0×00 简介

hardeningone是一款类Unix系统安全检查bash shell脚本，适合信安审计人员或信安测试人员使用。作者写这个检测脚本的初衷是为了做系统安全审计、网络安全配置和系统安全维护之用。

该脚本主要包括如下功能内容：

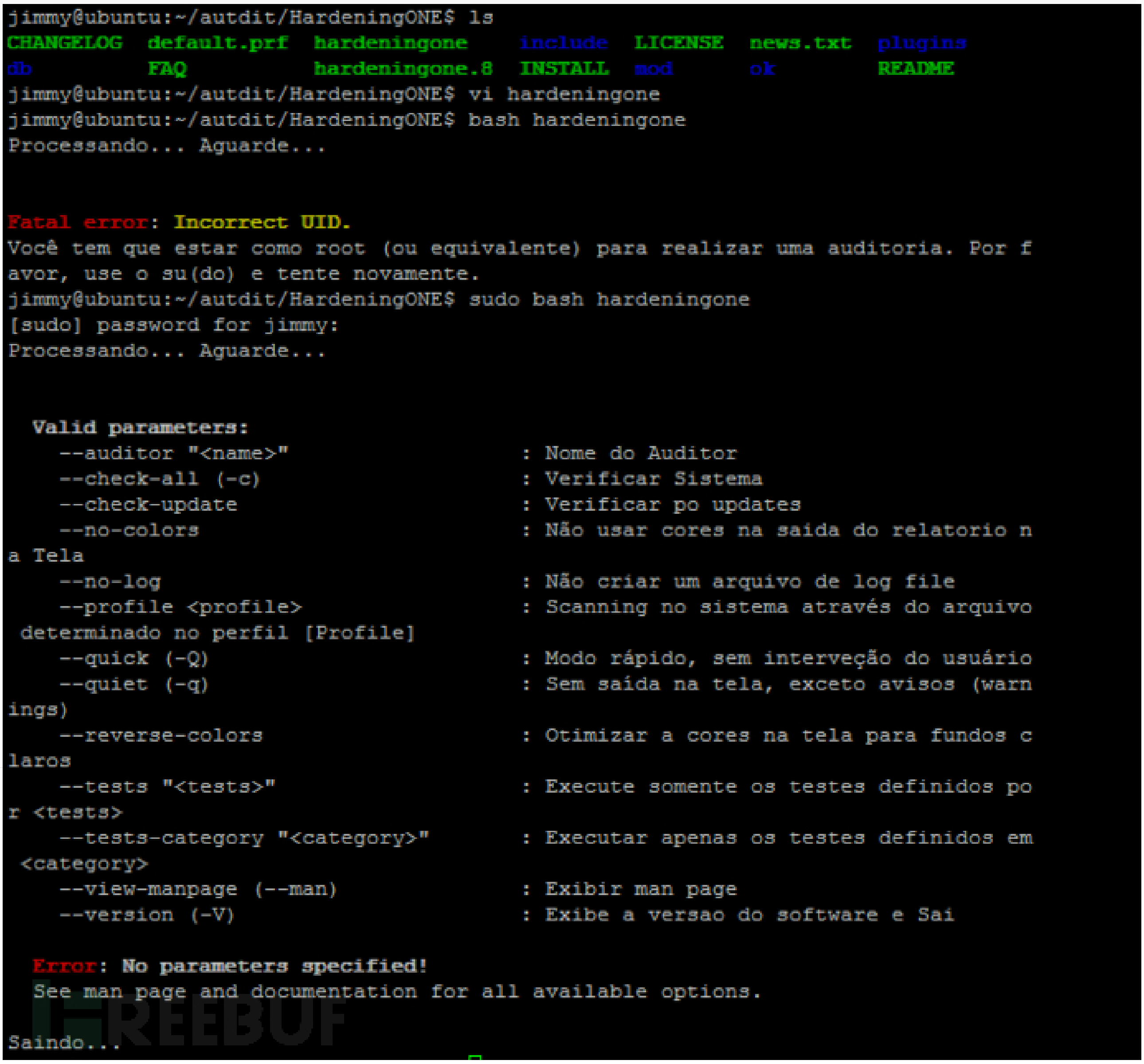
（1）系统基本安全检查

（2）文件完整性校验

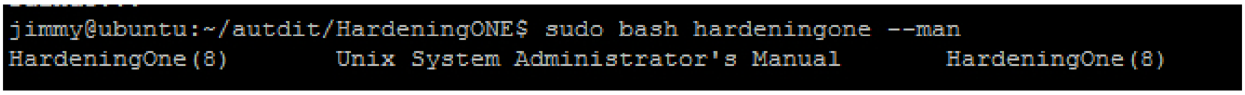
（3）系统与文件取证

（4）运行情况监控与报告

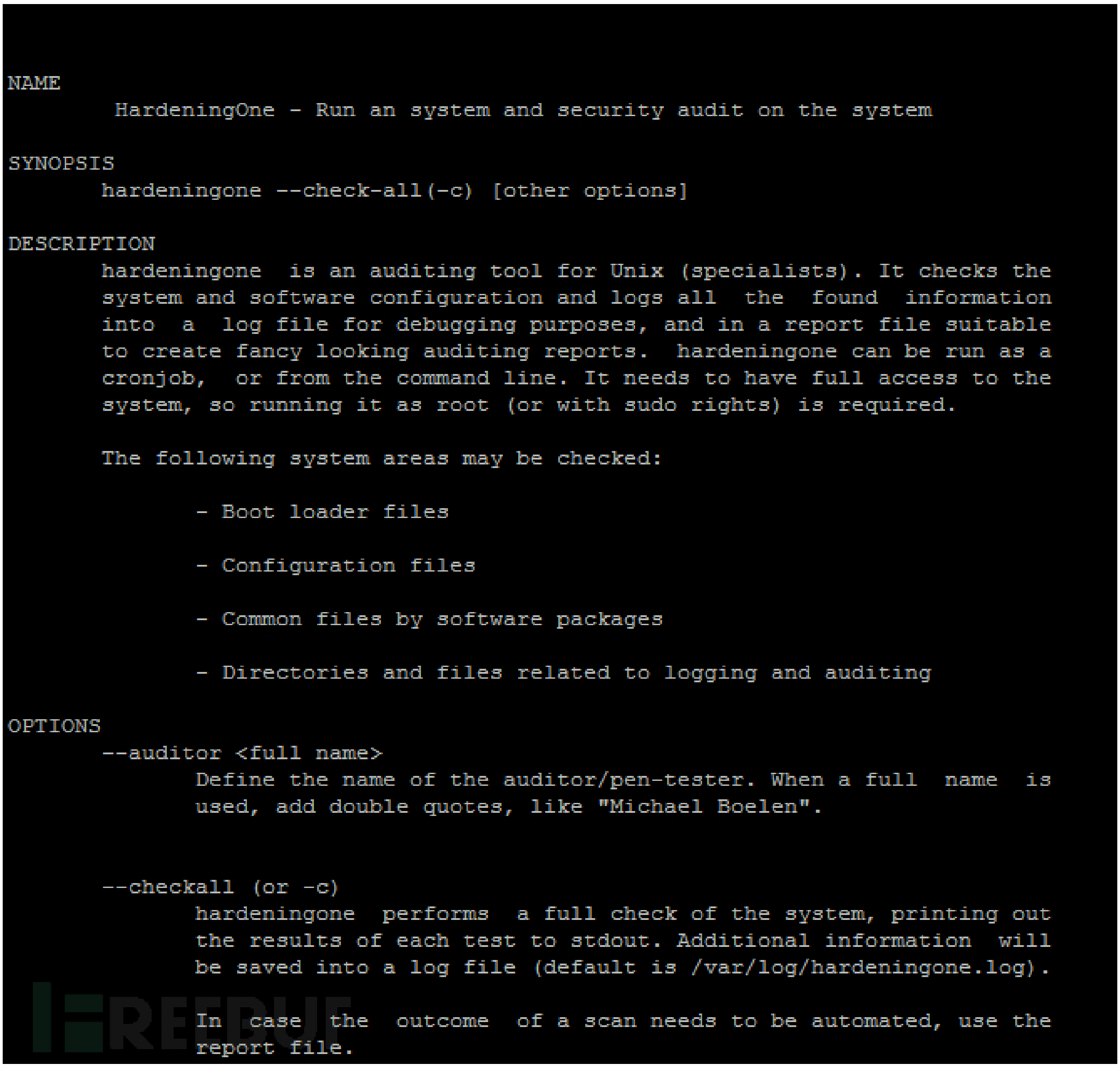
（5）其他的一些还在调试的功能



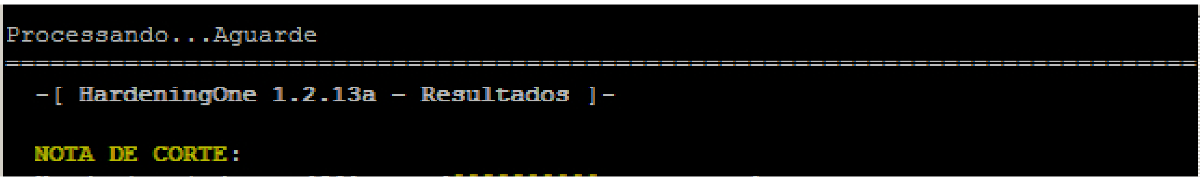
```
jimmy@ubuntu:~/autdit/HardeningONE$ ls
CHANGELOG  default.prf  hardeningone    include  LICENSE  news.txt  plugins
db         FAQ          hardeningone.8  INSTALL  mod      ok        README
jimmy@ubuntu:~/autdit/HardeningONE$ vi hardeningone
jimmy@ubuntu:~/autdit/HardeningONE$ bash hardeningone
Processando... Aguarde...


Fatal error: Incorrect UID.
Você tem que estar como root (ou equivalente) para realizar uma auditoria. Por f
avor, use o su(do) e tente novamente.
jimmy@ubuntu:~/autdit/HardeningONE$ sudo bash hardeningone
[sudo] password for jimmy:
Processando... Aguarde...


  Valid parameters:
    --auditor "<name>"                  : Nome do Auditor
    --check-all (-c)                    : Verificar Sistema
    --check-update                      : Verificar po updates
    --no-colors                         : Não usar cores na saida do relatorio n
a Tela
    --no-log                            : Não criar um arquivo de log file
    --profile <profile>                 : Scanning no sistema através do arquivo
 determinado no perfil [Profile]
    --quick (-Q)                        : Modo rápido, sem interveção do usuário
    --quiet (-q)                        : Sem saída na tela, exceto avisos (warn
ings)
    --reverse-colors                    : Otimizar a cores na tela para fundos c
laros
    --tests "<tests>"                   : Execute somente os testes definidos po
r <tests>
    --tests-category "<category>"       : Executar apenas os testes definidos em
 <category>
    --view-manpage (--man)              : Exibir man page
    --version (-V)                      : Exibe a versao do software e Sai

  Error: No parameters specified!
  See man page and documentation for all available options.

Saindo...
```



