第一周 环境准备任务

CentOS 7.6*

Nginx 1.12.2

PHP 5.4.16

MySQL 5.7

一、安装Nginx

1、修改yum源为阿里云yum源

- mv /etc/yum.repos.d/CentOS-Base.repo /etc/yum.repos.d/CentOS-Base.repo.backup
- wget -O /etc/yum.repos.d/CentOS-Base.repo http://mirrors.aliyun.com/repo/Centos-7.repo
- wget -P /etc/yum.repos.d/ http://mirrors.aliyun.com/repo/epel-7.repo
  yum clean all
- yum makecache

2、安装Nginx

- yum install nginx

3、启动Nginx和配置开机启动Nginx

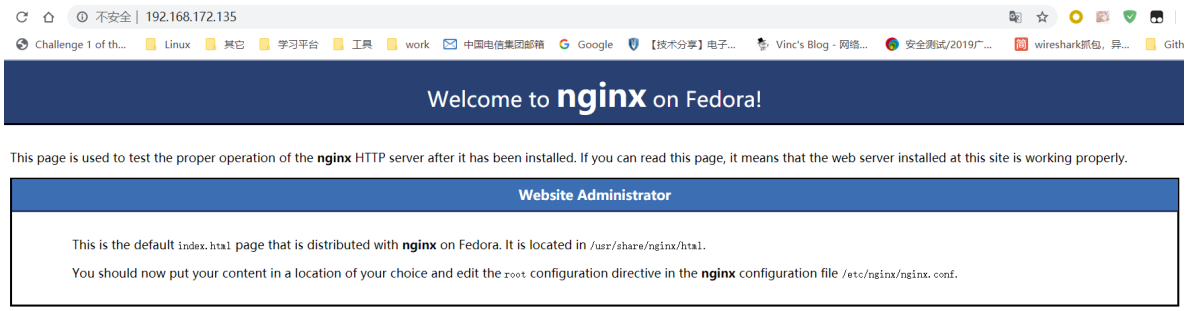
- systemctl enable nginx // 开机启动 nginx
- systemctl start nginx // 启动 nginx

4、查看Nginx服务状态

- systemctl status nginx

5、关闭防火墙即可访问

- systemctl stop firewalld



二、安装MySQL

1、添加MySQL5.7仓库

- sudo rpm -ivh https://dev.mysql.com/get/mysql57-community-release-el7-11.noarch.rpm

2、确认MySQL是否成功添加

- sudo yum repolist all | grep mysql | grep enabled

如下展示则表示添加成功

- mysql-connectors-community/x86_64 MySQL Connectors Community   enabled: 51
- mysql-tools-community/x86_64   MySQL Tools Community   enabled: 63
- mysql57-community/x86_64   MySQL 5.7 Community Server   enabled: 267

3、开始安装MySQL

- sudo yum -y install mysql-community-server

4、启动并设置开机启动MySQL

- sudo systemctl start mysqld
- sudo systemctl enable mysqld

5、查看root默认密码

- cat /var/log/mysqld.log | grep -i 'temporary password'

6、MySQL初始化设置，这个命令会进行设置root密码设置，移除匿名用户，禁止root用户远程连接等

- mysql_secure_installation

```
[root@192.168.172.132]# mysql_secure_installation

Securing the MySQL server deployment.

Enter password for user root:  ##输入上面的临时root密码

The existing password for the user account root has expired. Please set a new
password.

New password: ##设置新密码

Re-enter new password:  ##重复密码
The 'validate_password' plugin is installed on the server.
The subsequent steps will run with the existing configuration
of the plugin.
Using existing password for root.

Estimated strength of the password: 100
Change the password for root ? ((Press y|Y for Yes, any other key for No) : #是否
更改root密码

 ... skipping.
By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.
```

```
Remove anonymous users? (Press y|Y for Yes, any other key for No) : ##是否移除匿名用户

 ... skipping.


Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : y ##是否禁止root远程登录
Success.

By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.


Remove test database and access to it? (Press y|Y for Yes, any other key for No) : y ##是否删除测试数据库
 - Dropping test database...
Success.

 - Removing privileges on test database...
Success.

Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : y ##是否立即刷新权限
Success.

All done!
```

