Két módszer a fájlok védelmére

PClinuxOS Magazine – 2018. február

Írta: Paul Arnote (parnote)

A mai digitális világban a számítógépektől függünk sok-sok tekintetben. Egyik, amiben a számítógép különösen hasznos, az a létfontosságú, vagy fontos információkat tartalmazó fájlok őrzése.

Kevés elkeserítőbb dolog van annál, mint elveszíteni alapvetően létfontosságú fájlt. Lehet akár kép a nagymamáról halála előttről, lista a háztartási gépek sorozatszámáról, előadás, amin heteken keresztül dolgoztál, vagy titkosított jelszólista. Biztosan helyzetek sokaságát tudnád elképzelni, és olyanokat is, amik a te saját számítógépes életedre egyedien jellemzőek.

Tudd, hogy ezúttal nem a fájlok biztonságáról beszélünk. Vedd úgy, hogy bárki hozzáférhet a létfontosságú fájljaidhoz. Amiről most beszélünk, az annak az elősegítése, hogy a létfontosságú adatainkat ne lehessen könnyen törölni, akár véletlenül, akár szándékosan.

Szerencsére legalább két megoldás van a fájlok törlésének elkerülésére. Nézzük meg egyenként az eljárásokat.

1. módszer: már meglévő eszközök használata

Hiszed, vagy sem, az összes olyan eszköz, amire a fájljaid törlés elleni védelméhez szükség van, a PCLinuxOS telepítésének napjától rendelkezésre áll. Valószínűleg nem tudod, hol vannak, vagy hogyan használd. Az is lehet, hogy valamennyire már ismered ezeket az eszközöket, de elfelejtkeztél róluk. Bárhogy is legyen, ehhez a módszerhez kevés plusz kell, mert nem kell semmit sem telepíteni a gépre.

Pontosabban a chattr (change attribute) parancsról beszélek. ***Futtatásához admin jogosultság kell.*** Más tekintetben pedig elég egyértelmű. Noha a chattr paranccsal számos attribútum használható, mi elsősorban az i és az a opciókkal foglalkozunk. A többi jelölőről tájékozódhatsz, ha a parancssorban kiadod a **man chattr** parancsot. (Noha van „undeletable” (törölhetetlen) jelölő, az a PCLinuxOS-felhasználók többsége által használt ext3 és ext4 fájlrendszereken hatástalan.)

Add ki a következő parancsot (adminisztrátorként):

chattr +i afájlod.kiterj

Ez a fájl attribútumát „Immutable”-ra (érinthetetlen) cseréli. Amikor a fájl attribútuma immutable, SENKI, még az admin sem tudja törölni. A fájl nem módosítható. A fájl törléséhez (módosításához) a fájl attribútumát meg kell változtatni, eltávolítva az

immutable jelölőt. Az immutable jelölő eltávolítása így lehetséges:

chattr -i afájlod.kiterj

A parancsot ismét adminisztrátorként kell futtatni. Mihelyt az immutable-t eltávolítottad, a fájl – akár a számítógéped bármely más fájlja – törölhető (vagy módosítható) feltéve, hogy a megfelelő jogosultságokkal rendelkezel. Ha csak egyszerűen frissítenéd a fájlt és visszaállítanád az immutable jelölőt, ne felejtsd el újból futtatni a chattr parancsot a szerkesztést követően.

Látszólag sokat kell dolgozni a fájl védelme érdekében, de gondolj arra, milyen következményekkel jár egy pótolhatatlan fájl törlése. A parancs gyors és könnyen végrehajtható, és szó szerint hatalmas lelki nyugalmat kölcsönöz.

Ugyanakkor az i jelölő helyett az a is használható. Az a az „append only”-t (csak hozzáfűzés) takarja. Ezt használva szerkeszthető, módosítható és kiegészíthető marad a fájl, de nem törölhető. A parancs használatának formátuma majdnem azonos az i jelölőével, csak a-t kell behelyettesíteni, mint ahogy itt (admin-ként futtasd):

chattr +a afájlod.kiterj

Hasonló módon távolíthatod el a jelölőt, valahogy így:

chattr -a afájlod.kiterj

Ha eltávolítottad a jelölőt, a fájlt tudod törölni, mint a rendszer bármely másik fájlját. Noha az „append only” használata sokkal kényelmesebb, mégsem ad annyi védelmet, mint az immutable jelölő. Tehát, ha aggaszt a fájlod tartalmának megváltozása, akkor maradj meg az immutable jelölő használata mellett.

