

《信息系统安全》

实 验 指 导 手 册

华中科技大学网络空间安全学院
二零二三年 六月

目 录

实验四 系统安全(二)

第一章 实验目标和内容	2
1.1 LINUX 系统脆弱性检查与加固	2

实验四

系统安全(二)

第一章 实验目标和内容

1.1 Linux 系统脆弱性检查与加固

1.1.1 实验目的

操作系统安全配置不当是最常见的安全问题，这通常是由于不安全的默认配置、不完整的临时配置、开源云存储、错误的 HTTP 标头配置以及包含敏感信息的详细错误信息所造成的。因此，我们不仅需要所有的操作系统、框架、数据库和应用程序进行安全配置，而且必须及时修补和升级它们。

本实验的学习目标是让学生需使用 Linux 系统作为实验环境，并配置和管理相应的身份认证和策略。需实施安全审计措施，收集和分析系统日志，检测和响应安全事件，并了解如何通过该方法抵御攻击。

1.1.2 实验环境

- ✧ VMware Workstation 虚拟机。
- ✧ 操作系统：unix 系统
- ✧ 测试主机： 操作机 kali。

1.1.3 实验要求

- ✧ 对登录操作系统的用户进行身份标识和鉴别
- ✧ 具有登录失败处理功能，配置并启用结束会话、限制非法登录次

数和当登录连接超时自动退出等相关措施

- ✧ 进行远程管理时，配置措施防止鉴别信息在网络传输过程中被窃听
- ✧ 对登录的用户分配账户和权限
- ✧ 重命名或删除默认账户，修改默认账户的默认口令
- ✧ 启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计
- ✧ 关闭不需要的系统服务、默认共享
- ✧ 对可能存在的已知漏洞进行测试评估，及时更新补丁。

1.1.4 实验内容

任务 1:

应对登录操作系统的用户进行身份标识和鉴别。

步骤 1: 使用 college 身份登录系统, 验证登录操作系统是否需要密码, 如果不需要输入密码, 则不符合。

```
w@wdeMacBook-Pro ~ % ssh college@180.153.183.37
college@180.153.183.37's password: ?
```

加固方法: college 用户登录至系统, 并使用 “passwd” 命令添加/修改密码:

```
[college@pi-33190-110555 ~]$ passwd
更改用户 college 的密码。
为 college 更改 STRESS 密码。
(当前) UNIX 密码: █
```

步骤 2: root 身份登录后, 执行命令: “cat /etc/passwd”, 查看是否存在空口令, shadow 文件第二个字段为加密后的口令, 如下图所示, 为空则为空口令 (*或者!! 表示用户被锁定), 空口令则此项不符合。

```
[college@pi-33190-110555 ~]$ cat /etc/passwd
cat: /etc/passwd: 没有那个文件或目录
[college@pi-33190-110555 ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89:/:/var/spool/postfix:/sbin/nologin
chrony:x:998:996:/:/var/lib/chrony:/sbin/nologin
```

加固方法：使用 “passwd 用户名” 命令为空口令用户添加密码：

```
[college@pi-33190-110555 ~]$ passwd
更改用户 college 的密码。
为 college 更改 STRESS 密码。
(当前) UNIX 密码: █
```

步骤 3：输入命令：“cat /etc/login.defs” 查看密码长度和定期更换设置，

若密码有效期限较长/密码使用时间较短/密码长短最短值太小，则该项不合格。

```
# Directory where mailboxes reside, _or_ name of file, relative to the
# home directory.  If you _do_ define both, MAIL_DIR takes precedence.
# QMAIL_DIR is for Qmail
#
#QMAIL_DIR      Maildir
MAIL_DIR        /var/spool/mail
#MAIL_FILE      .mail

# Password aging controls:
#
#      PASS_MAX_DAYS   Maximum number of days a password may be used.
#      PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#      PASS_MIN_LEN     Minimum acceptable password length.
#      PASS_WARN_AGE    Number of days warning given before a password expires.
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_MIN_LEN    5
PASS_WARN_AGE   7
```

