Zabezpečení linuxového serveru

Petr Krčmář

1. února 2014

Patero zodpovědného admina

1. udržujte systém a software aktuální
2. vypněte zbytečné služby
3. omezte uživatele
4. zabezpečte SSH
5. čtěte logy

Udržování aktuálního software

- když Debian, tak jedině stable
- nainstalujte si `apticron`
- pravidelně sleduje aktualizace a posílá maily
- průměrně mi chodí mail týdně
- průměrně 5 balíčků v mailu
- minimum 1, maximum 31
- měsíčně přijede 20 aktualizací

Vypněte zbytečné služby

- sledujte a vypínejte služby, které nepotřebujete
- lepší než zavírat porty na firewallu
- každá služba navíc je potenciálním vstupem
- nebo použijte `nmap localhost`
- zvažte uzavření služeb pro konkrétní IP

Omezte uživatele (1/2)

- zakažte přihlašování uživatelům, kteří to nepotřebují
- uživatel != jen fyzický uživatel
- zabraňte aktivně přenosu nešifrovaných hesel
- vyházejte služby jako FTP, POP3, IMAP4 a podobné
- nahraďte SSL variantou, nebo SSH tunelem na localhost

Omezte uživatele (2/2)

- připojte `/tmp` `/var/tmp` a `/dev/shm` jako nodev, nosuid a noexec
- nastavte sticky bit na tmp a další adresáře
- nastavte uživatelům limity (`/etc/security/limits.conf`)
- omezte použití sudo
- omezte přístup do různých adresářů
- omezte počet SUID/SGID binárek
- `find / -perm -4000` a `find / -perm -2000`

SSH – hlavní brána dovnitř

- nejčastější díra dovnitř
- hádání hesel
- uživatelé se (obvykle) střílí od boku
- i získání běžného uživatele velké plus

Nejčastěji hádaní uživatelé

1. root
2. test
3. admin
4. oracle
5. nagios
6. user
7. guest
8. postgres
9. alex
10. teste

Co s tím?

1. Změnit port SSH serveru
2. Omezit některé (privilegované) uživatele
3. Vypnout přihlašování heslem
4. Povinné přihlašování klíčem
5. Sledování pokusů a jejich blokování

VPSFREE.CZ

SSH: změna portu serveru

- security through obscurity (utajením k bezpečnosti)
- **vždy** jen doplněk ke skutečné bezpečnosti
- Daniel Miessler vyzkoušel porty 22 + 24
- výsledek 7025:3 pokusům o připojení
- funguje to
- (http://jdem.cz/aaqr0)

SSH: změna portu prakticky

- v souboru `/etc/ssh/sshd_config` změňte položku Port 22
- poté nezapomeňte démona restartovat
- je možné mít i víc portů

SSH: omezení privilegovaných uživatelů

- znemožnění přímého přihlášení roota
- je potřeba projít přes běžný účet
- zamezení hádání nejběžnějšího účtu
- v souboru `/etc/ssh/sshd_config` změňte položku PermitRootLogin yes
- poté nezapomeňte démona restartovat

SSH: omezení dalších uživatelů

- vyházet všechny automatické účty
- oracle, debian, www, http . . .
- vyhodit vše, co není potřeba
- v souboru `/etc/ssh/sshd_config` volby:
- AllowGroups, AllowUsers, DenyGroups, DenyUsers
- za zavináč možno uvést i adresu (petr@1.2.3.4)
- možno použít wildcards (* a ?)

SSH: přihlašování klíčem

- využívá se asymetrické kryptografie
- místo předání hesla se podepisuje zpráva
- není třeba zadávat hesla
- klíče není možné hádat
- vygenerovat klíče `ssh-keygen`
- uložit na serveru do `~/.ssh/authorized_keys`
- zapnout v konfiguraci `PubkeyAuthentication`
- (http://jdem.cz/q6ez8)

VPSFREE.CZ

SSH: vypnutí přihlašování heslem

- povinný klíč pro každého uživatele
- v souboru `/etc/ssh/sshd_config` změňte položku
  PasswordAuthentication no
- ověříte příkazem
  $ ssh -o PubkeyAuthentication=no server
  Permission denied (publickey).

SSH: sledování pokusů o přihlášení

- fail2ban - univerzální sledovač logů
- má předepsané skripty i pro SSH
- sleduje `auth.log` a po překročení limitu dá ban
- sám se stará o rušení zákazů
- Pozor! Více klíčů = více pokusů
- konfigurace v `/etc/fail2ban`
- soubory `fail2ban.conf` a `jail.conf`

Čtěte logy

- odhalíte anomálie (neprošlo včera mail serverem osm milionů mailů?)
- nainstalujte si `Logwatch`
- umí dělat automatické souhrny
- velmi silně konfigurovatelný
- web, pošta, SSH, přihlašování…
- skripty v `/usr/share/logwatch/scripts/services`
- lze určit různou pravidelnost
- ale **musíte to číst**

Otázky?

Petr Krčmář
petr.krcmar@vpsfree.cz