

Novell AppArmor

www.novell.hu

TERMÉKISMERTETŐ

2005.09.28

Novell®

Tartalomjegyzék

| | |
|--|----------|
| Rendszervédelem a Novell AppArmor szoftverével..... | 2 |
| Bevezetés..... | 2 |
| Választható alkalmazásprofilok..... | 2 |
| Hálózati ügynökök..... | 3 |
| Hálózati alkalmazások..... | 3 |
| Webalkalmazások..... | 4 |
| Parancsfájl-nyelvek..... | 4 |
| Setuid programok..... | 4 |
| Cron-nal időzített feladatok..... | 5 |
| Profilkészítés..... | 5 |
| A genprof..... | 5 |
| A logprof..... | 5 |
| Az eredmények visszaigazolása..... | 6 |

Rendszervédelem a Novell AppArmor szoftverével

Alkalmazásbiztonság Linuxon

Az Immunix alapjaira épülő Novell AppArmor a ma kapható leghatékonyabb és legkényelmesebben használható Linux alkalmazásbiztonsági rendszer. Az AppArmor megvédi az operációs rendszert és az alkalmazásokat a támadások, vírusok és rosszindulatú szoftverek hatásaitól. Használatával minimalizálhatók a vállalkozást érő fenyegetések, megvédhetők a kulcsfontosságú adatok, csökkenthetők a hálózat adminisztrációs költségei és teljesíthetők a törvényi előírások.

Az AppArmor révén biztonsági irányelvek készíthetők a védelmet igénylő Linux-alkalmazásokhoz; ezek kidolgozását a program egy robusztus eszközkészlettel segíti, amely a Linux parancskonzolból vagy a SUSE LINUX YaST felületéről érhető el.

Ebben a dokumentumban leírjuk, hogyan alakíthatók ki a biztonsági irányelvek a Linux parancskonzol használatával.

Bevezetés

Néhány klasszikus jótanács annak érdekében, hogy az alkalmazások fölött a támadók ne vehessék át a hatalmat:

- Érdemes lezárni azokat a portokat, amelyekre nincs szükség
- Amennyire csak lehetséges, erősítsük meg a nyitott portokkal rendelkező alkalmazások biztonságát
- A lehető legkevesebb setuid root alkalmazást használjunk
- Általában is a lehető legkevesebb szoftvert telepítsük

Ezek a lépések jelentős erőfeszítéseket követelnek, és végrehajtásuk után a megerősített gép kevésbé kényelmesen használható. A Novell AppArmor megkönnyíti e tennivalók végrehajtását, valamint biztonságosabbá és kényelmesebben használhatóvá teszi a védett gépet. Az AppArmor hatékonyan védi a szükséges alkalmazásokat, és lényegesen nagyobb biztonsági értéket kínál annál, mint amit pusztán a veszélyeztetett alkalmazások számának csökkentése jelent.

Választható alkalmazásprofilok

A Novell AppArmor egyik legfontosabb használatkönnyítő funkciója a méretezhető biztonság. Más megoldások esetében a biztonsági irányelveket a teljes rendszerre alkalmazni kell, és számos esetben lehetetlen bármilyen rész kizárása az irányelvek hatálya alól. Ha az irányelv rossz, akkor előfordul, hogy ott állunk egy sérült rendszerrel, ami letiltja a saját számítógépre történő bejelentkezést.

Az AppArmor méretezhető biztonsági szolgáltatásával eldöntheti, hogy melyik programokat szeretné védeni. Ezzel jelentősen csökkenthető a számítógép védelmére fordított munka mennyisége, mivel csak azokhoz a programokhoz kell profilt készíteni, amelyek az adott környezetben ki vannak téve a támadásoknak.

A számítógépes rendszer hatékony megerősítése megköveteli a jogosultságokat ellenőrző programok számának minimálisra csökkentését, majd a programok lehető legnagyobb mértékű biztosítását. Az AppArmor profilok kikényszerítik az irányelvek betartását annak biztosítására, hogy a programok azt tegyék, ami a feladatuk, és semmi mást. Hozzon létre AppArmor profilt minden jogosultságellenőrző programhoz:

