IT Biztonság (VIHIAC01)
Házi feladat

AAA és hozzáférés-szabályzás

Szerző:
Ládi Gergő

2022. március 5.

Tartalomjegyzék

1. Általános információk

Ez a házi feladat számos rövid feladatból, kérdésből áll, melyek mind a harmadik előadás témaköreihez (hitelesítés, engedélyezés, hozzáférés-szabályzás) kapcsolódnak. Az egyes feladatok megoldásához esetlegesen szükséges többletinformációk a feladatok leírásában találhatók.

A feladatok megoldásának beadása a Moodle rendszeren keresztül, egy kvíz kitöltésével valósul meg. A kvízben olyan kérdéseket teszünk fel, melyeket a feladatok megoldása ismeretében könnyen meg lehet válaszolni. A kvízt fogjuk pontozni, annak pontszáma adja majd az ezen házi feladatra kapott pontokat. Maximum 10 pont szerezhető így. A megszerzett pontszámot azonban 20%-kal csökkentjük, ha a kvíz kitöltése a határidő után történik meg.

2. Feladatok

2.1. Felhasználók és csoportok kezelése

Adott négy fájl[1], melyek egy Debian Linux operációs rendszerről származnak: */etc/passwd*, */etc/shadow*, */etc/group* és */etc/gshadow*. A fájlok tartalmának tanulmányozása után, az előadáson hallottak alapján válaszold meg az alábbi kérdéseket!

2.1.1.

A beépített felhasználókat leszámítva milyen felhasználók léteznek a rendszerben?

2.1.2.

Milyen hash algoritmussal van tárolva *Amar*, *Kirrog* és *Imeyepo* jelszava?

2.1.3.

A fenti algoritmusok közül melyik számít a mai ismereteink szerint a legerősebbnek?

2.1.4.

Milyen salt tartozik *Imiat* felhasználóhoz? Mi az ő UID-je?

2.1.5.

A 999 feletti UID-jű felhasználók közül ki(k) nem léphet(nek) be jelszóval?

2.1.6.

Van-e két ugyanolyan jelszavú felhasználó a rendszerben?

Segítség: El lehet dönteni? Ha igen, hogyan; ha nem, miért nem?

[1] A feladatkiírást is tartalmazó .zip fájlban megtalálhatók.

2.1.7.

Tudjuk, hogy az egyik felhasználó jelszava: *Aquadel*
Ki ő? Hogyan találtad meg?

Segítség: Az első ötlet nem biztos, hogy megoldásra vezet, viszont a feladat két teljesen független logika mentén is megoldható. (Ezek közül az egyik kreatívabb gondolkodást igényel, avagy *think outside the box.*)

2.1.8.

Az egyik felhasználó jelszava könnyen kideríthető. Ki ő, és mi a jelszava? NEM az előző kérdésben szereplő felhasználóra gondoltam!

2.1.9.

A beépített csoportokat leszámítva milyen csoportok léteznek a rendszerben?

2.1.10.

Kik a *research* csoport tagjai?

2.1.11.

Mi *Amar* felhasználó elsődleges csoportjának neve és GID-je?

2.2. Engedélyezés, hozzáférés-szabályzás

Az előző feladatban ismertetett fájlokon kívül rendelkezésünkre áll az alábbi kimenet is egy *ls* parancstól:

```
kirrog@arcanum:/schematics$ ls -la
total 8
drwxrwxr-t  8 root       research  4096 Feb 17 23:35 .
drwxr-xr-x 26 root       root      4096 Feb 16 14:51 ..
-rwxrw----  6 imiat      research  1820 Mar  3 18:11 something
-rwxr-----  6 imiat      research  1341 Mar  3 18:18 somethingsomething
```

A fájlok tartalma és a kimenet ismeretében válaszold meg az alábbi kérdéseket!

2.2.1.

Milyen felhasználóval vagyok éppen bejelentkezve? Van-e jelen pillanatban rendszergazda jogköröm?

2.2.2.

