AAA and Access Control

IT Biztonság

2. Házi Feladat

**Feladatok**

**2.1. Felhasználók és csoportok kezelése**

**2.1.1**. **A beépített felhasználókat leszámítva milyen felhasználók léteznek a rendszerben?**

* A nem rendszerszintű felhasználók 1000-től kapják. A passwd file utolsó 8 sorában találhatók a keresett felhasználók.
* evelynn, karthus, jax, malphite, annie, sona, heimerdinger, leona

**2.1.2. Milyen hash algoritmussal van tárolva Evelynn, Sona és Annie jelszava?**

* A hashelt jelszavak shadow fileban találhatóak *$algorithm$salt$hash* formátumban.
* Evelynn: 5 - SHA-256, Sona: 6 - SHA-512, Annie: 1 - MD5

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

* Az SHA-512 algoritmus.

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

* A hashelt jelszavak shadow fileban találhatóak *$algorithm$salt$hash* formátumban. A UID a passwd fileból olvasható ki.
* Salt: YgVQv3fSdlYwR, UID: 1003

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

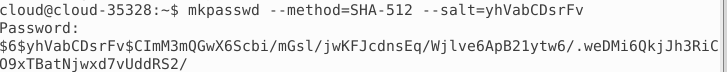
* Azok akiknél a shadow fileban ! vagy \* található a jelszó helyén.
* systemd-coredump és karthus nem léphet be jelszóval.

**2.1.6. Van-e két ugyanolyan jelszavú felhasználó a rendszerben? El lehet-e dönteni?**

**Ha igen, hogyan; ha nem, miért nem?**

* Ha megnézzük a hashelt jelszavakat, akkor azok a hash algoritmus és a salt függvényében változnak.
* Mivel különböző algoritmusok vannak használva, különböző salt értékekkel nem lehet eldönteni van-e két azonos jelszó.

**2.1.7. Tudjuk, hogy az egyik felhasználó jelszava: EasyDiamond Ki ő? Hogyan találtad meg?**

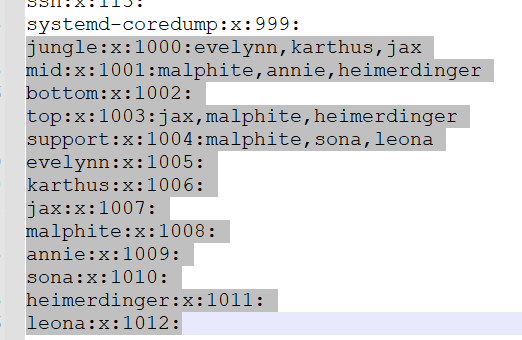
* Megnézem, hogy az adott salttal és algoritmussal milyen hashelt jelszót kapunk az EasyDiamond-ból. Ha ez egyezik, a shadow fileban tárolt hashalt jelszóval, akkor megvan a keresett felhsználó.
* leona jelszava az EasyDiamond
* 

**2.1.8. Az egyik felhasználó jelszava könnyen kideríthető. Ki ő, és mi a jelszava?**

**NEM az előző kérdésben szereplő felhasználóra gondoltam!**

* A shadow file hash-jei között a *X014elvznJq7E* hash eltér a többitől, ezért utána néztem és kiderült, hogy ez a default jelszó. Aminél az X0 a salt és unix crypttel van hashelve.
* A heimerdinger felhasználó jelszava toor.

**2.1.9. A beépített csoportokat leszámítva milyen csoportok léteznek a rendszerben?**

* A group filet megnézve derül ki. Annak is az 1000 és afölötti id-val rendelkezők.
* jungle, mid, bottom, top, support és az összes felhasználóhoz tartozik egy vele megegyező nevű csoport: evelynn, karthus, jax, malphite, annie, sona, heimerdinger, leona
* 

**2.1.10. Kik a support csoport tagjai?**

* Megtalálhatóak a group file support sorának végén felsorolva.
* malphite,sona,leona
* 

**2.1.11. Mi Karthus felhasználó elsődleges csoportjának neve és GID-je?**

* A passwd fileban megtalálható az elsődleges csoport ID-je amit aztán megkeresve a group fileban megkapjuk a nevét is.
* GID: 1000, név: jungle

**2.2. Engedélyezés, hozzáférés-szabályzás**

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

* Sona felhasználó van bejelentkezve. Nincs rendszergazda jogköre.

**2.2.2. Tudja-e olvasni Annie a jelenlegi könyvtár tartalmát, azaz a fájlok listáját?**

* Annie a mid group tagja.
* Tudja olvasni a könyvtár tartalmát.

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

* Karthus a jungle group tagja, míg Heimerdinger a mid és top groupoké.
* Egyikük sem tud létrehozni a könyvtárban.

**2.2.4. Tudja-e törölni Malphite a somefile fájlt?**

* Malphite a mid, top és support groupok tagja. Viszont a könyvtár filejait csak a tulajdonos törölheti.
* Nem tudja a somefile filet törölni.

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

* A somefile mérete 2419 a someotherfile mérete pedig 1830.
* A someotherfile mérete kisebb, jogosultsági bitjei számsorral: 750

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

* Leona a tulajdonos, *chmod ugo+r somefile* paranccsal

**2.3. Egyéb feladatok**

**2.3.1. Jelszótörés**

* SHA1 hash algoritmust használtak a megadott hashakhez. Ezeket megpróbáltam simán bruteforceal és szótáralapon is visszafejteni többszörös hashalést is alkalmazva.
* 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8 - “password”
* da39a3ee5e6b4b0d3255bfef95601890afd80709 - “”(üres)
* 246cccbfe23bcfcdc047864def059c34c76c68ae - “Quicksilver”
* ca2409aa4d95dc507a9b9708b3dd3f9b33965df0 - “awafee”
* 6b629347bcc874573be28d533d702363ebf62e35 - “Significant21”
* dda88e7780438d154147db094dfa5ea8e1eb98c9 - nem találtam megfejtést

**2.3.2. Have I been pwned?**

* A *me@gergoladi.me* email cím esetén volt találat.
* Armor Games oldal lett feltörve, 2019 januárjában. Hozzáfért adatok: Bios, Dates of birth, Email addresses, Genders, Geographic locations, IP addresses, Passwords, Usernames
* 