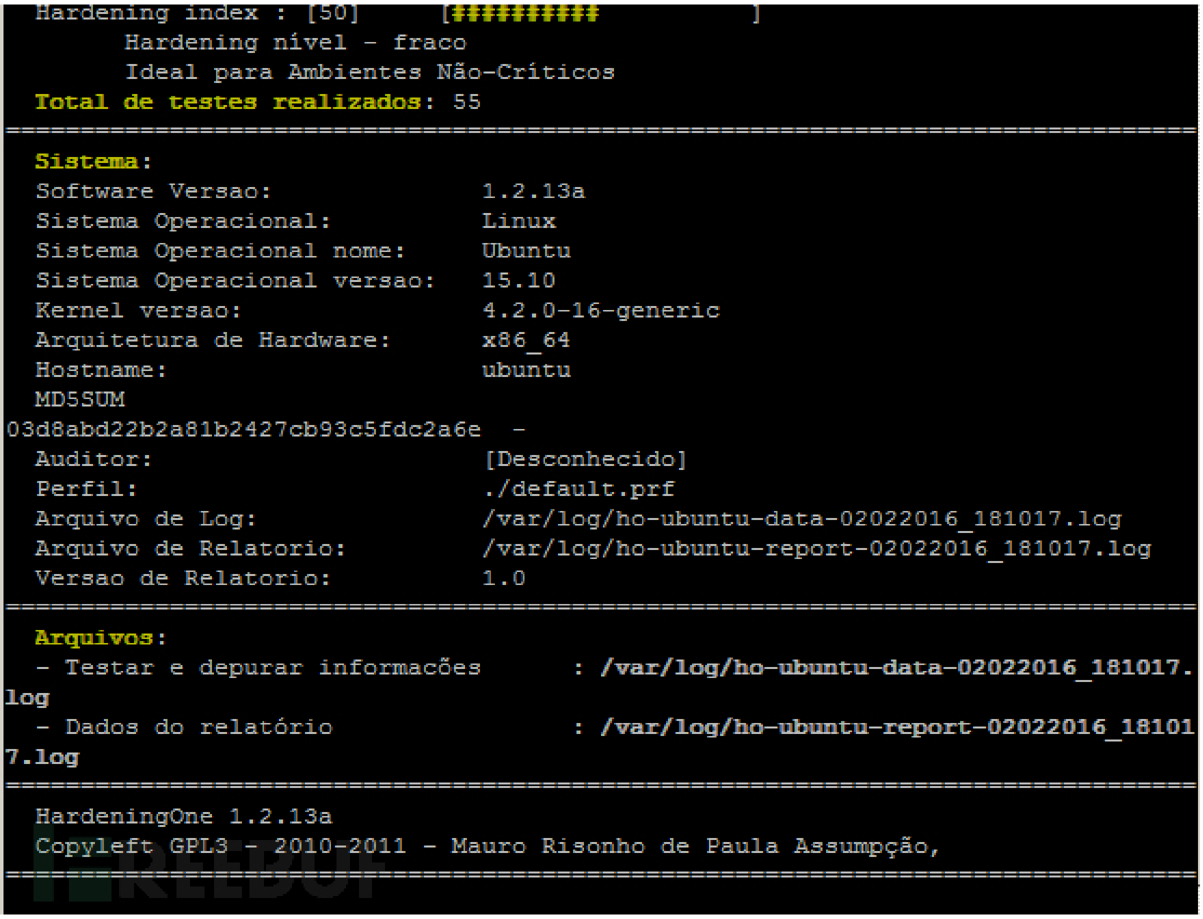
```
jimmy@ubuntu:~/autdit/HardeningONE$ sudo bash hardeningone --man
HardeningOne(8)          Unix System Administrator's Manual         HardeningOne(8)
```



```
NAME
        HardeningOne - Run an system and security audit on the system

SYNOPSIS
       hardeningone --check-all(-c) [other options]

DESCRIPTION
       hardeningone  is an auditing tool for Unix (specialists). It checks the
       system and software configuration and logs all  the  found  information
       into  a  log file for debugging purposes, and in a report file suitable
       to create fancy looking auditing reports.  hardeningone can be run as a
       cronjob,  or from the command line. It needs to have full access to the
       system, so running it as root (or with sudo rights) is required.

       The following system areas may be checked:

              - Boot loader files

              - Configuration files

              - Common files by software packages

              - Directories and files related to logging and auditing

OPTIONS
       --auditor <full name>
              Define the name of the auditor/pen-tester. When a full  name  is
              used, add double quotes, like "Michael Boelen".


       --checkall (or -c)
              hardeningone  performs  a full check of the system, printing out
              the results of each test to stdout. Additional information  will
              be saved into a log file (default is /var/log/hardeningone.log).

              In  case  the  outcome  of a scan needs to be automated, use the
              report file.
```



```
Processando...Aguarde
==============================================================================
  -[ HardeningOne 1.2.13a - Resultados ]-

  NOTA DE CORTE:
```



```
  Hardening index : [50]     [###########          ]
        Hardening nível - fraco
        Ideal para Ambientes Não-Críticos
  Total de testes realizados: 55
================================================================================
  Sistema:
  Software Versao:              1.2.13a
  Sistema Operacional:          Linux
  Sistema Operacional nome:     Ubuntu
  Sistema Operacional versao:   15.10
  Kernel versao:                4.2.0-16-generic
  Arquitetura de Hardware:      x86_64
  Hostname:                     ubuntu
  MD5SUM
03d8abd22b2a81b2427cb93c5fdc2a6e  -
  Auditor:                      [Desconhecido]
  Perfil:                       ./default.prf
  Arquivo de Log:               /var/log/ho-ubuntu-data-02022016_181017.log
  Arquivo de Relatorio:         /var/log/ho-ubuntu-report-02022016_181017.log
  Versao de Relatorio:          1.0
================================================================================
  Arquivos:
  - Testar e depurar informacões      : /var/log/ho-ubuntu-data-02022016_181017.
log
  - Dados do relatório                : /var/log/ho-ubuntu-report-02022016_18101
7.log
================================================================================
  HardeningOne 1.2.13a
  Copyleft GPL3 - 2010-2011 - Mauro Risonho de Paula Assumpção,
================================================================================
```

