Projektni zadatak 10.

Implementirati servis koji ima ulogu Syslog servera koji je zadužen da na centralizovan i uniforman način zapisuje događaje pristigle od različitih Syslog klijenata. Ulogu Syslog klijenata ima Application Firewall koga čine dve pod-komponente:

- Sistem za whitelist firewall konfiguraciju, kojim se definiše lista dozvoljenih komunikacionih protokola i portova. Svaka izmena ove konfiguracije (na aplikativnom nivou) izaziva generisanje bezbednosnog događaja.
- Sistem za detekciju pokušaja korišćenja nedozvoljenih protokola ili portova. Kada se detektuje ova aktivnost, generiše se bezbednosni događaj.

Navedeni događaji se zapisuju u posebnim log datotekama, a zatim se šalju notifikacije Syslog serveru, koji sve poruke loguje u uniformnom formatu (Criticality, Timestamp, Source, Message, State).

Autentifikacija između Syslog servera i ovih klijenta vrši se pomoću sertifikata, neophodno je izvrsiti custom validaciju na sledeci nacin :

- klijentski sertifikat (whitelist firewall) je validan ako je izdat od strane istog CA kao i serverski.
- klijentski sertifikat (za detekciju pokusaja) je validan ako je izdat u prethodnih mesec dana.
- serverski sertifikat je validan ako nije self-signed.

Drugu grupu Syslog klijenata čine *Consumer* komponente koje se pretplaćuju na događaje logovane u okviru Syslog servera. Postoje tri grupe *Consumer* klijenata: *Readers, Operators* i *Admins*. Da bi Consumer mogao da se pretplati na događaje određenog tipa i ispisuju ih na svojoj konzoli potrebno je da ima privilegiju *Read*. Za izmenu stanja poruke (npr. atribut State = Open, Close) mora da ima privilegiju *Update*, dok je za brisanje poruke potrebno da ima privilegiju *Delete*. Komunikacija između Syslog servera i ovih klijenta vrši se preko Windows protokola, u skladu sa opisanim RBAC modelom.

Dodatno, potrebno je obezbediti periodično ažuriranje log datoteke backup Syslog servera sa kojim glavni Syslog server uspostavlja komunikaciju preko sertifikata. Sertifikati se smatraju validnim ukoliko su izdati od strane sertifikata čiji CommonName je SYSLOG_CA i period važenja im je duži od 3 godine u trenutku autentifikacije

Prilikom ažuriranja, digitalno potpisati podatke koji se šalju.