Praćenje rada i zaštita računarskih mreža pfSense sistemom

Svetlana Mančić, Nađa Gavrilović

Sadržaj – Maliciozne aktivnosti na mreži su problem koji se danas nameće svim korisnicima Interneta. Napretkom alata i tehnika za sajber napade, oni postaju sve sofisticiraniji, što njihovu detekciju čini sve težim zadatkom. U današnje vreme, jedan od primarnih zahteva korisnika mreže jeste sigurna mrežna infrastruktura koja će omogućiti siguran prenos i skladištenje podataka. Cilj ovog rada je projektovanje i implementacija sistema za zaštitu dela računarske mreže Elektronskog fakulteta u Nišu, baziranom na pfSense sistemu instaliranim na APU4 uređaju. PfSense sistem konfigurisan je tako da vrši ulogu *firewall* uređaja i loguje sve informacije o blokiranim paketima. Na postavljenom pfSense sistemu instaliran je i Snort IDS paket za detekciju napada na mreži. Dodatno, podaci koje generišu pfSense i Snort IDS prikupljeni su, vizuelizovani i analizirani upotrebom ELK (*ElasticSearch-Logstash-Kibana*) sistema. U radu je detaljno opisana implementacija predloženog sistema za zaštitu mreže, kao i proces prikupljanja, skladištenja i analize podataka. Takođe, dat je vizuelni prikaz analize podataka dobijenih u toku rada.

I. UVOD

Tehnološki napredak modernog doba omogućio je da se Internet koristi u veoma važnim oblastima, kao što su bankarstvo, zdravstvo, školstvo itd. Mogućnosti koje Internet pruža, neprestan porast broja korisnika, dostupnost i lakoća pristupa informacijama dovode u pitanje bezbednost korisnika. Maliciozne aktivnosti postaju sve sofisticiranije, dok tehnike njihovog prikrivanja postaju sve razvijenije. Bezbedna mrežna infrastruktura postala je primarni zahtev korisnika mreže, kako bi prenos i skladištenje njihovih podataka bili zaštićeni [1].

Veliki broj korisnika mreže nije dovoljno informisan o bezbednosti na Internetu, samim tim se i ne štiti adekvatno od različitih pretnji. Posledica su sve češći napadi na korisnike i njihove poverljive podatke različitim tehnikama socijalnog inženjerstva (eng. *Social Engineering*) [2].

U cilju zaštite korisnika mreže i same mrežne infrastrukture, jedne od najvažnijih komponenti sigurosnih sistema su *firewall* uređaji i sistemi za detekciju napada (IDS). *Firewall* predstavlja sistem za zaštitu mreže, koji prati aktivnosti na računarskoj mreži i kontroliše dolazni i odlazni saobraćaj upotrebom definisanih bezbednosnih pravila [3]. Kako bi zaštita bila potpuna, IDS sistemi koriste se u cilju detekcije neautorizovanih pristupa mreži i generisanja upozorenja. Jedan od najčešće korišćenih sistema za detekciju napada je Snort IDS [1].

Cilj ovog rada je projektovanje i implementacija sistema za zaštitu dela računarske mreže Elektronskog fakulteta u Nišu pfSense sistemom, instaliranim na APU4 uređaju. PfSense postavljen je tako da vrši *firewall* ulogu i loguje sve informacije o blokiranim paketima. Dodatno, u cilju proširenja funkcionalnosti pfSense sistema, na njemu je instaliran i Snort paket za detekciju mrežnih napada. Svi podaci koje pfSense i Snort generišu, šalju se do ELK (*ElasticSearch-Logstash-Kibana*) sistema, gde se skladište, analiziraju i vizuelno prikazuju. U radu će biti opisana implementacija predloženog sistema za zaštitu mreže, kao i proces prikupljanja podataka koje sistem generiše, njihovog skladištenja i krajnje vizuelizacije. Takođe, biće dat vizuelni prikaz analize prikupljenih mrežnih podataka, koji olakšava detekciju malicioznih aktivnosti.