- **Hálózati ügynökök:** A szerver- és kliensprogramok nyitott portokkal rendelkeznek, a hálózati ügynökök pedig olyan szerverprogramok, amelyek ezeken a hálózati portokon válaszolnak. A felhasználói kliensek (például a levelezőkliensek és a webböngészők) szintén rendelkeznek nyitott portokkal és szintén ellenőriznek jogosultságokat. Ezek a programok megfelelő jogosultsággal futnak ahhoz, hogy írhasanak a felhasználó saját könyvtáraiba és feldolgozhassák a potenciális veszélyt jelentő távoli források (például ellenséges webhelyek vagy e-mailben érkezett kártékony kódok) bemeneteit.
- **Webalkalmazások:** A webböngészőkön keresztül meghívott CGI PERL parancsfájlok, PHP-oldalak és még összetettebb webalkalmazások.
- **Setuid programok:** A setuid vagy setgid programok a programfájl tulajdonosaként szereplő felhasználó vagy csoport nevében futnak, nem pedig az azokat meghívó felhasználó nevében.
- **Cron-nal időzített feladatok:** Azok a programok, amelyeket a cron démon rendszeresen lefuttat, elolvassák bizonyos fajta források bemenetét. Ezeknek speciális jogosultságokkal, néha akár root jogosultsággal kell futniuk (a cron például naponta lefuttatja a /usr/bin/updatedb feladatot azért, hogy az slocate adatbázisba bekerüljenek a legfrissebb adatok, és elegendő jogosultsággal rendelkezik az összes rendszerfájl nevének elolvasásához).

Hálózati ügynökök

A profilokat igénylő hálózati szerverdémonok megkereséséhez vizsgálja meg a gép nyitott portjait, gondolja végig az ezeken válaszoló programokat, és adjon meg profilokat minél több programhoz. Ha minden nyitott hálózati porttal rendelkező programhoz profilt rendel, akkor a támadók nem juthatnak be a gép fájlrendszerébe anélkül, hogy ne találkoznának egy Novell AppArmor profillal.

A szerver nyitott hálózati portjait kézzel is megkerestetheti a gépen kívülről egy keresővel (pl.: nmap) vagy belülről a netstat használatával, majd áttekintheti a gépet annak meghatározására, hogy mely programok felelnek a nyitott portokon.

Hálózati alkalmazások

Egy sokkal jobban automatizált módszer a Novell AppArmor *unconfined* nevű programjának használata. Ez az eszköz a „netstat -nlp” parancs használatával végignézi a számítógép nyitott portjait, felderíti a hozzárendelt programokat, megvizsgálja a betöltött AppArmor profilokat és jelenti a programokat és a hozzájuk tartozó profilokat. Ha egy program nincs védőórizetben, nem kerül be a jelentésbe.

Megjegyzés: Az *unconfined* eszköz futtatásához root jogosultság kell, és nem futhat egy AppArmor profilon belül. Nem különbözteti meg egymástól a hálózati csatolókat, vagyis minden védőórizet nélküli folyamatról jelentést ad, még azokról is, amelyek a belső LAN-csatolón figyelnek. Ha egy program több hálózati csatolón is figyel, akkor többször is jelentésre kerülhet, így a kimenetben egy bejegyzés többször is szerepelhet.

Webalkalmazások

A webalkalmazások megkereséséhez elemezni kell a webservert-beállításokat. Az Apache webservert rendkívül jól konfigurálható és a webalkalmazások számos könyvtárban tárolhatók a helyi beállításoktól függően. A SUSE LINUX Enterprise Server 9 alapértelmezésben a `/srv/www/cgi-bin/` mappában tárolja a webalkalmazásokat.

Az egyes webalkalmazások saját Novell AppArmor profilokkal végzett korlátozása a lehető legkisebbre csökkenti azok jogosultságait, és ezzel a támadó lehetőségeit arra, hogy a program felett átvegye az uralmat. Választhatja azt is, hogy kevesebbet energiát fordít a rendszer biztosítására (a biztonság csökkenése árán), és ehelyett az Apache AppArmor profilon belül futtatja a webalkalmazásokat.

Annak a kiválasztása, hogy egy webalkalmazás saját profillal rendelkezik, vagy az Apache profilját használja, a `genprof` és `logprof` profilkezelő segédprogramokban történik, amelyek leírása a Profilkészítés részben található. Amikor az Apache végrehajt egy folyamatot, akkor a profilkezelő segédprogram rákérdez, hogy rendeljen-e profilt ehhez a folyamathoz, vagy az örökölje az Apache profilját.

Parancsfájl-nyelvek

Számos webalkalmazást írnak értelmezett parancsfájl-nyelvekben; ilyen például a PERL, a PHP vagy a Python.

