







IT BIZTONSÁG





A kategória támogatója: EURO ONE Számítástechnikai Zrt.

Ismertető a feladathoz

A 4. forduló után elérhetőek lesznek a helyezések %-os formában: azaz kiderül, hogy a kategóriában a versenyzők TOP 20% - 40% -60% -ához tartozol-e!

Szeretnénk rá felhívni figyelmedet, hogy a játék nem Forma-1-es verseny! Ha a gyorsaságod miatt kilököd a rendesen haladó versenyzőket, kizárást vonhat maga után!

Kártékony kód visszafejtés

Ajánlott programok: Windows, <u>VSCode</u> vagy hasonló kódszerkesztő

Felhasznált idő: 00:00/40:00

Elért pontszám: 0/23

Indítás utáni csatolmányok

1. feladat 0/0 pont

A céges levélszűrőn fennakadt egy érdekes levél, ami egy gyanús csatolmányt tartalmaz. A feladat kielemezni ezt a csatolmányt, és megállapítani, hogy mit csinál.

Miért van ISO fájlba becsomagolva?

Válasz

	B 4	-1		C-!+ (-+	
	iviegn	eneziti	a vis:	szafejtést	

Jobban tömörül így a csatolmány



 Elkerüli ezzel az "internetről letöltött" jelzést Ez a válasz helyes, de nem jelölted meg.

Nincs rá különösebb indok

Magyarázat

Kedves Versenyzők!

A feladatot 0 pontosra állítottuk:

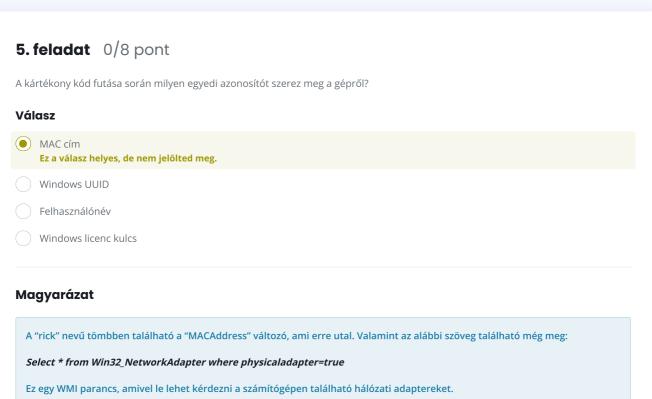
Habár a feladat írásakor ez még így volt, legfrissebb Windows rendszeren a helyesnek jelölt állítás már nem igaz. Köszünjük megértéseket! (2022.11.11.) Elkerüli ezzel az "internetről letöltött" jelzést: Windows esetében az internetről letöltött fájlok kapnak egy speciális attribú tumot, így az operációs rendszer képes korlátozni a működését (például Office fájlok esetén védett nézetet alkalmaz, vagy exe futtatása előtt figyelmezteti a felhasználót). Azáltal, hogy a vírus egy ISO-ba van csomagolva, a benne lévő fájlok nem kapják meg ugyanezt a jelölést, ezzel megkerülve egy védelmi mech anizmust. 2. feladat 0/3 pont Hogyan indul el a kártékony kód? Válasz Az ISO csatolásakor automatikusan lefut a vírus A "Csatolmányok" mappa megnyitásakor indul el a vírus Ez a válasz helyes, de nem jelölted meg. Nem tartalmaz vírust ez a fájl Magyarázat A "mappa" valójában egy parancsikon, ami elindítja a vírus fájl. 3. feladat 0/4 pont Melyek a kártékony kód futásának lépései? Válasz cmd.exe -> powershell -> Javascript Ez a válasz helyes, de nem jelölted meg. cmd.exe -> powershell powershell -> cmd.exe -> VBScript powershell -> cmd.exe Magyarázat A parancsikon elindítja a cmd.exe-t, ami ezután meghívja a powershell-t egy speciális paranccsal, hogy rejtett maradjon az ablak. A powershell ezután cscript segítségével futtat egy Javascript fájlt (pontosabban JScript fut le, ami ugyanúgy Javascript).

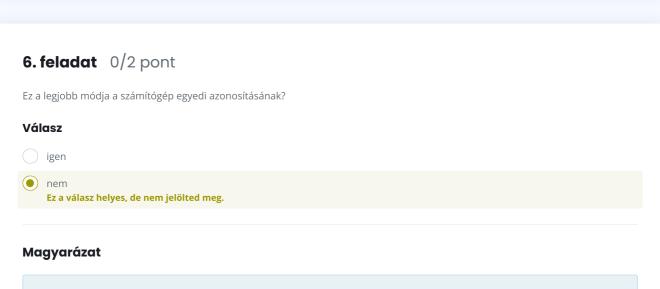
4. feladat 0/6 pont

Mivel kommunikál a kártékony kód?

Válasz

Google szerverekkel				
Localhost-tal Ez a válasz helyes, de nem jelölted meg.				
Észak-Koreával				
A vírus nem próbál meg sehova se kapcsolódni				
Magyarázat				
Localhost (127.0.0.1), erre próbál meg elküldeni egy kérést.				
Ez a cím a "rick" nevű tömbben található, hexadecimálisan kódolva.				
5. feladat 0/8 pont				





Nem. Egy számítógépnek több MAC címe is lehet, és a MAC cím nem biztos, hogy valódi hálózati kártyához tartozik, valamint szoftveres és hardveres változtatások miatt könnyedén megváltozhat ez az érték.

Legfontosabb tudnivalók 🖸 Kapcsolat 🖸 Versenyszabályzat 🖂 Adatvédelem 🗗

© 2023 Human Priority Kft.

KÉSZÍTETTE **C**��**ne**

Megjelenés