A való életben a két jelölő másokkal kombinálva használható. Például, ha egy könyvtárat akarsz levédeni, az összes tartalmazott fájljával egyetemben, egyszerűen add ki a parancsot így:

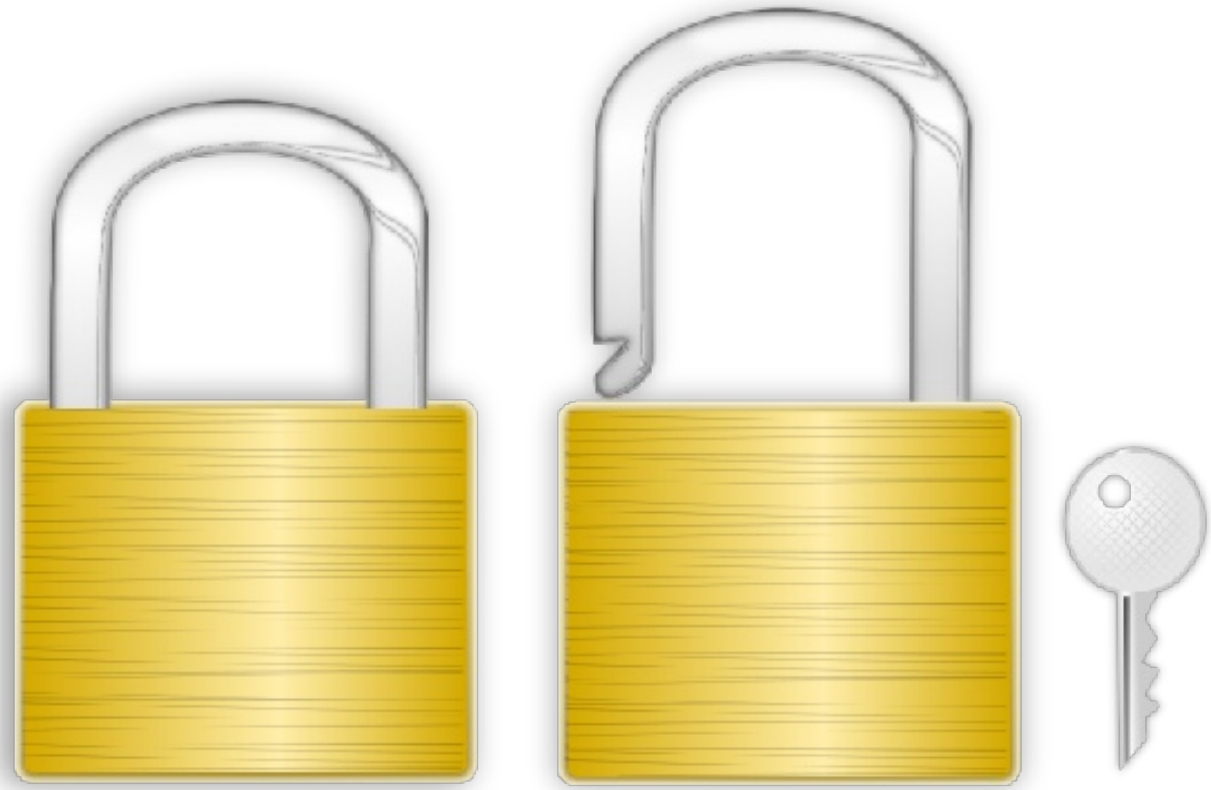
chattr -R +i /home/username/directory

Az -R opció azt jelenti, hogy a könyvtár tartalmára is vonatkozik. (rekurzív) Így a könyvtár és az összes tartalmazott fájl immutable lesz. Használhatod még az „append only” jelölővel is. Ilyetén módon sem a könyvtár, sem a fájljai nem lesznek törölhetőek egészen addig, amíg az „immutable”, vagy az „append only” jelölőt el nem távolítod (**-i**, vagy **-a**).

A chattr parancsban lehetőség van a szabványos helyettesítő jelek alkalmazására. Hasonló eredményhez vezethet, ha a könyvtárba belépsz és kiadod a parancsot valahogy így:

chattr +i *.*

Ez a könyvtár valamennyi fájlját immutable-re állítja és így lehetetlenné teszi a törlését.

