Főzzünk Linuxszal: Elfelejtett biztonság

Jobb ha nem használjuk ugyanazt a jelszót több azonosítóhoz. Tekintve, hogy mennyi jelszóigényes kiszolgáló és weblap létezik, mit tehet ilyenkor egy biztonság-tudatos főszakács? Nézzük meg, hogyan tehetjük kényelmessé és biztonságossá a jelszó pásztorkodást.

Hol van az a borrendelés ***Henri Különleges Boraitól***, ***François***? Úgy tűnik kezdünk kifogyni a kedvenceimből. ***Henri*** általában otthon van ezen a téren. Nem adott neked visszaigazolást? Ah, kitűnő. Akkor megvan a rendelés? Nem? Hogy érted, hogy valahol biztonságban van? Most akkor meg van, vagy nincs? Értem. Úgy gondoltad, hogy fontos, ezért titkosítottad a rendelést és eldobtad az eredeti üzenetet. Had találjam ki, ***mon ami***, nem emlékszel a jelszóra amivel titkosítottad az üzenetet. Ahogy gondoltam. Rendben, mutasd milyen programot használtál.

Steganográfia, François? Saját arcképedbe rejtetted a borrendelést? Le vagyok nyűgözve! Ezzel a problémával egy kicsit később foglalkozunk, ***François***. Nincs túl sok időnk, vendégeink bármelyik pillanatban itt lehetnek. Ah, de hát már itt is vannak.

Üdvözlet, ***mes amis Chez Marcelnél***, a világ legfinomabb francia ***Linux*** éttermében és a világ legnagyszerűbb borospincéjében. Amely sajnos jelenleg lehet, hogy csak a második legjobb a világon. Úgy tűnik hűséges pincérem elkavarta a rendelést és nem akarta elmondani nekem. Igen, ***François***, tudom, hogy tudod hol van. Menj a pincébe és hozd fel a portugáliai 2000-es ***Douro***-t. Kiváló vörös, ***mes amis***, testes és erős bor, gyönyörű sötét gyümölcsillattal és egy csepp misztikummal. ***Vite***, ***François***!

Míg ***François*** felhozza a bort, elmondom hogyan próbálta meg biztos helyre tenni a borrendelést. Mint kiderült, ***Stefan Hetzl Steghide*** nevű programját használta, hogy a listát saját fényképébe rejtse (*1. ábra*).

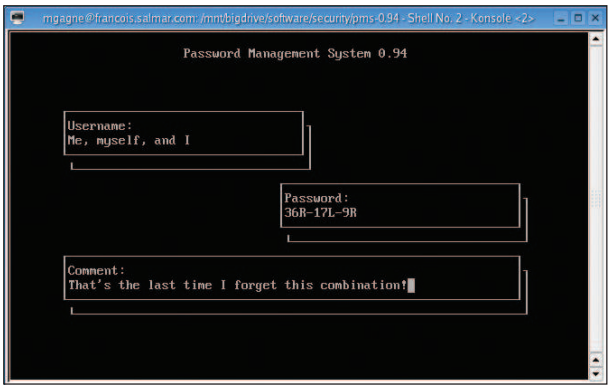
Ezt a módszert szteganográfiának nevezik. A módszerrel tetszőleges üzenetet rejthetünk egy másik üzenetbe (vagy mint ebben az esetben egy grafikus képbe). Tulajdonképpen, egy titkos üzenetekkel megtűzdelt képekkel teli weblapot is létrehozhatunk, és senki nem fog sejteni semmit. A ***Steghide***-ot a ***Steghide*** honlapjáról gyűjthetjük be (lásd a hálózati forrásokat). A kiadott futtatható állományokat könnyen meg fogjuk találni. Ha a ***Steghide***-ot forrásból szeretnénk fordítani, szükségünk lesz a ***libmhash***, ***libjpeg***, ***zlib*** és ***libmcrypt*** fejlesztői könyvtárakra. Ezek után már könnyű dolgunk van, a szokásos öt lépéses kitömörítés és fordítás menettel találkozunk:

1. ábra Ebbe a képbe rejtve valahol egy jókora borrendelést találunk

```
tar -xzvf steghide-0.5.1.tar.gz
cd steghide-0.5.1
./configure
make
su -c “make install”
```

A borrendelés elrejtése esetében ***François*** a következő parancsot használta a dokumentum képbe ágyazásához:

```
steghide embed -cf francois.jpg -ef wine_order.txt
```



2. ábra PMS nem csak jelszavakhoz használható. Akár a szekrénykódunkat is tárolhatjuk benne.