加固方法：使用命令“sudo vi /etc/login.defs”之后，按“i”，修改上述数值，最后保存即可。

PASS_MAX_DAYS #登录密码有效期限，不得大于 60 天

PASS_MIN_DAYS #登录密码最短使用时间，不得小于 3 天

PASS_MIN_LEN #登录密码最短长度，不得小于 8 天

PASS_WARN_AGE #登录密码过期提前提醒时间，不得小于 7 天

```
# Password aging controls:
#
#     PASS_MAX_DAYS   Maximum number of days a password may be used.
#     PASS_MIN_DAYS   Minimum number of days allowed between password changes
#     PASS_MIN_LEN     Minimum acceptable password length.
#     PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS 60
PASS_MIN_DAYS 3
PASS_MIN_LEN 8
PASS_WARN_AGE 7
```

步骤 4：输入命令：“cat /etc/pam.d/system-auth”，查看密码复杂度配置，查看是否有以下项：password requisite pam_cracklib.so retry=5 difok=3 minlen=8 dcredit=-3 ucredit=-2 lcredit=-4 ocredit=-1，若无上述内容则该项不合规

retry=5 # 修改密码，可以重试的次数（若该值较大则此项不合格）

difok=3 # 与旧密码不同的字符个数（若该值较小则此项不合格）

minlen=8 # 新密码最小长度（若该值较小则此项不合格）

dcredit=-3 # 数字个数。大于 0，最多；小于 0，最少（若该值为 0 则此项不合格）

ucredit=-2 # 大写字母个数。大于 0，最多；小于 0，最少（若该值为 0 则此项不合格）

lcredit=-4 # 小写字母个数。大于 0，最多；小于 0，最少（若该值为 0 则此项不合格）

ocredit=-1 # 特殊字符个数。大于 0，最多；小于 0，最少（若该值为 0 则此项不合格）

上述各个参数值不存在或某项值不合格则此项不合格。

```
[college@pi-33190-110555 ~]$ cat /etc/pam.d/system-auth
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth      required      pam_env.so
auth      required      pam_faildelay.so delay=2000000
auth      sufficient    pam_unix.so nullok try_first_pass
auth      requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth      required      pam_deny.so

account    required      pam_unix.so
account    sufficient    pam_localuser.so
account    sufficient    pam_succeed_if.so uid < 1000 quiet
account    required      pam_permit.so

password   requisite     pam_pwquality.so try_first_pass local_users_only retry=3 auth
ok_type=
password   sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password   required      pam_deny.so

session    optional      pam_keyinit.so revoke
session    required      pam_limits.so
-session   optional      pam_systemd.so
session    [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session    required      pam_unix.so
```

加固方法：按照上述规则，编辑该文件（sudo vi /etc/pam.d/system-auth），替换对用内容为上述内容：

```

#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth      required      pam_env.so
auth      required      pam_faildelay.so delay=2000000
auth      sufficient     pam_unix.so nullok try_first_pass
auth      requisite      pam_succeed_if.so uid >= 1000 quiet_success
auth      required      pam_deny.so

account    required      pam_unix.so
account    sufficient     pam_localuser.so
account    sufficient     pam_succeed_if.so uid < 1000 quiet
account    required      pam_permit.so

password    requisite     pam_cracklib.so retry=5 difok=3 minlen=8 dcredit=-3 ucredit=-2 lcredit=-4 ocredit=-1
#password    requisite      pam_pwquality.so try_first_pass local_users_only retry=3 auth
tok type=
password    sufficient     pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session    optional      pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
-
-
-- INSERT --

```

任务二：

应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施

步骤 1：输入命令：“cat /etc/pam.d/system-auth”查看登录失败处理功能是否开启，若无下述内容则该项不符合

```

auth      required      pam_tally2.so onerr=fail deny=3 unlock_time=300
even_deny_root root_unlock_time=300

```

```
[college@pi-33190-110555 ~]$ cat /etc/pam.d/system-auth
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth      required      pam_env.so
auth      required      pam_faildelay.so delay=2000000
auth      sufficient    pam_unix.so nullok try_first_pass
auth      requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth      required      pam_deny.so

account    required      pam_unix.so
account    sufficient    pam_localuser.so
account    sufficient    pam_succeed_if.so uid < 1000 quiet
account    required      pam_permit.so

password   requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authn
password   sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password   required      pam_deny.so

session    optional     pam_keyinit.so revoke
session    required      pam_limits.so
-session   optional     pam_systemd.so
session    [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session    required      pam_unix.so
```

