服务器安全加固指南

V1.0

HPB 芯链

2018 年 10 月

目录

第1章 阅读总览

1.1 适用范围

为了提高 HPB 节点服务器的安全性，HPB 芯链决定采纳安全审计公司的服务器安全加固方案，适用于使用 Linux 版本操作系统的 HPB 节点服务器，本指南旨在指导节点用户对其服务器进行安全合规性检查和配置。

1.2 阅读建议

编号	内容	说明
1	服务器安全检测脚本使用指导	指导节点用户下载、运行服务器安全检测脚本，检查服务器安全配置。详情参考第二章。
2	检查项详情	详细介绍脚本里涉及到的 22 个检查项及其配置修改步骤。详情参考第三章。

第2章 服务器安全监测脚本使用指导

2.1 使用步骤

为了简化用户的操作步骤，HPB 芯链将提供服务器安全检测脚本，用户运行脚本后将自动对服务器的 Linux 系统进行安全配置检查。

编号	步骤	说明
1	下载脚本	命令："**git clone** *https://github.com/hpb-project/systemcheck*"
2	设置权限	命令："**cd** *systemcheck*" 命令："**chmod +x** *systemcheck.sh*"
3	运行脚本	命令："**sudo** *./systemcheck.sh*" 提示：用户需根据提示输入当前账户的登录密码； 出现"未安装 chkconfig,是否安装(y/n)"时，用户需输入"y"。
4	查看结果	命令:"**vi** *servercheck.txt*" 提示：通过的检查项会提示"安全"，未通过的会提示"不安全"。 如需修改配置，用户可参考第三章检查项详情。 第 n 个检查项对应第 3.n 节。

HPB 芯链建议用户将运行结果中未通过的检查项修改为安全配置，修改步骤详见第三章。

2.2 使用示例

(1) 步骤 1 下载服务器安全检测脚本

打开终端，输入"**git clone** *https://github.com/hpb-project/systemcheck*";

```
hpb@dell-PowerEdge-R730:~$ git clone https://github.com/hpb-project/systemcheck
Cloning into 'systemcheck'...
remote: Enumerating objects: 8, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (6/6), done.
Unpacking objects: 100% (8/8), done.
remote: Total 8 (delta 2), reused 8 (delta 2), pack-reused 0
Checking connectivity... done.
hpb@dell-PowerEdge-R730:~$
```

(2) 步骤 2 设置文件权限

输入"**cd** *systemcheck*"

```
hpb@dell-PowerEdge-R730:~$ cd systemcheck
hpb@dell-PowerEdge-R730:~/systemcheck$
```

继续输入设置文件权限

输入”**chmod +x** *systemcheck.sh*”

```
hpb@dell-PowerEdge-R730:~/systemcheck$ chmod +x systemcheck.sh
hpb@dell-PowerEdge-R730:~/systemcheck$
```

(3) 步骤 3 运行脚本

输入”**sudo** *./systemcheck.sh*”,根据提示输入当前用户的登录密码，文件将会自动检测服务器配置；

```
hpb@dell-PowerEdge-R730:~/systemcheck$ sudo ./systemcheck.sh
[sudo] password for hpb:
开始检查...
 1.检查密码有效期设置
 2.检查密码强度检查配置
 3.检查空口令账号
 4.检查账户锁定配置
 5.检查除 root 之外的账户 UID 为 0
 6.检查环境变量包含父目录
 7.检查环境变量包含组权限为 777 的目录
......
```

用户需等待片刻，当提示”未安装 chkconfig,是否安装 (y/n) :”时，用户需输入”y”安装 chkconfig；出现“检查完成，请仔细阅读 servercheck.txt 文件”信息表示安全检测已完成。

```
19.检查运行的服务
19. 未安装 chkconfig,是否安装 (y/n) :y
Reading package lists... Done
Building dependency tree
Reading state information... Done
......
Setting up sysv-rc-conf (0.99-7) ...
安装成功
20.检查 core dump 状态
检查完成, 请仔细阅读 servercheck.txt 文件
```

(4) 步骤 4 查看运行结果

输入"**vi** *servercheck.txt*"，将会显示运行结果，结果中共有 22 个检查项，通过的检查项会提示“安全”，未通过的检查项会提示“不安全”，HPB 芯链建议用户将未通过的检查项改为安全配置，用户可参考第三章查看具体检查项的修改步骤。

