CYBER SECURITY

1. forduló

Continental
The Future in Motion

A kategória támogatója: Continental

Ismertető a feladatlaphoz

Kérjük, hogy a feladatlap indítása előtt mindenképp olvasd el az alábbi útmutatót:

MINDEN kérdésre van helyes válasz.

Olyan kérdés NINCS, amire az összes válasz helyes, ha mégis az összes választ bejelölöd, arra a feladatra automatikusan 0 pont jár.

Több válaszlehetőség esetén a helytelen válasz megjelölése mínusz pontot ér.

A radio button-os kérdésekre egy helyes válasz van.

Ha lejár a feladatlap ideje, a rendszer AUTOMATIKUSAN beküldi azt az addig megjelölt válaszokkal.

Azokat a feladatlapokat, amelyekhez csatolmány tartozik, javasoljuk NEM mobilon elindítani, erre az érintett feladatlapok előtt külön felhívjuk a figyelmet.

Az adatbekérős feladatokra NEM jár részpontszám, csak a feleletválasztósakra.

Helyezéseket a 4. forduló után mutatunk, százalékos formában: adott kategóriában a TOP 20-40-60%-hoz tartozol.

Ha egyszerre több böngészőből, több ablakban vagy több eszközről megnyitod ugyanazt a feladatlapot, nem tudjuk vállalni az adatmentéssel kapcsolatban esetlegesen felmerülő anomáliákért a felelősséget!

A ChatGPT használata nem tiltott, de az arra való hivatkozással észrevételt NEM fogadunk el!

A feltűnően rövid idő alatt megoldott feladatlapok kizárást vonnak maguk után, bármilyen más gyanús esetben fenntartjuk a jogot a forduló érvénytelenítésére!

Jó versenyzést kívánunk!

Köszöntünk a Cyber security kategóriában!

Bízunk benne, hogy hétről-hétre izgalmas feladatokkal tudjuk az érdeklődésedet fenntartani!

A kriptográfiai kulcsok kezelésekor külön figyelmet kell fordítanunk (különösen szimmetrikus kulcsok esetén) a megfelelően biztonságos tárolásra. Ennek oka, sok esetben a szimmetrikus kulcsok kiszivárgása flotta szintű sebezhetőséget is okozhat.

(Aki az elmúlt években is játszott velünk, találkozott ehhez hasonló feladattal már, de most kicsit újratekertük :))

`Indítás utáni csatolmányok`

1. feladat 20 pont

Egy AES-128-as kulcsot egy változóként rögzítettünk a rendszer EEPROM-jában. Azt itt tárolt adatok hexadecimális formában tárolódnak. A feladatunk a hanyagul elhelyezett kulcs megtalálása. Ezt követően AES ECB módszerrel vissza kell fejteni a következő titkosított szöveget (padding mechanizmusként a PKCS7-es standard lett használva):

0x19DB452EE321ABBF240D9130B7430687

A megoldás a padding nélküli szövegrész!

Az eredmény bekérést szövegesen szeretném bekérni.

Válasz

Megoldások beküldése