onerr=fail 表示定义了当出现错误时的缺省返回值；

even_deny_root 表示也限制 root 用户；

deny 表示设置普通用户和 root 用户连续错误登陆的最大次数，超过最大次数，则锁定该用户；

unlock_time 表示设定普通用户锁定后，多少时间后解锁，单位是秒；

root_unlock_time 表示设定 root 用户锁定后，多少时间后解锁，单位是秒；

加固方法：编辑该文件(sudo vi /etc/pam.d/system-auth)，替换对应内容为上述内容：

```
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.

auth required pam_tally2.so onerr=fail deny=3 unlock_time=300 even_denry_root root_unlock
time=300
#auth      required      pam_env.so
auth      required      pam_faildelay.so delay=2000000
auth      sufficient     pam_unix.so nullok try_first_pass
auth      requisite      pam_succeed_if.so uid >= 1000 quiet_success
auth      required      pam_deny.so

account    required      pam_unix.so
account    sufficient     pam_localuser.so
account    sufficient     pam_succeed_if.so uid < 1000 quiet
account    required      pam_permit.so

password   requisite      pam_pwquality.so try_first_pass local_users_only retry=3 authn
ok type=
password   sufficient     pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password   required      pam_deny.so

session    optional      pam_keyinit.so revoke
session    required      pam_limits.so
-session   optional      pam_systemd.so
session    [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session    required      pam_unix.so
```

步骤 2: 输入命令: “cat /etc/profile”, 检查超时自动退出功能, 若无 TMOU=300 export TMOU 俩行内容, 则不合规

```
umask 002
else
umask 022
fi

for i in /etc/profile.d/*.sh /etc/profile.d/sh.local ; do
if [ -r "$i" ]; then
if [ "${-#*i}" != "$-" ]; then
. "$i"
else
. "$i" >/dev/null
fi
fi
done

unset i
unset -f pathmunge
```

加固方法：使用命令“sudo vi /etc/profile”若无上述内容则自行添加，若数值不合理则修改其数值为下图所示内容：

```
for i in /etc/profile.d/*.sh /etc/profile.d/sh.local ; do
    if [ -r "$i" ]; then
        if [ "${-#*i}" != "$-" ]; then
            . "$i"
        else
            . "$i" >/dev/null
        fi
    fi
done
TMOUT=300
export=TMOUT
unset i
unset -f pathmunge
```

任务三：

当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

步骤 1：访谈系统管理员，进行远程管理的方式,登录进入操作系统查看是否运行了 sshd 服务：ps -e | grep sshd，查看相关的端口是否打开，netstat -an|grep 22，若使用 ssh 方式进行远程管理，则可以防止鉴别信息在传输过程中被窃听，该项合规。

```
[college@pi-33190-110555 ~]$ ps -e | grep sshd
 755 ?        00:00:00 sshd
1528 ?        00:00:00 sshd
1705 ?        00:00:00 sshd
[college@pi-33190-110555 ~]$ netstat -an|grep 22
tcp        0      0 0.0.0.0:22          0.0.0.0:*           LISTEN
tcp        0      0 36.192.168.0.6:22  39.192.168.0.6:63009 ESTABLISHED
tcp6       0      0 :::22              :::*               LISTEN
unix 2      [ ACC ]     STREAM  LISTENING  18022    private/rewrite
unix 3      [ ]       STREAM  CONNECTED  16622    /run/systemd/journal/stdout
unix 2      [ ]       DGRAM   13822
unix 3      [ ]       STREAM  CONNECTED  15226    /run/systemd/journal/stdout
unix 3      [ ]       STREAM  CONNECTED  15225
unix 3      [ ]       STREAM  CONNECTED  14722    /run/dbus/system_bus_socket
```

加固方法：若需要进行远程管理，且未使用 ssh 服务进行，则使用命令：开启 ssh 服务：sudo service sshd restart

```
[college@pi-33190-110555 ~]$ sudo service sshd restart
Redirecting to /bin/systemctl restart sshd.service
[college@pi-33190-110555 ~]$ sudo service sshd status
Redirecting to /bin/systemctl status sshd.service
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset:
   enabled)
   Active: active (running) since 三 2021-07-14 15:12:45 HKT; 9s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 32425 (sshd)
    CGroup: /system.slice/sshd.service
            └─32425 /usr/sbin/sshd -D

7月 14 15:12:45 pi-33190-110555 systemd[1]: Starting OpenSSH server daemon...
7月 14 15:12:45 pi-33190-110555 sshd[32425]: Server listening on 0.0.0.0 po....
7月 14 15:12:45 pi-33190-110555 sshd[32425]: Server listening on :: port 22.
7月 14 15:12:45 pi-33190-110555 systemd[1]: Started OpenSSH server daemon.
Hint: Some lines were ellipsized, use -l to show in full.
```