提示：第 n 项检查项对应第 3.n 节，共 22 个检查项。

```
hpb@dell-PowerEdge-R730:~/systemcheck$ vi servercheck.txt
1. 未配置密码超时时间,不安全
建议:
 执行 sed -i '/PASS_MAX_DAYS/s/99999/90/g' /etc/login.defs 设置密码的有效时间为 90 天
2. 未配置密码强度检查,不安全
建议:
 执行 echo "passwd requisite pam_cracklib.so difok=3 minlen=8 ucrediit=-1 lcredit=-1
dcredit=-1">> /etc/pam.d/
systemd-auth 设置密码需要包含大小写字母及数字，且长度至少为 8
3. 未发现空密码账户,安全
```

第3章 检查项详情

3.1 密码有效期设置

3.1.1 配置修改步骤

编号	步骤	说明
1	切换 root 用户	命令：”**su root**” 提示：用户需根据提示输入 root 账户密码
2	设置密码有效期（90 天）	命令：”**sed -i** '*/PASS_MAX_DAYS/s/99999/90/g*' */etc/login.defs*”

3.1.2 配置修改示例

(1) 步骤一 切换成 root 用户

打开终端，输入”**su root**”，根据提示输入 root 账户密码；

```
hpb@dell-PowerEdge-R730:~$ su root
Password:
root@dell-PowerEdge-R730:/home/hpb#
```

(2) 步骤二 设置密码有效期

输入”**sed -i** '*/PASS_MAX_DAYS/s/99999/90/g*' */etc/login.defs*”即可设置密码的有效时间为 90 天，该命令无返回信息。

```
root@dell-PowerEdge-R730:/home/hpb# sed -i '/PASS_MAX_DAYS/s/99999/90/g'
/etc/login.defs
```

3.2 密码强度检查配置

3.2.1 配置修改步骤

编号	步骤	说明
1	切换 root(已切换的用户可跳过)	命令：”**su root**” 提示：用户需根据提示输入 root 账户密码
2	配置密码强度检查	命令：”**echo** "*passwd requisite pam_cracklib.so difok=3 minlen=8 ucrediit=-1 lcredit=-1 dcredit=-1*">>

		/etc/pam.d/systemd-auth"

3.2.2 配置修改示例

(1) 步骤一 切换成 root 用户

打开终端，输入"**su root**"，根据提示输入 root 账户密码；

提示：已经切换成 root 用户的可以跳过该步骤。

```
hpb@dell-PowerEdge-R730:~$ su root
Password:
root@dell-PowerEdge-R730:/home/hpb#
```

(2) 步骤二 配置密码强度检查

输入"**echo** "*passwd requisite pam_cracklib.so difok=3 minlen=8 ucrediit=-1 lcredit=-1 dcredit=-1*">> */etc/pam.d/systemd-auth*"即可设置密码需要包含大小写字母及数字且长度至少为 8，该命令无返回信息；

```
root@dell-PowerEdge-R730:/home/hpb# echo "passwd requisite pam_cracklib.so difok=3
minlen=8 ucrediit=-1 lcredit=-1 dcredit=-1">> /etc/pam.d/systemd-auth
root@dell-PowerEdge-R730:/home/hpb#
```

3.3 空口令账户

3.3.1 配置修改步骤

编号	步骤	说明
1	切换 root(已切换的用户可跳过)	命令："**su root**" 提示：用户需根据提示输入 root 账户密码
2	设置账户密码	命令："**passwd** *账户名*" 提示：用户需将账户名换成自己未设置密码的账户名； 按照提示输入两次新密码即可。

3.3.2 配置修改示例

(1) 步骤一 切换成 root 用户

打开终端，输入"**su root**"，根据提示输入 root 账户密码；

提示：已经切换成 root 用户的可以跳过该步骤。

```
hpb@dell-PowerEdge-R730:~$ su root
Password:
root@dell-PowerEdge-R730:/home/hpb#
```

(2) 步骤二 设置账户密码

输入"**passwd** *账户名*"，根据提示输入新密码，重复输入后密码设置成功。

提示：用户需将账户名换成自己未设置密码的账户名，示例中账户为"test"。

```
root@dell-PowerEdge-R730:/home/hpb# passwd test
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

3.4 账户锁定配置

3.4.1 配置修改步骤

编号	步骤	说明
1	切换 root(已切换的用户可跳过)	命令："**su root**" 提示：用户需根据提示输入 root 账户密码
2	设置账户锁定策略	命令："**echo** "*auth required pam_tally.so onerr=fail deny=10 unlock_time=300*" >> */etc/pam.d/systemd-auth*"

3.4.2 配置修改示例

(1) 步骤一 切换成 root 用户

打开终端，输入"**su root**"，根据提示输入 root 账户密码；

提示：已经切换成 root 用户的可以跳过该步骤。