A teljesítmény fokozására számos webhely használja a `mod_perl`, `mod_php` és `mod_python` modulokat, hogy ezeknek a programnyelveknek az értelmezőjét közvetlenül az Apache webservertben helyezze el. Így gyorsabbá válik a működés, mivel az Apache szoftvernek nem kell végrehajtania egy nagy értelmezőprogramot egy kicsi parancsfájl futtatására, csak megnyitja a parancsfájlt és közvetlenül értelmezi. Ez azonban veszélyezteti a biztonságot, mivel a webalkalmazások az Apache processzen belül futnak, az Apache jogosultságait használva. A Novell AppArmor hatékony lehetőséget kínál az egyes webalkalmazások védőőrzetére még akkor is, ha azok az Apache által használt modulokon (például a `mod_perl`, `mod_php` vagy `mod_python` modulokon) belül futnak.

Az AppArmor Apache `mod_change_hat` modul meghívja az AppArmor `change_hat()` API-t, így az Apache a végrehajtható parancsfájl nevének megfelelően egy alprofilra válthat. Ha nem talál specifikus profilt a parancsfájlhoz, akkor az értelmezőhöz rendelt alapértelmezett profil használható. Ez javíthatja a biztonságot például azzal, hogy minden PHP-oldalt egy hasonló profilhoz rendel, amely elegendő jogosultsággal rendelkezik az összes PHP-oldal működéséhez, de sokkal korlátozottabb, mint az Apache profil.

Setuid programok

A fájlrendszer átvizsgálásával megkereshetők a setuid programok. A következő parancs például meg fogja találni a setuid root beállítással futó programokat:

```
find/-user root -perm -4000 -print
```

A setuid vagy setgid programokat érdemes védőőrzetbe helyezni a Novell AppArmor használatával, mivel minden felhasználó számára engedélyezik a `setuid` vagy `setgid` beállítások jogosultságait. E jogosultságok védelmének egyetlen garanciája a programok hibátlansága; ha hiba van a szoftverben, akkor egy jogosultságokkal nem rendelkező felhasználó kényszerítheti a programot egy tetszés szerinti kód lefuttatására azzal, hogy kellőképpen „kreatív” bemenetet biztosít, és ezzel root jogosultságra tehet szert. Az AppArmor védőőrzet biztosítja, hogy a program csak a szükséges feladatokat lássa el, és ezzel eredménytelenné teszi a jogosultságokkal nem rendelkező felhasználók hasonló támadásait.

Cron-nal időzített feladatok

A *cron* démon által futtatott feladatok megkeresésére át kell tekinteni a helyi cron konfigurációt. Ez azonban sajnos eléggé összetett feladat, mivel számos fájlt kell megvizsgálni. Az ismétlődő cron feladatok a következő fájlokból futnak:

- /etc/crontab
- /etc/cron.d/*
- /etc/cron.daily/*
- /etc/cron.hourly/*
- /etc/cron.monthly/*
- /etc/cron.weekly/*

A root felhasználó cron-nal időzített feladatainak esetében a feladatok módosíthatók a „crontab -e”, illetve kilistázhatók a „crontab -l” paranccsal.

Profilkészítés

Ha kiválasztotta a megfelelő programokat, akkor létre kell hozni azokhoz a profilokat. A Novell AppArmor *genprof* és *logprof* segédprogramok ennek a folyamatnak a nagy részét automatizálják: kérdéseket tesznek fel, amelyekre válaszolva interaktív módon dönthet a biztonsági szolgáltatásokról és így véglegesítheti a programprofilokat.

A *genprof*

A kiindulási hely a *genprof* segédprogram. A root parancsértelmezőbe írja be a „genprof foo” parancsot, ahol a „foo” a profillal ellátni kívánt program neve. A *genprof* megkeresi a foo programot, és egy induló becslést ad a program becsülhető profiljáról, majd „tanuló módra” állítja be a profilt, amikor is a profilszabályok még nem kerülnek kikényszerítésre, de a megsértésük már naplózva van. A *genprof* ezután felkéri Önt a program elindítására egy másik ablakban, és ahogy a szoftver a használat során végigfut a műveletein, a segédprogram összeállít egy naplófájlt, amely leírja a program helyes működési módját.

Futtassa végig a programot egy teljes minőségbiztosítási (QA) cikluson, próbálja ki az összes fontos funkciót és legyen óvatos azzal kapcsolatban, hogy ne futtasson semmilyen támadást a program ellen. Ha végzett, térjen vissza a *genprof* ablakba és nyomja meg az „s” billentyűt az elemzés (scan) elindítására. A *genprof* ezután feltesz egy sor kérdést arra vonatkozólag, hogy hogyan reagáljon bizonyos fájlhozzáférési eseményekre.