步骤 2：若未使用 SSH 方式进行远程管理，则查看是否使用了 Telnet 方式进行远程管理，查看 Telnet 服务的状态：systemctl status telnet.socket，若为下图所示则证明不存在 Telnet 服务，则该项合规。

```
[college@pi-33190-110555 ~]$ systemctl status telnet.socket
Unit telnet.socket could not be found.
```

加固方法：linux 默认不存在 Tlenet 服务，故此项合规。

任务四：

应对登录的用户分配账户和权限

步骤 1: 检查重要文件和目录权限设置是否合理, Linux 系统对文件的操作权限包括四种: 读 (r, 4); 写 (w, 2); 执行 (x, 1); 空 (-, 0), 文件的权限分为属主 (拥有者)、属组、其它用户和用户组的权限。配置文件权限值不能大于 644, 对于可执行文件不能大于 755。

输入命令: `ls -l`:

```
[college@p-33190-2118225856-1620-57712 ~]$ ls -l
总用量 1020728
drwxrwxr-x 4 college college      68 7月 12 23:13 1
drwxrwxr-x 9 college tomcat      220 6月 22 11:53 apache-tomcat-8.5.68
drwxrwxr-x 8 college college     106 12月 28 2010 jboss
drwxr-xr-x 8 college college     233 4月 11 2015 jdk1.7.0_80
drwxr-xr-x 2 root   root          6 6月 22 22:38 PASSWORD
drwxrwxr-x 2 college tomcat       19 6月 28 19:14 tomcat_webapps
-rw-rw-r-- 1 college college 1045221652 6月 22 21:41 wls1211_generic.jar
[college@p-33190-2118225856-1620-57712 ~]$
```

加固方法: 对特定的文件夹, 使用命令: “`chmod 644 文件夹名`”或对特定的可执行文件使用名“`chmod 755 文件名`”

任务五:

应重命名或删除默认账户, 修改默认账户的默认口令

步骤 1: 输入命令: “`sudo more /etc/shadow`” 查看是否存在默认的、无用的用户, 若存在上述用户则该项不合规。(该实验初始默认

的系统用户只有 root)

```
[colleage@kali:~]$ sudo more /etc/shadow
[sudo] colleage 的密码:
root:1$66c/iaX0dNa0Lgppp$J3SodyFWUJNmJ0ArkWXS1eucO9g0pXC3tbyT8hN2cZhXWtPwSvW1uocWcZ9/BYDE7sKJh
lUgy62c::10:99999:7::
bin:*:17632:0:99999:7::
daemon:*.17632:0:99999:7::
adm:*.17632:0:99999:7::
lp:*.17632:0:99999:7::
sync:*.17632:0:99999:7::
shutdown:*.17632:0:99999:7::
halt:*.17632:0:99999:7::
mail:*.17632:0:99999:7::
operator:*.17632:0:99999:7::
games:*.17632:0:99999:7::
ftp:*.17632:0:99999:7::
nobody:*.17632:0:99999:7::
systemd-networkd::17735:::
dbus::17735:::
polkitd::17735:::
sshd::17735:::
postfix::17735:::
chrony::17735:::
gluster::17735:::
tcpdump::17735:::
colleage:1868KVNjU/eqblXlKf$wbJ8pKOEj2wpU0p.WfXyh.HfSvwQ19bmhEUOpbCJUpGhkUoH9OxIJhuSOIo3.K/PMstIog
GNnZp0:188000:0:99999:7::
```

加固方法:

root 作为 Linux 系统的重要默认用户，要求禁止远程登录，加固命令如下：

```
sudo vim /etc/ssh/sshd config
```

去掉“#”号，并改为“No”，代表禁止远程登录。

删除默认、无用的用户，使用命令“`userdel -rf 用户名`”：（该实验默认系统用户只有 `root`，不做删除掩饰）

使用“passwd 用户名”修改默认用户的口令:

```
[college@pi-33190-110555 ~]$ sudo passwd college
更改用户 college 的密码。
新的 密码: 
```