Nakon uvoda, u drugom poglavlju biće data teoretska osnova neophodna za implementaciju predloženog sistema. Biće diskutovan princip rada pfSense sistema i Snort IDS paketa, kao i Logstash alata koji je korišćen za prikupljanje podataka sa pfSense sistema u cilju dalje analize. U trećem poglavlju biće opisan implementirani sistem. U četvrtom poglavlju biće dat prikaz rada predloženog sistema. Zaključak će biti dat u petom poglavlju.

II. TEORETSKA OSNOVA

A. *PfSense*

Projekat pfSense je besplatna *firewall* distribucija koja se bazira na FreeBSD operativnom sistemu. Pored toga što je moćna i prilagodljiva *firewall* platforma, pfSense ima mogućnost rutiranja. Dodatno, uključuje veliki broj softverskih paketa koji proširuju osnovne funkcionalnosti pfSense sistema. Osim podešavanja iz komandne linije, sistemom se može upravljati i u okviru dostupnog veb interfejsa [4].

Za razliku od većine komercijalnih *firewall* sistema, PfSense je softver koji je moguće instalirati na proizvoljnom hardveru, koji ispunjava minimalne zahteve i pogodan je za potrebe različitih okruženja [4]. Postoji nekoliko načina implementacije pfSense sistema – u ulozi *firewall* uređaja, rutera, sviča i *wireless* rutera [5].

Svetlana Mančić je student osnovnih akademskih studija na Katedri za računarstvo i informatiku, Elektronski fakultet, Univerzitet u Nišu, Aleksandra Medvedeva 14, 18000 Niš, Srbija, E-mail: svetlanamancic@elfak.rs

Nađa Gavrilović je student doktorskih akademskih studija na Katedri za računarstvo i informatiku, Elektronski fakultet, Univerzitet u Nišu, Aleksandra Medvedeva 14, 18000 Niš, Srbija, e-mail: nadja.gavrilovic@elfak.rs

U SOHO (*Small Office Home Office*) okruženju, *firewall* funkciju i rutiranje često obavlja isti uređaj. Kod mreža sa više mrežnih segmenata, pfSense se može koristi za njihovo povezivanje i rutiranje između njih [5].

Kada bi nad nekoliko interfejsa bio kreiran *bridge* kako bi se interfejsi povezali (bez podele *broadcast* domena) pfSense bi mogao obavljati funkciju sviča. Međutim, ovaj način implementacije se retko koristi, jer su podešavanja standardnog sviča jednostavnije i daju bolje performanse jer se ne vrši filtriranje paketa [5].

Moderne mreže uključuju i bežično povezivanje. Korišćenjem pfSense sistema moguće je povezati bežične uređaje uz dodavanje *wireless* mrežne kartice, koju podržava FreeBSD. Međutim, bolja opcija je upotreba standardnog *wireless* rutera, podešavanje pristupne tačke, a zatim povezivanje rutera na LAN port pfSense sistema [5].

Najčešći način implementacije pfSense sistema je *firewall*. U tom slučaju, pfSense se postavlja tako da predstavlja vezu lokalne mreže i Interneta. Port koji je povezan na Internet je WAN interfejs, a lokalna mreža je na LAN interfejsu. Ukoliko se koristi ovaj način implementacije, osim *firewall* funkcije, pfSense može vršiti i rutiranje. Broj interfejsa nije ograničen na dva, već može biti i više interfejsa na kojima su lokalne mreže [5].

Osnovni zadatak pfSense *firewall* uređaja je uspostavljanje barijere između pouzdane lokalne mreže i nepouzdane spoljne mreže, odnosno Interneta. Svaki *firewall* ima sposobnost filtriranja paketa, odnosno ispitivanja ulaznog i izlaznog saobraćaja i donošenja odluke o prosleđivanju ili odbacivanju ispitanog paketa [5].

Ingress filtering se odnosi na filtriranje paketa koji dolaze na lokalnu mrežu sa spoljne mreže. *Egress filtering* se odnosi na filtriranje paketa koji se sa lokalne mreže salju na Internet ili drugi interfejs [4].

Firewall pravila imaju tri opcije po kojima mogu postupati [5]:

- *Pass* - propušta pakete kroz *firewall*,
- *Block* - odbacuje pakete bez obaveštavanja pošiljaoca,
- *Reject* - odbacuje pakete i šalje *port unreachable* poruku pošiljaocu na osnovu čega on može da zaključi da je *firewall* odbacio paket.

