CYBER SECURITY

3. forduló

Continental
The Future in Motion

A kategória támogatója: Continental

RENDELKEZÉSRE ÁLLÓ IDŐ:

20:00

Ismertető a feladathoz

Fontos információk

> Ezután a forduló után automatikusan jár a kitartóknak szóló garantált ajándékunk, érdemes kitöltened a feladatlapot! :)
>
> Ha kifutsz az adott feladatlap kitöltésére rendelkezésre álló időből, a felület **automatikusan megpróbálja beküldeni** az addig megadott válaszokat.
>
> A kérdésekre **mindig van helyes válasz,** olyan kérdés viszont nincs, amelyre az összes válasz helyes!

Egyéb információkat a versenyszabályzatban találsz!

Harmadik forduló

A feleletválasztós elméleti rész záró kérdéseihez érkeztünk, ezek megválaszolásával tudsz majd tovább haladni a gyakorlatiasabb feladatokhoz. Ezen kérdésekben felbukkanó technológiák és technikák ismerete is nagyban szükséges a megfelelő védekezési mechanizmusok megtervezéséhez és kiépítéséhez.

Felhasznált idő: 02:04/20:00 **Elért pontszám:** 0/10

1. feladat 0/1 pont

Milyen hátrányai vannak egy penetrációs tesztnek?

(jelöld az összes helyes választ!)

Válaszok

- [x] Nem tudjuk vele megtalálni a rendszerünk összes lehetséges sebezhetőségét .
- [ ] Felfedezhetünk nem ismert sérülékenységet a rendszerben.
- [x] Adatvesztéssel vagy sérüléssel járhat.
- [x] Szolgáltatás kiesések sok pénzbe kerülhetnek.

Magyarázat

2. feladat 0/1 pont

Hogyan lehet reset-elni a jelszóval védett BIOS-konfigurációt?

(jelöld az összes helyes választ!)

Válaszok

- [ ] Tápegység kikapcsolásával
- [x] CMOS elem eltávolításával
- [x] Cél szoftver felhasználásával
- [x] Alaplapi jumper segítségével

Magyarázat

3. feladat 0/1 pont

Mi az a MITM támadás?

Válasz

- ○ Message in the middle. Olyan támadás, amikor a támadó megváltoztatja a két fél közötti üzeneteket.
- ○ Man in the middle. Olyan támadás, amikor a támadó belehallgat két fél közötti kommunkációba.

Magyarázat

4. feladat 0/1 pont

Mi az az ARP és hogyan működik?

Válasz

- ○ Ez egy protokoll, amelyet az IPv4-címmel társított MAC-cím keresésére használnak.
- ○ Address Recovery Program, amellyel IPV4 címeket lehet visszakeresni MAC-cím alapján.

Magyarázat

5. feladat 0/1 pont

Minek a rövidítése a CSRF?

Válasz

- ○ Cross-Site Request hamisítást jelent.
- ○ Cross-Site Request ellenőrzést jelent.

Magyarázat

6. feladat 0/1 pont

Mi az a botnet?

Válasz

- ◯ Malware -el fertőzött és irányított eszközök összessége az interneten.
- ◯ Hackerek egy adott hálózaton feltört eszközeinek összessége.

Magyarázat

7. feladat 0/1 pont

Mi az a 2FA?

Válasz

- ◯ Kétfunkciós applikáció hitelesítés
- ◯ Kétfaktoros hitelesítés
- ◯ Kettős cím továbbításos hitelesítés

Magyarázat

8. feladat 0/1 pont

Mi a különbség a szimmetrikus és az aszimetrikus titkosítás között?

Válasz

- ◯ A szimmetrikus titkosításnál ugyanazt a kulcsot használjuk a fordításhoz, míg az aszimmetrikusnál külön kulcsok vannak a titkosításra és a visszafejtésre.
- ◯ Az aszimmetrikus titkosításnál ugyanazt a kulcsot használjuk a fordításhoz, míg a szimmetrikusnál külön kulcsok vannak a titkosításra és a visszafejtésre.

Magyarázat

9. feladat 0/1 pont

Melyik WAF tartozik a Cyber Security fogalmai közé?

Válasz

- ◯ Web Application Firewall
- ◯ Web Application Framework
- ◯ Web Access Firewall

Magyarázat

10. feladat 0/0 pont

Miért van szükség DNS monitorozásra webszervereken?

(jelöld az összes helyes választ!)

Válaszok

- ☑ Domainek státuszának nyomonkövetése.
- ☐ Elősegíti a DNS feloldást.
- ☑ Az új domaineket könnyebben támadják meg malware vagy egyéb szoftverekkel.
- ☑ Domainek lejárata előtt e-mail értesítéseket kaphatunk.

Magyarázat

11. feladat 0/0 pont

Mit tudunk tenni a biztonsági kockázatokkal, ha felfedtük őket a rendszerünkben?

(jelöld az összes helyes választ!)

Válaszok

- [x] Lecsökkenteni
- [x] Elkerülni
- [ ] Megszüntetni
- [x] Elfogadni

Magyarázat

12. feladat 0/1 pont

Milyen biztonsági támadásokat indítanak publikus wi-fi hálózatok ellen?

(jelöld az összes helyes választ!)

Válaszok

- [x] Karma
- [x] Brute force
- [ ] Daemon Tools támadás
- [x] Sniffing

Magyarázat