A foo program általában hozzányúl bizonyos fájlokhoz, és a *genprof* megkérdezi, hogy pontosan meghatározott jogokat kíván-e rendelni a betű szerint megadott fájlnevekhez, vagy inkább bizonyos fájlmintákhoz rendelne jogokat. A minta tartalmazhat helyettesítő karaktereket vagy egy `#include` utasítással egy szabálykészletet is, hogy ne csak erre az eseményre vonatkozzon, hanem a naplófájlban található több másikra és a jövőbeli eseményekre is.

A *logprof*

A *logprof* segédprogram működése nagyon hasonlít a *genprof*-éhoz azzal a kivétellel, hogy a Novell AppArmor profilok további tökéletesítésére tervezték, nem pedig a kiinduló létrehozáshoz. A *logprof* a futtatás során átvizsgálja az aktuális rendszernaplót az AppArmor események után; rákérdez, hogy melyik esetében mi a teendő és a *genprof*-nál említettekhez hasonló mintákat javasol.

A minőségbiztosítási vizsgálat akár külön is választható a profilkészítéstől. A méretes minőségbiztosítási tesztcsomagokkal rendelkező nagy alkalmazások esetében egyszerűen elküldheti az alkalmazást és egy sor AppArmor profilt tanulási módban a minőségbiztosítási osztálynak tesztelésre. Az AppArmor profilok nem változtatják meg a tesztelt alkalmazás működési módját, bár a naplózási műveleteket a profil nyíltan nem engedélyezi. A naplófájlok a minőségbiztosítási vizsgálat végén összegyűjthetők és e-mailben visszaküldhetők a biztonsági profilok fejlesztőinek. Ők ezután ezeket offline, a vizsgált programtól elkülönítve is futtathatják és egyre tökéletesíthetik a programok *logprof* profilját anélkül, hogy bármilyen módon hozzá kellene férniük a minőségellenőrzést végző gépekhez vagy a tesztcsomaghoz.

Az eredmények visszaigazolása

Az AppArmor alapelve szerint a számítógépvédelem megerősítésének utolsó lépése a beállítások biztonságosságának ellenőrzése. A profilkészítési munka hatékonyságának vizsgálatára futtassa le ismét az *unconfined* programot (lásd: Hálózati ügynökök) és vizsgálja meg a kimenetet annak megtekintésére, hogy a támadásnak kitett programoknak van-e már profiljuk.

Ha a számítógép hálózati kiszolgálóként működik, akkor a támadások valószínűleg a hálózatról érkeznek. Így az *unconfined* programnak a hálózati portokat figyelő hálózati szolgáltatásoktól érkező szabványos kimenete pontosan tükrözi azokat a fenyegetéseket, amelyeknek a gép ki van téve. Ha az *unconfined* jelentéseket produkáló összes program össze van rendelve AppArmor profilokkal, akkor a támadó számára lehetetlen, hogy közvetlenül elérje a fájlrendszert anélkül, hogy bele ne ütközne a beállított AppArmor irányelvekbe.

A legrosszabb eset (például a számítógépes rendszerben támadással okozható károk) elemzésére vizsgálja meg az *unconfined* program által kilistázott profilokat. Erre a *vim* az ideális eszköz, mivel ez színekkel kiemelve mutatja a profilokat (a sárgával jelölt szabályok az írási szabályok). Azoknak a fájloknak a halmaza, amelyekben egy támadó kárt tehet, a profilokban felsorolt írható fájlok halmaza. Ez most jóval kisebb, mint amelyet a támadó az AppArmor irányelv-kikényszerítések nélkül elérhetne.

Összefoglalás

A hálózati szerverek védelmére minden veszélyeztetett, védőőrizet nélküliként felsorolt programhoz érdemes hozzárendelni egy Novell AppArmor profilt. Ha bármelyik program védőőrizet nélküliként van felsorolva, lépjen vissza e dokumentum megfelelő részébe, és alkalmazzon rá egy AppArmor profilt. Ismételje ezt egészen addig, amíg minden program nem rendelkezik profillal. Ha végzett, akkor az AppArmor profilok megvédik a rendszert a rosszindulatú külső támadóktól, minimalizálják a veszélyeket, védik a kulcsfontosságú vállalati adatokat, csökkentik a hálózati adminisztrációs költségeket és segítenek betartani az előírásokat.