U okviru liste pravila definisanih na jednom interfejsu, pravilo koje će se primeniti nalazi se *first match* politikom, tj. pravila se čitaju s vrha liste ka dnu i prvo pravilo sa kojim se nađe poklapanje se primenjuje [4].

B. Snort IDS

Snort je jedan od najčešće korišćenih sistema za detekciju napada na mrežu. Zasniva se na potpisima, koji definišu šta se može smatrati malicioznom aktivnošću na mreži i tako omogućavaju detekciju napada [6]. Setovi potpisa predstavljaju Snort pravila, koja se formalno definišu na sledeći način [7]:

<akcija><protokol><izvorna_IP_adresa><izvorni_port>
<smer><odredišna_adresa><odredišni_port><opcije>

Pravilo može sadržati jednu ili više opcija, od kojih se svaka sastoji od ključne reči koja definiše opciju, i argumenata koji navode detalje opcije [7]. Ako se polja iz paketa podudaraju sa nekim pravilom, Snort će generisati upozorenje, koje se prikazuje u realnom vremenu [8].

Snort je dostupan kao paket koji je moguće instalirati i podešavati kao dodatak funkcionalnosti pfSense sistema.

C. Logstash

ELK sistem predstavlja kolekciju tri javno dostupna alata koji se koriste u cilju prikupljanja, skladištenja i vizuelizacije podataka različitog porekla i strukture. Logstash komponenta služi za sakupljanje i transformaciju podataka, koji se šalju do ElasticSearch komponente. Ona sadrži indekse za skladištenje podataka definisane strukture, dok se Kibana alat koristi za krajnju vizuelizaciju prikupljenih podataka.

Logstash je ključna komponenta ELK sistema koja služi za dinamičko prihvatanje podataka sa više izvora, njihovu transformaciju i slanje bez obzira na format i složenost. Podaci su pre prikupljanja često skladišteni na različitim sistemima, u različitim formatima. Svaki tip podatka se može transformisati korišćenjem širokog spektra input, filter i output logstash *plugin*-ova [9].

Logstash ima dva neophodna elementa, input i output, i jedan opcioni element, filter. Input element prihvata podatke sa različitih izvora, filter ih može modifikovati i proširiti na način koji se definiše u konfiguraciji, a output element šalje podatke odredištu. Dodatno, input i output podržavaju *codec* elemente, koji samostalno omogućavaju kodiranje i dekodiranje podataka bez potrebe za definisanjem posebnog filtera [9].

Najčešće korišćeni tipovi inputa su: *file*, *syslog*, *redis*, *beats* i *udp*. U ovom radu korišćeni su *udp* i *syslog*, koji funkcionišu tako što čitaju podatke dobijene preko mreže. U konfiguraciji, potrebno je definisati port na kom Logstash prima podatke, pri čemu je moguće definisati više različitih portova, ako postoji više izvora [9].

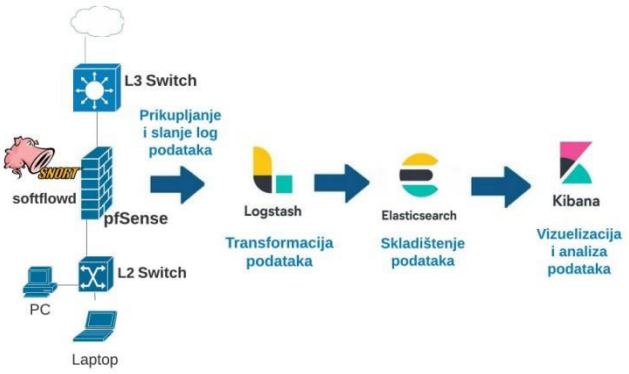
Filter komponenta vrši procesiranje i transformaciju podataka. U slučaju da se navede više njih, primenjuju se u redosledu navođenja. Dostupan je veliki broj filtera, od kojih su korišćeni *geoip*, *grok* i *mutate*. *Geoip* filter dodaje informacije vezane za geografsko lociranje IP adresa. *Grok* filter transformiše nestruktuirane podatke u strukuirane i čini ih pogodnim za primenu ElasticSearch upita. *Mutate* filter omogućava da se vrše izmene atributa podataka kao što su preimenovanje, brisanje i zamena [9].