7、修改配置文件/etc/my.cnf,添加下面两行，配置默认编码为UTF-8

- character_set_server=utf8
- init_connect='SET NAMES utf8'

三、PHP环境配置

1、安装php和php-fpm

#首先安装epel

- yum -y install epel-release

#安装php、php-fpm

- yum -y install php php-fpm

#查看php版本号

- php -v

2、安装php-mysql

- yum install php-mysql

3、启动php-fpm和设置php-fpm开机启动

- systemctl start php-fpm
- systemctl enable php-fpm

4、配置Nginx支持.php

- vim /etc/nginx/nginx.conf

#修改默认的location块，使其支持.php文件

```
  location / {
        root   html;
        index  index.php index.html index.htm;
    }
```

#接下来配置保证对于 .php 文件的请求将被传送到后端的 PHP-FPM 模块， 取消默认的 PHP 配置块的注释，并改为以下的内容：

```
location ~* \.php$ {
        fastcgi_index   index.php;
        fastcgi_pass    127.0.0.1:9000;
        include         fastcgi_params;
        fastcgi_param   SCRIPT_FILENAME    $document_root$fastcgi_script_name;
        fastcgi_param   SCRIPT_NAME        $fastcgi_script_name;
    }
```

#重启Nginx发现有如下报错

```
$ systemctl start nginx
Job for nginx.service failed because the control process exited with error code.
See "systemctl status nginx.service" and "journalctl -xe" for details.
```

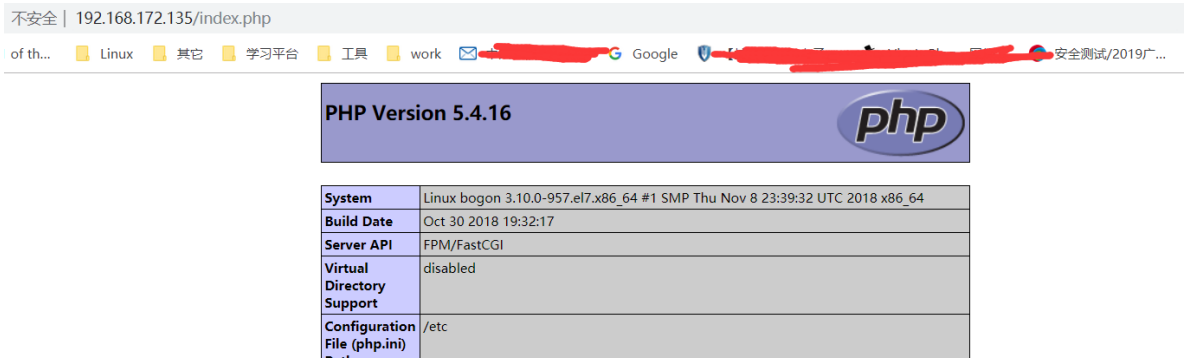
#最后网上查找得知手误输入少了一个分号导致，添加后正常启动。

```
      location / {
              root   html;
              index  index.php index.html index.htm;
      }
```

#创建测试文件

```
    [root@localhost ~]# rm /usr/share/nginx/html/index.html
    [root@localhost ~]# echo "<?php phpinfo(); ?>" >>
/usr/local/nginx/html/index.php
```

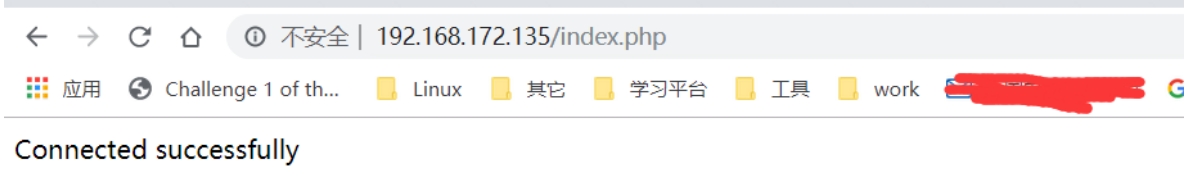
#访问IP/index.php可以看到phpinfo



#修改index.php内容，测试MySQL连接

```
<?php
   $dbhost = 'localhost:3036';
   $dbuser = 'root';
   $dbpass = 'root';
   $conn = mysql_connect($dbhost, $dbuser, $dbpass);
   if(! $conn )
   {
     die('Could not connect: ' . mysql_error());
   }
   echo 'Connected successfully';
   mysql_close($conn);
   ?>
```

