BSEP Projekat
Pitanja i odgovori

1. **Da li možete da objasnite projektni zadatak tj. šta se očekuje da implementiramo?**

   Imamo jedan sistem koji nazivamo SIEM centar. Taj sistem treba da obezbedi određenim korisnicima, pre svega administratoru, da prati situacije koje se dešavaju u vojnim jedinicama. Vojna jedinica ima kod sebe neki računar u svojim kasarnama, i oni žele da prate uz pomoć nekih alata stanje tih računara, logove i sve što se dešava. Kada dođe do neke neželjene situacije okidaju se alarmi. Naš sistem instalira jednog agenta na računar u vojnoj jedinici. Taj agent skuplja sve logove koji su nam bitni. Taj agent mora da filtrira logove koji imaju smisla za nas, odnosno koji nam nešto znače, npr bitan nam je log koji je error (navedeno u specifikaciji još primera). Agent može da dodaje i neke informacije koje su bitne i ceo taj skup logova šalje SIEM centru. Na SIEM centar se loguje neki administrator i on može da prati šta se dešava. Može da čita logove i alarme.

   Potrebna nam je komponenta koja će na osnovu logova da okida alarme. Preporuka je da se ova komponenta kreira kao rule based sistem. Definišemo pravila koja će okidati alarme. Glavni deo projekta je da napravimo sistem koji obezbeđuje monitoring nekih računara, odnosno da imamo prikaz nekih alarma koji su se okinuli zato što su se desili neki logovi.

2. **Šta se očekuje da bude urađeno za KT1?**

   Implementirati alat za podršku infrastrukture javnih ključeva (PKI). Prvo pročitati detaljno pdf koji je postavljen za vežbe 3. Tu je objašnjeno šta je PKI. Treba proučiti na internetu šta su dobre prakse trenutno.

   PKI je sistem koji će administratoru da omogući da izdaje sertifikate. Potreban je i frontend za ovu komponentu. Ne moramo da ulazimo u priču oko SIEM centra i agenata. Treba omogućiti administratoru da se uloguje na PKI sistem i da može da kreira sertifikate na zahtev, za naše entitete u sistemu. Imamo na frontu formu gde će admin unositi od tog datuma do tog datuma, toj organizaciji, sve što mi smatramo da ima smisla da stoji od podataka.

   Potrebno je i da imamo mogućnost da se sertifikat povuče. Tu treba da razmislimo koji su trenuci kada se neki sertifikat povlači i kako treba da bude povučen. Za naše sertifikate na neki način treba da skladištimo status, da li je aktivan ili nije.

   Distribucija sertifikata – u redu je da za prvu kontrolnu tačku ne implementiramo ovaj deo već da imamo za početak samo ideju kako to treba uraditi.

3. **Kako treba da izgledaju Windows i Linux mašine? Da li je to nova aplikacija?**

   Neće ocenjivati kakve smo mi funkcionalnosti implementirali u nekoj petoj aplikaciji čije logove mi pratimo. Ocenjuje se kako smo sve povezali i kako

kupimo logove. Možemo da napravimo specijalizovanu aplikaciju koja će da radi neki posao, ali možemo i samo da generišemo neke skripte koje će da nam izbacuju neke logove. Treba da vodimo računa o tome da su nam potrebni i neki konfiguracioni fajlovi. Treba obezbediti da se u okviru agenta može definisati putanja do foldera u kom aplikacija generiše logove koje pratimo. Treba da pokrijemo više slučajeva. Obavezno je da kupimo logove operativnog sistema. Napravimo da prati i npr logove Spring aplikacije.

4. **Da li IAM komponenta treba ručno da se napravi?**

   Komponenta za dodatne poene. Ne moramo od nule da pravimo, možemo da koristimo neka gotova rešenja.

5. **Gde treba da se čuvaju sertifikati?**

   Istražiti koje su najbolje prakse, postoji i u pdf-ovima sa vežbi. Na primer (heap ???) store. Istražiti u kojim delovima naše aplikacije ovo može da se koristi.

6. **Profesor je napomenuo da CA-ovi treba da se izvrsavaju na posebnim instancama. Sta se pod tim tacno misli i ocekuje od nas?**

   Ne treba na posebnim instancama.

7. **Koje biblioteke biste nam preporucili za rad sa sertifikatima?**

   Spring Security, tu je pkrivena većina stvari.