Output tipovi koji se najčešće koriste su *elasticsearch*, *file*, *graphite* i *statsd*. U radu je korišćen *elasticsearch* output, koji upisuje obrađene podatke u ElasticSearch indekse, u kojima se podaci skladište i dostupni su za dalju analizu i vizuelizaciju [9].

III. PREGLED IMPLEMENTIRANOG SISTEMA

Sistem predložen u ovom radu sastoji se od pfSense *firewall* sistema instaliranog na APU4 hardveru, sa dodatno instaliranim Snort IDS sistemom. APU4 ima 30GB SSD i 4GB RAM memorije, poseduje jedan serijski, četiri gigabitna i dva USB porta. Kako bi NetFlow funkcionalnosti bile dostupne na pfSense sistemu, neophodna je instalacija i *softflowd* paketa, koji loguje sav mrežni saobraćaj koji prođe kroz instalirani sistem.

Prikaz arhitekture predloženog sistema dat je na slici 1. U cilju analize mrežnog saobraćaja, pfSense podatke iz svojih *firewall* i Snort logova šalje na ELK sistem. Logstash transformiše podatke i šalje ih ElasticSearch komponenti, koja se sastoji od 5 mašina ukupnog kapaciteta 320GB, gde se podaci skladište. Kibana, poslednja komponenta ELK kolekcije, vizuelizuje podatke iz ElasticSearch indeksa. Na isti način kao i pfSense, paket *softflowd* šalje svoje dodatne logove na ELK sistem, u cilju dalje analize. U okviru rada, konfigurisana je Logstash komponenta, dok su ElasticSearch klaster i Kibana prethodno bili postavljeni i konfigurisani.



Slika 1. Prikaz arhitekture sistema

Povezivanje je izvršeno tako da se jedan od gigabitnih portova APU4 uređaja koristi za menadžment pristup pfSensu radi podešavanja i interfejs kome je on dodeljen i nazvan je LAN_ZA_MENADZMENT. Dva gigabitna porta koriste se za veze sa L2 i L3 svičevima i njihovi interfejsi nazvani su LAN_KA_RACUNARIMA i LAN_KA_SVICU, respektivno.

Na interfejsu LAN_ZA_MENADZMENT mrežna podešavanja (IP adresa, maska i *gateway*) su statički podešena. Na portovima koji se koriste za veze sa svičevima kreirani su svi potrebni VLAN-ovi koji postoje na delu fakultetske mreže koja se štiti. Kako bi pfSense mogao biti postavljen između L2 i L3 sviča (kao na slici 1), bez podele broadcast domena, neophodno je povezati interfejse LAN_KA_RACUNARIMA i LAN_KA_SVICU kreiranjem *bridge*-a. Potrebno je kreirati novi interfejs i njemu dodeliti *bridge*, kako bi filtriranje paketa moglo da se vrši između L2 i L3 sviča.

