

# Ubuntu Server Hardening Script

Dokumentácia v 1.0

# Účel skriptu

Skript je určený na automatizovanú konfiguráciu systémov s OS Ubuntu Server, prípadne Debian s cieľom dosiahnutia základnej úrovne ich zabezpečenia. Účelom je aplikovanie všeobecných bezpečnostných odporúčaní, ktoré sú spoločné pre všetky systémy bez ohľadu na ich určenie. Pokročilé zabezpečenie (hardening) nie je cieľom tohto skriptu z dôvodu potrebnej znalosti systému, jeho požiadaviek a obmedzení.

## Používanie skriptu

Rozbaľte archív tar.gz.

Pred spustením skontrolujte nastavenia v súboroch \*.default:

- firewall.sh.default: základná konfigurácia iptables
- dennaKontrola.sh.default: bude spúšťaný každých 24h systémom Cron
- chkrootkit.default: logrotate konfigurácia pre Chkrootkit
- rkhunter.default: logrotate konfigurácia pre Rkhunter
- maldetect.default: logrotate konfigurácia pre Maldetect (potrebná manuálna inštalácia)
- snort.default: logrotate konfigurácia pre Snort (potrebná manuálna inštalácia)

Skript je potrebné spustiť v príkazovom riadku nasledovným príkazom:

```
sudo perl hardening.pl <cesta>
```

Kvôli zmene systémových nastavení je potrebné spúšťanie pomocou “sudo”.

<cesta>: cesta k adresáru, do ktorého budú uložené pomocné skripty

Od v0.8 je možné skript spúšťať opakovane, pričom sú kontrolované predchádzajúce nastavenia a v prípade potreby je používateľ vyzvaný potvrdiť prepísanie súborov (napr. FW).

## Opis funkcionality

Táto časť podrobne opisuje jednotlivé kroky, ktoré sú vykonávané skriptom. Pred zmenou jednotlivých konfiguračných súborov skript vytvorí ich zálohu vo formáte nazov\_suboru.bak.

Vykonávané kroky:

1. Nastavenia proxy
2. Firewall (iptables, psad)
3. Automatické bezpečnostné aktualizácie
4. Zakázanie prihlásenia systémových účtov

5. Hardening parametrov kernelu
6. Zákaz reštartu bez prihlásenia
7. Hardening SSH
8. Zakázanie login bannerov
9. Konfigurácia clamav, rkhunter, chkrootkit, maldetect, snort (ak sú nainštalované)
10. Nastavenie denných kontrol

## Odporúčané balíky

Je odporúčané, aby pred spustením skriptu boli nainštalované nasledovné balíčky:

```
psad unattended-upgrades clamav rkhunter chkrootkit
```

Ak niektorý balíček nie je prítomný, nastavenia sú preskočené. V prípade doinštalovania balíkov možno skript opätovne spustiť pre nastavenie nových balíčkov (ich prítomnosť je kontrolovaná automaticky).

## Nastavenia proxy

Skript deteguje aktuálne nastavenia proxy a umožňuje interaktívne nastavenie systémového proxy v súbore `/etc/environment`:

```
export http_proxy="http://$httpProxyIP:$httpProxyPort"
export https_proxy="http://$httpsProxyIP:$httpsProxyPort"
```

a tiež APT proxy (proxy pre balíčkovací systém) v súbore `/etc/apt/apt.conf.d/02proxy`:

```
Acquire::http::Proxy "http://httpProxyIP:$httpProxyPort";
```

Tieto nastavenia nie sú vyžadované pre ďalší beh skriptu, ale zlepšujú bezpečnosť systému definovaním jednotného výstupného bodu pre HTTP a HTTPS prevádzku.

## Firewall

Skript nastavuje štandardný linuxový firewall IPTables a adaptívny firewall PSAD.

### IPTables

Základné pravidlá vo forme “white-list” sú prednastavené v súbore `firewall.sh.default`, ktorý je skopírovaný do adresára zadaného pri spustení skriptu (štandardne `/home/<user>/scripts`).

Sú povolené iba služby potrebné pre beh samotného systému a pre ďalšie služby bežiace na serveri je potrebné doplnenie potrebných pravidiel. Súbor obsahuje aj odporúčania na zvýšenie bezpečnosti FW.

Pravidlá sa aplikujú spustením skriptu `firewall.sh`.

## PSAD

Následovné parametre sú nastavené v `/etc/psad/psad.conf`:

- `ENABLE_AUTO_IDS Y; #Automatické blokovanie podozrivej aktivity (v prípade problémov s konektivitou je potrebné nastaviť na N)`
- `IPTABLES_BLOCK_METHOD Y; #Blokovanie je realizované v IPTABLES`

Signatúry sú aktualizované v skripte `dennaKontrola`. Na zobrazenie štatistík je možné použiť príkaz `sudo psad -Status`.