```
hpb@dell-PowerEdge-R730:~$ su root
Password:
root@dell-PowerEdge-R730:/home/hpb#
```

(2) 步骤二 设置账户锁定策略

输入"**echo** "*auth required pam_tally.so onerr=fail deny=10 unlock_time=300*" >> */etc/pam.d/systemd-auth*"即可设置连续输错 10 次则锁定账户，该命令无返回信息；

提示：解锁账户的命令为”**faillog -u** *<user>* **-r**”。

```
root@dell-PowerEdge-R730:/home/hpb#  echo "auth required pam_tally.so onerr=fail
deny=10 unlock_time=300" >> /etc/pam.d/systemd-auth
root@dell-PowerEdge-R730:/home/hpb#
```

3.5 UID 为 0 的账户

3.5.1 配置修改步骤

编号	步骤	说明
1	切换 root(已切换的用户可跳过)	命令：”**su root**” 提示：用户需根据提示输入 root 账户密码
2	修改 UID 为 0 的账户	命令：”**usermod -u** *<new-uid> <user>*” 命令：”**groupmod -g** *<new-gid> <user>*”

3.5.2 配置修改示例

(1) 步骤一 切换成 root 用户

打开终端，输入”**su root**”，根据提示输入 root 账户密码；

提示：已经切换成 root 用户的可以跳过该步骤。

```
hpb@dell-PowerEdge-R730:~$ su root
Password:
root@dell-PowerEdge-R730:/home/hpb#
```

(2) 步骤二 修改 UID 为 0 的账户

输入”**usermod -u** *<new-uid> <user>*”；继续输入”**groupmod -g** *<new-gid> <user>*”。

提示：<user>为账户名，需替换为 UID 为 0 的账户名；<new-uid>需替换为新 uid；<new-gid>为参数。

3.6 环境变量包含父目录

如果环境变量中存在父目录，建议用户修改配置，环境变量中不要带有父目录。

3.7 环境变量包含组权限为 777 的目录

如果环境变量中包含组权限为 777 的目录，建议用户使用 chmod 命令修改运行结果中目录的权限。

3.8 远程连接安全性

如果远程连接安全性未通过检测，建议用户和管理员联系确认运行结果中的文件是否必要，如非必要，应当删除。

3.9 Umask 配置

3.9.1 配置修改步骤

编号	步骤	说明
1	切换 root(已切换的用户可跳过)	命令：”**su root**” 提示：用户需根据提示输入 root 账户密码
2	umask 未配置	命令：”**echo** "*umask 027*" >> */etc/profile*” 命令：”**echo** "*umask 027*" >> */etc/bash.bashrc*”
2’	umask 配置不安全	命令：”**vi** */etc/profile*” 移动光标找到 umask 参数，将其后的数字修改为”027” 命令：”**vi** */etc/bash.bashrc*” 移动光标找到 umask 参数，将其后的数字修改为”027”

3.9.2 配置修改示例

(1) 步骤一 切换成 root 用户

打开终端，输入”**su root**”，根据提示输入 root 账户密码；

提示：已经切换成 root 用户的可以跳过该步骤。

```
hpb@dell-PowerEdge-R730:~$ su root
Password:
root@dell-PowerEdge-R730:/home/hpb#
```

(2) 步骤二 umask 未配置

输入”**echo** "*umask 027*" >> */etc/profile*”即可，该命令无返回信息；

输入”**echo** "*umask 027*" >> */etc/bash.bashrc*”即可，该命令无返回信息；

```
root@dell-PowerEdge-R730:/home/hpb#  echo "umask 027" >> /etc/profile
root@dell-PowerEdge-R730:/home/hpb# echo "umask 027" >> /etc/bash.bashrc
```

(3) 步骤二’ umask 配置不安全

输入”**vi** */etc/profile*”;按”↓”键将光标移动到 umask 参数上，将其紧跟的数字修改为”027”；

```
root@dell-PowerEdge-R730:/home/hpb# vi /etc/profile
if [ -d /etc/profile.d ]; then
  for i in /etc/profile.d/*.sh; do
    if [ -r $i ]; then
      . $i
    fi
  done
  unset i
fi
umask 027
TMOUT=180