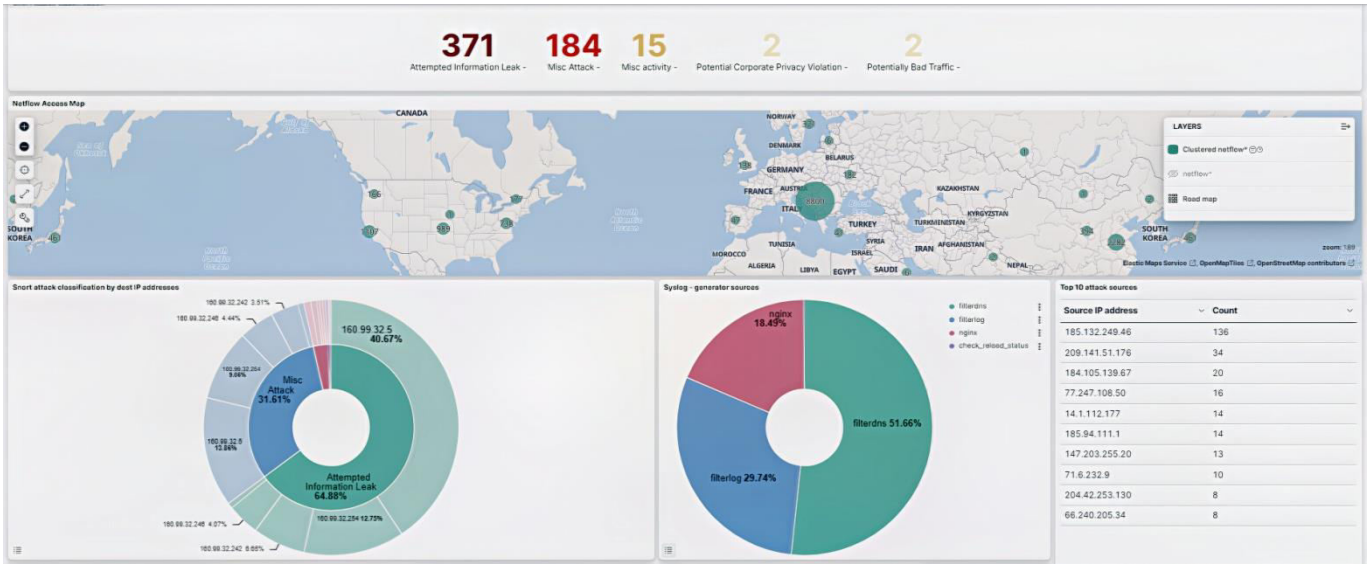
Tokom instalacije sistema, kreirana su *firewall* pravila za filtriranje saobraćaja i instalirani su paketi Snort i *softflowd*. U okviru podešavanja vezanih za Snort, izvršeno je preuzimanje javno dostupne baze Snort pravila. Bitno je podesiti koja se mreža štiti Snort IDS sistemom konfiguracijom HOME_NET opcije na interfejsima. HOME_NET se podešava tako što se kreira alijas koji obuhvata deo fakultetske mreže koji se štiti predloženim sistemom. EXTERNAL_NET opcija se konfiguriše tako da obuhvata sve mreže koje nisu uključene u HOME_NET.

Zatim, Snort IDS je podešen da detekciju napada vrši na *bridge* interfejsu. Na interfejsu se primenjuje celokupna baza preuzetih pravila. Snort je konfigurisan u modu detekcije, kako bi slao upozorenja o potencijalnom napadu, ali bez blokiranja izvorišta ili odredišta. Snort upozorenja se upisuju u pfSense log tako da se zajedno sa postojećim pfSense *firewall* logovima šalju Logstash-u.

Logstash prikuplja podatke sa dva izvora preko kanala na različitim UDP portovima. Jedan izvor čine podaci sa pfSense-a (*firewall* i Snort log), a drugi *softflowd* log podaci o celokupnom saobraćaju koji prolazi kroz pfSense. Pojedinačni izvori podataka definisani su posebnim konfiguracionim fajlovima.

Kod input dela pfSense konfiguracionog fajla koristi se postojeći *syslog plugin*. Filter deo konfiguracije ima više uslova. U zavisnosti od tipa log podatka (pošto su formati poruka različiti) primenjuje se odgovarajući *grok* šablon na osnovu kog se od nestruktuiranih podataka dobijaju značajni atributi i njihove vrednosti. U output delu se vrši slanje prikupljenih podatka ka ElasticSearch komponenti. Podaci dobijeni od Snort-a upisuju se u jedan, a od pfSense-a u drugi ElasticSearch indeks. Značajni podaci koje daje Snort su: izvorna i odredišna ip adresa, izvorni i odresišni port, klasa napada, prioritet, akcija, protokol itd. PfSense *firewall* sistem generiše podatke o blokiranim paketima, i to u formi interfejsa, preduzete akcije, izvorne i odredišne IP adrese i porta, itd.

U *softflowd* konfiguracionom fajlu input deo sadrži *udp plugin* za koji je definisan *codec* netflow, koji vrši dekodiranje dobijenih podataka u NetFlow formatu. U filter delu se za *source_ip* i *destination_ip* koristi *geoip* filter za dobijanje koordinata u cilju analize mrežnog saobraćaja iz ugla geografskog položaja. Output upisuje podatke u treći, zasebni netflow ElasticSearch indeks. Značajni podaci koji se dobijaju od softflowd paketa su izvorišna i odredišna IP adresa, izvorišni i odredišni port, podaci o geografskom položaju (koordinate, grad, država i sl.), količina prenetih podataka.



