Používáme SUDOers

Vložil/a cm3l1k1 [1], 22 Březen, 2006 - 20:56

- GNU/Linux a BSD [2]
- Security [3]

I na velkých serverech, kde se o každou síťovou službu stará jiný člověk, musí být root jen jeden! Zde si ukážeme, jak to lze celkem jednoduše, bezpečně a efektivně vyřešit pomocí sudoers.

Ve firmách, kde se např. vyvíjí/testuje software, konfigurují síťové služby, vytváří nové dhcp/dns/mail záznamy apod., se o to vše nutně nemusí starat jeden administrátor, ale může jich být několik. Nicméně by se určitě jejich práva měla omezit na potřebnou míru a nedávat jim hned právo roota. Pokud někdo spravuje účty Qmailu a jinak se o chod serveru nestará, tak určitě nemá mít přístup superuživatele, ale jen taková práva, které ke své práci potřebuje, čímž se podstatně sníží bezpečnostní riziko a možnost chyby lidského faktoru. V tomto článku bych vám chtěl přiblížit, jak se o práva v řízení systému podělit pomocí sudo(ers).

sudo (superuser do) -- umožňuje administrátorovi dát určitým osobám (nebo skupinám) možnost spustit definované příkazy s právy roota. Tento článek nijak nesouvisí s příkazem su, kterým spustíte shell pod zadaným uživatelem. My využijeme konfigurační soubor **/etc/sudoers**, kde budeme definovat, co který uživatel smí spouštět s právy roota (či jakéhokoliv uživatele).

Upozornění: nikdy needitujte sudoers normálním editorem, ale jen přes **visudo**!

Základní syntaxe vypadá takto:
$uzivatel $stroj = ($user_pod_kterym_pobezi) $prikaz_s_parametry

Zpočátku je v /etc/sudoers tento záznam:
root   ALL=(ALL) ALL

Říká nám tím: uživatel root může na všech systémech spouštět s právy všech uživatelů (tj. především roota, ale jde o to, že může spouštět příkazy i pod jinými uživateli) všechny příkazy.

Pokud bychom například v systému chtěli dát práva uživateli webmaster:
webmaster   localhost = (apache) ALL, (root) /usr/bin/su apache

Takže co jsme vlastně nastavili? Uživatel webmaster může na lokální stanici spouštět jakékoliv příkazy pod uživatelem apache (localhost = (apache) ALL) a spustit shell s oprávněním uživatele apache ((root) /usr/bin/su apache). Pokud by jsme nastavili jen (root) /usr/bin/su tak by se su spouštělo s právy roota a mohli by jsme spustit shell pod jakýmkoliv uživatelem, což není zrovna ideální ;).
Další co byste měli vědět, že pokud uživatel webmaster tedy spustí příkaz: **sudo /usr/bin/su apache**, tak bude požádán o heslo. Ne však heslo roota, ale jeho vlastní (webmastera!). Je to kvůli vyšší bezpečnosti, aby bylo zaručeno, že jen někdo nepřišel k otevřenému terminálu a zároveň webmaster nebude potřebovat heslo roota. Heslo se uloží po dobu 5-ti minut, takže jej není nutné zadávat pokaždé (samozřejmě jak čas, tak i nutnost zadávat heslo lze nastavit).

Mějme skupinu chpass, která může měnit hesla uživatelům, ale rozhodně ne rootovi:
%chpass   ALL = (root) /usr/bin/passwd [a-zA-Z0-9_-]*, !/usr/bin/passwd root

Skupinu tedy poznáme tak, že je před ní znak **%**. Tito uživatelé můžou měnit heslo na jakémkoliv stroji komukoliv, ale znak **!** způsobí, že nesmějí spustit passwd root a tím mu změnit heslo.

