A black background with red text

Description automatically generated

***IT381 Zaštita i bezbednost informacija***

***Domaći zadatak br. 13***

***Ime i prezime: Jovan Pavkovic***

***Broj indeksa: 4442***

**Rešenje domaćeg zadatka**

Proces sertifikacije web servera, bilo da se radi o Microsoft IIS (Internet Information Server) ili Apache Web serveru, uključuje nekoliko ključnih koraka.

Koraci za sertifikaciju Web servera:

1. Generisanje Ključeva:

* Prvi korak je generisanje javnog i privatnog ključa. Ovaj ključni par obezbeđuje enkripciju podataka između web servera i korisničkih pregledača.

1. Nabavka SSL/TLS Sertifikata:

* Sertifikat se dobija od pouzdane certifikacione agencije (CA). To može biti komercijalna CA poput VeriSign ili besplatna CA poput Let's Encrypt.
* CA će izdati potpisan sertifikat koji potvrđuje identitet vlasnika web servera.

1. Instalacija Sertifikata na Web Server:

* Sertifikat se instalira na web serveru uz pomoć administratorskih alatki, kao što su MMC (Microsoft Management Console) za IIS ili Apache konfiguracione datoteke.
* Ovaj korak omogućava serveru da koristi sertifikat za enkripciju podataka.

1. Konfiguracija SSL/TLS Postavki:

* Postavke na web serveru se konfigurišu za podršku SSL/TLS protokola.
* Specifični parametri, kao što su podržane verzije protokola i algoritmi šifrovanja, se prilagođavaju kako bi se optimizovala bezbednost i performanse.

1. Podešavanje Virtualnih Hostova (Ako je Primenjivo):

* Ako server hostuje više sajtova, virtualni hostovi se konfigurišu kako bi svaki imao svoj set sertifikata i enkripcione postavke.

1. Testiranje:

* Pre nego što se sertifikat stavi u produkciju, vrši se testiranje kako bi se proverila ispravnost konfiguracije.
* Alati poput online alata za proveru SSL/TLS bezbednosti pomažu u identifikaciji potencijalnih problema.

1. Održavanje i Ažuriranje:

* Sertifikati imaju ograničeno trajanje, pa je važno pratiti njihov rok važenja.
* Periodično ažuriranje ključeva i sertifikata poboljšava bezbednost.

Šta se dešava između Web Browsera i servera?

1. Browser pokušava da se poveže sa web sajtom koji je obezbeđen SSL-om. Browser zahteva da se server identifikuje
2. Server šalje browseru kopiju svog SSL sertifikata
3. Browser proverava da li je SSL sertifikat pouzdan. Ako jeste, šalje poruku serveru
4. Sever šalje digitalno potpisanu potvrdu za otpočinjanje SSL kriptovane sesije
5. Kriptovani podaci se prenose između browsera i servera.

Osnovni elementi SSL sertifikata?

Postoje 3 osnovna elementa u procesu koji je gore opisan: protokol komunikacije (SSL), akreditivi za utvrđivanje identiteta (SSL sertifikat), i treća strana koja garantuje za te akreditive (sertifikaciono telo).

* Kompjuteri koriste protokol koji omogućavaju da različiti sistemi funkcionišu zajedno. Web serveri i web browseri se oslanjaju na Secure Sockets Layer (SSL) protokol kako bi omogućili kriptovanu komunikaciju. Zahtev browsera da se server identifikuje (da pokaže „isprave“) je funkcija SSL protokola.
* Akreditivi za utvrđivanje identiteta su uobičajeni i u našem svakodnevnom životu: vozačka dozvola, pasoš, propusnica. SSL sertifikat je vrsta digitalnog sertifikata koja služi kao akreditiv u online svetu. Svaki SSL sertifikat potvrđuje identitet za jedan domen i web server.
* Naše poverenje u akreditive zavisi od poverenja u organizaciju koja ga je izdala. Sertifikaciona tela na različite načine utvrđuju verodostojnost informacija koje im dostavljaju pojedinci ili organizacije. Priznata sertifikaciona tela, kao što su Digicert, Thawte i GeoTrust, uživaju poverenje browsera, zbog čega browseri sajtove sa sertifikatima ovih sertifikacionih tela označavaju kao bezbedne.

Životni ciklus SSL sertifikata?

Kada vam je potrebna zaštita za web sajt, lako možete da zatražite SSL sertifikat i instalirate ga.

1. Generišite Certificate Signing Request (CSR) za web server koji planirate da zaštitite. Ako nemate pristup serveru, kontaktirajte vašeg hosting provajdera i zahtevajte da vam generišu CSR
2. Izaberite SSL sertifikat i pošaljite CSR
3. Zajedno sa CSR-om pošaljite podatke dve kontakt osobe za sertifikat. Tehnički kontakt treba da bude osoba koja će primiti i instalirati sertifikat, a administrativni kontakt osoba koja potvrđuje porudžbinu i komunicira sa sertifikacionim telom
4. Nakon uspešne autentifikacije preuzmite SSL sertifikat
5. Pratite uputstva za instalaciju sertifikata na vaš web server
6. Preuzmite pečat poverenja i instalirajte ga na web sajt

SSL sertifikati mogu važiti maksimalno 1 godinu i pre isteka sertifikata, najranije 90 dana pre, imate mogućnost da ga obnovite. Za obnovu sertifikata potrebno je da generišete novi CSR i da ponovo prođete proceduru autentifikacije, nakon koje se izdaje novi SSL sertifikat koji morate da instalirate na mesto starog.

Primer za SSL sertifikate: <https://letsencrypt.org/sr/how-it-works/>