应授予管理用户所需的最小权限，实现管理用户的权限分离：

步骤 2: 应严格限制具有 root 级权限的账户, 其他用户仅应通过使

```
#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

用 sudo 被赋予 root 级权限。通过以下命令 `sudo ls -l /etc/passwd`，核查 root 级权限都授予哪些账户，发现只有 root 用户拥有 root 权限，故此项合规。

加固方法：删除该其他拥有 root 权限的用户。

```
[college@pi-33190-110555 ~]$ sudo ls -l /etc/passwd
-rw-r--r-- 1 root root 1307 6月 28 16:56 /etc/passwd
[college@pi-33190-110555 ~]$
```

任务六：

应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计

步骤 1：输入查看系统日志服务命令：`service rsyslog status` 看到系统日志默认为开启，该项合规

```
[college@pi-33190-110555 ~]$ service rsyslog status
Redirecting to /bin/systemctl status rsyslog.service
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since 2021-07-12 12:30:44 HKT; 2 days ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
   Main PID: 779 (rsyslogd)
    CGroup: /system.slice/rsyslog.service
            └─779 /usr/sbin/rsyslogd -n
```

步骤 2: 输入命令: `service auditd status`, 发现未开启, 该项不符合

```
[college@pi-33190-110555 ~]$ service auditd status
Redirecting to /bin/systemctl status auditd.service
● auditd.service - Security Auditing Service
   Loaded: loaded (/usr/lib/systemd/system/auditd.service; disabled; vendor preset: enabled)
   Active: inactive (dead)
     Docs: man:auditd(8)
           https://github.com/linux-audit/audit-documentation
```

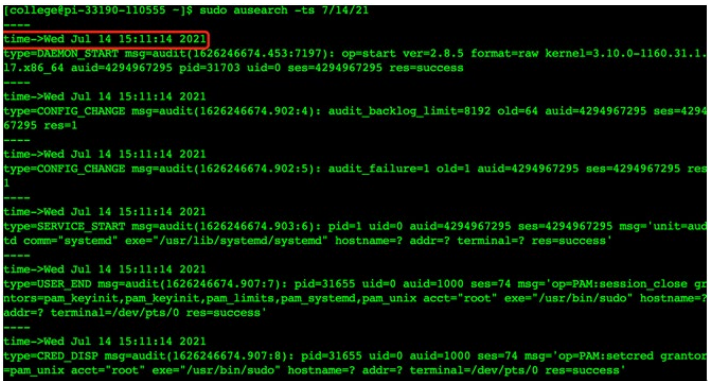
加固方法: 输入命令: `sudo service auditd start`, 即可成功开启。

```
[college@pi-33190-110555 ~]$ sudo service auditd start
[sudo] college 的密码:
Redirecting to /bin/systemctl start auditd.service
[college@pi-33190-110555 ~]$ sudo service auditd status
Redirecting to /bin/systemctl status auditd.service
● auditd.service - Security Auditing Service
   Loaded: loaded (/usr/lib/systemd/system/auditd.service; disabled; vendor preset: enabled)
   Active: active (running) since 2021-07-14 15:11:14 HKT; 15s ago
     Docs: man:auditd(8)
           https://github.com/linux-audit/audit-documentation
   Process: 31712 ExecStartPost=/sbin/auditctl --load (code=exited, status=0/SUCCESS)
   Process: 31702 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
   Main PID: 31703 (auditd)
    CGroup: /system.slice/auditd.service
            └─31703 /sbin/auditd
```

任务七：

审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息

步骤 1：以有相应权限的身份登录进入操作系统, 使用命令” sudo ausearch -ts today”，其中，-ts 后面的参数指定日期后的 log, 例如：查看今天的日期也可以用下图格式查询：（月/日/年）