## Automatické bezpečnostné aktualizácie

Sú zabezpečené prostredníctvom balíka `unattended-upgrades`. Skript nastaví v konfiguračnom súbore `/etc/apt/apt.conf.d/50unattended-upgrades` nasledovný riadok:

```
"${distro_id}:${distro_codename}-security"; #automatické bezpečnostné aktualizácie
```

Následne sú povolené periodické aktualizácie v `/etc/apt/apt.conf.d/10periodic`.

## Blokovanie systémových účtov

Blokovanie prihlásenia systémových účtov s `uid < 500` zabezpečuje skript `login-block.sh` nastavením login shell na `/usr/sbin/nologin`.

## Bezpečné nastavenie parametrov jadra OS

Následovné parametre sú nastavené v `/etc/sysctl.com`:

- `net.ipv4.ip_forward=0` #akázanie forwardovania paketov (ak zar. neslúži ako router).
- `net.ipv4.conf.all.rp_filter=1` #aktivovanie reverse-path filtra (základná ochrana proti spoofingu) . *Poznámka: Pri asymetrickom routovaní je potrebné nastaviť na 0.*
- `net.ipv4.conf.default.rp_filter=1` #rovnaké ako predchádzajúce nastavenie s rozdielom, že bude platné aj pre budúce (doplnené) interfacý.
- `net.ipv4.tcp_syncookies=>1` #aktivovanie mechanizmu syncookies, ktorý slúži na ochranu proti SYN-flood DoS útokom.
- `net.ipv4.conf.all.accept_redirects=0` #zákaz reagovania na ICMP redirect správy, ktoré môžu byť zneužívané na zmenu routovania paketov.
- `net.ipv4.conf.default.accept_redirects=0` #rovnaké ako predchádzajúce nastavenie s rozdielom, že bude platné aj pre budúce (doplnené) interfacý.
- `net.ipv4.conf.all.secure_redirects=0` #zákaz reagovania na ICMP redirect správy aj v prípade, že zdrojom je známy router.

- `net.ipv4.conf.default.secure_redirects=0` #rovnaké ako predchádzajúce nastavenie s rozdielom, že bude platné aj pre budúce (doplnené) interfaci.
- `net.ipv4.conf.all.send_redirects=0` #zákaz posielania ICMP redirect správ (nie sme router).
- `net.ipv4.conf.all.accept_source_route=0` #ignorovanie source route parametra v paketoch
- `net.ipv4.conf.default.accept_source_route=0` #rovnaké ako predchádzajúce nastavenie s rozdielom, že bude platné aj pre budúce (doplnené) interfaci.
- `net.ipv4.conf.all.log_martians=1` #zapnutie logovania adries s nekorektnou adresou.
- `net.ipv4.icmp_echo_ignore_broadcasts=1` #ignorovanie broadcast a multicast ping-u.
- `net.ipv4.icmp_ignore_bogus_error_messages=1` #vypnutie logovania chybných odpovedí.
- `net.ipv6.conf.all.disable_ipv6=1` #zakázanie IPV6

## Zakázanie reštartu bez prihlásenia

Zakázanie možnosti reštartovať server pomocou ctrl-alt-del na úvodnej prihlasovacej obrazovke bez prihlásenia. Podľa verzie systému je reštart zakázaný v `/etc/init/control-alt-delete.conf` alebo pomocou `systemctl` (`systemctl mask ctrl-alt-delete.target`).

## Základné zabezpečenie služby SSH

Skript nastavuje nasledovné parametre pre službu SSH v `/etc/ssh/sshd_config`:

- `PermitRootLogin no` #zakázanie prihlásenia prepoužívateľa root
- `X11Forwarding no` #zakázanie tunelovania výstupu grafických programov cez SSH
- `AllowTcpForwarding no` #zakázanie vytvárania SSH tunelov pre TCP
- `AllowGroups sshLogin` #povolenie prihlásenia len pre členov skupiny

## Zakázanie “bannerov” pri prihlásení

Vypnutie úvodných “bannerov” pri prihlasovaní používateľa cez konzolu a SSH pomocou vymazania obsahu súborov `/etc/issue` a `/etc/issue.net`.

