CYBER SECURITY

2. forduló

Continental
The Future in Motion

A kategória támogatója: Continental

RENDELKEZÉSRE ÁLLÓ IDŐ:

25:00

Ismertető a feladathoz

Fontos információk

Ha kifutsz az adott feladatlap kitöltésére rendelkezésre álló időből, a felület **automatikusan megpróbálja beküldeni** az addig megadott válaszokat

A kérdésekre **mindig van helyes válasz**! Ha csak egy helyes válasz van az adott kérdésre, radio button-os választási lehetőségeket fogsz látni.

Olyan kérdés viszont nincs, amelyre az összes válasz helyes!

Egyéb információkat a versenyszabályzatban találsz!

Második forduló

Folytatjuk ismerkedésünket az elméleti alapokkal, további feleletválasztós kérdések segítségével, melyek az autóelektronika tervezési és gyártási folyamatai során, azok védelme kapcsán is napi szinten előjönnek.

Felhasznált idő: 02:03/25:00 **Elért pontszám:** 0/13

1. feladat 0/1 pont

Mik az általános céljai a kiberbiztonságnak?

(jelöld meg az összes célt!)

Válaszok

- [x] Titoktartás

- [x] Integritás
- [x] Hitelesség
- [ ] Egyszerűsítés
- [x] Elérhetőség

Magyarázat

Frissítés (2021.11.18): Elfogadja a feladatíró, ha a hitelesség nem került bejelölésre, ez esetben sincs pontlevonás.

2. feladat 0/1 pont

Szimmetrikus kulcsos titkosítás az alábbi célok közül melyikre ad megoldást?

Válasz

- ◯ Titoktartás
- ◯ Integritás
- ◯ Hitelesség
- ◯ Elérhetőség

Magyarázat

3. feladat 0/1 pont

Aszimetrikus kulcsos titkosítás esetén elérhető lenne több cél lefedése a titoktartás mellett?

Válasz

- ◯ Igen
- ◯ Nem

Magyarázat

Frissítés (2021.11.18.) a versenyzői visszajelzéseket figyelembe véve a helyes válasz az igen, az szimmetrikus kulcs további lehetőséget ad pl. az integritásra és a hitelesítésre is.

4. feladat 0/1 pont

Mi igaz a kiberbiztonságra?

Válaszok

- [x] Védelmet nyújt a hardware, software, és az adataink számára a támadóktól.
- [x] Védelmet nyújt az információkhoz való hozzáféréstől, megváltoztatásától vagy törlésétől.
- [ ] Védelmet nyújt a fizikai behatolásokkal szemben.

Magyarázat

5. feladat 0/0 pont

Melyek a kiberbiztonság főbb elemei?

(jelöld meg az összes helyes elemet!)

Válaszok

- [x] Információ biztonság
- [x] Hálózat biztonság
- [x] Üzemelési biztonság
- [ ] Fizikai biztonság
- [x] Alkalmazás biztonság
- [x] Végfelhasználók oktatása
- [x] Üzletmenet-folytonossági tervezés

Magyarázat

Frissítés (2021.11.23.): versenyzői visszajelzések alapján a Fizikai biztonság is ide sorolható. Mivel szabályzatunk szerint egy kérdésre nem lehet az összes válasz helyes, a feladatot 0 pontosra állítottuk.

6. feladat 0/1 pont

Melyek igazak a kriptográfiára?

(jelöld az összes helyes állítást!)

Válaszok

- [x] A kriptográfia egy olyan technika, ahol valamilyen információt védünk a támadó feleknek nevezett entitásoktól.
- [ ] A kriptográfiát a középkorban használták először az információ védelmére.
- [x] Egy kommunikációs folyamat során továbbított nyilvános üzenetet akkor nevezünk titkos(ított)nak, ha a feladó olyan formá(tum)ban küldi, amit olvasni vagy fogadni esetleg többen is tudnak, de megérteni csak a fogadók egy megcélzott csoportja.

