Ispitna pitanja na predmetu Sigurnost računalnih sustava
Upravljanje informacijskom sigurnošću

1. Kada je računalni sustav siguran?
2. Što je ranjivost/prijetnja/napad?
3. Navesti definiciju inromacijske/kibernetičke sigurnosti.
4. Navesti osnovne/sve sigurnosne zahtjeve?
5. Što je povjerljivost?
6. Kako se ostvaruje neporecivost?
7. Na koji način se može ostvariti autentičnost bez korištenja asimetrične kriptografije?
8. Što predstavlja kratica CIA u računalnoj sigurnosti?
9. Od kojih se komponenata sastoji sigurnost prema Bishopovoj taksonomiji.
10. Navesti nekoliko domena informacijske sigurnosti.
11. Što su sigurnosne kontrole?
12. Navesti jednu od taksonomija sigurnosnih kontrola.
13. Navesti nekoliko prijetnji povjerljivosti i integritetu u domeni kontrole pristupa.
14. Navesti nekoliko primjera preventivnih fizičkih kontrola.
15. Navesti nekoliko primjera detekcijskih fizičkih kontrola.
16. Navesti nekoliko primjera preventivnih tehničkih kontrola.
17. Navesti jedan primjer detekcijske tehničke kontrole.
18. Navesti nekoliko primjera preventivnih administrativnih kontrola.
19. Pojasniti svojstva biometrijskih sigurnosnih sustava koja su definirana sljedećim parametrima: FRR, FAR, CER.
20. Navesti i opisati najpoznatiji model za uspostavu povjerljivosti.
21. Navesti 5 stupnjeva sigurnosti prilikom kategorizacije resursa.
22. Navesti frazu koja dobro opisuje Bell-LaPadula model povjerljivosti.
23. Što čini rešetku (lattice)?
24. Neka tri kategorije EUR, US i JAP čine rešetku u dva nivoa. U nižem nivou su sljedeći elementi: {(0),(US)}, a u višem nivou su {(EUR), (EUR, US), (EUR, JAP)}. Neka subjekt A ima sljedeće sigurnosno dopuštenje: {ograničeno, (EUR)}, a objekt X je klasificiran {povjerljiv, (US)}. Može li subjekt A pristupiti objektu X? DA/NE Obrazložiti odgovor.
25. Navesti frazu koja dobro opisuje Biba model za uspostavu integriteta.
26. Navesti nekoliko mrežnih alata za unapređenje mrežne sigurnosti.
27. Što je rizik?
28. Nakon što identificiramo i procjenimo rizik, on se može: _____, _____, _____ ili _____.
29. Navesti tri faze u procesu upravljanja rizikom.
30. Procjena rizika može se obaviti na sljedeći način: _____ i/ili _____.
31. Opisati kvantitativni pristup procjene rizika.
32. Koliko iznosi vjerojatnost ostvarenja prijetnje ako je procijenjeni rizik za taj resurs 100 KN/god, faktor izloženosti 10%, a procijenjena vrijednost resursa 100.000 KN?
33. Koji je najveći nedostatak kvantitativnog pristupa?
34. Navesti nedostatke kvalitativnog pristupa.
35. Opisati neku metodu kvalitativne procjene rizika.
36. Kako je moguće postići najbolje rezultate u procjeni rizika?
37. Čemu služi norma ISO/IEC 27000/27001/27002?
38. Što je sigurnosna politika?
39. Opisati PDCA model upravljanja informacijskom sigurnošću.
40. Čemu služi skup normi PKCS?
41. Što je to kriptografski token?