BEZBEDNOSNI MONITOR

Bezbednost u sistemima elektronskog poslovanja
Verzija 1
2018.

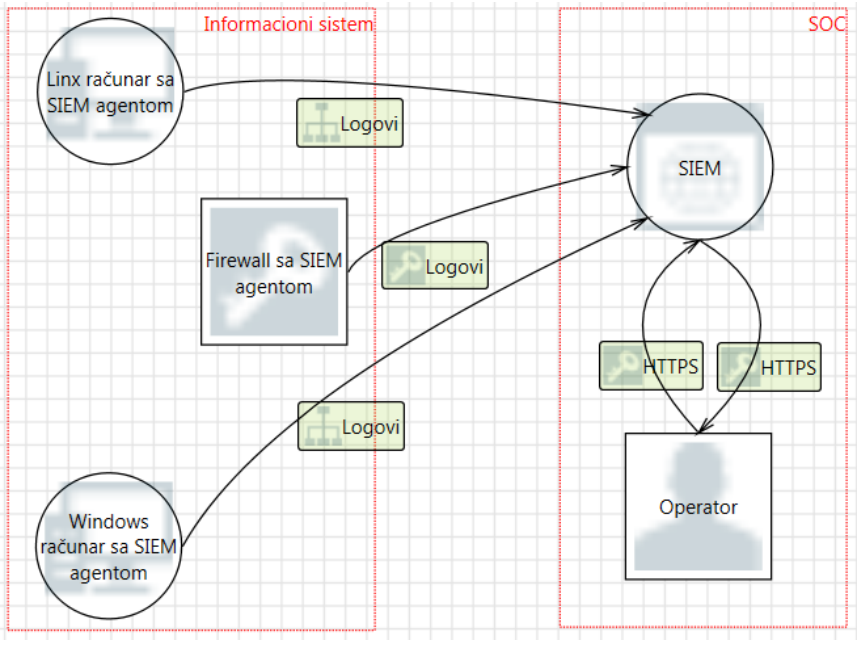
U okviru projektnog zadatka iz predmeta Bezbednost u sistemima elektronskog poslovanja potrebno je implementirati *security information and event management* (SIEM) monitoring sistem. SIEM alata predstavlja softver koji posmatra proizvoljan softverski sistem u produkciji i prikuplja, normalizuje, filtrira i korelira događaje koje posmatrani sistem generiše tokom svog rada, kako bi detektovao, alarmirao i reagovao na potencijalne napade i bezbednosne probleme.

SIEM alat vrši svoj posao centralizovanim skupljanjem i analizom log datoteka. Upotrebom sistema zasnovanim na pravilima, ovaj alat korelira događaje koji se dešavaju u sistemu u nekom vremenskom periodu i na osnovu njih odlučuje da li će okinuti nekakav alarm. Ilustrativan primer ove funkcionalnosti je detekcija i alarmiranje kada se deset puta u minutu izvrši prijava na sistem sa istim korisničkim imenom.

Tehnologije koje se koriste za implementaciju bilo koje celine ovog sistema su proizvoljne.

1. ARHITEKTURA SISTEMA

Scenario projekta podrazumeva da se SIEM alat koristi za monitoring proizvoljnog informacionog sistema. SIEM alat je postavljen na odvojen računar u *security operations center* (SOC), dok su njegovi agenti raspoređeni na ostalim računarima preduzeća (Slika 1).



SLIKA 1 ARHITEKTURA RAČUNARSKOG POSTROJENJA

2. STAVKE SPECIFIKACIJE

U ovom poglavlju su definisani podsistemi, dokumenti i bezbednosni mehanizmi koji trebaju da budu implementirani u sklopu projekta.

2.1 SIEM PODSISTEM

SIEM podsistem se sastoji od dve različite aplikacije, SIEM agenta i SIEM centra.

2.1.1 SIEM AGENT

SIEM agent predstavlja jednostavnu aplikaciju koja se postavlja na računar čiji logovi žele da se prate. Agent ima konfiguracioni fajl koji sadrži spisak direktorijuma koji sadrže logove koje treba da prati na datoj mašini. Kao minimalan skup log datoteka, agenti moraju biti u stanju da čitaju logove operativnog sistema (Linux i Windows), kao i logove proizvoljnog broja drugih izvora (npr. veb-server, aplikacija, firewall).