## Bezpečnostné nástroje

Odporúčané anti-malware a IDS nástroje:

- Clamav (<http://www.clamav.net/index.html>)

- Rkhunter (<http://rkhunter.sourceforge.net/>)
- Chkrootkit (<http://freecode.com/projects/chkrootkit/>)
- Linux Malware Detect (<https://www.rfxn.com/projects/linux-malware-detect/>)
- Snort (<https://snort.org/>)

Pre program clamav sa nastaví v súbore `/etc/clamav/freshclam.conf` HTTP proxy, cez ktoré sa budú sťahovať denné aktualizácie databázy signatúr:

- `HTTPProxyServer $IP`
- `HTTPProxyPort $Port`

Pre Rkhunter, Chkrootkit a Maldetect sú základné nastavenia dostačujúce. Nastavia sa iba logovacie súbory a ich rotovanie pomocou logrotate (súbory `rkhunter.default`, `chkrootkit.default`, `maldetect.default`).

V súbore `/etc/rkhunter.conf`:

```
LOGDIR="/cesta/k/logu"
```

Pre Chkrootkit je log nastavený pri spúšťaní kontroly v skripte `dennaKontrola`.

## Konfigurácia denných kontrol

Do adresára `/etc/cron.daily` je skopírovaný skript `dennaKontrola.sh.default`, čo zabezpečí aktualizácie a kontrolu antivírusovými nástrojmi každých 24h.

Nakoniec zmení vlastníka adresára skriptov na používateľa v ktorého adresári je hardening skript spustený.

Poznámka: Chkrootkit a Rkhunter sú spúšťané v `dennaKontrola`, preto sú zakázané v `/etc/cron.daily` odobrať execute oprávnení.

## Inštalácia maldetect a snort

Nástroje maldetect a snort je možné nainštalovať pomocou skriptov `maldet-install.sh` a `snortsig-install.sh`.

## Možnosti ďalšieho zabezpečenia

### Vypnutie nepotrebných služieb

```
initctl list
```

```
initctl show-config <service-name>
```

```
update-rc.d -f <service-name> remove
```

Príklady služieb, ktoré je vhodné vypnúť: cups, samba, graphical environment...

## Zabezpečenie bootloadera heslom

`sudo grub-mkpasswd-pbkdf2` #generovanie hashu hesla)

Pridať nasledovné riadky do '/etc/grub.d/40\_custom' :

`set superusers="username"` #nastavenie superusera pre grub

`password_pbkdf2 <username> <vygenerovaný hash z predch. kroku>`

pridajte prepínač '--unrestricted' do 'CLASS' v '/etc/grub.d/10\_linux':

príklad: `CLASS="--class gnu-linux --class gnu --class os  
--unrestricted"`

`sudo update-grub` #refresh GRUB konfiguracie

Tieto príkazy povolia bootovanie bez zadania hesla, čo je vhodné pri vzdialenom reštartovaní. Na zmenu parametrov je potrebné zadať príslušné heslo.

## Zamknutie súboru resolv.conf

Nastavte immutable bit pre daný súbor v rozšírených atribútoch:

`chattr +i /etc/resolv.conf`

`lsattr <filename>` #kontrola príznakov, ktoré sú nastavené

Poznámka: Resolvconf balík bude generovať chybové hlásenia o zamietnutom prístupe pri zmene tohto súboru, ktoré je potom možné ignorovať.

## Kontrola integrity systému

Na kontrolu integrity súborového systému je možné použiť program Tripwire. Je vhodné ho nainštalovať hneď po konfigurácii OS, ideálne pred pripojením servera do Internetu.

Praktický úvod k tomuto programu je možné nájsť napr na:

<https://www.digitalocean.com/community/tutorials/how-to-use-tripwire-to-detect-server-intrusions-on-an-ubuntu-vps>

## Šifrovanie diskov

Šifrovanie diskov / partícií je vhodné napríklad v prípade, že potrebujete s PC cestovať a máte obavy z krádeže údajov na disku. V prípade serverov je vhodné zvažovať šifrovanie napr. v prípade, že obsahuje citlivé dáta a je pravdepodobnosť jeho servisovania mimo organizácie.

Na šifrovanie disku, prípadne partícií je na platforme Linux možné použiť nástroj LUKS (Linux Unified Key Setup): <http://www.root.cz/clanky/proc-a-jak-na-sifrovani-disku-v-linuxu/>

Ďalšou možnosťou je šifrovanie súborového systému, t.j. súborov a adresárov napr. Pomocou EncFS: <http://www.root.cz/clanky/encfs-sifrovani-souboru-jinak-a-bez-problemu/>

Takisto moderné distribúcie podporujú nastavenie šifrovania diskov už pri inštalácii.

## Referencie

[https://benchmarks.cisecurity.org/tools2/linux/CIS\\_Ubuntu\\_14.04\\_LTS\\_Server\\_Benchmark\\_v1.0.0.pdf](https://benchmarks.cisecurity.org/tools2/linux/CIS_Ubuntu_14.04_LTS_Server_Benchmark_v1.0.0.pdf)

<http://www.symantec.com/connect/articles/linux-firewall-related-proc-entries>

<http://cr.yp.to/syncookies.html>