

Textul si imaginile din acest document sunt licentiate

Attribution-NonCommercial-NoDerivs  
CC BY-NC-ND



Codul sursa din acest document este licentiat

Public-Domain

Esti liber sa distribui acest document prin orice mijloace consideri (email, publicare pe website / blog, printare, sau orice alt mijloc), atat timp cat nu aduci nici un fel de modificari acestuia. Codul sursa din acest document poate fi utilizat in orice fel de scop, de natura comerciala sau nu, fara nici un fel de limitari.

# Cum putem securiza un sistem Raspberry Pi?

Suntem obișnuiți să considerăm placa Raspberry Pi un sistem de dezvoltare a cărui scop este unul strict funcțional la fel ca și în cazul unei plăci echipate cu un microcontroler. Uităm adesea că avem de a face cu o placă ce rulează un sistem de operare și care necesită un set de reguli de securitate asemănătoare unui sistem de calcul de uz general (desktop sau server). În momentul în care integrăm placa de dezvoltare într-un proiect real, mai ales într-un proiect cu conectivitate Internet, lipsa implementării unor măsuri de securitate compromite fără discuție scopul proiectului – degeaba funcțional sistemul se comportă corect atâta timp cât el poate fi afectat foarte ușor de incidente malițioase sau accidente de utilizare.



Există multe documentații ce dezbat acest subiect și parcurgerea lor poate să creioneze mai bine dimensiunea și seriozitatea problemei:

Securing Your Raspberry Pi: From Passwords to Firewalls

<http://www.makeuseof.com/tag/securing-raspberry-pi-passwords-firewalls/>

IoT Security: Tips to Protect your Device from Bad Hackers

<https://www.hackster.io/charifmahmoudi/iot-security-tips-to-protect-your-device-from-bad-hackers-768093>

Make your Raspberry Pi more secure

<http://iot-projects.com/index.php?id=make-your-raspberry-pi-more-secure>

Securing Your Raspberry Pi

<https://www.madirish.net/566>

How to set up a secure Raspberry Pi web server, mail server and Owncloud installation

<https://www.pestmeester.nl/>

<https://www.robofun.ro/forum/>

## Raspberry Pi Firewall and Intrusion Detection System

<http://www.instructables.com/id/Raspberry-Pi-Firewall-and-Intrusion-Detection-Syst/>

## Setting up a (reasonably) secure home web-server with Raspberry Pi

<https://mattwilcox.net/web-development/setting-up-a-secure-home-web-server-with-raspberry-pi>

În cadrul lecției de față vom structura regulile de securitate specifice unei plăci Raspberry Pi în trei categorii dictate de nivelul la care se aplică:

- ✓ Securitate fizică
- ✓ Reguli minimale de operare
- ✓ Instrumente suplimentare de securitate

### Securitatea fizică a unei plăci Raspberry Pi

Fără a avea intenția de a cădea în desuet trebuie subliniată importanța integrității fizice a sistemului de calcul. Degeaba asigurăm o securitate logică impecabilă dacă din punct de vedere fizic sistemul este amenințat de incidente de funcționare electrică sau mecanică. Unele dintre cele mai importante reguli ce trebuie respectate în utilizarea plăcii Raspberry Pi sunt:

- ✓ Asigurarea unei **surse de alimentare stabilizată și de putere electrică suficient de mare**. Nu se recomandă utilizarea unor surse de tensiune ieftine. În cazul în care sistemul asigură o funcționalitate critică (controlul unei centrale termice sau a unui sistem de securitate) este recomandată utilizarea suplimentară a unui sistem UPS. Se recomandă utilizarea alimentatorului oficial al plăcii de dezvoltare:



<https://www.robofun.ro/raspberry-pi-si-componente/alimentator-raspberry-pi-2.5-a>

- ✓ Utilizarea unei **carcase** este absolut necesară. Această are rolul de proteja placa de dezvoltare de praf și alte mizerii dar și de a preîntâmpina distrugerea acesteia din cauza unei descărcări electrostatice. Improvizarea unei învelitori de carton sau din alte materiale moi nu este recomandă. Se



<https://www.robofun.ro/forum/>

poate alege o variantă potrivită în funcție de domeniul de utilizare a sistemului final:

<https://www.robofun.ro/raspberry-pi-si-componente/raspberry-cutii>

- ✓ Utilizarea unui **radiator** sau / și a unui **ventilator** pentru microprocesorul plăcii de dezvoltare nu se face doar în cazul forțării frecvenței procesorului (overclocking). Menținerea unei temperaturi scăzute pentru procesor crește durata de funcționare a acestuia și crește fiabilitatea sistemului final.



