Zabezpečení linuxového serveru

Petr Krčmář

3. listopadu 2013

Prezentace už teď na webu

www.petrkrcmar.cz

ROOT.CZ

Anketa

Kdo z vás má vlastní server/VPS?

ROOT.CZ

Patero zodpovědného admina

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

ROOT.CZ

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

ROOT.CZ

Vypněte zbytečné služby

- sledujte a vypínejte služby, které nepotřebujete
- lepší než zavírat porty na firewallu
- každá služba navíc je potenciálním vstupem

```
# netstat -tulpn
```

- nebo použijte `nmap localhost`
- zvažte uzavření služeb pro konkrétní IP

ROOT.CZ

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 STARTTLS, nebo SSH tunelem na localhost

ROOT.CZ

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`
- zvažte zapnutí AppArmor

ROOT.CZ

SSH – hlavní brána dovnitř

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

ROOT.CZ

Nejčastěji hádaní uživatelé

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

ROOT.CZ

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

ROOT.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 minimálně jako obrana před 0day útoky
- (jdem.cz/8p4m4)
- lepší ale použít vyšší porty nebo 443 (případně sslh)

ROOT.CZ

SSH: změna portu prakticky

- v souboru `/etc/ssh/sshd_config` změňte položku

```
Port 22
```

- je možné mít i víc portů
- poté nezapomeňte démona restartovat

```
# netstat -tlpn | grep sshd
```

ROOT.CZ

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
```

- buď na `no` nebo na `without-password`
- poté nezapomeňte démona restartovat

ROOT.CZ

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 ?)

ROOT.CZ

SSH: zamknutí uživatelů v adresáři

- možnost zamknout uživatele automaticky v chrootu
- možnost vynucení SFTP = zákaz terminálu
- bezpečná náhrada za FTP, jednoduše nasaditelné

```
Match group sftpusers
    ChrootDirectory     /sftp/%u   # v %h je home
    ForceCommand        internal-sftp
    X11Forwarding       no
    AllowTcpForwarding  no
```

- pozor na práva domovského adresáře
  - vlastníkem musí být root a jen on může zapisovat
- (jdem.cz/euqe4)

ROOT.CZ

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`
- (jdem.cz/q6ez8)

ROOT.CZ

SSH: vypnutí přihlašování heslem

- povinný klíč pro každého uživatele
- v souboru `/etc/ssh/sshd_config` změňte položky

```
PasswordAuthentication no
ChallengeResponseAuthentication no
```

- ověříte příkazem

```
$ ssh -o PubkeyAuthentication=no server
Permission denied (publickey).
```

ROOT.CZ

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`
- (jdem.cz/8d6v9)

ROOT.CZ

Čtěte logy

- odhalíte anomálie
  - Neprošlo včera mail serverem osm milionů mailů?
  - Nezkouší někdo často používat sudo?
  - Nelozí něco divného po web serveru?
- 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**

ROOT.CZ

Otázky?

Petr Krčmář
petr.krcmar@iinfo.cz

ROOT.CZ