezonski faktor, S_t:

$$S_t = \beta\left(\frac{y_t}{l_t}\right) + (1-\beta)S_{t-s} \quad (3)$$

gde su: α, β i $\gamma \in [0,1]$ konstante izglađivanja; s je broj sezona u godini (npr. za mesečne podatke s=12, za kvartalne podatke s=4); y_t je ulazni podatak vremenske serije za vreme t.

Ova metoda je veoma pogodna kada vremenska serija ima linearan trend sa multiplikativnim sezonskim uticajem kod koje se nivo serije, indeks rasta i sezonski uticaj mogu sporo menjati tokom vremena.

Izračunavanje prognoziranih vrednosti u trenutku t, dato je sledećim izrazom:

$$\hat{y}_{t+m}(t) = (l_t + b_t m)S_{t+m-s}\,, \text{za } m = 1, 2, 3, \ldots \quad (4)$$

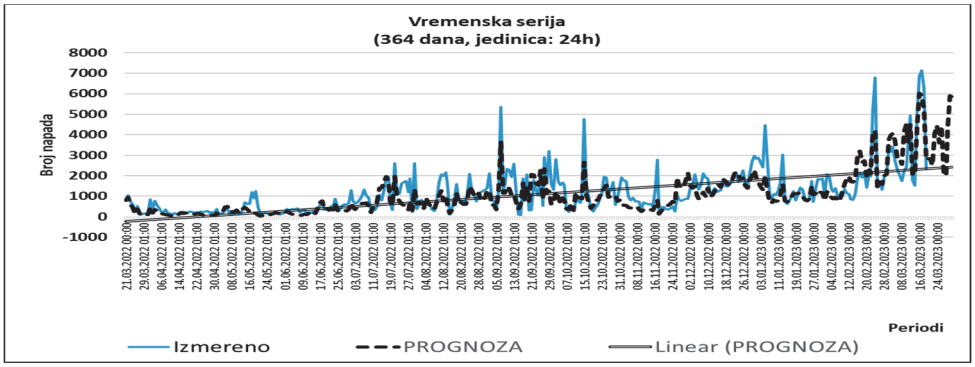
Izbor konstanti α, β i γ u *Holt-Winters*-ovom modelu zahteva posebnu pažnju. Optimizacija konstanti izglađivanja treba da dâ najmanju sumu kvadrata grešaka (SSE):

$$SSE = \sum_{t=1}^{T}[y_t - \hat{y}_t(t-1)]^2 \quad (5)$$

Ovo je moguće izvršiti uz korišćenje *Excel Solver* alata.