Magyarázat

7. feladat 0/1 pont

Mi a különbség az IDS és az IPS között?

Válasz

- ( ) Az IDS érzékeli a behatolásokat. Az adminisztrátor feladata ezeket elhárítani. Az IPS rendszer megtalálja és automatikusan el is hárítja azt.
- ( ) Az IPS érzékeli a behatolásokat. Az adminisztrátor feladata ezeket elhárítani. Az IDS rendszer megtalálja és automatikusan el is hárítja azt.

Magyarázat

8. feladat 0/1 pont

Milyen funkciók várhatók el egy modern tűzfaltól?

(jelöld az összes helyes választ!)

Válaszok

- [x] Rendszer és hálózat védelem
- [ ] Memória védelem
- [x] Malware védelem
- [x] Vírus védelem
- [x] Távoli hozzáférés védelem

Magyarázat

9. feladat 0/1 pont

Mire használjuk a Traceroute-ot?

Válasz

- ( ) Hálózati alkalmazás, kilistázza az összes pontot, amin egy adott csomag áthalad. Kapcsolat megszakadására, hiba keresésre alkalmazzuk.
- ( ) Hálózati alkalmazás, kilistázza az összes nyitott átjárót a hálózaton. Hiba keresésére, biztonsági lyukak felmérésére alkalmazzuk.
- ( ) Hálózati alkalmazás, kilistázza az összes nyitott portot, amin egy adott csomag áthaladhat.

Magyarázat

10. feladat 0/0 pont

Mi a különbség a HIDS és a NIDS között?

Válasz

- ( ) HIDS egy hoszt aktivitását figyeli biztonsági szempontból. A NIDS a hálózaton levő összes eszközt figyeli.

- ○ NIDS egy hálózati eszköz rendszer aktivitását figyeli biztonsági szempontból. A HIDS a hoszt aktivitását figyeli.

Magyarázat

Frissítés (2021.11.18): a két válaszlehetőség egy elírás miatt ugyanazt jelenti, ezért a feladatot 0 pontosra állítottuk.

11. feladat 0/1 pont

Mi az SSL?

Válasz

- ○ Secured Software Layer. Ezzel lehet titkosított kapcsolatokat létrehozni két szoftver réteg között.
- ○ Secure Socket Layer. Ezzel lehet titkosított kapcsolatokat létrehozni egy webszerver és egy webböngésző között.

Magyarázat

12. feladat 0/1 pont

Mivel lehet megelőzni a Brute Force támadásokat?

(jelöld az összes helyes választ!)

Válaszok

- ☐ jelszóemlékeztető használatával
- ☑ rögzített minimális jelszó hosszal
- ☑ jelszó komplexitásának növelésével
- ☑ sikertelen belépések korlátozásával

Magyarázat

13. feladat 0/1 pont

Mi az a port scanning?

Válasz

- ◯ Nyitott portok és az adott hálózati eszközön elérhető szolgáltatások azonosítására szolgáló technika.
- ◯ Összes aktív port felmérése a hálózaton.

Magyarázat

14. feladat 0/1 pont

A felsoroltak közül melyek az OSI-model rétegei?

(jelöld az összes helyes választ!)

Válaszok

- ☑ Fizikai réteg
- ☑ Adatkapcsolati réteg
- ☑ Szállítási réteg
- ☐ Virtuális réteg
- ☑ Viszony réteg
- ☑ Megjelenítési réteg
- ☑ Alkalmazási réteg
- ☑ Hálózati réteg
- ☐ Tömörítő réteg

Magyarázat

15. feladat 0/1 pont

Mit jelent a 80/20 szabály hálózatépítésben?

Válasz

- ◯ A hálózat forgalmának 80%-a legyen lokális és 20%-a valamilyen VPN-en keresztül.
- ◯ A hálózat forgalmának 20%-a legyen lokális és 80%-a valamilyen VPN-en keresztül.

Magyarázat