<https://www.robofun.ro/raspberry-pi-si-componente>

- ✓ Ignorată adesea, componenta ce stochează sistemul de operare al plăcii de dezvoltare – **cardul de memorie** – este un element extrem de important pentru buna funcționare a sistemului final. Carduri cu viteză mică de acces, uzate sau cu defecte de fabricație conduc la probleme ce pot fi anevoios de diagnosticat și crează multe bătăi de cap.



## Reguli minimale de operare

Aceste reguli trebuie implementate indiferent de scopul sistemului (dezvoltare sau proiect operațional) fiind esențiale în operare eficientă a plăcii de dezvoltare Raspberry Pi și reprezentând un nucleu de bune practici aplicabil pentru sisteme de calcul diverse (de la routere WiFi până la servere):

- ✓ **Schimbarea datelor de conectare implicite.** Minimal se recomandă schimbarea parolei utilizatorului *pi* cu ajutorul comenzii *passwd* dar mult mai bine este crearea unui cont utilizator nou și ștergerea contului *pi*. În acest fel sistemul nu poate fi accesat utilizând date de conectare bine cunoscute.
- ✓ **Utilizarea versiunii potrivite a sistemului de operare.** Pentru placa de dezvoltare Raspberry Pi sunt disponibile mai multe variante (distribuții) ale sistemului de operare Linux. Fiecare dintre aceste variante are un anumit specific ce este potrivit unui anumit domeniu de utilizare. Chiar distribuția oficială a plăcii, distribuția Raspbian, are două versiuni: *Raspbian Jessie with PIXEL* și *Raspbian Jessie Lite* (cea din urmă nu include interfața grafică ci doar consolă

de tip linie de comandă) – dacă sistemul final nu va include un ecran grafic este o risipă de resurse să se utilizeze versiunea completă (with PIXEL). În plus, un sistem de operare încărcat (cu multe pachete software instalate) prezintă mai multe riscuri de securitate.



(instalarea interfeței grafice doar pentru a controla sistemul de la distanță prin intermediul VNC este o opțiune extrem de infantilă, controlul cel mai bun al unui sistem Linux se realizează la nivel de linie de comandă – utilizați SSH)

- ✓ **Mentținerea software-ului la zi.** Instalarea ultimelor versiuni ale pachetelor software ce compun distribuția Linux nu este un moft ce ține de noi funcționalități introduse – apariția unor noi versiuni de programe este dictată de multe ori de rezolvarea unor probleme (bug-uri) de securitate.

```
!!! sudo apt-get update !!!  
!!! sudo apt-get upgrade !!!
```

- ✓ **Dezinstalarea sau dezactivarea pachetelor software nefolosite.** Fiecare pachet software este un posibil furnizor de probleme de securitate. Dezinstalarea pachetelor neutilizate este una dintre cele mai bune soluții. O completare a acestei reguli constă în dezactivarea serviciilor neutilizate (de exemplu, serviciul SSH reprezintă un risc ridicat de securitate, este recomandată oprirea acestui serviciu dacă nu îl utilizăm). O listă a serviciilor (a programelor ce pornesc odată cu sistemul de operare) se poate obține cu ajutorul comenzii:

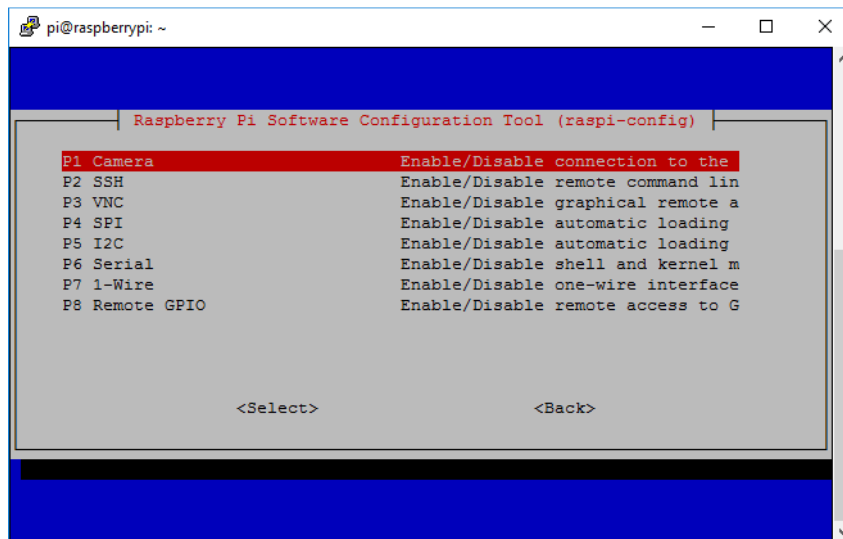
```
sudo service --status-all | grep +
```

dezactivarea unui serviciu se va face cu ajutorul comenzii:

