

### 3. Zadaća iz predmeta "Zaštita i sigurnost informacijskih sustava"

*Zaokružite ispravne odgovore:*

- 7-16 Kako se višepojavnost (polyinstantiation) koristi za zaštitu višerazinske baze podataka ?
- A. Ona sprečava korisnike niže sigurnosne razine da zaključuju o podacima više sigurnosne razine
  - B. Ona potvrđuje da svi ograničeni podatci unutar sustava zadovoljavaju specifikacije integriteta
  - C. Ona osigurava da su svi mehanizmi u sustavu odgovorni za provođenje sigurnosne politike za bazu podataka
  - D. Ona osigurava da će dvije operacije na istoj sigurnosnoj razini biti u konfliktu ako one pristupaju istom podatku, a najmanje jedna od njih je operacija ažuriranja (update).
- 7-18 Zaključivanje o osjetljivim podacima se može smanjiti korištenjem jednog od navedenog:
- A. Tehnike višepojavnosti
  - B. Primjenom tehnika zasnovanih na pravilima
  - C. Višerazinskom klasifikacijom podataka
  - D. Transformacijom ispravnog stanja
- 7-19 Što od navedenih svojstava transakcijske obrade osigurava da kada transakcija završi uspješno (commit završetak), izmjena baze (update) se provodi ispravno i u slučaju pojave greške na sustavu, kada transakcija završava s abortom ?
- A. Atomnost (Atomicity)
  - B. Konzistentnost (Consistency)
  - C. Izolacija (Isolation)
  - D. Postojanost (Durability)
- 8-44 Koji su pogodni protokoli za VPN (Virtual Private Network) vezu ?
- A. S/MIME and SSH
  - B. TLS and SSL
  - C. IPsec and L2TP
  - D. PKCS# and X.509
- 8-45 Koje od navedenih pravila za sigurnosnu stijenu (firewall) nije za očekivati da bude instalirano u konfiguraciji sigurnosne stijene koja povezuje internu mrežu i Internet ?
- A. Dozvoli sav promet prema i od lokalnih računala(host)
  - B. Dozvoli sav ulazni promet za ssh (Secure Shell) promet
  - C. Dozvoli sve ulazne tcp (transmission control protocol) veze
  - D. Dozvoli sav promet sistemskog zapisa na poslužitelj server.abc.org

- 8-36 Što je od navedenog istinito u odnosu na Kerberos ?
- A. On koristi kriptografiju javnih ključeva
  - B. On kriptira podatke nakon što je dodijeljena karta, ali lozinke se izmjenjuju u čistom tekstu
  - C. On ovisi o simetričnim šiframa (enkripciji)
  - D. On je druga strana autentifikacijskog sustava
- 8-37 Koji od navedenih potencijalnih problema sigurnosne stijene (firewall) treba biti zapisan ?
- A. Reboot
  - B. Svi navedeni izbori
  - C. Restart sigurnosne stijene
  - D. Izmjene u konfiguracijskoj datoteci
- 8-38 Koji je nedostatak NIDS-a (Network-based Intrusion Detection System) ?
- A. Ne može analizirati kriptiranu informaciju
  - B. Vrlo je skup za uspostavu
  - C. Vrlo je skup za upravljanje
  - D. Nije učinkovit
- 8-39 HDIS (Host Intrusion Detection System) normalno koristi informaciju iz slijedećih izvora :
- A. Zapisa operacijskog sustava (audit trails) i sistemskog dnevnika (systems log)
  - B. Zapisa operacijskog sustava (audit trails) i mrežnih paketa
  - C. Mrežnih paketa i sistemskog dnevnika (systems log)
  - D. Alarma operacijskog sustava i sistemskih dnevnika (systems log)
- 8-40 Koje je primarno rješenje koje koristi IDS (Intrusion Detection System) sustav za analizu, kako bi detektirao napad ?
- A. Detekcija zlouporabe i detekcija anomalija
  - B. Detekcija dnevnika (log) i detekcija anomalija
  - C. Detekcija zlouporabe i rana detekcija ispada
  - D. Detekcija ispitivanjem (scan) i detekcija anomalija