Firejail, egyszerü Sandbox PCLinuxOS-en

PClinuxOS Magazine – 2018. november

Írta: Alessandro Ebersol (Agent Smith)

A futási környezet védelme a Linux egyik legfontosabb jellemzője. Az egyik legismertebb technika a Chroot virtuális környezet az alkalmazások biztonságos futtatására. Ám a Chroot beállítása elég komplikált és használata is legalább ennyire bonyolult. De tegyük fel, hogy olyasmikre van szükséged, amit a géped biztonsági megoldása a Chroot képes nyújtani. Hogyan érjük el? Mindennapi helyzetre vállaljuk fel a Chroot beállításának bonyodalmait? Valójában már van egy könnyed biztonsági megoldás Linuxra, amit Firejail-nek neveznek.

Mit csinál a Firejail?

A Firejail a namespaces-t és a sec-comp-bpf-et alkalmazza Linuxra az alkalmazások, a fájlrendszer és az operációs rendszer forrásainak egymástól történő izolálására oly módon, hogy ú.n. Sandbox-ot készít, ami az alkalmazásokat elválasztja az operációs rendszertől. Lehetővé teszi egy folyamat és összes leszármazottja számára, hogy saját független hozzáférésük legyen a kernel globálisan megosztott forrásaihoz, mint a hálózati veremhez, a folyamattáblához és az assemblytáblához.

A C-ben írt, gyakorlatilag minden függőség nélküli program bármely 3.x utáni kernellel rendelkező linuxos gépen fut. A sandbox könnyűsúlyú, alacsony a plusz terhelése. Nincsenek komplikált, szerkesztendő beállító fájlok, nincs nyitott csatlakozási pont, nincs futó démon a háttérben. Minden biztonsági megoldást közvetlenül a kernelben alkalmaz, ami elérhető minden linuxos számítógépen. A programot GPL v2 licence alatt adták ki.

A működése megértéséhez át kell tekintenünk a namespaces és a sec-comp-bpf jelentését.

Namespaces

Sok szó esik a konténerekről. Valójában manapság ez a legmenőbb technológiája, mivel lehetővé teszi virtuális gépek nagyon egyszerű létrehozását. A konténerek végső célja történetesen a folyamatok egy csoportjában azt az illúziót kelteni, hogy a rendszerben egyedül vannak. Alkalmazásakor ez a tulajdonság sok gyakorlati haszonnal járhat, mint az egyszerű virtualizáció, az ellenőrző-, és helyreállító pont.

Ahhoz, hogy egy konténerben a folyamatok úgy érezzék, mintha egyedüliek lennének a rendszerben, sokféle globális rendszer-erőforrást kell bevonni a leválasztáshoz, amitől úgy túnne, mintha az egyes konténereknek saját erőforrásaik lennének. Ezt a különféle globális erőforrásokhoz „namespaces” adásával érik el. Minden egyes namespace az adott erőforrásra izolált rálátást ad azon folyamatok csoportjának, amelyek ezen namespaceához tartoznak. A namespaces-t a 2.6.23-as kerneltől kezdődően alkalmazták és a 3.8-as kernelnél vált kiforrottá.

A Linux jelenleg 6 különféle namespaces-t alkalmaz: pid, user, uts, ipc, mnt és net.

így minden ilyen namespace működése során létrehoz egy kapszulát, amibe az alkalmazások bezárhatók és úgy érezhetik, mintha egyedüliként birtokolnák a rendszer erőforrásait.

Nem mennék bele mélyebben az egyes namespacek alkotóelemeibe, mivel ennek az írásnak ez nem témája, csak a Firejail. Ha szeretnéd beásni magad a namespaces-ekbe ezt a cikket ajánlom figyelmedbe.

Seccomp-bpf

A seccomp-bpf a „security computig mode”-ot takarja. Ez a Linux 3.5-ös kernel egyszerű de hatékony sandbox szimulációs eszköze. Lehetővé teszi, hogy a felhasználó egy „rendszerhívó” szűrőhöz (syscall) csatlakoztasson egy process-t és származékait, amivel csökkenti a kernel támadási felületét. A Eccomp szűrők Berkeley Packet Filter (BPF) formátumúak.

