2_Engineer05 管理 web 进阶动态 web 安全 webSamba

环境准备:防火墙设置

虚拟机 server

```
]# firewall-cmd --set-default-zone=trusted
```

虚拟机 desktop

```
]# firewall-cmd --set-default-zone=trusted
```

一 文件夹权限

针对 DocumentRoot 网页目录的权限控制

httpd 运行身份(用户/组):apache

二 客户机地址限制

使用 <Directory> 配置区段

每个文件夹自动继承其父目录的 ACL 访问权限

除非针对子目录有明确设置

<Directory 目录的绝对路径>

.. ..

Require all denied|granted

Require ip IP 或网段地址 .. ..

</Directory>

案例 1:配置网页内容访问

在 Web 网站 http://server0.example.com 的 DocumentRoot 目录下创建一

个名为 private 的子目录,要求如下:

1.创建目录

```
]# cat /etc/httpd/conf.d/nsd01.conf  #查看 DocumentRoot
]# mkdir /var/www/abc01/private
```

2.从 http://classroom.example.com/pub/materials/private.html 下载一个文件副本到这个目录,重命名为 index.html, 不要对文件 index.html 的内容作任何修改

```
]# cd /var/www/abc01/private
]# wget http://classroom.example.com/pub/materials/privat
e.html
]# mv private.html index.html
]# firefox server0.example.com/private
```

3.从虚拟机 server0 上,任何人都可以浏览 private 的内容,但是从其他系统不能访问这个目录的内容

```
[root@server0 /]# vim /etc/httpd/conf/httpd.conf
[root@server0 /]# vim /etc/httpd/conf.d/nsd02.conf
<Directory  "/var/www/abc01/private">
   Require ip 172.25.0.11    #仅允许 172.25.0.11 访问
</Directory>
[root@server0 /]# systemctl restart httpd
```

虚拟机 desktop:

```
[root@desktop0 ~]# firefox server0.example.com/private
Forbidden
You don't have permission to access /private on this server.
```

案例 2:使用自定 Web 根目录

调整 Web 站点 http://server0.example.com 的网页目录,要求如下:

1 新建目录 /webroot,作为此站点新的网页目录

```
]# mkdir /webroot
]# echo '<h1> wo shi webroot' > /webroot/index.html
[root@server0 /]# vim /etc/httpd/conf.d/nsd01.conf
     <VirtUalHost *:80>
       ServerName server0.example.com
       DocumentRoot /webroot
     </VirtUalHost>
```

2 修改访问控制

```
[root@server0 /]# vim /etc/httpd/conf.d/nsd02.conf
<Directory  "/webroot">
Require all granted   #允许所有人可以访问
</Directory>
[root@server0 /]# systemctl restart httpd
```

3 修改 SELinux 策略:安全上下文值(打标签) 布尔值策略 非默认端口开放

```
]# semanage --help
]# semanage fcontext -l | less   #查看所有上下文值
]# ls -Zd /var/www/    #专查看目录上下文值
]# ls -Zd /webroot/
```

方式 1:参照标准目录,重设新目录的属性

格式: chcon [-R] --reference=模板目录 新目录

```
]# chcon  -R  --reference=/var/www  /webroot/
]# ls -Zd /webroot/
```

4 测试:

```
[root@desktop0 ~]# firefox server0.example.com
```

三 部署动态网站

静态网站的运行

服务端的原始网页 = 浏览器访问到的网页

由 Web 服务软件处理所有请求

文本(txt/html)、图片(jpg/png)等静态资源

动态网站的运行

服务端的原始网页 ≠ 浏览器访问到的网页

由 Web 服务软件接受请求,动态程序转后端模块处理

PHP 网页、Python 网页、JSP 网页.....