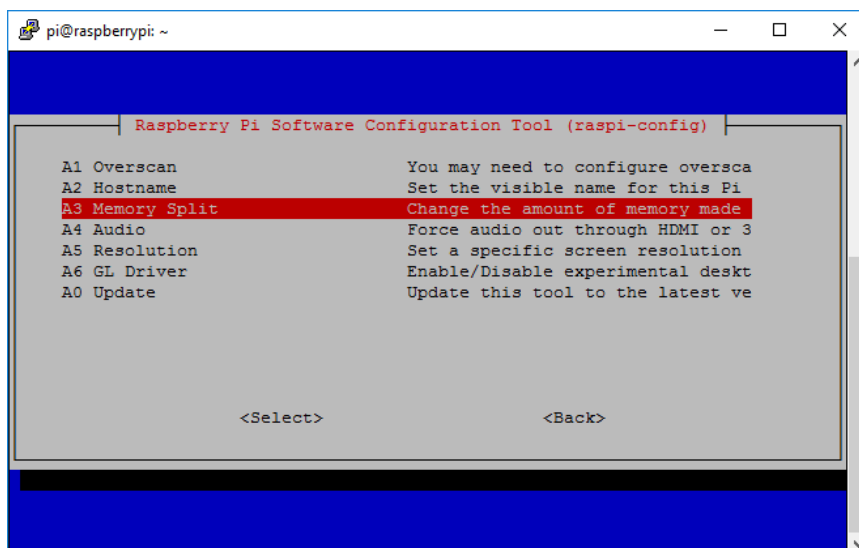
```
sudo systemctl disable nume_serviciu
```

- ✓ **Configurarea resurselor hardware în conformitate cu scopul sistemului.**  
Chiar dacă în sine o resursă hardware, activată și neutilizată, nu implică o vulnerabilitate de securitate, este bine să avem activate doar resursele hardware utilizate (aici vorbim de porturile I/O, I2C, SPI, port serial etc.). Acest lucru se poate configura cu ajutorul comenzii:

```
sudo raspi-config
```



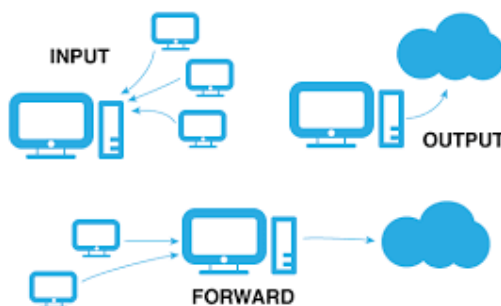
Un exemplu suplimentar îl reprezintă memoria plăcii de dezvoltare, este recomandată micșorare memoriei alocate procesorului grafic dacă nu utilizăm interfața grafică eliberând astfel mai multă memorie pentru CPU (se poate face acest lucru din Advanced -> Memory Split).



## Instrumente suplimentare de securitate

În cele ce urmează vom prezenta o serie de programe care, utilizate corect, pot crește nivelul de securitate a unui sistem Raspberry Pi.

**Firewall/iptables** – este un mecanism intern al sistemului de operare ce permite filtrarea comunicațiilor de rețea. Filtrarea se realizează după reguli încadrate în trei mari categorii: INPUT – conexiuni de rețea de intrare, OUTPUT – conexiuni de rețea de ieșire, FORWARD – conexiuni de rețea ce traversează sistemul. Cu ajutorul acestui mecanism se poate decide ce conexiuni de rețea va accepta sistemul nostru, de la ce adrese, ce servicii (ce porturi) sunt accesate etc. De exemplu, următoarele două instrucțiuni:



```
sudo iptables -A INPUT -s xxx.xxx.xxx.xxx -j ACCEPT  
sudo iptables -A INPUT -j REJECT
```

vor avea ca efect acceptarea conexiunilor de la adresa IP `xxx.xxx.xxx.xxx` și rejectarea oricărei alte conexiuni – sistemul nostru va putea fi accesat doar de la adresa IP indicată. Aceasta este o practică foarte bună dacă adresele sistemelor cu care comunică sistemul nostru sunt fixe. Pentru a lista toate regulile de filtrare se poate folosi comanda:

```
sudo iptables -L
```

**Fail2ban** – este un utilitar ce permite blocarea comunicației de rețea cu o anumită adresă IP în urma activității malițioase generate de la acea adresă: mai multe încercări de conectare la distanță nereușite, scanarea de vulnerabilități de la distanță ș.a.m.d. Funcționarea acestuia se bazează pe scanarea fișierelor jurnal ale diverselor servicii sistem (SSH, web, mail) și, în cazul detectării unor activități rău intenționate, pe introducerea unei restricții temporare în sistemul iptables.