Források

- Linux namespaces: a Firejail mögötti fő technológia a Linux Namespaces. Ez egy egyszerű technológia az applikáció izolációjának első eleme.
- Fájlrendszer konténer: az applikációs konténerek automatikusan készülnek, amikor a sandbox elindul és megsemmisülnek a sandbox bezárásával.
- Biztonsági szűrők: jelenleg a következő biztonsági szűrőket (security filters) alkalmazzák - seccomp-bpf, protocol, noroot user namespace, Linux capabilities, X11 sandboxing.

- Hálózati támogatás: a Firejail képes a sandboxhoz új TCP/IP interfészt csatlakoztatni virtuális hálózati kártyával, saját útválasztó táblával és tűzfallal.

- Biztonsági profilok: a /etc/firejail alatt található a profil, ami leírja a fájlrendszer-konténert, a biztonsági szűrőket és a hálózati konfigurációt.

- Forrás allokálás: linuxos vezérlőcsoportok és határok használatával lehetővé teszi olyasmik allokálását, mint a CPU-idő, rendszermemória és hálózati sávszélesség.

- Univerzális csomagformátumok: a Firejail alapból támogatja az AppImage formátumot. Egyszerűen hozzá kell adni az -appimage parancssori opciót és a csomagot csatolja és végrehajtja a sandbox-on belül. A Firejail támogatja még az Ubuntu Snap csomagolást is szabványos biztonsági profil alkalmazásával.

- Sandbox auditálás: az auditálás lehetővé teszi, hogy felhasználó kiszúrja a profil biztonsági réseit. Az alkalmazás a sandbox háttérprogramját lecseréli egy teszt verzióra. Alap auditáló program elérhető, de tetszőleges program is alkalmazható.

- Statisztika és monitoring: a Firejail opciók széles tárházával teszi lehetővé sandbox-ban lévő alkalmazás sokoldalú megfigyelését. Ez lehet CPU-, memória-, sávszélesség-használat, rendszerhívások figyelése, illetve exec- és fork-eseményfigyelés, valamint fájlok és könyvtárak blacklist loggolása.

- Grafikus felhasználói felület: önálló programcsomagként elérhető egy Firetools GUI alkalmazás.

Telepítés

PCLinuxOS alatti telepítéshez terminálban rendszergazdaként add ki az apt-get install firejail firetools parancsot, vagy használj Synaptic-ot.

Használat

Alkalmazás firejail-védelemmel futtatásához (alapbeállítású profillal) a következőt futtasd:

$ firejail

A Firejail meghatározott profillal futtatásához (több mint 400 linuxos alkalmazáshoz található firejail profil):

firejail -profile = filename.profile

A program tartalmazta profilokon túl saját profil is készíthető és menthető a ~/.config/firejail alá.

Az ide mentett profilok elsőbbséget élveznek a programmal érkező profilokkal szemben.

Amennyiben az összes programot Firejail alatt akarod használni root-ként írd be # firecfg

Ez létrehoz egy szimbolikus hivatkozást a /usr/local/bin-ben, ami a /usr/bin/firejail-re mutat azon programok esetében, amik rendelkeznek firejail profillal.

Alant egy alap Firejail profil látható:

##############################

 # Generic GUI application profile

##########################

include /etc/firejail/disable-mgmt.inc

include /etc/firejail/disable-secret.inc

include /etc/firejail/disable-common.inc

blacklist $ {HOME} /. pki / nssdb

blacklist $ {HOME} /. LastPass

blacklist $ {HOME} /. keepassx

blacklist $ {HOME} /. password-store

caps.drop all

seccomp

protocol unix, inet, inet6

netfilter

noroot

Tegyük fel, szeretnéd megakadályozni, hogy egy alkalmazás hozzáférjen a felhasználói dokumentum-könyvtárhoz. Ennek érdekében add a következő sort az újonnan létrehozott profilhoz:

blacklist $ {HOME} / Documents

Így, az ezzel a profillal futó programok nem érik el a / Documents könyvtárat a /home-odban.

