IT Biztonság (VIHIAC01)
Házi feladat

AAA és hozzáférés-szabályzás

Szerző:
Ládi Gergő

2021. március 1.

Tartalomjegyzék

1. Általános információk

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

Megoldásként egy igényesen formázott, .pdf formátumú dokumentáció beadását várjuk, amely minden egyes megválaszolt kérdéshez (feladatponthoz) tartalmazza:

- a feladat sorszámát,
- valamiféle levezetést, amelyből kiderül, hogyan jutottál el a megoldáshoz,
- a feladat megoldását,
- opcionálisan kép(ek)et, amennyiben úgy ítéled meg, hogy ez segíti a válaszod megértését, emeli a megoldásod színvonalát.

A házi feladat beadási határideje után egy Moodle kvízt is ki kell majd töltened, amelyben olyan kérdések lesznek, melyeket a feladatok megoldása ismeretében könnyen meg lehet válaszolni. A kvízt fogjuk pontozni, abból fog származni az ezen házi feladatra kapott pont. Maximum 10 pont szerezhető így. A házi feladat teljesítettnek tekintett, ha a kérdésekre átlagosan legalább 40%-ban jó választ adsz. A megszerzett pontszámot azonban 20%-kal csökkentjük, ha a megoldások beadása a határidő után történik.

Az esetleges csalások kiszűrése érdekében a beadott megoldások egy véletlen választott részhalmazát összevetjük a hozzájuk tartozó kvíz eredményével, és ha ellentmondásokat, inkonzisztenciákat tapasztalunk, vagy ha úgy ítéljük meg, hogy a kvízben adott helyes válaszok alátámasztása nem található meg a beadott megoldásban, akkor pontlevonást alkalmazunk.

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 *Evelynn*, *Sona* és *Annie* jelszava?

2.1.3.

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

2.1.4.

Milyen salt tartozik *Malphite* 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? El lehet-e 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: *EasyDiamond*
Ki ő? Hogyan találtad meg?

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 *support* csoport tagjai?

2.1.11.

Mi *Karthus* 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:

```
sona@jungle:/check$ ls -la
total 8
drwxrwxr-t  8 root       support  4096 Feb 17 23:35 .
drwxr-xr-x 26 root       root     4096 Feb 16 14:51 ..
-rwxrwx---  6 leona      support  2419 Feb 17 23:37 somefile
-rwxr-x---  6 leona      support  1830 Feb 17 23:37 someotherfile
```

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 *Annie* a jelenlegi könyvtár tartalmát, azaz a fájlok listáját?

2.2.3.

Tud-e új fájlokat létrehozni a jelenlegi könyvtárban *Karthus*?
Na és *Heimerdinger*?

2.2.4.

Tudja-e törölni *Malphite* a *somefile* 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 *somefile* 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:
`6b629347bcc874573be28d533d702363ebf62e35`
`5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8`
`dda88e7780438d154147db094dfa5ea8e1eb98c9`
`246cccbfe23bcfcdc047864def059c34c76c68ae`
`da39a3ee5e6b4b0d3255bfef95601890afd80709`
`ca2409aa4d95dc507a9b9708b3dd3f9b33965df0`

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, de segítségképp két ilyet is (*hashcat* és *John the Ripper*) előre feltelepítettünk a tárgyhoz tartozó BME cloudos virtuális gépre, így a feladat megoldható anélkül is, hogy bármit is telepítened kellene a saját gépedre. 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.