```
[college@pi-33190-110555 ~]$ sudo ausearch -ts 7/14/21
time-->Wed Jul 14 15:11:14 2021
type=DAEMON_START msg=audit(1626246674.453:7197): op=start ver=2.8.5 format=raw kernel=3.10.0-1160.31.1.el7.x86_64 auid=4294967295 pid=31703 uid=0 ses=4294967295 res=success
time-->Wed Jul 14 15:11:14 2021
type=CONFIG_CHANGE msg=audit(1626246674.902:4): audit_backlog_limit=8192 old=64 auid=4294967295 ses=4294967295 res=1
time-->Wed Jul 14 15:11:14 2021
type=CONFIG_CHANGE msg=audit(1626246674.902:5): audit_failure=1 old=1 auid=4294967295 ses=4294967295 res=1
time-->Wed Jul 14 15:11:14 2021
type=SERVICE_START msg=audit(1626246674.903:6): pid=1 uid=0 auid=4294967295 ses=4294967295 msg='unit=auditd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
time-->Wed Jul 14 15:11:14 2021
type=USER_END msg=audit(1626246674.907:7): pid=31655 uid=0 auid=1000 ses=74 msg='op=PAM:session_close grantors=pam_keyinit,pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
time-->Wed Jul 14 15:11:14 2021
type=CRED_DISP msg=audit(1626246674.907:8): pid=31655 uid=0 auid=1000 ses=74 msg='op=PAM:setcred grantors=pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'
```

应关闭不需要的系统服务、默认共享

步骤 1：使用命令” systemctl | grep running “ 查看当前正在运行的服务，若存在不需要的系统服务或恶意服务，则该项不合规。

加固方法：使用命令“sudo systemctl stop 服务名.service”关闭指定的服务。

```
college@pi-33190-110555 ~$ systemctl | grep running
session-1.scope          loaded active running Session 1 of user college
chronpd.service          loaded active running MTP client/daemon
crond.service             loaded active running Command Scheduler
dbus.service              loaded active running D-Bus System Message Bus
getty@tty1.service        loaded active running Getty on tty1
irqbalance.service        loaded active running irqbalance daemon
lvm2-lvm2d.service         loaded active running LVM2 metadata daemon
mail-server.service       loaded active running Microsoft Exchange Server Database Engine
mysqld.service            loaded active running MySQL Server
NetworkManager.service   loaded active running Network Manager
polkit.service            loaded active running Authorization Manager
postfix.service           loaded active running Postfix Mail Transport Agent
re-local.service          loaded active running /etc/rc.d/rc.local Compatibility
rhcsmcertd.service        loaded active running Enable periodic update of entitlement certificates
rsyslog.service           loaded active running System Logging Service
serial-getty@tty01.service loaded active running Serial Getty on tty01
sshd.service              loaded active running OpenSSH server daemon
systemd-journald.service   loaded active running Journal Service
systemd-logind.service     loaded active running Login Service
systemd-udev.service       loaded active running udev Kernel Device Manager
tuned.service             loaded active running Dynamic System Tuning Daemon
dbus.socket               loaded active running D-Bus System Message Bus Socket
lvm2-lvm2d.socket         loaded active running LVM2 metadata daemon socket
systemd-journald.socket    loaded active running Journal Socket
systemd-udev-control.socket loaded active running udev Control Socket
systemd-udev-kernel.socket loaded active running udev Kernel Socket
```

步骤 2: Linux 系统自身不存在默认共享，创建共享文件夹需安装 samba

输入命令 rpm -qi samba 检查是否已经安装 samba:

```
[college@pi-33190-110555 ~]$ rpm -qi samba
未安装软件包 samba
[college@pi-33190-110555 ~]$
```

加固方法：无需加固

应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。

步骤 1：使用命令 `rpm -qa grep patch` 查看补丁更新情况：

```
[college@pi-33190-110555 ~]$ rpm -qa grep patch
grep-2.20-3.el7.x86_64
patch-2.7.1-12.el7_7.x86_64
[college@pi-33190-110555 ~]$
```

加固方法：使用命令 `sudo yum update` 输入 college 密码，更新系统。

```
[[college@pi-33190-110555 ~]$ sudo yum update
[sudo] college 的密码：
```

安全加固

实验步骤即为加固过程，主要包含以下项目：

身份鉴别：

- 1) 对登录操作系统的用户进行身份标识和鉴别
- 2) 设置登录失败处理功能，
- 3) 配置并启用结束会话、限制非法登录次数和当登录连接超时自动

退出等功能

4) 禁用 Telnet 远程管理

访问控制:

- 1) 对登录的用户分配账户和权限
- 2) 重命名或删除默认账户, 修改默认账户的默认口令
- 3) 授予管理用户所需的最小权限, 实现管理用户的权限分离

安全审计:

- 1) 启用安全审计功能, 审计覆盖到每个用户, 对重要的用户行为和重要安全事件进行审计
- 2) 设置审计记录

入侵防范:

- 1) 关闭不需要的系统服务、默认共享
- 2) 定期漏扫, 及时更新补丁