



# Linux i rootkit'y

? U XmgngfYa cdYfUWbma c bUg\_ca dfca ]rck lã BUk ]Y'Y gdcg:Vl k " 6UFXnc Wãgfc lk cfrmgjõ k ]fi gnãfrc'lbm] ]bbma Uk UFY k W'i dcnmg\_Lb]UWbbrnW ]bzcfã UW] i a ]YgnVibcnW bUUh\_cck UbrnW \_ca di YfUW" K XcV]Y dck gnYWbc W]g]WY -bYfbYfz dcdi `UfbY gHÜã gjõ dfi Vmk m\_cfrmgfLb]Ua cVh\_ca di Yfí k Xc gk cfnYb]Ug]WYdfnYgãdWY^ NUdca cVã fi brnW Xn]i f k gngfYa UW cdYfUWbbrnW ]bgfU i Y gjõ a Uk UFYz\_hí fy[ c nLXUb]Ya Yghk m\_cbnk Lb]Y c\_fY `cbY[ c hmoi UH\_j "K gnggh\_]Y nLUf cbY \_ca di Yfmrnk " nca V]YzWY\_Uã bUWbfrUbmfcu\_LhfcndcWãdV]UUh\_j bUcZ]Ufõ 'U\_ã a c YVnã'bd" gYfk Yf ]bgmii W] frãXck Y^ NUFU cbY \_ca di Yfmrnk cfrã hnk " VctbYfz\_hí fmXc gYfck Lb]U bUWã WY^ k m\_cfrmgf Y gjã = F 7 " K gngfYa ]Y @]bi l a ]a c VUFXnc gnWY^bY^ UFW]Y\_hí fm gLã Y[ c 'ãXfU gngfYa i ž a c bU nbUY ä `i\_ž nU dca cVã \_hí fmW a c `]k Y gHÜY gjõ k dfck UXnYb]Y n c `]k Y[ c \_cXi " GLã \_cX k k ]õ\_gnc W] gngfYa í k @]bi l fãk mW b]Y Yghb]WYnd]YWbznãVc a i g] bU'd]Yfk i nng\_Lã dfLk UfcchfU' K i nng\_Lb]i dfLk fcchfU dca cVãY gã hnk " F cct? ]hmí Gã hc dfc[ fLã mdca cVãY k i \_frik Lb]i n c `]k Y[ c \_cXi k gngfYa ]Y" F cct? ]hmbUWã WY^XngfmrVi ck LbY gã nU dca cVã gdfYdLufck LbrnW dUWY\_ nLk ]YfUãWãW bUfnoXn]U gngfYa ck YZ U WlUgYa bLk Yh'ãXfc gngfYa i k W'i i \_fmrV]UXn]U Lb]U\_cXi n c `]k Y[ c" 7 nLgYa dcXa ]Yb]UbmYghd'\_ V]bUfbrmdfcWg gg\Xbd" k W'i i a c `]k ]Yb]UnXU bY[ c nUc[ck Lb]U gjõ Xc gngfYa i nU dca cVã gdfWU bY[ c `Lg U'

-gfb]Y Y \_]\_Ua YrcX bU i Wfcb]Yb]Y gjõ dfnYX Y[ c hmoi UH\_Lã ]" >YXbã n bU'dfcggnW nLgUk 'U\_]Y^bUY mg]õ lfrma UãZ Ygh\_cfrmgfLb]Y YXnb]Y n dcXd]gUbrnW fYdcnrcf]i k n dU\_]YfLã ] Xc XUbY^XngfmrVi W] 8 UY bLã hc [ k UfUWã dck gnYWbc W]\_cXi k b]W nLk UfmrW fYk " \_ca dfca ]fUWU gYfk Yfí k n dUWã\_Lã ] VãXn]Y gnWY^ fncdncbLbUe" =bbã a YrcXã Ygh gdfLk XnLb]Y gngfYa i nU dca cVã bUfnoXn] g\_Lbi 'ãWãW d\_] ] i dfLk b]Yb]U dcX\_ãhYa na ]Lb a c[ãWãW k ]UXVnã c dfi V]Y dfnYWk mWb]U gngfYa i "