Ha már borról beszélünk, ***François*** visszatért. Légy oly kedves, ***mon ami***, és tölts a vendégeinknek. Nos, a parancs futtatása után egy jelszót kell megadnunk:

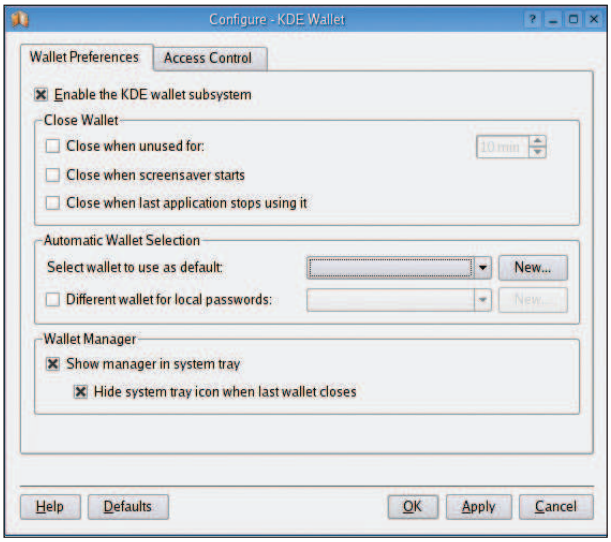
```
Enter passphrase:
Re-Enter passphrase:
embedding “wine_order.txt” in “francois.jpg”...
➥done
```

Eredményképpen a titkos üzenet elrejtését megelőző változattal azonos kinézetű képet kapunk, de a mérete megváltozik. Ha az adatokat ki akarjuk nyerni a képből, nekünk (vagy akinek a képet elküldtük) csak az `extract` paramétert kell megadnunk a következő paranccsal:

```
steghide extract -sf francois.jpg
Enter passphrase:
```

Amennyiben sikeresen megadtuk a helyes adatokat, a rejtett állomány a lemezre kerül. Nos, éppen ez az a pont ahol a dolgok elkezdenek rosszra fordulni. Miután elfelejtettük a jelszót, nincs többé módszer az információ kinyerésére.
A valós életben néhányan közülünk alkalmanként elveszítjük a kulcsunkat. Mások rendszeresen elvesztik, aminek következményeként egy vállalati feltaláló kijött a kulcscsomóra szerelhető csipogóval. Feltételezve, hogy a keresőt már nem veszítjük el, csak megnyomjuk a gombot és a kulcs magas hangon csipogva jelzi melyik díszpárna mögé csúszott be éppen.
A jelszavak esetében hasonló az alapötlet. A legegyszerűbb módszer leírni a jelszavakat valahová vagy egy szöveges állományba menteni őket. Ez azonban nem különösebben biztonságos. Ugyanakkor a jelszó és jelszöveg lista készítése egyre nagyobb értelmet nyer, ahogy jelszavak tucatjait, néha százait kell megjegyeznünk. Mennyivel egyszerűbb lenne, ha csak egyetlen jelszót kéne megjegyeznünk!
Itt kerülnek a képbe a jelszókezelők.
Az első ilyen amibe belefutottam ***Dennis Pries Password Management System (azaz PMS)*** rendszere volt. Ez azért tetszett, mert tisztán szöveges terminálablakban is futtatni lehetett, következésképpen bárhol legyünk is, egy héjbejelentkezésből használni tudjuk. A programot a ***SourceForge*** honlapján találhatjuk meg (lásd a forrásokat), ahol a forrást és a ***Debian*** csomagot egyaránt letölthetjük.