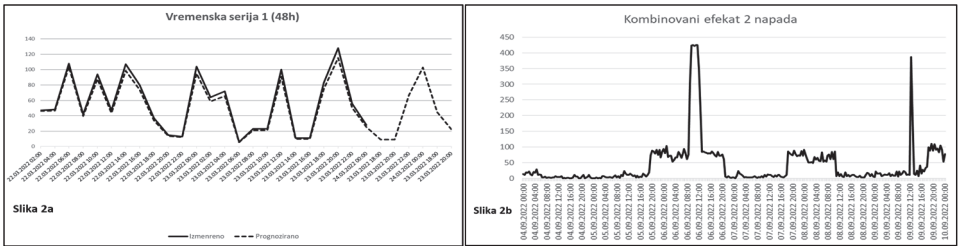
4. Eksperimentalni rezultati

Za potrebe analize učestanosti *brute-force* napada, izvršena je ekstrakcija vremenske serije iz *Fail2ban log* datoteke registrovanih napada u realnom okruženju mreže Saobraćajnog fakulteta (SF NET) za period od godinu dana (21.03.2022.–21. 03.2023. godine, slika 1). U ovoj datoteci evidentirani su neispravni unosi korisničkih akreditiva, pri čemu se pod napadom podrazumeva višestruki pokušaj unosa, koji je rezultovao blokadom izvorišne IP adrese. Drugim rečima, broj napada istovremeno predstavlja i broj blokiranih IP adresa. *Log* podaci su strukturirani metodom formiranja klastera događaja prema pripadnosti korespondentnim vremenskim intervalima u trajanju od 5, 30, 120 i 1440 minuta (24 časa), čime su dobijene vremenske serije na dnevnom, nedeljnom, mesečnom i godišnjem nivou. Vremenska serija na godišnjem nivou (slika 1) ima blago rastući trend i delimično prisutan sezonski uticaj. Sezonska varijacija takođe blago raste sa porastom trenda i to u slučaju kratkotrajnih i intenzivnih napada u ravnomernim vremenskim intervalima (07.09.2022, 15.10.2022., 17.11.2022, 05.01.2023. i 24.02.2023. godine).



Slika1. Vremenska serija dobijena iz log fajlova Fail2ban za jednogodišnji period

Vremenska serija na nedeljnom nivou, u kojoj su događaji grupisani u klastere u odnosu na osnovni period aktivnosti od 2 časa, daje drugačiji uvid u prirodu *brute-force* napada. Naime, u uzorcima ove vremenske serije, u zavisnosti od datuma, uočene su dve tipične pojave – česte sezonske varijacije, koje rastu sa porastom trenda, koje su uočljive na vremenskim intervalima od 48 časova (slika2a). Pored navedenih, mogu se uočiti i periodični napadi nižeg intenziteta sa dužim trajanjem, kao i periodični napadi srednjeg intenziteta koji mogu biti kombinovani sa kratkotrajnim napadima visokog intenziteta (slika 2b).



Slika2. Vremenska serija sa periodom 2h: sezonska komponenta (a) i kombinovani napad (b)

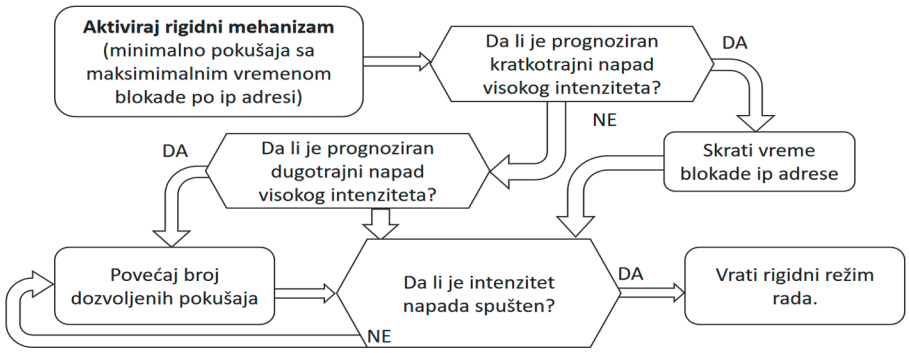
Izrazita sezonska komponenta može se takođe uočiti na pojedinim segmentima vremenske serije sa osnovnim periodom od 30 minuta. Međutim, ova pojava nije redovna i pritom je često kombinovana sa napadima slučajnog karaktera, zbog čega nije uzeta u obzir u daljoj analizi. Imajući u vidu navedenu analizu dobijenih vremenskih serija izvršeno je prognoziranje intenziteta *brute-force* napada. U ovom eksperimentu, primenjena je *Holt-Winters* multiplikativna metoda, imajući u vidu karakteristike sezonskih varijacija u slučaju vremenskih serija prikazanih na slikama 1 i 2a. Prognozirane vrednosti prikazane su na slikama isprekidanim linijama. Na početku eksperimenta, izabrane su podjednake vrednosti 0,5 za sva tri koeficijenta izglađivanja (α, β i γ). Prognoziranje je izvršeno uz pomoć posebno napravljenog šablona u programskom paketu MS Excel. Rezultati prognoziranja nadalje su podvrgnuti proveri upotrebom standardnih testova *Mean Absolute Error* (MAE), *Mean Square Error* (MSE) i *Mean Absolute*

Percentage Error (MAPE), uz upotrebu alata *Solver*, kojim je izvršena pretraga za onim vrednostima koeficijenata izglađivanja, koji daju njihove minimalne vrednosti (Tabela 1).