:wq（先按下”ESC”键，再输入”:wq”就可以保存文件并退出）
```

输入”**vi** */etc/bash.bashrc*”;按”↓”键将光标移动到 umask 参数上，将其紧跟的数字修改为”027”；

```
root@dell-PowerEdge-R730:/home/hpb# vi /etc/bash.bashrc
if [ -d /etc/profile.d ]; then
  for i in /etc/profile.d/*.sh; do
    if [ -r $i ]; then
      . $i
    fi
  done
  unset i
fi
umask 027
TMOUT=180

:wq（先按下”ESC”键，再输入”:wq”就可以保存文件并退出）
```

3.10 重要文件和目录的权限

用户需要仔细检查运行结果中显示的文件和目录的权限，如果权限太低,请及时修改。

3.11 未授权的 SUID/SGID 文件

用户需检查运行结果中显示的目录/文件是否可疑,如果可疑,请及时删除。

3.12 任何人都有写权限的目录

用户需检查运行结果中显示的目录是否有必要任何人都可写,如非必要,请及时修改权限

3.13 任何人都有写权限的文件

用户需检查运行结果中显示的文件是否有必要任何人都可写,如非必要,请及时修改权限

3.14 没有属主的文件

如果存在没有属主的文件，用户需为运行结果中显示的文件增加属主,如有可疑文件,请及时删除。

3.15 异常的隐藏文件

用户需检查运行结果中文件是否可疑,如果可疑,请及时删除

3.16 登录超时配置

3.16.1 配置修改步骤

编号	步骤	说明
1	切换 root(已切换的用户可跳过)	命令：”**su root**” 提示：用户需根据提示输入 root 账户密码
2	增加登录超时配置	命令：”**echo** "*TMOUT=180*" >> */etc/profile*”

3.16.2 配置修改示例

(1) 步骤一 切换成 root 用户

打开终端，输入”**su root**”，根据提示输入 root 账户密码；

提示：已经切换成 root 用户的可以跳过该步骤。

```
hpb@dell-PowerEdge-R730:~$ su root
Password:
root@dell-PowerEdge-R730:/home/hpb#
```

(2) 步骤二 增加登录超时配置

输入”**echo** "*TMOUT=180*" >> */etc/profile*”即可，该命令无返回信息；

```
root@dell-PowerEdge-R730:/home/hpb# echo "TMOUT=180" >> /etc/profile
root@dell-PowerEdge-R730:/home/hpb#
```

3.17 ssh 和 telnet 运行状态

如果 ssh 处于未运行状态，建议用户安装并开启 ssh 服务；

如果 telnet 处于运行状态，建议用户停止 telnet 服务。

3.18 Root 远程登录限制

3.18.1 配置修改步骤

编号	步骤	说明
1	切换 root(已切换的用户可跳过)	命令：”**su root**” 提示：用户需根据提示输入 root 账户密码
2	不允许 root 远程登录	命令：”**vi** */etc/ssh/sshd_config*” 移动光标找到”PermitRootLogin”参数，将其后的”yes”改为”no”。 提示：如果该参数后为非”yes”的其他值，则无需修改。

3.18.2 配置修改示例

(1) 步骤一 切换成 root 用户

打开终端，输入”**su root**”，根据提示输入 root 账户密码；

提示：已经切换成 root 用户的可以跳过该步骤。

```
hpb@dell-PowerEdge-R730:~$ su root
Password:
root@dell-PowerEdge-R730:/home/hpb#
```

(2) 步骤二 不允许 root 远程登录

输入”**vi** */etc/ssh/sshd_config*”，在打开的文件中移动光标到 PermitRootLogin 的位置，如果其紧跟的参数为”yes”，则需将”yes”改为”no”。

提示：如果其紧跟的参数为其他值，则可以不用修改配置。