Pored praćenja upisa novih stavki u posmatrane log datoteke, agent treba da podrži filtrirano prosleđivanje novih upisa ka SIEM centru. Filteri su definisani u vidu regularnih izraza u sklopu konfiguracije agenta.

Za potrebe projekta, tri agenta treba da budu raspoređena na tri različite mašine informacionog sistema. Ovi agenti posmatraju dostupne logove i prosleđuju ih SIEM centru. Generisanje logova treba da bude izvršavano prikladnim skriptama koje stvaraju smislene stavke loga. Logove generisati poštujući syslog format.

2.1.2 SIEM CENTAR

SIEM centar predstavlja aplikaciju koja vrši obradu logova koje prihvata od agenata. Ovaj alat pruža veb-interfejs koji operateru prikazuje relevantne podatke i pruža dozvoljene funkcionalnosti. SIEM centar treba da podrži sledeće funkcionalnosti:

- Prihvatanje, indeksiranje i skladištenje logova dobavljanih od strane SIEM agenata;
- Prikaz i pretraga logova po različitim poljima, sa mogućnošću upotrebe regularnih izraza;
- Pregled alarma i kreiranje pravila za okidanje alarma;
- Generisanja izveštaja bitnih aktivnosti u određenom vremenskom periodu (broj logova po sistemu, broj logova po mašinama, broj alarma po sistemu, broj alarma po mašini, itd.).

2.1.3 ALARMI

Dizajniranje komponente za kreiranje i okidanje alarma predstavlja najveći izazov ovog sistema, gde je neophodno omogućiti kreiranje alarma koji se okida za proizvoljan broj konkretnih događaja u nekom vremenskom periodu. Mali podskup ovih događaji uključuje:

- Neuspešni pokušaji prijave na sistem na istoj mašini. Prijava može biti na nivou operativnog sistema ili na nivou simuliranog informacionog sistema;
- Neuspešni pokušaji prijave na sistem sa istim korisničkim imenom. Prijava može biti na nivou operativnog sistema ili na nivou simuliranog informacionog sistema;
- HTTP zahtevi koji su pristigli na vatreni zid sa IP adresa koje nisu očekivane od strane vatrenog zida;
- Pojava loga čiji tip je ERROR.

2.2 BEZBEDNOST RESURSA

Osetljivi podaci sa kojim aplikacija radi treba da budu obezbeđeni u skladištu, u transportu i tokom upotrebe. Identifikovati osetljive podatke i definisati i implementirati prikladne bezbednosne kontrole.

Podaci čije skladištenje se ne može izbeći treba da budu šifrovani ili heširani ukoliko je to prikladno. Logovi koji se razmenjuju treba da budu digitalno potpisani od strane agenta koji ih šalje, i komunikacija treba da bude

zaštićena od reply napada. Komunikacija između veb-čitača i servera treba da bude zaštićena sigurnom konfiguracijom HTTPS protokola. Sertifikate generisati putem Let's Encrypt servisa ili OpenSSL-a.

2.3 Upravljanje korisnicima

Korisnički interfejs namenjen operateru SIEM alata treba da podrži prikladne mehanizme za autentifikaciju i autorizaciju. Mehanizmi autentifikacije treba da podrže bezbednu prijavu na sistem, odjavu i promenu lozinke. Registraciju korisnika izvršiti upotrebom SQL skripti.

Autorizacija podrazumeva kontrolu pristupa po RBAC modelu, gde postoji rola operatera koji može da posmatra alarme i pretražuje logove, kao i rola administratora koji može da kreira pravila alarma, pregleda okinute alarme i pretražuje logove.

Dodatni zadatak za četvoročlane timove

Proširiti arhitekturu sistema tako da agenti budu hijerarhijski organizovani. U ovakvom rešenju SIEM agent na Windows i Linux računaru se javljaju SIEM agentu na vatrenom zidu, koji prosleđuje njihove logove SIEM centru.

SIEM centar treba da bude proširen sa komponentom za upravljanje SIEM agentima. Ovaj podsistem sadrži hijerarhijski model agenata, i pruža administratorskoj roli dinamičku konfiguraciju agenta, što podrazumeva:

- Izmenu direktorijuma koji udaljeni agent posmatra;
- Izmenu agenta kojem udaljeni agent prosleđuje logove.

U sklopu ovog bonus zadatka je potrebno osigurati strogu kontrolu pristupa, gde agent prihvata poruke samo od agenata od kojih očekuje poruku, a odbacuje sve ostale.