#打开浏览器访问IP/index.php，出现连接成功提示



四、服务器加固

1、运行Linux服务器基线检查脚本，输出excel表，检查不合规项，共发现5类不合规项，23个不合规检查点

- sh check_server_linux.sh 192.168.172.135

2、协议安全加固

#检查是否禁用root用户远程访问系统、检查ssh协议是否使用版本2，

参考步骤:
(1).执行备份:
#cp -p /etc/ssh/sshd_config /etc/ssh/sshd_config_bak
(2).新建一个普通用户并设置高强度密码(防止设备上只存在root用户可用时,无法远程访问):
#useradd username
#passwd username
(3).禁止root用户远程登录系统

3.1.编辑文件/etc/ssh/sshd_config(vi /etc/ssh/sshd_config),修改PermitRootLogin值为no并去掉注释.
PermitRootLogin no #则禁止了root从ssh登录。
3.2.重启ssh服务
#/etc/init.d/sshd restart
(4).修改ssh协议版本
4.1.编辑文件/etc/ssh/sshd_config(vi /etc/ssh/sshd_config),修改Protocol的值为2并去掉注释.
Protocol 2
4.2.重启ssh服务
#/etc/init.d/sshd restart

3、账户口令安全加固

#检查口令生存期

- 编辑文件/etc/login.defs,查看账号口令生存周期最大值:PASS_MAX_DAYS配置为1~90之间.
- 编辑文件/etc/login.defs,查看账号口令生存周期最小值:PASS_MIN_DAYS配置为10.
- 编辑文件/etc/login.defs,查看账号口令过期提前告警时间:PASS_WARN_AGE配置为7.

参考步骤:
(1)、执行备份:
#cp -p /etc/login.defs /etc/login.defs_bak
(2)、修改策略设置,编辑文件/etc/login.defs(vi /etc/login.defs),在文件中加入如下内容(如果存在则修改,不存在则添加):
PASS_MAX_DAYS 90
PASS_MIN_DAYS 10
PASS_WARN_AGE 7

#检查口令复杂度

- 检查口令长度
- 检查口令中包含的数字个数
- 检查口令中包含的小写字母个数
- 检查口令中包含的大写字母个数
- 检查口令中包含的特殊字符个数

"加固参考步骤:

- Linux（Redhat、CentOs、Fedora系统)

编辑文件/etc/pam.d/system-auth,在文件中找到如下内容:

password requisite pam_cracklib.so 将其修改为:

password requisite pam_cracklib.so try_first_pass retry=3 dcredit=-1 lcredit=-1 ucredit=-1 ocredit=-1 minlen=8
备注：至少包含一个数字、一个小写字母、一个大写字母、一个特殊字符、且密码长度>=8

- Linux（Suse系统)
  Suse9编辑/etc/pam.d/passwd、Suse10或以上编辑/etc/pam.d/common-password ， 在文件中加入如下内容(如果文件中存在password的行请首先注释掉):

password required pam_pwcheck.so nullok

password requisite pam_cracklib.so dcredit=-1 lcredit=-1 ucredit=-1 ocredit=-1 minlen=8 use_authtok

password required pam_unix2.so nullok use_first_pass use_authtok

- Linux（Debin、Ubuntu或者Linux Mint系统）
  编辑/etc/pam.d/common-password，并将其放在password required pam_unix.so use_authtok nullok md5 下面。

password requisite pam_cracklib.so 将其修改为:
password requisite pam_cracklib.so retry=3 minlen=8 difok=3 dcredit=-1 lcredit=-1 ucredit=-1 ocredit=-1