```
root@dell-PowerEdge-R730:/home/hpb# vi /etc/ssh/sshd_config

# Authentication:
LoginGraceTime 120
PermitRootLogin prohibit-password
StrictModes yes

:wq（先按下"ESC"键，再输入":wq"就可以保存文件并退出）
```

3.19 运行的服务

用户需检查运行结果中显示的服务，并尽量关闭不必要的服务。

提示：关闭服务的命令为"**chkconfig --level $level** *<服务名>*"

3.20 Core dupm 状态

3.20.1 配置修改步骤

编号	步骤	说明
1	切换 root(已切换的用户可跳过)	命令："**su root**" 提示：用户需根据提示输入 root 账户密码
2	修改 limits 文件	命令："**vi** */etc/security/limits.conf*" 在文档末尾"End of file"前输入 "* soft core 0 * hard core 0"

3.20.2 配置修改示例

(1) 步骤一 切换成 root 用户

打开终端，输入"**su root**"，根据提示输入 root 账户密码；

提示：已经切换成 root 用户的可以跳过该步骤。

```
hpb@dell-PowerEdge-R730:~$ su root
Password:
root@dell-PowerEdge-R730:/home/hpb#
```

(2) 步骤二修改 limits 文件

输入"**vi** */etc/security/limits.conf*";

将光标移到文档末尾”End of file”的上一行，

输入”* soft core 0

* hard core 0”。

提示:如果无法键入，则按下字母”I”键即可开启”INSERT”输入状态。

```
root@dell-PowerEdge-R730:/home/hpb#

#ftp        hard   nproc       0
#ftp        -      chroot      /ftp
#@student   -      maxlogins   4
* soft core 0
* hard core 0
# End of file
:wq（先按下”ESC”键，再输入”:wq”就可以保存文件并退出）
```

3.21 rsyslog 状态

3.21.1 配置修改步骤

编号	步骤	说明
1	切换 root(已切换的用户可跳过)	命令：”**su root**” 提示：用户需根据提示输入 root 账户密码
2	配置并启动 rsyslog	命令:”**vi** */etc/rsyslog.conf*”; 在文件末尾输入: ”***.err;kern.debug;daemon.notice /var/adm/messages**” 命令:”**sudo mkdir** */var/adm*” 命令:”**sudo touch** */var/adm/messages*” 命令:”**sudo chmod 666** */var/adm/messages*” 命令:”**sudo systemctl restart** *rsyslog*”

3.21.2 配置修改示例

(1) 步骤一 切换成 root 用户

打开终端，输入”**su root**”，根据提示输入 root 账户密码;

提示：已经切换成 root 用户的可以跳过该步骤。

```
hpb@dell-PowerEdge-R730:~$ su root
Password:
root@dell-PowerEdge-R730:/home/hpb#
```

(2) 步骤二 配置并启动 rsyslog

输入"**vi** */etc/rsyslog.conf*" 打开 rsyslog.conf 文件；

按下字母"I"键即可打开输入"INSERT"状态;

用"↓"键移动光标到文件最后一行，输入:

"***.err;kern.debug;daemon.notice /var/adm/messages**";

按下"ESC"键，再输入"**:wq**"就可以保存文件并退出；

```
root@dell-PowerEdge-R730:/home/hpb# vi /etc/rsyslog.conf


#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
*.err;kern.debug;daemon.notice /var/adm/messages


:wq（先按下" ESC" 键，再输入" :wq" 就可以保存文件并退出）
```

继续输入"**sudo mkdir** */var/adm*"，该命令无返回信息;

继续输入"**sudo touch** */var/adm/messages*" ，该命令无返回信息;

继续输入"**sudo chmod 666** */var/adm/messages*" ，该命令无返回信息;

继续输入"**sudo systemctl restart** *rsyslog*" ，该命令无返回信息.

```
root@dell-PowerEdge-R730:/home/hpb# sudo mkdir /var/adm
root@dell-PowerEdge-R730:/home/hpb# sudo touch /var/adm/messages
root@dell-PowerEdge-R730:/home/hpb# sudo chmod 666 /var/adm/messages
root@dell-PowerEdge-R730:/home/hpb# sudo systemctl restart rsyslog
```

3.22 Boe 功能兼容性检测

未安装 BOE 板卡的服务器可跳过该检查项；当该检查项未通过时，用户需提供运行结果里显示的系统信息并通过"附录 技术支持"联系 HPB 工作人员以寻求帮助。

附录 技术支持

如果您需要更多的帮助，您需要联系 HPB 芯链工作人员获取更多的技术支持。

服务热线电话：+86 021-5895 9195（中国）

技术支持邮箱：node@hpb.io

HPB 技术社区：http://blockgeek.org/

HPB 官网地址：http://www.hpb.io/

电报：https://t.me/hpbglobal

脸书：HPB Blockchain

推特：@HPBGlobal

红迪网：r/HPBGlobal