IT BIZTONSÁG

5. forduló

A kategória támogatója: EURO ONE Számítástechnikai Zrt.

Ismertető a feladathoz

Hálózati forgalom elemzés

Ajánlott programok: Wireshark

Felhasznált idő: 00:00/40:00 **Elért pontszám:** 0/20

Indítás utáni csatolmányok

1. feladat 0/2 pont

Az egyik webszerveren gyanús adatforgalmat érzékeltek. A víruskereső nem mutatott ki semmit, viszont az IDS rendszer gyanús tevékenységet érzékelt, és készített a hálózati forgalomról egy capture fájlt. A csatolt fájl egy támadás hálózati forgalmát tartalmazza.

Meddig tartott a támadás? (másodpercben)

Válasz

- ○ 30
- ○ 60
- ● 90
  Ez a válasz helyes, de nem jelölted meg.
- ○ 120

Magyarázat

Az utolsó csomag idejéből látszik.

2. feladat 0/3 pont

Mi a támadó IP címe?

Válasz

- 192.168.0.10
- 192.168.0.11
- 10.13.37.1
- 10.13.37.69
  Ez a válasz helyes, de nem jelölted meg.

Magyarázat

A csomagokból látszik, hogy ez az IP cím csatlakozik a 80-as portra.

3. feladat 0/5 pont

Hogyan hatolt be a támadó?

Válasz

- SQL injekcióval
- Futtatható fájl feltöltésével
  Ez a válasz helyes, de nem jelölted meg.
- Lokális fájl inklúzióval
- Brute force támadással

Magyarázat

A támadó az ***/upload.php***-n keresztül töltött fel egy PHP fájlt, az ***/images/*** alá

4. feladat 0/7 pont

Mit lopott el a támadó?

Válasz

- Jelszó adatbázist
- Bankkártya adatokat
- SSL tanúsítványt
- SSH privát kulcsot
  Ez a válasz helyes, de nem jelölted meg.

Magyarázat

Az üzenetek a támadó és a szerver között base64-ben kódoltak, és gzip-el tömörítettek. Dekódolás után látszik, hogy a támadó futtatta az alábbi parancsot:

cat /home/developer/.ssh/id_rsa

5. feladat 0/3 pont

Az ellopott adatok függvényében mi lenne a legmegfelelőbb intézkedés?

Válasz

- ○ Jelszavak megváltoztatása
- ○ Bank értesítése
- ○ Tanúsítvány újra generálása
- ● SSH kulcs eltávolítása az azon használt szervereken
  Ez a válasz helyes, de nem jelölted meg.
- ○ Nincs teendő

Magyarázat

-