A ***PMS*** fordításához dupla kitömörítés és az öt lépéses fordítás szükséges. Először is csomagoljuk ki a tarolt és gzippelt állományt (`tar -xzvf pms-0.94.tar.gz`). Belekukkantva a forráskönyvtárba egy contrib alkönyvtárat láthatunk, ahol a forrásfájlból a kicsomagolás és fordítás szokásos öt lépésével elkészíthetjük a ***cdk***-t. A ***cdk*** telepítése után lépjünk vissza a ***PMS*** forráskönyvtárába, fordítsuk le és telepítsük.
A jelszókezelőt a `pms` paranccsal indíthatjuk. Első indításkor meg kell adnunk a mesterjelszót. Ez az egyetlen jelszó vagy jelszöveg, amit mostantól meg kell jegyeznünk, ezt viszont alaposan. Ha elfelejtjük a mesterkulcsot soha nem látjuk viszont a többi jelszavunkat. A ***PMS*** egyszerű menüjével gépneveket vehetünk fel, törölhetünk és nevezhetünk át. Ezek lesznek azok a helyek, ahová be kell jelentkeznünk. Először is vegyünk fel egy gépnevet (például, ***www.somewhere.dom***) majd fűzzünk megjegyzést hozzá (például: központi rendszer). Ezután ismét a főmenüben találjuk magunkat. Itt válasszuk a ***User Functions (Felhasználói Műveletek)*** pontot. Ebben a menüpontban vehetjük fel vagy törölhetjük az előző lépésben megadott géphez tartozó felhasználói azonosítókat. Egyúttal itt jeleníthetjük meg a felhasználóhoz tartozó elveszettnek hitt jelszavainkat is.
Mielőtt továbblépnénk, szeretnék rámutatni, hogy a gépnév és a felhasználói név akármi lehet. Gépnévként beírhatom azt is, hogy „iskolai zár”, felhasználónévnek, hogy „kombináció” jelszónak pedig magát a kombinációt. Bár eredetileg bejelentkezési információk őrzésére tervezték, a program más célra is jól használható (*2. ábra*).
A másik dolog amit mindig el szoktunk felejteni, a rengeteg meglátogatott weblaphoz rendelt jelszavak. Az on-line banki rendszerektől kezdve a hírújságokig ahol ingyenes azonosítóra van szükségünk a cikkek olvasásához, idővel irgalmatlan sok jelszó gyűlik össze. Aztán ott vannak az üzenetküldőkhöz és az e-mail bejegyzésekhez tartozó jelszavaink, az ***FTP*** helyek és még hosszan sorolhatnánk. Jelentősen leegyszerűsítené a dolgunkat, ha mindezt az információt valahogy átlátszóan tudnánk kezelni munka közben.
Van esetleg valamilyen eszköz ami beépül az asztalba?
A válasz természetesen igen. A ***KDE 3.2***, és a legújabb 3.3 verziójában a felhasználók beépített a jelszókezelővel rendelkeznek. ***George Staikos KDE Wallet Manager*** rendszeréről van szó, amely a `kwalletmanager` programot futtatja.
A program első indításakor nem készül tárca (wallet). Ugyanakkor a rendszertálcán egy apró tárca ikont találunk. Amennyiben a tárcakezelő ikonja még nincs nyitva, kattintsunk az ikonra, mire megnyílik egy (leginkább üres könyvtárra emlékeztető) üres doboz. Kattintsunk a ***Beállítások (Settings)*** gombra a menüben és válasszuk a ***Tárcabeállítások (Configure Wallet)*** pontot.
Új űrlapablak jelenik meg, ahol a legtöbb elem nem elérhető. Kattintsunk a ***KDE tárca alrendszer engedélyezése (Enable the KDE Wallet Subsystem)*** pontra. Most már néhány további lehetőséget is elérhetünk (*3. ábra*).
Figyeljük meg az ***Automatikus Tárcaválasztás (Automatic Wallet Selection)*** nevű középső részt. Meg kell adnunk melyik tárcát szeretnénk alapértelmezettként használni. Rögtön ez alatt kiválaszthatjuk a helyi jelszavakhoz használt tárcát (erről hamarosan még bővebben szó lesz).
Ha először futtatjuk a ***KDE Tárcát***, nem valószínű, hogy



3. ábra A KDE Tárcakezelő beállítása jelszótároláshoz

van létező tárcánk; Kattintsunk az ***Új (New)*** gombra és adjunk nevet a tárcánknak. Nyugodtan adhatjuk a saját nevünket ahogy én is tettem. Miután begépeltük a nevet és ráböktünk az ***OK***-ra, a megjelenő ***KDE tárcakezelő varázsló (KDE Wallet Manager Wizard)*** alap vagy kifinomult beállítási lehetőségei közül választhatunk, ahol az alap a javasolt mód. A kifinomult változatban kicsit több információs képernyőt találunk és a helyi jelszavainkhoz külön tárcát választhatunk. Én az alapot választottam és csak egy tárcát készítettem.

Bármelyiket is választottuk a varázsló egy idő után rákérdez a tárca megnyitásához szükséges mesterjelszóra.