Volba, která nepožaduje heslo uživatele je NOPASSWD: např.
cm3l1k1 localhost = NOPASSWD:/usr/bin/emerge, /usr/bin/ebuild, /usr/sbin/emerge-webrsync

Aliasy

Takže úvod máme napsaný a teď si ukážeme, jak si zjednodušit psaní pravidel. Pokud budete psát opravdu větší konfigurační soubor, tak se aliasy hodí, protože změny se provádí jen v definovaných proměnných.
Máme čtyři druhy aliasů: User_Alias, Runas_Alias, Host_Alias a Cmnd_Alias.

```
User_Alias uzivatele = user1, user2
Runas_Alias spustit_jako = user1, user2
Host_Alias site = hostname1, hostname2
Cmnd_Alias prikazy = command1, command2
```

Příklad použití:

```
User_Alias  webmasteri = alice, bob
User_Alias  spravci = cm3l1k1
Host_Alias  privatnisit = 10.0.11.0/25, 10.0.11.128/28
Cmnd_Alias  webmastericmd = (apache) ALL, (root) /usr/bin/su apache
Cmnd_Alias  spravcicmd = /usr/bin/emerge, /usr/bin/ebuild, /usr/sbin/emerge-webrsync

webmasteri  localhost = webmastericmd
spravci  privatnisit = spravcicmd
```

Jak vidíte, použití je velice snadné a lze tím ušetřit spoustu práce u velkých konfiguračních souborů.

Nastavení defaultního chování

Tohle je ta část, kde si můžete vyhrát s nastavením a chováním sudoers. Doporučuji si projet manuálove stránky, nebo mrknout na homepage sudo:
http://www.courtesan.com/sudo/man/sudoers.html#defaults [4]

Jak jsem třeba zmiňoval, že po zadání hesla u sudo se v paměti uchovává po 5 minut, tak tímto záznamem:

Defaults timestamp_timeout=0, passwd_tries=2

způsobíme, že se nás sudo bude ptát na heslo pokaždé a nebude se vůbec ukládat do paměti. Druhý záznam povoluje maximální počet chybných zadání hesla.

Voleb je velká řada, a pokud byste se v nich chtěli vyřádit, tak se podívejte na výše uvedený odkaz manuálových stránek. Nejdřív bychom si však mohli ukázat takový jednoduchý příklad nastavení defaults.

```
Defaults  syslog=auth,log_year,logfile=/var/log/sudo.log,
                mail_no_perms, tty_tickets, loglinelen=0, !fqdn,
                mailto="nekdo@nekde.cz"
```

Aktivujeme si logování; logujeme i roky; určíme, že se bude logovat do souboru /var/log/sudo.log; na email nám bude chodit oznámení, když někdo použije sudo příkaz, který nemá povolený; tohle nevim úplně přesně, takže radši nebudu spekulovat; vypneme zalamování řádků logu; vypneme logování FQDN (celé názvy počítačů), protože pokud bude DNS server nějak nedostupný, tak se sudo nebude možné pracovat; mailová adresa kam se budou zasílat vyžádané logy.

Závěr

Na konec článku bych chtěl upozornit, abyste si dávali velký pozor, co komu povolíte, protože člověk s možností spuštění editoru pod rootem má možnost editovat i /etc/shadow ! Přistupujte k tomu obezřetně a práva udělujte jen tomu, kdo to opravdu potřebuje a komu v rámci možností věříte. Ještě jedna rada pro paranoiky: díky sudoers můžete všem programům odebrat suid, sgid bit a nastavit konkretní práva i na konkretní parametry předávané programům ;o)

Odkazy:

Manuálové stránky sudo -- http://www.courtesan.com/sudo/sudo.html [5]
Příklad souboru sudoers -- http://www.courtesan.com/sudo/sample.sudoers [6]

URL článku: https://www.security-portal.cz/clanky/pou%C5%BE%C3%ADv%C3%A1me-sudoers

Odkazy:
[1] https://www.security-portal.cz/users/cm3l1k1
[2] https://www.security-portal.cz/category/tagy/gnu/linux-bsd
[3] https://www.security-portal.cz/category/tagy/security
[4] http://www.courtesan.com/sudo/man/sudoers.html#defaults
[5] http://www.courtesan.com/sudo/sudo.html
[6] http://www.courtesan.com/sudo/sample.sudoers