Tabela 1. Vrednosti koeficijenata izglađivanja i rezultati testova pouzdanosti prognoziranja

Vrem. serija	α	β	γ	MSE	MAE	MAPE (%)
1	0.07318	0.017727	0.60527	395.998	342684.748	40.521
2a	4.54E-08	2.2E-307	1	4.31119	29.17463	7.81982

Dobijeni rezultati prognoziranja iniciraju na zamenu *Fai2ban* polisa. Shodno navedenom, predlaže se da se zamena realizuje automatizovanim procesom baziranim ma upotrebi *bash* skripta operativnog sistema, u skladu sa tokom događaja koji je prikazan na slici 3.



Slika3. Tok događaja iniciran prognoziranim vrednostima

Zamena polise uvek počinje i završava se aktiviranjem rigidne politike, koja pruža najveći stepen zaštite. Ovaj koncept je zasnovan na pretpostavci da primena rigidne politike pruža puni vid zaštite i da se određenom vremenskom periodu može dozvoliti delimična relaksacija, da bi sistem bio zadržan u funkcionalnom stanju za krajnje korisnike. Shodno navedenom, u zavisnosti od prognoziranog tipa napada skript će aktivirati one polise koje imaju više gradacija, bilo da se radi o promeni vrednosti "praga", "vremena zaštite" ili vrednosti "*jail*" parametara.

5. Zaključak

Brute-force napadi ostaju i dalje stalna pretnja koja se razvija u domenu sajber bezbednosti. *Fail2Ban*, sa svojom sposobnošću da blokira IP adrese nakon uzastopnih neuspešnih pokušaja prijave, nudi efikasnu protivmeru. Po identifikaciji napada, ovaj program preduzima mere da spreči dalji neovlašćeni pristup, obično aktiviranjem *firewall* modula radi privremenog ili trajnog blokiranja IP adrese, koja je povezana sa zlonamernim pokušajem prijavljivanja na posmatrani sistem. Konfiguracija *Fail2Ban* programa ima vitalnu ulogu u ostvarivanju visokog stepena zaštite uz minimiziranje operativnih troškova administracije. Izbor između rigidnih i relaksiranih *Fail2Ban* politika uključuje kompromise, u obliku čitavog niza različitih polisa koje predstavljaju balans između krajnjih rešenja, koji zavisi od jedinstvenih okolnosti organizacije, okruženja pretnji i

ponašanja korisnika. Različiti scenariji napada koji se mogu desiti zahtevaju primenu koncepta automatizacije procesa zaštite, u kojima se vrši aktivacija one polise, koja bi predstavljala adekvatan odgovor na identifikovani napad. U ovom radu, predložen je pristup automatizaciji procesa zaštite od *brute-force* napada, koji se bazira na primeni odgovarajuće polise zaštite u odnosu na prognozirani intenzitet napada. Pristup baziran na prognoziranju intenziteta napada, motivisan je činjenicom da preventivni oblik zaštite predstavlja najbolji vid odgovora na pretnje. Shodno navedenom izvršen je eksperiment u kome je ispitana mogućnost upotrebe *Holt-Winters* multiplikativne metode, imajući u vidu da je moguće identifikovati karakteristike sezonskih varijacija u slučaju pojedinih vremenskih serija, koje su dobijene kroz proces struktuiranja događaja, zabeleženih u *log* datotekama.

Fail2Ban ne može biti jedino rešenje koje se primenjuje i u tom kontekstu neće biti efikasan protiv visoko sofisticiranih napadača koji koriste distribuirane *botnete* ili mreže koje imaju pristup velikom broju IP adresa. U takvim slučajevima, kombinacija bezbednosnih mera je neophodna za sveobuhvatnu zaštitu. Zbog toga u budućnosti, borba protiv *brute-force* napada nastaviće da se razvija, kao odgovor na nove pretnje koje zahtevaju inovativna rešenja. Shodno navedenom, postoji stalna potreba da se *Fail2Ban* i slični alati prilagode za rešavanje ovih izazova.