8. **Kome se sve može izdati sertifikat, da li je to krajnji korisnik (neki vojnik ili administrator) ili neka grupa, npr. vojna jedinica, da li to može biti softver (siem centar, siem agent kao aplikacija ili instanca siem agenta koja radi na nekom konkretnom računaru)?**

   Recimo imamo vojnu jedinicu koja želi da koristi naš sistem, ta vojna jedinica takođe ima svog administratora i generišemo sertifikat na email tog administratora. Ovo je samo primer, ne moramo ovako. Imamo neku nacionalnu jedinicu vojske neke države koja generiše sertifikat za tu i tu vojnu jedinicu, a tih vojih jedinica može biti više.

9. **Šta se podrazumeva pod distribucijom sertifikata, na koji način onaj kome je sertifikat izdat treba da koristi i čuva taj sertifikat? Da li se ti izdati sertifikati trebaju integrisati sa browser-om radi podrške https protokola?**

   Pogledati 2. pitanje. Treba omogućiti https komunikaciju. Distribuciju sami da proučimo.

   Ako dodajemo novu jedinicu, SIEM centar2, novog admina, koji bi bio tok slanja sertifikata? Kako instalirati sertifikat na neku novu mašinu? Šta kada imamo mašinu na kojoj je istekao sertifikat? Šta onda radimo? Ovo su pitanja na koja sami treba da odgovorimo. Istražiti na internetu. ☺

10. **Da li navedene podsisteme (IAM, PKI, SIEM centar) treba realizovati kao zasebne servise/mikroservise tj. serverske aplikacije ili možemo imati monolitnu aplikaciju?**

    Kao mikroservise. Istražiti na internetu. ☺

11. **Da li ekstenzije koje ulaze u sertifikate može administrator da definise ili postoji fiksne eksenzije?**

    Istražiti na internetu. ☺

    Možemo da organizujemo strukturu lanaca sertifiata tako da imamo kontinent, državu, organizaciju, pa vojne jedinice.

12. **Da li biste mogli dodatno da pojasnite zahteve za ocenu 10? Nije najjasnije nad kojim delovima aplikacije treba da se izvrže penetration i performance test? Takođe šta podrazumeva odeljak Secure deployment and disposal? Tj šta bi tu trebalo da uradimo?**

    Biće dodato objašnjenje u specifikaciju.

13. **Sta je minimum potrebno za ocenu 6?**

    Sve sa sertifikatima. Javiće kasnije.

14. **Koje tehnologije treba koristiti, java, Spring?**

    Šta god hoćemo.

15. **Da li je moguće da nam pokažete kod koji nam može koristiti ili metode neke, ili primere dobrih projekata ranijih generacija, na osnovu pdf-a se jako malo razume kako treba projekat da izgleda?**

16. **Možete li pojasniti liniju "PKI treba da uzme u obzir validnost sertifikata u kontekstu izbora izdavaoca"?**

    Proveriti datume, potpise, lanac sertifikata, status, ključeve. Ne implementiramo ručno.

17. **Na koji način treba se vrši komunikacija između SIEM Agenta i SIEM Centra, kao i između PKI i SIEM Agenta?**

    Istražiti na internetu. ☺

    Komunikacija mora da bude secure, objašnjeno na kraju pdf-a sa vežbi 3.

18. **Koje je vremensko ogranicenje sertifikata?**

    Istražiti na internetu. ☺

19. **Da li je potrebno implementirati single sign-on za k1?**

    Ne mora, to je za ocenu 10.

20. **Koji sve CA-ovi mogu da postoje ili postoji samo SIEM centar kao Root CA za ovaj sistem?**

    Istražiti na internetu. ☺

21. **Šta predstavljaju nestandardni zapisi logova?**

    Kada imamo log koji nije po formi koju smo očekivali. Npr winodws ima taj i taj format, ali logovi neke aplikacije ne moraju da budu po windows formatu.

22. **Da li je moguće da čitav tim diplomira nad ovim projektom odnosno da li postoji još ta opcija da se isti iskoristi za diplomski rad?**

    Verovatno da, svako po neki deo projekta. Pitati profesora.

23. **Da li kada se izada sertifikat za vojnu jedinicu onda sve masine u toj vojnoj jedinici koriste taj sertifikat ili za svaku masinu poseban?**

    Istražiti na internetu. ☺

24. **Da li je ideja da se izdati sertifikati koriste od strane browsera za https komunikaciju?**

    ?

25. **Koliko git repozitorijuma treba da kreiramo?**

    Idealno samo jedan.
    Dodati folder sa dodatnom literaturom koju smo koristili, dijagramima itd.

- Omogućiti i prikaz node-ova u hijerarhiji sertifikata.