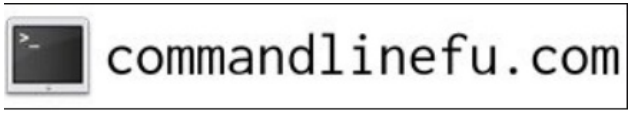
Meghatározott könyvtárakat csak olvashatóvá tehetsz ilyen módon:

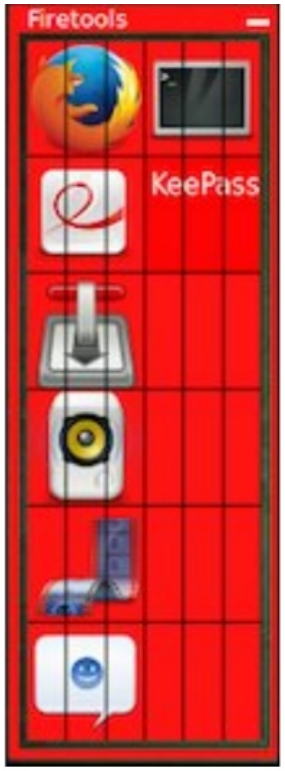
read-only ${HOME}/Documents

A profilok széleskörűen alkalmazhatók, jelentős szórással. A beállítási parancsok megismeréséhez ezt a Wiki-t keresd: https://wiki.archlinux.org/index.php/Firejail ami elég alapos.

Firetools használata

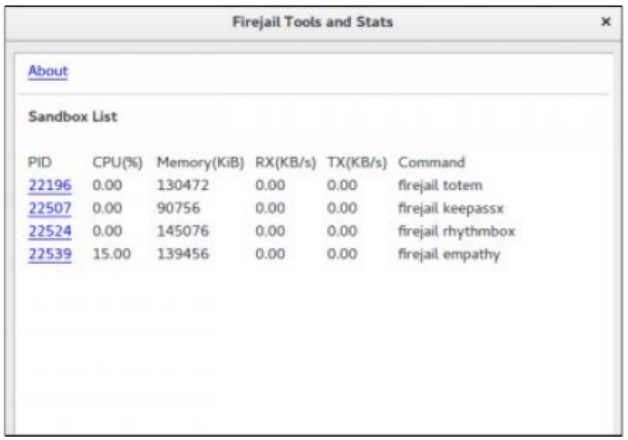
Nézzük meg a Firejail felhasználói felülete a Firetools működését. Terminálból add ki a firetools parancsot az eszköz indításához. Két dolgot kell látnod: a Fretools ablakot és egy prompt-ot a rendszertálcán futó alkalmazáshoz.





A Fiertools-ban előre beállított alkalmazások

A Firetools-ban találsz néhány előre konfigurált alkalmazást. Ezekből indításhoz vagy dupla kattintás az alkalmazás indítóján, vagy jobbal kattintás az indítón és Futtatás kiválasztása kell. A Firetools rendelkezik monitorral, amit indítva megnézhető, hogy mik futnak Firejail-lel. A GUI felületen bárhol jobbal kattintva válaszd az Eszközöket (tools). Amikor a monitor megjelenik, kilistázza az összes sandbox-ban futó alkalmazást.



A firejail-ben futó alkalmazások

Záró gondolatok

Miért is használjunk Firejail-t PCLinuxOS alatt?

Nos, néhány alkalmazási lehetőséget nézzünk meg. A Firejail javíthatja a számos alkalmazás biztonságát, legyen az asztali, vagy kisebb szerver-alkalmazás, esetleg üzleti, iskolai, hivatali vagy kormányzati szervnél.

Kioszk-gépet készítesz és korlátozod az elérését. Nem engeded, hogy hozzáférjen a /home könyvtárhoz és a rendszer kikapcsolásához.

És ami még fontosabb, biztonsági szintet készítesz appimage–formátumba csomagolt fájloknak, amik egyre népszerűbbek, és amik felhasználhatók lennének malware-rel fertőzésre, illetve azok terjesztésére.

Remélem tetszeni fog a Firejail, a PCLinuxOS biztonsági tárházának egyik eleme (az AppImage szinte könyörögnek az ilyen eszközökért).