Literatura

[1] K. Hynek, T. Beneš, T. Čejka / H. Kubátová, „Refined detection of SSH brute-force attackers using machine learning," u *ICT Systems Security and Privacy Protection: 35th IFIP TC 11 International Conference, SEC 2020, Maribor, Slovenia, September 21–23, 2020, Proceedings 35*, 2020.

[2] C. Jaquier, „Fail2Ban GitHub repository," [Na mreži]. Available: https://github.com/fail2ban/fail2ban.

[3] Crooks, David and Vâlsan, Liviu and Mohammad, Kashif and McKee, Shawn and Clark, Paul and Boutcher, Adam and Padée, Adam and Wójcik, Michal and Giemza, Henryk and Kreukniet, Bas, „Operational security, threat intelligence & distributed computing: the WLCG Security Operations Center Working Group," *EPJ Web Conf.,* t. 214, p. 03029, 2019.

[4] J. Park, J. Kim, B. B. Gupta / N. Park, „Network log-based SSH brute-force attack detection model.," *Computers, Materials & Continua,* t. 68, 2021.

[5] M. Hölbl, K. Rannenberg / T. Welzer, ICT Systems Security and Privacy Protection, Springer, 2020.

[6] M. Idhom, H. E. Wahanani / A. Fauzi, „Network Security System on Multiple Servers Against Brute Force Attacks," *2020 6th Information Technology International Seminar (ITIS),* pp. 258-262, 2020.

[7] S. Latha / S. J. Prakash, „A survey on network attacks and Intrusion detection systems," u *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2017.

[8] J. Luxemburk, K. Hynek / T. Čejka, „Detection of https brute-force attacks with packet-level feature set," u *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, 2021.

[9] S. Soufiane, R. Magan-Carrion, I. Medina-Bulo / H. Bouden, „Preserving authentication and availability security services through multivariate statistical network monitoring,“ *Journal of Information Security and Applications,* t. 58, p. 102785, 2021.

[10] C. P. Da Veiga, C. R. P. Da Veiga, A. Catapan, U. Tortato / W. V. Da Silva, „Demand forecasting in food retail: A comparison between the Holt-Winters and ARIMA models,“ *WSEAS transactions on business and economics,* t. 11, p. 608–614, 2014.

[11] S. Rubab, M. F. Hassan, A. K. Mahmood / S. N. M. Shah, „Forecasting volunteer grid workload using Holt-Winters' method,“ u *2015 International Symposium on Technology Management and Emerging Technologies (ISTMET)*, 2015.

[12] M. J. Gundalia / M. B. Dholakia, „Prediction of maximum/minimum temperatures using Holt Winters method with Excel spreadsheet for Junagadh region,“ *International journal of engineering research & technology,* t. 1, p. 1–8, 2012.

[13] V. Lepojević / P. M. Anđelković, „Forecasting electricity consumption by using holt-winters and seasonal regression models,“ *Facta universitatis-series: Economics and Organization,* t. 8, p. 421–431, 2011.

Abstract:
Brute-force attack is a hacking method that poses a threat to a wide range of online systems and accounts, including computers, networks, servers and online services. Fail2Ban service as an adequate response to this type of attacks can achieve different protection efficiency depending on the applied protection policy. The strict protection policy in Fail2Ban service has numerous implications, including increased load of server resources and reduced service availability to end users. Conversely, an overly relaxed protection policy is "user friendly" and reduces server load, but results in increased likelihood of user credentials and passwords being hacked. As a compromise solution, the choice of protection policy that belongs to the class of so-called balanced policies is imposed. In this paper, the emphasis is given to the selection of a balanced protection policy level based on the forecasted brute-force attack intensity that is performed by the Holt-Winters method. The results are obtained by monitoring the real server system operation in the authors' institution local network.

Keywords: *brute-force attacks, Fail2Ban service, protection policy, forecasting, Holt-Winters method.*

FORECASTING OF THE BRUTE-FORCE ATTACKS INTENSITY IN FUNCTION OF THE PROTECTION LEVEL OPTIMIZATION

Slobodan Mitrović, Valentina Radojičić, Goran Marković