备注：设置严密的密码策略需要PAM模块来启用cracklib，cracklib在Redhat、CentOS、Fedora默认安装了，而Debin、Ubuntu或者Linux Mint可能未安装（如果common-password未找到pam_cracklib.so关键字或者配置好密码策略后，修改密码时提示：passwd：模块未知，则表示未安装），安装命令：sudo apt-get install libpam-cracklib"

4、其它安全加固

#登陆超时时间设置，检查是否设置定时帐户自动登出时间

参考配置:
(1).执行备份：
#cp -p /etc/profile /etc/profile_bak
(2).在/etc/profile文件增加以下两行(如果存在则修改,否则手工添加)：
#vi /etc/profile
TMOUT=300
#TMOUT按秒计算
export TMOUT

#检查是否使用PAM认证模块禁止wheel组之外的用户su为root

- 检查是否使用PAM认证模块进行su权限控制
- 检查是否禁止wheel组之外的用户su为root
- 检查该系统是否为Suse Linux
- 检查该系统是否为Ubuntu Linux

加固参考步骤:

第一步：编辑su文件(vi /etc/pam.d/su)

- Linux（Redhat系统适用、CentOs系统供参考）

(1)redhat4.x(32位)在文件开头加入如下两行(有则修改,没有则添加):

auth　　sufficient　/lib/security/$ISA/pam_rootok.so

auth　　required　/lib/security/$ISA/pam_wheel.so use_uid

注意：auth与sufficient之间由两个tab建隔开,sufficient与动态库路径之间使用一个tab建隔开

(2)redhat4.x(64位)在文件开头加入如下两行(有则修改,没有则添加):

auth　　sufficient　/lib64/security/$ISA/pam_rootok.so

auth　　required　/lib64/security/$ISA/pam_wheel.so use_uid

注意：auth与sufficient之间由两个tab建隔开,sufficient与动态库路径之间使用一个tab建隔开

(3)redhat5.x和redhat6.x在文件开头加入如下两行(有则修改,没有则添加):

auth　　sufficient　　pam_rootok.so

auth　　required　　pam_wheel.so use_uid

注意：auth与sufficient之间由两个tab建隔开,sufficient与动态库路径之间使用一个tab建隔开

- Linux（Ubuntu系统）

在文件中加入一行(有则修改,没有则添加)
auth　　required　pam_wheel.so group=wheel

第二步：将用户添加到wheel组

注意:(第一步加固表明只有wheel组中的用户才能使用su命令切换到root用户，因此必须将需要切换到root的用户添加到wheel组,以使它可以使用su命令成为root用户)

添加方法:usermod -G wheel username　#username为需要添加至wheel组的用户名称。

备注：如果系统不存在wheel组，则新增，新增方法：groupadd wheel。

5、认证授权加固

#检查/etc/profile文件umask缺省值

参考步骤:
一、首先对/etc/profile进行备份
#cp /etc/profile /etc/profile.bak
二、编辑文件/etc/profile,在文件末尾加上如下内容:
umask 027
三、执行以下命令让配置生效
#source /etc/profile

6、日志审计加固

#启用远程日志功能

- 检查redhat设备是否设置远程日志服务器，实际值为远程日志服务器地址或者域名,有值则合规
- 检查suse设备是否设置远程日志服务器

加固参考步骤:
第一步：

linux（Redhat、Ubuntu、CentOs、其他linux内核版本）

(1).编辑文件 /etc/syslog.conf 或者 /etc/rsyslog.conf，增加如下内容:

`*.*　　@Syslog` 日志服务器IP
注意：*和@之间存在的是tab键，非空格。

linux（Suse9版本）

(1).编辑文件/etc/syslog.conf 增加如下内容:

`*.*　　@Syslog` 日志服务器IP
注意：*和@之间存在的是tab键，非空格。

linux（Suse10或以上版本）
第一步:

(1)如属于/etc/syslog-ng/syslog-ng.conf 格式文件,则编辑文件,增加如下内容:

destination logserver { udp(""192.168.56.168"" port(514)); };

log { source(src); destination(logserver); };

注：以上ip：192.168.56.168日志服务器IP.

