Ibiza_vizsga_2023

Az informatikai biztonság alapjai (Debreceni Egyetem)

27. Milyen hash függvényeket használunk a digitális aláírásoknál?
    a. őskép ellenálló
    b. ütközésmentes
    c. gyengén ütközésmentes
28. Mely állítás(ok) igaz(ak)?
    a. A digitálisan aláírt üzenet hosszabb, mint az üzenet.
    b. Az érvényes digitális aláírás biztosítja az üzenet letagadhatatlanságát.
    c. A digitális aláírás biztosítja az üzenet bizalmasságát.
    d. A digitális aláírás a hitelesség eszköze.
29. Mely(ek) a PKI Regisztrációs Hivatalának feladata(i)?
    a. Kulcspárok generálása.
    b. Tanúsítványok tárolása.
    c. Ügyfelek hitelesítése.
    d. Visszavonási lista tárolása.
30. Mely(ek) a PKI Hitelesítő Hivatal feladata(i)?
    a. Tanúsítványok visszavonása.
    b. Kulcspárok generálása.
    c. Tanúsítványkérések összeállítása.
    d. Tanúsítványok aláírása.

17. Mely állítás igaz?
    a. A titkosító algoritmus általában randomizált.
    b. A visszafejtő algoritmus egyik bemenete mindig a titkos kulcs.
    c. A titkosító algoritmus egyik bemenete mindig a titkos kulcs.
    d. A kulcsgeneráló algoritmus kimenete a titkos kulcs.
18. Az aszimmetrikus titkosítás kulcsgeneráló algoritmusának bemenete:
    a. biztonsági paraméter
    b. titkos kulcs
    c. nyilvános kulcs
    d. nyílt üzenet
19. Mely algoritmus biztosan determinisztikus?
    a. kulcsgeneráló
    b. titkosító
    c. visszafejtő
20. Mely állítás(ok) igaz(ak)?
    a. Az IBK az informatikai biztonsággal kapcsolatos stratégiai elképzeléseket tartalmazza.
    b. AZ IBK részletesen megadja a rendszergazda feladatait.
    c. Az IBSZ tartalmazza az infrastruktúra védelmét szolgáló intézkedéseket.
21. Melyek az RSA algoritmus titkos adatai?
    a. RSA modulus
    b. exponens, mely relatív prím fi(n)-hez, ahol n a modulus
    c. a nagy prímek
    d. fi(n), ahol n a modulus
22. Mely állítás(ok) igaz(ak)?
    a. Az RSA titkosító algoritmusa randomizált.
    b. A tankönyvi RSA titkosítással szemben több sikeres támadást is találtak.
    c. Napjainkban az RSA modulus 4096bites.
    d. Bizonyított, hogy a prímfaktorizáció problémája ugyanolyan nehéz, mint az RSA probléma.
23. Igaz –e, hogy az RSA visszafejtő exponensének kiszámítása a nyilvános kulcsból ugyanolyan nehéz, mint a modulus prímfaktorizációja.
    a. igen
    b. nem
24. Milyen eszközöket alkalmaznak a Fejlett Perzisztens Fenyegetések?
    a. nulladik napi támadás
    b. célzott adathalász e-mail
    c. malvertising
    d. clickjacking
25. Mely jellemzők igazak a botnetekre?
    a. Zombie gépek hálózata.
    b. Alkalmasak spam küldésére.
    c. Összegyűjtik a billenytűlenyomásokat.
26. Létezik injektív hash függvény?
    a. igen
    b. nem