Pentru utilizare primul pas este instalarea pachetului software:

```
sudo apt-get install fail2ban
```

După care se va edita fișierul `/etc/fail2ban/jail.local` și se vor introduce reguli de supraveghere. Următorul bloc este un exemplu bun pentru serviciul SSH (orice adresă IP cu trei încercări nereușite de conectare va fi blocată timp de 15 minute, excepție făcând adresele locale din clasa 192.168.0.0/16):

```
[ssh]
enabled = true
port = ssh
filter = sshd
action = iptables[name=SSH, port=ssh, protocol=tcp]
mail-whois-lines[name=%(__name__)s, dest=%(destemail)s, logpath=%(logpath)s]
logpath = /var/log/auth.log
maxretry = 3
bantime = 900
ignoreip = 192.168.0.0/16
```

Pentru ca modificările în fișierul de configurare să aibă efect vom reporni serviciul:

```
sudo /etc/init.d/fail2ban restart
```

Mai multe informații despre programul *fail2ban* puteți găsi la adresa:

[http://www.fail2ban.org/wiki/index.php/Main\\_Page](http://www.fail2ban.org/wiki/index.php/Main_Page)



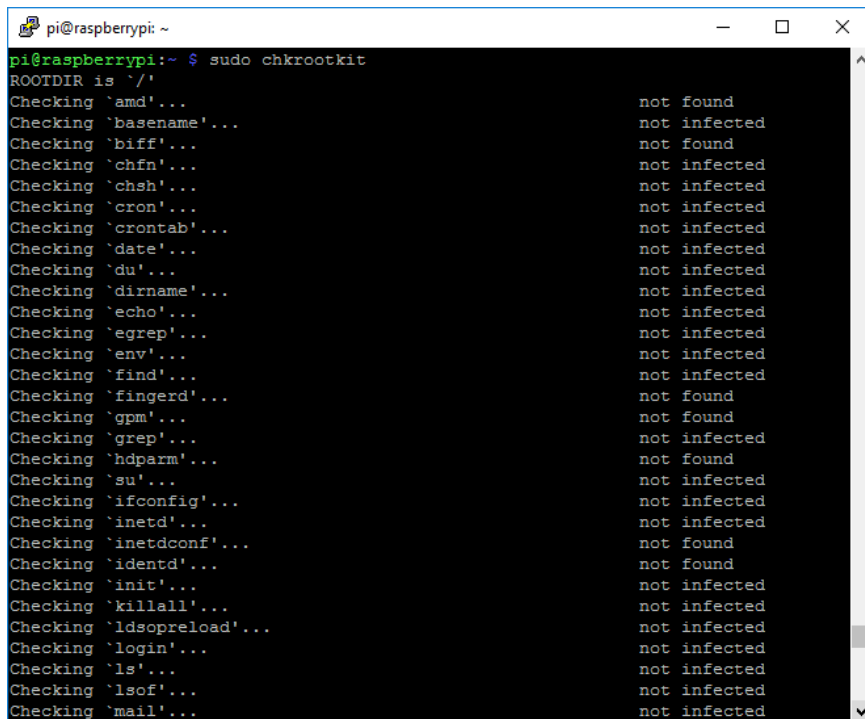
**rkhunter & chkrootkit** – sunt două programe menite să scaneze sistemul împotriva unor aplicații malițioase (rootkit-uri). Chiar dacă incidența infectării cu aplicații de tip virus este mică în cazul sistemelor Linux asta nu înseamnă că nu există amenințări la adresa sistemului de fișiere local. Rootkit-urile sunt programe, cel mai adesea rău intenționate, care modifică fișiere sistem ascunzând alte aplicații sau permițând accesul de la distanță unor persoane neautorizate. De cele mai multe ori deținătorul sistemului nici nu e conștient de infectarea acestuia. Cele două aplicații verifică integritatea fișierelor sistem și detectează aplicațiile de tip rootkit. Instalarea aplicațiilor se face cu ajutorul comenzii:

```
sudo apt-get install chkrootkit rkhunter libwww-perl
```



Rularea aplicației *chkrootkit* se face cu ajutorul comenzii:

```
sudo chkrootkit
```