(2)如属于/etc/rsyslog.conf 格式文件,则编辑文件,增加如下内容:
`*.*    @Syslog` 日志服务器IP
注意：*和@之间存在的是tab键，非空格。

第二步：

重启syslog或rsyslog服务：
service syslog restart 或 /etc/init.d/syslog restart
service rsyslog restart 或 /etc/init.d/rsyslog restart

备注：Ubuntu 系统可能出现账号权限问题，需要提权，例如：sudo service syslog restart

#检查是否记录安全事件日志

- 检查syslog是否配置安全事件日志
- 检查rsyslog是否配置安全事件日志
- 检查syslog-ng是否配置安全事件日志

加固参考步骤:
第一步：
Linux（Redhat、Ubuntu、CentOs、其他linux内核版本）

(1)编辑文件/etc/syslog.conf 或者 /etc/rsyslog.conf,在文件中加入如下内容:

*.err;kern.debug;daemon.notice /var/log/messages
(2)其中/var/log/messages为日志文件，如果该文件不存在,则创建该文件,命令为：touch /var/log/messages
  备注：Ubuntu系统日志文件为:/var/log/dmesg；

(3)修改文件权限为640，命令为:chmod 640 /var/log/messages

Linux（Suse9版本）
(1)编辑文件/etc/syslog.conf,在文件中加入如下内容:

*.err;kern.debug;daemon.notice -/var/log/messages

(2)其中/var/log/messages为日志文件,如果该文件不存在,则创建该文件,命令为:touch /var/log/messages

(3)修改文件权限为640，命令为:chmod 640 /var/log/messages

Linux（Suse10或以上版本）
(1)如是/etc/syslog-ng/syslog-ng.conf 格式文件,编辑文件,在文件中加入如下内容:

filter f_msgs { level(err) or facility(kern) and level(debug) or facility(daemon) and level(notice); };

destination msgs { file(""/var/log/messages""); };

log { source(src); filter(f_msgs); destination(msgs); };

(2)如是/etc/rsyslog.conf 格式文件,编辑文件,在文件中加入如下内容:
*.err;kern.debug;daemon.notice   -/var/log/messages

(3)其中/var/log/messages为日志文件,如果该文件不存在,则创建该文件,命令为:touch /var/log/messages

(4)修改文件权限为640，命令为:chmod 640 /var/log/messages

第二步：
重启syslog或rsyslog服务：
service syslog restart 或 /etc/init.d/syslog restart
service rsyslog restart 或 /etc/init.d/rsyslog restart

备注：Ubuntu 系统可能出现账号权限问题，需要提权，例如：sudo service syslog restart

#日志文件安全

- 检查syslog服务状态
- 检查系统中是否存在权限>640的日志文件

检测步骤:

第一步：使用以下命令查看日志文件的权限

redhat5.x之前

#LOGDIR=if [-f /etc/syslog.conf];then cat /etc/syslog.conf| grep -v "^[[:space:]]#"|*awk '(($2!~/@/) && ($2!~//*) && ($2!~/-/)) {print $2}';fi;

#ls -l $LOGDIR 2>/dev/null|grep -v "[r-][w-]-[r-]-----"|awk '{print $1" "$8" "$9}';

#unset LOGDIR

redhat6.x之前:

#
#ls -l $LOGDIR 2>/dev/null|grep -v "[r-][w-]-[r-]-----"|awk '{print $1" "$8" "$9}';

#unset LOGDIR

suse:

#LOGDIR=cat /etc/syslog-ng/syslog-ng.conf|grep -v "^[[:space:]]*#"|grep "^destination"|grep file|cut -d" -f2;

#ls -l $LOGDIR 2>/dev/null|grep -v "[r-][w-]-[r-]-----"|awk '{print $1" "$8" "$9}';

#unset LOGDIR

判定条件:

不存在权限>640的日志文件则合规,否则不合规

第二步:
#chmod 640 file　　#检测步骤中输出的权限>640的日志文件