Ez a szuperfelhasználó jelszó lesz az amit nem szeretnénk elfelejteni- az, amely az összes többi ajtaját nyitja. Jól válasszunk, és ne felejtsük el az ***„Igen, személyes adataimat is szeretném a KDE tárcában tartani" („Yes, I wish to use the KDE wallet to store my personal information")*** négyzetet megjelölni.

Ha a varázslóval végeztünk, majdnem készen is vagyunk. A felbukkanó üzenetablak tudatja velünk, hogy az alkalmazás (a varázsló) szeretné létrehozni az új tárcát. A kérelmet a tárcához tartozó jelszóval kell jóváhagynunk. Figyeljük meg ezt az űrlapot. Ehhez hasonlót fogunk látni minden ***KDE*** folyamatban amikor valamelyik alkalmazás jelszót keresve meg szeretné nyitni a tárcát. Amíg ki nem jelentkezünk, a tárca nyitva marad. Lépjünk be egy weblapra ahol jelszót és felhasználónevet kérnek tőlünk (például megnyithatjuk a banki elérésünket). Miután kitöltöttük az információkat és ráböktünk az ***Elküld*** vagy ***Enter*** gombra (űrlaptól függően), a ***KDE*** tárcakezelő ablaka jelenik meg figyelmeztetve, hogy egy alkalmazás (jelen esetben a ***Konqueror***) megpróbálta megnyitni az alapértelmezett tárcát (amit éppen most készítettünk). A *4. ábrán* láthatjuk mire gondoltam. Írjuk be a mesterjelszót és bökjünk a ***Folytatásra (Continue)***. Egy utolsó figyelmeztetést kapunk, miszerint a titkosított adatok elmentésre kerülnek, és ezt jóvá kell hagynunk. Kattintsunk az Igen gombra. Most vessünk egy pillantást a tálcára és látni fogjuk, hogy az ikon zárt tárcáról kissé nyitott tárcára változott.

4. ábra A tárca megnyitásához meg kell adnunk a mesterjelszót

E rendszer szépsége, hogy az adatok automatikusan beíródnak nekünk amikor legközelebb meglátogatjuk a lapot. Ez minden ***KDE*** alkalmazásra igaz, amely jelszót kér tőlünk, tehát például az üzenetküldőre is.

Egyetlen buktató van, mégpedig nem is kicsi. Mint említettem, csak egyetlen egyszer kell begépelnünk a mesterjelszót minden ***KDE*** folyamathoz, ami leegyszerűsíti a dolgokat. De vigyázat: most, hogy a rendszert képessé tettük a jelszavaink automatikus megadására, az asztalunk biztosítása igencsak fontossá válik. Ne feledjük el lezárni az asztalt mielőtt elmegyünk. Másik megoldás, hogy visszalépünk a ***KDE*** tárca beállítások űrlapjára és megismerkedünk a ***Tárcazárás (Close Wallet)*** lehetőségeivel. Beállíthatjuk, hogy egy megadott idő után automatikusan záruljon be, például, amikor a képernyő pihentető elindul (azaz amikor általában nem vagyunk ott) vagy amikor a tárcát használó utolsó alkalmazás is becsukódik. Ha így járunk el, egyel kevesebb dologra kell emlékeznünk.

A faliórára pillantva, ***mes amis***, úgy látszik ismét utolért bennünket a záróra. Mint láthattuk több lehetőségünk is van jelszavaink tárolására így nem kell tucatnyi titokzatos betű és számkombinációt megjegyeznünk. Talán, ha sikerül meggyőzni ***François***-t, hogy ilyen eszközöket használjon a jövőben, nem lesz több eltűnt rendelés. Addig is, abban biztos vagyok, hogy sikerül meggyőzni, hogy még egyszer töltse teli vendégeink poharát. És a bortartalékok miatt ne aggódjon senki. Személyesen gondoskodom róla, hogy a borospince színültig legyen mire legközelebb találkozunk. Addig is, ***mes amis***, egészségünkre. A ***votre santé! Bon appétit!***

Linux Journal 2005. január, 129. szám

A cikkhez tartozó források:
➲ ***www.linuxjournal.com/article/7860***

Marcel Gagné (mggagne@salmar.com) Mississaugaban él Ontario államban. Ő a szerzője a Moving to the Linux Business Desktop (ISBN 0-131-42192-1) című könyvnek amely a harmadik műve az Addison-Wesley gondozásában. A valós életben a rendszerintegrációval és hálózati tanácsadással foglalkozó Salmar Consulting, Inc. elnöke. Egyúttal pilóta, sci-fi és fantasy novellákat ír és silány origami T-Rex figurákat hajtogat.