Pitanja za ispit otvorenog tipa

1. Aktivni napadi
2. Pasivni napadi
3. Osnovne faze napada
4. Najčešće primenjivane vrste napada i pretnji
5. Upravljanje rizikom
6. Osnovne vrste ranjivosti
7. Procedure nakon incidenta (Incident Response – IR)
8. Model bezbednosti
9. BLP model
10. BIBA model
11. Clark Wilson model
12. Sigurnosne arhitekture, oznake i režimi
13. Ranjivosti u sistemskoj sigurnosnoj arhitekturi
14. Sertifikacija i akreditacija
15. Diffle-Hellman algoritam
16. AES algoritam
17. RSA algoritam
18. Kriptografija javnim kljucevima
19. Simetricni kriptografski sistemi
20. Kriptoanaliza
21. Kriptosistem
22. Digitalni potpis
23. Hash funkcije
24. Digitalna koverta i digitalni potpis email dokumenata
25. Standard za digitalni potpis
26. Provera verodojstojnosti poruke
27. Kod za autentifikaciju poruke
28. Sertifikaciono telo
29. Detekcija upada
30. IDS zasnovan na hostu
31. IDS baziran na mreži
32. Tehnike detekcije upada
33. Honeypots – lažni mamci
34. SNORT
35. OSI model
36. Bezbednosni servisi i menanizmi
37. IPSec protokol
38. Upravljanje kljucevima
39. Authentication Header (AH)
40. Encapsulating Security Payload (ESP)
41. Web bezbednost i application layer security
42. Bezbednost transportnog sloja
43. Autentifikacija i autorizacija
44. SSL protokol
45. Kerberos protokol
46. Bezbedni sistem elektronske pošte
47. Mrežni zaštitni zid
48. Filtriranje paketa
49. Dinamičko ispitivanje paketa
50. Mrežni prolazi na sloju konekcija
51. Lokacije zaštitnih zidova
52. Konfiguracija zaštitnog zida
53. Zastitni zid zasnovan na hostu
54. Virtualna privatna mreža
55. Distribuirani zaštitni zidovi
56. Bezbednost lokalnih bezicnih mreza i standardi
57. Sigurnosni propusti u IEEE802.11 i zahtevi i pretnje
58. Gubitak poverljivosti, integriteta i raspoloživosti
59. Protokol IEEE802.11i
60. Bezbednost mobilnih mreza i ličnih bezicnih mreža
61. Bezbedni sadržaj
62. Linux modeli bezbednosti
63. Bezbednost sistema datoteka
64. Linux/UNIX dozvole
65. Linux ranjivosti
66. Ojačanje Linux sistema
67. SELinux
68. MS Windows bezbednosna arhitektura
69. Ojačanje Windows sistema
70. Odbrana naloga
71. Security descriptor
72. Odbrana mreže
73. Windows ranjivosti
74. Lokalni domen naloga
75. Windows privilegije
76. Niske privilegije usluge naloga, smanjenje privilegija
77. Bezbednost elektronskog poslovanja
78. Proces placanja i transakcije placanja
79. Bezbednost elektronskih sistema placanja
80. Bezbednost mobilne trgovine i digitalnog novca