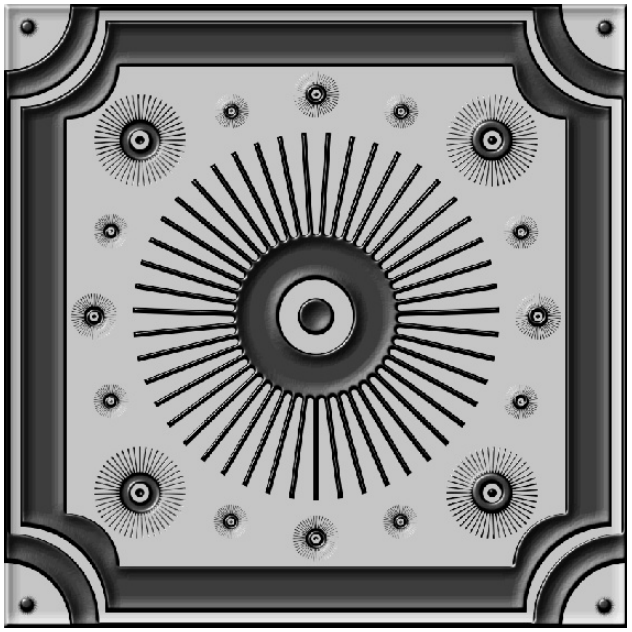


2. módszer: a Python rm-protection alkalmazása

Ennek használatához pár további dolgot telepíteni kell a számítógépre. Először is telepítened kell a **python-pip**-et a PCLinuxOS tárolójából. Ez a többi Python szkript és program telepítője. Ezután le kell töltened a GitHub-ról a **python-rm**-et. Zip formátumban töltsd le, majd bontsd ki a saját /home könyvtárad egy könyvtárába. Ezután, parancssorból su-val válj rendszergazdává és futtasd a **pip-install útvonal/a/programhoz (ahol az útvonal/a/ programhoz az a hely, ahová kics**omagoltad az rm-protection-t). Például, ha az rm-protection fájljait a ~/Letöltések/rm-protection alá csomagoltad ki, akkor a parancsod legyen pip install /home/felhaszn/Letöltések/rm-protection/rm-protection.

A GitHub rm-protection „csomag” két programja: az rm-p és a protect. Határozd meg, hogy mely fájlokat védsz meg. Parancssorba írd be protect atefájlod.kiterj (a fájlnév előtt teljes útvonalat is meghatározhatsz). Ezután kérni fog tőled egy hitelesítő kérdést. Te döntöd el, hogy mi legyen, tehát olyat válassz, amire csak te tudod a választ. Ezután add meg a választ az előbb kitalált azonosító kérdésre. A választ az aktuális könyvtárban tárolja egy .atefájlod.kiterj.rm-protection név alatt („atefájlod.kiterj” megegyezik a védeni kijelölt fájl nevével).

A fájl törléséhez írd be **rm-p atefájlod.kiterj**. A hitelesítő kérdés megjelenik. Ha a válaszod helyes, akkor a fájlodat törli. Ha nem válaszolsz helyesen,



akkor nem törli. Valóban ilyen egyszerű. Alant egy minta az rm-p használatáról:

rm-p: /home/user/atefájlod.kiterj: Mi a kedvenc Linuxod?
Answer: Ubuntu
rm-p: Wrong answer! (rossz válasz) /home/user/yourfile.ext will not be removed
rm-p: The answer is stored in /home/user/.yourfile.ext.rm-protection
rm: missing operand
Try 'rm --help' for more information.

Természetesen a fenti példa a hitelesítő kérdésre adott **rossz** választ mutatja be. Amennyiben a kérdésre jó választ kap, egyszerűen törli a fájlt, minden további szöveges kimenet nélkül.

Jegyezd meg, hogy a válasz nagybetű-érzékeny. Vagyis a „pclinuxos” nem azonos a „PCLinuxOS”-sel, ami pedig különbözik a „PCLINUXOS”-től. Az rm-protect csak a sima felhasználói fájlokat védi. A root továbbra is képes törölni a felhasználó(k) fájljait, még ha védettek is.

Ahogy a chattr esetén a protect és az rm-protect parancsok ismerik az -R opciót, ami az adott könyvtárat csakúgy, mint a könyvtár által tartalmazott fájlokat is levédi.

Összegzés

A két módszer eltérő megközelítést alkalmaz egyetlen céllal: megvédeni a fájljaidat a törléstől. Ne keverd ezt össze a fájl biztonságával. Ez CSAK a törléstől óvja a fájljaidat – legyen az véletlen, vagy szándékos. A „védett” fájljaid tartalma továbbra is olvasható bárki által, megfelelő jogosultsággal a gépedre.

Ez a módszer nem véd meg a merevlemezed formázással történő törlésétől, de úgy gondolom, hogy olyankor semmi sem védi meg azokat. Az egyetlen módszer a kritikus, létfontosságú és fontos fájljaid biztonságban tartására, hogy megfelelő mentéseket végzel.