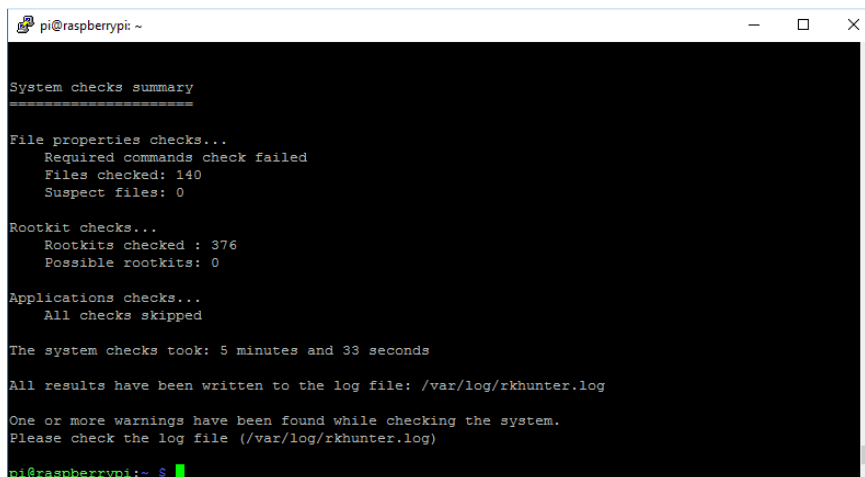


```
pi@raspberrypi: ~  
pi@raspberrypi:~$ sudo chkrootkit  
ROOTDIR is '/'  
Checking `amd'... not found  
Checking `basename'... not infected  
Checking `biff'... not found  
Checking `chfn'... not infected  
Checking `chsh'... not infected  
Checking `cron'... not infected  
Checking `crontab'... not infected  
Checking `date'... not infected  
Checking `du'... not infected  
Checking `dirname'... not infected  
Checking `echo'... not infected  
Checking `egrep'... not infected  
Checking `env'... not infected  
Checking `find'... not infected  
Checking `fingerd'... not found  
Checking `gpm'... not found  
Checking `grep'... not infected  
Checking `hdparm'... not found  
Checking `su'... not infected  
Checking `ifconfig'... not infected  
Checking `inetd'... not infected  
Checking `inetdconf'... not found  
Checking `identd'... not found  
Checking `init'... not infected  
Checking `killall'... not infected  
Checking `ldsopreload'... not infected  
Checking `login'... not infected  
Checking `ls'... not infected  
Checking `lsof'... not infected  
Checking `mail'... not infected
```

Aplicația *rkhunter* se poate utiliza cu ajutorul comenzilor:

```
sudo rkhunter --update
```

```
sudo rkhunter --check
```



```
pi@raspberrypi: ~  
System checks summary  
=====
```

```
File properties checks...  
  Required commands check failed  
  Files checked: 140  
  Suspect files: 0
```

```
Rootkit checks...  
  Rootkits checked : 376  
  Possible rootkits: 0
```

```
Applications checks...  
  All checks skipped
```

```
The system checks took: 5 minutes and 33 seconds
```

```
All results have been written to the log file: /var/log/rkhunter.log
```

```
One or more warnings have been found while checking the system.  
Please check the log file (/var/log/rkhunter.log)
```

```
pi@raspberrypi:~$
```



**logwatch** – este o aplicație de monitorizare și raportare pentru fișierele jurnal sistem (log-uri). Chiar dacă este un instrument pasiv (de monitorizare), utilizarea acestuia poate preveni foarte multe incidente de securitate prin alertarea timpurie a deținătorului sistemului. Instalarea acestui program se face cu ajutorul comenzii:

```
sudo apt-get install logwatch
```

După instalare aplicația *logwatch* va rula zilnic și va raporta prin email către administratorul sistemului (utilizatorul *root*) sumarul fișierelor jurnal sistem. Ajustarea parametrilor de funcționare se poate face prin editarea fișierului */usr/share/logwatch/default.conf/logwatch.conf* . Testarea aplicației se poate face cu ajutorul comenzii:

```
sudo logwatch --range=today
```

Instrumentele software prezentate nu reprezintă decât câteva exemple de aplicații ce pot ajuta utilizatorii să mențină un nivel de securitate adecvat pentru sistemele lor Raspberry Pi. Există și alte aplicații ce pot fi utilizate în funcție de scopul și domeniul de utilizare a sistemului. Vă recomandăm încă două aplicații interesante de explorat:

Snort – sistem de detecție și prevenție a intruziunilor (IDPS), foarte util în cazul sistemelor de tip gateway.

<https://www.snort.org/>



ClamAv – sistem open-source antivirus, necesar în cazul implementării unor servere de fișiere.

<https://www.clamav.net/>