Slika 2. Vizuelni prikaz prikupljenih podataka

IV. PRIKAZ DOBIJENIH PODATAKA

Za vizuelizaciju i analizu podataka dobijenih od pfSense-a, Snort IDS sistema i *softflowd* paketa korišćen je Kibana alat. Kreirani su dijagrami koji omogućavaju praćenje značajnih parametara sistema. Na slici 2 data je komandna tabla (eng. *dashboard*) koja daje vizuelni prikaz prikupljenih podataka u toku poslednjih 7 dana.

Dijagram na vrhu slike brojčano pokazuje različite vrste napada u toku 7 dana, koje je detektovao Snort IDS sistem. Na mapi sveta su obeležene lokacije izvornih IP adresa svih paketa koji prolaze kroz pfSense, detektovanih od strane softflowd paketa. Prvi s leva dijagram ispod mape pokazuje različite vrste napada na mrežu u procentima, koje je zabeležio Snort IDS, i za svaku vrstu napada odredišne adrese ka kojima je upućen maliciozni saobraćaj. Dijagram u sredini procentualno prikazuje udeo svakog tipa log podatka u sa pfSense sistema. Tabela u donjem desnom uglu sadrži deset IP adresa sa kojih je najviše paketa detektovao Snort IDS. Na taj način su zabeleženi najčešći izvori malicioznog saobraćaja ka zaštićenoj mreži.

Implementirani sistem omogućava prikupljanje podataka sa više različitih izvora, njihovo struktuiranje i proširenje podacima o geografskom položaju. Takođe, sistem omogućava rad sa velikom količinom log podataka, jer koristi ElasticSearch skladište velikog kapaciteta. Konačno, vizuelizacija podataka omogućava njihovu jednostavnu analizu, kao i vizuelnu korelaciju podataka iste mreže, ali sa različitih izvora. Na taj način, implementirani sistem pruža mogućnost jednostavne detekcije napada u realnom vremenu.

V. ZAKLJUČAK

U ovom radu implementiran je sistem za zaštitu dela računarske mreže Elektronskog fakulteta u Nišu pfSense sistemom instaliranim na APU4 hardveru. PfSense ima *firewall* ulogu i loguje sve informacije o blokiranim paketima, dok dodatno instalirani Snort IDS služi za detekciju mrežnih napada. Podaci koje generiše predloženi sistem prikupljeni su, analizirani i vizuelizovani upotrebom ELK sistema. U radu su date arhitektura i implementacija predloženog sistema, kao i proces prikupljanja i analize mrežnih podataka. Takođe, dat je i vizelni prikaz analize prikupljenih podataka.

ZAHVALNICA

Autori se zahvaljuju prof. dr Vladimiru Ćiriću na uloženom trudu, savetima, motivaciji i podršci.

LITERATURA

[1] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, ”Survey of intrusion detection systems: techniques, datasets and challenges”, Cybersecurity, Vol. 2, 2019.
[2] J. M. Kizza, Guide to Computer Network Security, 4th. ed. Springer, Publishing Company, Incorporated, 2017.
[3] X. He, “Research on Computer Network Security Based on Firewall Technology”, IOP Publishing, 2020.
[4] C. Buechler, J. Pingle, “pfSense: The Definitive Guide”, 2009.
[5] D. Zientara, “Mastering pfSense”, Packt Publishing, 2016.
[6] S. Dwiyatno, W. A. Andriani, A. P. Sari, Sulistiyono, “Implementation of Snort IPS Using pfSense as Network Forensic in Smk XYZ”, Atlantis Press SARL, 2020.
[7] W. Stallings, L. Brown, „Computer security – Principles and Practice“, Pearson, 2008.
[8] B. Caswell, J. Twycross, T. Hesketh-Roberts, „Snort – IDS and IPS Toolkit“, Syngress Publishing, 2007.
[9] S. Chhajed, „Learning ELK Stack“, Packt Publishing, 2015.