ZÁRÓVIZSGA FELKÉSZÜLÉSI KÉRDÉSSOR

Kiberbiztonsági MA

2024/2025/2

Kockázatelemzés, kockázatkezelés

1. Mi a kockázat, mi az a kockázatarányos védelem?
2. Mutassa be a CRAMM támadási modelljét!
3. Mutassa be, hogy milyen fenyegetésekkel számolunk!
4. Ismertesse az Ibtv. szerinti biztonsági osztályba sorolás módját!
5. Milyen kockázatkezelési szabványokat ismer?
6. Milyen kockázatelemzési eljárásokat ismer?
7. Melyek a kockázatelemzés főbb lépései?
8. Mutasson be egy kockázatelemzéshez használható kárértéktáblázatot!
9. Mely védelmi intézkedések csökkentik a fenyegetések által okozott károk nagyságát?
10. Mely védelmi intézkedések csökkentik a fenyegetések bekövetkezési gyakoriságát?
11. Mutassa be az adatvagyonleltár tartalmát és elkészítésének módszerét!
12. Mi a kockázatkezelés célja?
13. Mutassa be a kockázatkezelés főbb lépéseit!
14. Mi az RTO?
15. Mi az RPO?
16. Milyen kockázatkezelési opciókat ismer?
17. Mi a maradványkockázat és mit jelent annak elfogadása?

18. Ismertesse a kockázatmenedzsmentet támogató IT GRC szoftverek jellemzőit!

Hálózatok és rendszerek biztonsága

19. Ismertesse az OSI modell felépítését, az egyes rétegek jellemzőit!
20. Ismertesse a TCP/IP modell felépítését, az egyes rétegek jellemzőit!
21. Ismertesse az IP címek típusait!
22. Mutassa be a statikus és dinamikus címhozzárendelést!
23. Ismertesse a protokollok szerepét a hálózatokban!
24. Ismertesse az alkalmazási protokollokat és szolgáltatásokat!
25. Mutassa be a fizikai és logikai topológiák jellemzőit!
26. Mutassa be a különböző hálózati topológiákat!
27. Ismertesse a hozzáférési réteg felépítését, jellemzőit!
28. Ismertesse az elosztási réteg felépítését, jellemzőit!
29. Ismertesse a kapcsolók feladatait, jellemzőit a hálózaton!
30. Ismertesse a forgalomirányítók feladatait, jellemzőit a hálózaton!
31. Ismertesse a hálózati címfordítás elvét!
32. Ismertesse a virtuális helyi hálózatok jellemzőit!
33. Ismertesse az informatikai biztonságpolitika alapelveit!
34. Ismertesse a tűzfalak típusait, jellemzőit!
35. Ismertesse a DMZ típusait és jellemzőit!
36. Ismertesse a virtuális magánhálózatok jellemzőit!
37. Mutasson be legalább három hálózati biztonsági megoldást!
38. Mutassa be a kockázatok csökkentésére alkalmazható eljárások körét!

1083 Budapest, Üllői út 82. | +36 1 432 9000
POSTACÍM 1441 Budapest, Pf. 60. | antk@uni-nke.hu, antk.uni-nke.hu