0×01 安装

hardeningone无需进行安装，仅仅只需你通过github下载到系统中，在文件目录里面运行即可（注意文件运行权限）。如果你想让该程序一定要安装的话，按照如下步骤进行：

–创建一个目录，例如/usr/local/hardeningone，然后将压缩包解压到这个目录（tar xfvz hardeningone-version.tar.gz）

–使用hardeningone.spec文件创建一个RPM包，可以运行如下命令实现

run ‘rpmbuild -ta hardeningone-version.tar.gz’ (建立一个RPM包)

run ‘rpm -ivh ’ (安装RPM包)

0×02 更新

如果你想图省事进行更新，你可以写个shell脚本去移除旧的版本，然后解压安装新的版本。

0×03 支持的系统

考虑到不同的系统平台环境有不同的安全策略设定，hardeningone是基于BSD和Linux进行开发的脚本。主要适用于如下系统：

Linux

FreeBSD

OpenBSD

```
OpenBSD

Mac OS X

Solaris
```

0×04 使用

hardeningone能够作为Cronjob来运行，或者直接在命令行下运行，由于检查内容中涉及部分高权限项，故运行该脚本前需要赋予足够的权限，例如以root身份运行或给予sudo权限。

```
OPTIONS
       --auditor
              Define the name of the auditor/pen-tester. When a full  name  is
              used, add double quotes, like "Michael Boelen".



       --checkall (or -c)
              hardeningone  performs  a full check of the system, printing out
              the results of each test to stdout. Additional information  will
              be saved into a log file (default is /var/log/hardeningone.log).

              In  case  the  outcome  of a scan needs to be automated, use the
              report file.

       --check-update (or --info)
              Show program, database and update information

       --cronjob
              Perform automatic scan with cron safe  options  (no  colors,  no
              questions, no breaks).

       --no-colors
              Do not use colors for messages, warnings and sections.

       --no-log
              Redirect all logging information to /dev/null, prevent sensitive
              information to be written to disk.


       --quick (-Q)
              Do a quick scan (don't wait for user input)

       --quiet (-q)
              Try to run as silent as possible, showing  only  warnings.  This
              option activates --quick as well.
```

```
    --reverse-colors
                  Optimize screen output for light backgrounds.

    --tests TEST-IDs
                  Only run the specific test(s). When using multiple tests, add
                  quotes around the line.

                  Multiple parameters are allowed, though some parameters can only
                  be used together with others. When running hardeningone without
                  any parameters, help will be shown and the program will exit.
```

项目地址

***参考来源：github，我是酱油男编译，转载请注明来自FreeBuf黑客与极客（FreeBuf.COM）**