9. Mely állítás(ok) igaz(ak)?
   a. A féreg olyan vírus, mely gazdaprogram nélkül képes terjedni
   b. A féreg szoftverek sebezhetőségeit aknázza ki.
   c. A férgek hálózati kapcsolatok, megosztott média, e-mailek csatolmányain keresztül terjedhetnek.
   d. A férgek nulladik napi támadásokkal terjedhetnek.
10. Mely állítás(ok) igaz(ak)?
   a. A malvertising esetén a támadó fizet az olyan hirdetésekért, melyek kártékony programokat tartalmaznak.
   b. Clickjacking olyan támadás, mely során a támadó ráveszi a felhasználókat, hogy kártékony tartalmakat like-oljanak.
   c. A social engineering (pszichológiai támadás) olyan támadás, mely során a támadó átverve a felhasználókat ráveszi őket, hogy veszélyeztessék rendszerüket.
11. Mely állítás(ok) igaz(ak)?
   a. A trójaiak nem sokszorozódnak.
   b. A trójaiak egyszerűen csak hasznos programok.
   c. A trójaiak hátsó kapukat állítanak be.
   d. A trójaiak büntető rutinjai a botnetek kialakítása.
12. Mely intézkedéseket lehet meghozni a tűz elleni védelemnél?
   a. A közös falak legalább egy órán át tűzálló legyen.
   b. A légkondicionálók úgy legyenek megtervezve, hogy a tüzet ne terjesszék.
   c. Kézi tűzoltó készülék legyen elhelyezve.
13. Mely állítás(ok) igaz(ak)?
   a. A fizikai védelem feladata az adatok tárolását, feldolgozását és továbbítását biztosító szoftverek védelme.
   b. A fizikai védelem feladata az adatok tárolását, feldolgozását és továbbítását biztosító hardverek védelme.
   c. A fizikai védelem feladata az adatok tárolását, feldolgozását és továbbítását biztosító fizikai erőforrások védelme.
14. Melyik állítás igaz?
   a. Egy titkosítási séma megadásánál elegendő megadni a titkosító, visszafejtő és kulcsgeneráló algoritmusokat.
   b. Ahhoz, hogy a titkosítási séma ne legyen feltörhető a kulcstér mérete megszámlálhatóan végtelen.
   c. A szimmetrikus titkosítás titkosító és visszafejtő kulcsa lehet bitről bitre ugyanaz.
   d. Minden titkosítási séma titkos kulcsát kulcscsere algoritmussal kell eljuttatni a másik félhez.
15. Mely titkosítási sémák alkalmasak video állományok titkosítására?
   a. aszimmetrikus
   b. szimmetrikus
16. Mely titkosítási sémára igaz, hogy a visszafejtő kulcs csak nehezen számolható ki a titkosítóból?
   a. aszimmetrikus
   b. szimmetrikus

Vizsga 2023. dec. 13.

1. Mely állítás(ok) igaz(ak)?
   a. A kockázat a sérülékenység mértéke.
   b. Az ügyviteli védelem az informatikai rendszer szabályozását foglalja magába.
   c. A forgalom elemzése egy aktív támadás. — hamis, mert passzív
   c. Az üzenet visszajátszása során a támadó mindig visszaküldi az üzenetet a küldőjének.
2. Mely állítás(ok) igaz(ak)?
   a. Az egészségügyi adatok bizalmasságának sérülési szintje magas.
   b. Kétféle sérülési szintet különböztetünk meg: alacsony és magas.
   c. Egy rendszer sértetlenségének sérülése eredményezheti a tárolt adatok bizalmasságának sérülését.
3. Hogyan kategorizálhatjuk a támadásokat?
   a. aktív és passzív
   b. belső és külső
   c. kicsi és nagy
4. Hogyan kategorizálhatjuk a védelmi intézkedéseket?
   a. fizikai, ügyviteli, technikai/algoritmikus
   b. aktív, passzív
   c. preventív, korrektív, detektív
5. Mit jelent az Open Design tervezési alapelv?
   a. A biztonsági mechanizmusokat bárki szabadon megváltoztathatja.
   b. A biztonsági mechanizmusok algoritmusai nyilvánosak.
6. Mely állítások igazak?
   a. A fenyegetés egy olyan támadás, mely sérti az informatikai vagy annak elemeinek biztonságát.
   b. A sérülékenység a rendszer olyan gyengesége, melyen keresztül egy fenyegetés megvalósulhat.
   c. A támadás módja szerint lehet aktív és passzív.
   d. A gyakorlatban előforduló támadások nagy hányada külső támadás.
7. Mely állítás(ok) igaz(ak)?
   a. A fizikai védelem estén a fizikai infrastruktúra a személyzetet is jelenti.
   b. A fizikai fenyegetések esetén két kategóriát különböztetünk meg: a környezeti fenyegetések és természeti csapások.
   c. A számítógép belső hőmérséklete nem lehet nagyobb, mint a szoba hőmérséklete.
   d. A túlfeszültség processzorokban, memóriában okozhat kárt.
8. Mely állítás(ok) igaz(ak)?
   a. A vírusok fertőzött állományok futtatásával terjednek.
   b. A vírus nem sokszorozódik.
   c. A vírusnak nincs szüksége gazdaprogramra a terjedéséhez
   d. A vírusok csak makrókkal ellátott dokumentumokkal terjednek.