Tudja-e olvasni *Nelle* a jelenlegi könyvtár tartalmát, azaz a fájlok listáját?

2.2.3.

Tud-e új fájlokat létrehozni a jelenlegi könyvtárban *Chanac*?
Na és *Kirrog*?

2.2.4.

Tudja-e törölni *Kirrog* a *somethingsomething* fájlt?

2.2.5.

Melyik a kisebb méretű fájl? Ha egy számsorral kellene jellemezned a jogosultsági bitjeit, mi volna ez a számsor?

2.2.6.

Ki a *something* fájl tulajdonosa? Milyen paranccsal tudnál olvasási jogot adni a fájlra mindenkinek, ha te lennél a tulajdonos?

2.3. Egyéb feladatok

2.3.1. Jelszótörés

Régi mentéseim között kutakodva találtam egy listát, melyen korábbi jelszavaim szerepelnek, hashelve. Sajnos semmi egyébre nem emlékszek a listát illetően, de azért szeretném tudni, mik lehettek a régi jelszavaim.

A lista:
`fa6b8562f4fc60547b75ab3dd6859b000445fa98`
`29d88ae363dfae757d8828e36d82af454cb1ed85`
`d68003e8eaa957d20854412635e69a70fda38f83`
`ffa64038a05bf0d3535577c55d32a71b8739a786`
`f6e81a2e41ae36dca6fc0aafc1126a787bd8cd60`
`a0b6c9310ee39350366d5640984262ad2caddc83`

Milyen hash algoritmussal készültek a fenti hashek? Próbáld meg minél többhöz meghatározni, hogy mi volt az a plaintext, amelynek ez lett a lenyomata (hashe)!

A hashek – hogy ne ebből a dokumentumból kelljen kimásolni őket – megtalálhatók a feladatkiíráshoz mellékelt *2.3.1_hashes.txt* állományban is.

Segítség #1: A hashek "feltöréséhez" tetszőleges jelszótörő program használható, például a (*hashcat* vagy a *John the Ripper*). Természetesen ezektől eltérhetsz, így ha már volna egy harmadik, jól bevált programod erre a célra, azt is használhatod.

Segítség #2: Nem biztos, hogy egyféle megközelítéssel minden hash esetében sikerrel fogsz járni, de egyáltalán az sem, hogy összességében minden hasht sikerül majd feltörnöd. Ha egy adott módszerrel órák alatt sem sikerül előrébb jutni, érdemes lehet stratégiát váltani.

2.3.2. Have I been pwned?

Az előadáson láthattuk, hogy rendszeresen törnek fel weboldalakat, ahonnan aztán sok esetben a támadók kezébe kerül a felhasználói adatbázis, a felhasználók mindenféle személyes adatával együtt. Létezik egy oldal, a https://haveibeenpwned.com/, amelyet Troy Hunt, egy biztonsági

szakember üzemeltet. Igyekszik összegyűjteni minden nyilvánosságra kerülő és a Dark Weben felbukkanó adatbázist, hogy ezek segítségével meg lehessen nézni, ha valakinek ilyen módon kiszivárogtak az adatai.

Az oldal segítségével ellenőrizd, voltam-e áldozata valamilyen adatlopásnak! Ha voltam, melyik oldalt törték fel a támadók? Mikor? Melyik címemmel voltam regisztrálva? Pontosan milyen adatokhoz férhettek hozzá velem kapcsolatban? Az e-mail címeim:

- Gergo.Ladi@CrySyS.hu
- gergo.ladi@sch.bme.hu
- me@gergoladi.me
- Gergo.Ladi@kszk.bme.hu

2.3.3. Szorgalmi feladat: Have YOU been pwned?

Az előző feladathoz hasonlóan ellenőrizd, hogy te magad voltál-e már hasonló adatlopás áldozata! Ha igen, mit törtek fel a támadók? Ezzel pontosan mit tudtak meg rólad?

Megjegyzés: Ez a feladat szorgalmi, így ha nem szeretnéd egy számodra ismeretlen oldalon megadni az e-mail-címedet, nem kötelező.