>YXbma n H\_]W bUfnoXn] Yghdfc[ fLã **chkrootkit**ž XUY bLã cb a c `]k c ä dfnYg\_Lbck Lb]U gngfYa i k Xc ä gnV\_] gdcg' V cvfLhi 'ãWãWnã 'U\_] dfc[ fLã `i V d'\_ b]Y ncgfU mdcXa ]Yb]cbY" K nk c Lb]Y dfc[ fLã i Vn dUfLã Yfí k k m\_cbi Y g\_Lbck Lb]Y n dY bna k mk ]YhYb]Ya gnWY[ í í k Wã a c Y b]Y Vnã WmY^bYz XUY[ c' dc' YWã k nk c Lb]Y bUgãdi 'ãW.

W\_fcc]h]e

HU\_]Y k nk c Lb]Y k mk ]Yh] dc dfnYg\_Lbck Lb]i \_ca di YfU YXnb]Y cgfnY Yb]U' BUY mXc\_ Lxb]Y dfnYbU]nck lã k ntb]\_ Xn]U Lb]U g\_LbYfLã Vc b]Y nLk gnY k g\_Lhi Y'cb bUdfLk Xn]k á ]bzY\_Wã" 8`Udfm\_ LXi k m^WY n' dfc[ fLã i .

Yã\$. D5 7? 9H GB = : 9F f]g]b#A W]Yb]h O, ++Q

cnbUWU YXnb]Y hmYz Y k na ]Yb]cbmdfcWg fK W]Yb]h E'blg i Wi Y'VfcLXWã] k žVã k 'dfmLUX\_j \_]Yb]U 8 < 7 D' Ygh'U\_ bU'VUFXn]Y^bcfa Ubrna nLUWck Lb]Ya "

>YgnWY W]\_Lk gna ] VUFXn]Y^ fcnVi Xck Ubrna dfc[ fLã Ya Xc k ngri \_]k Lb]U F cct? ]fí k Ygh **rkhunter**" A U cb c k ]Y Y VUFXn]Y^ n c cbY a YWU]na m g\_Lbck Lb]Uã U Wã bUWY\_Lk gnYz a c bU dcXn]Y]ã dfcWg g\_Lbck Lb]U bU YfUdmf]\_Lbck Lb]Y dfLk ž g\_Lbck Lb]Y V]bUf]i k ž k ngri \_]k Lb]Y F cct? ]fí k ž ]hd'z 8 cXU\_hck c' gLã 'dfc[ fLã 'dc k nk c Lb]i k \_cbg:' k VUFXn]Y^ dfnY'fmgmgdcg' V dfnYXgUk ]U\_c'Y'by YfUdmf]\_Lbck Lb]U c fU'k ntb]\_ ] gk c Y^dfUWfí

Dfmr\_ Lx'k nk c Lb]U hm\_c'g\_LbYfU dcfí k .

f\_`i bYf!!YbWY dcf]g

```
[ Rootkit Hunter version 1.3.2 ]
Checking the network...
Performing check for backdoor ports
Checking for UDP port 2001 [ Not found ]
Checking for TCP port 2006 [ Not found ]
Checking for TCP port 2123 [ Not found ]
Checking for TCP port 14856 [ Not found ]
Checking for TCP port 47107 [ Not found ]
Checking for TCP port 60922 [ Not found ]

System checks summary
=====
File properties checks...
All checks skipped

Rootkit checks...
All checks skipped

Applications checks...
All checks skipped

The system checks took: 2 seconds

All results have been written to the logfile (/var/log/rkhunter.log)

No warnings were found while checking the system.
```

A m`ōZ Y k gngVhZLb] @]bi | flē\_ī fmgā dfnY\_cbLb] c Y[ c b]YdcXk U Ubna VYnd]YwY gk ]Y dck ]bb] nU]bYfYgck Uā gjō k na ]Yb]cbna ] k m Y^dfc[ fUa Ua ]z YVm]W`\_ca di hYfmb]Y nUg] ] mUfa ]] VctbYfi "