为站点 webapp0.example.com 配置提供动态 Web 内容,要求如下:

3.1 部署 Python 页面文件

```
]# cat /etc/httpd/conf.d/nsd01.conf  #查看 DocumentRoot
]# cd /var/www/abc03
]# wget http://classroom.example.com/pub/materials/webinf
o.wsgi
]#  ls
```

3.2 页面跳转(页面别名\地址重写)方便用户的访问

当用户访问 webapp0.example.com 将 webinfo.wsgi 页面进行呈现

格式: Alias 网络路径 实际路径

Alias / /var/www/abc03/webinfo.wsgi

当用户访问的时网页文件根目录时,跳转到/var/www/abc03/webinfo.wsgi

```
[root@server0 /]# vim /etc/httpd/conf.d/nsd01.conf
    <VirtUalHost *:80>
    ServerName webapp0.example.com
    DocumentRoot /var/www/abc03
    Alias  /   /var/www/abc03/webinfo.wsgi
    #当用户访问的是网页文件根目录时,跳转到/var/www/abc03/
    webinfo.wsgi
```

```
        </VirtUalHost>
    [root@server0 /]# systemctl restart httpd
    [root@desktop0 ~]# firefox webapp0.example.com
```

3.3 翻译 Python 页面代码

```
    [root@server0 /]# yum -y install mod_wsgi
    [root@server0 /]# vim /etc/httpd/conf.d/nsd01.conf
        <VirtUalHost *:80>
          ServerName webapp0.example.com
          DocumentRoot /var/www/abc03
          WsgiScriptAlias  /  /var/www/abc03/webinfo.wsgi
    </VirtUalHost>
    [root@server0 /]# systemctl restart httpd
```

页面内容显示:

UNIX 时间戳:从 1970-1-1 0:0:0 到达现在时间,所经历的秒数

```
    [root@desktop0 ~]# firefox webapp0.example.com
```

3.4 此虚拟 Web 主机侦听在端口 8909

```
    [root@server0 /]# vim /etc/httpd/conf.d/nsd01.conf
        Listen 8909              #设置 httpd 程序监听 8909 端口
        <VirtUalHost *:8909>     #设置虚拟 Web 主机监听 8909 端口
          ServerName webapp0.example.com
```

```
        DocumentRoot /var/www/abc03
        WsgiScriptAlias /  /var/www/abc03/webinfo.wsgi
    </VirtUalHost>
]# semanage port -l  | grep http  #查看关于 http 开放的端口
]# semanage port -a -t http_port_t  -p tcp 8909
//此命令会占用较多内存, -a 添加  -t 类型  -p 协议
]# systemctl restart httpd
```

测试验证: firefox webapp0.example.com:8909

总结:访问时端口优先级最高

四 安全 Web 服务

4.1 PKI 公钥基础设施

Public **K**ey **I**nfrastructure,公钥基础设施

公钥:主要用来加密数据

私钥:主要用来解密数据(与相应的公钥匹配)

数字证书:证明拥有者的合法性/权威性(单位名称、有效期、公钥、颁发机构及签 名、.....)

Certificate Authority,数字证书授权中心:负责证书的申请/审核/颁发/鉴定/撤销等管　理工作

数据证书授权中心:虚拟机 classroom

4.2 虚拟机 server: 为站点 www0.example.com 配置安全加密的 Web 内容

部署网站证书(营业执照)

]# cd **/etc/pki/tls/certs/**

]# wget http://classroom.example.com/pub/tls/certs/server0.crt

]# ls

部署网站的根证书(工商局的信息)

]# cd **/etc/pki/tls/certs/**

]# wget http://classroom.example.com/pub/example-ca.crt

]# ls

部署解密数据的私钥

]# cd **/etc/pki/tls/private/**

]# wget http://classroom.example.com/pub/tls/private/server0

.key

]# ls

安装可以进行加密支持的软件 **mod_ssl**

[root@server0 /]# yum -y install mod_ssl

[root@server0 /]# vim **/etc/httpd/conf.d/ssl.conf**

 59 DocumentRoot "/var/www/abc02"

 60 ServerName www0.example.com:443

100 SSLCertificateFile /etc/pki/tls/certs/server0.crt

     #指定网站证书

107 SSLCertificateKeyFile /etc/pki/tls/private/server0.key

#指定解密的私钥

122 SSLCACertificateFile /etc/pki/tls/certs/example-ca.crt

#指定网站的根证书

[root@server0 /]# systemctl restart httpd

[root@server0 /]# firefox https://www0.example.com

我已了解可能的风险--->添加例外---->确认安全例外

五 Samba 共享服务

Windows 与 Linux 跨平台的共享

smb(用户验证通信协议) cifs(Samba 独有文件系统)

程序名(服务名):smb

虚拟机 server:

1.安装软件包

[root@server0 /]# yum -y install samba

2.创建 Samba 共享帐号

建立在本地用户的基础上

采用独立的密码,与用户登录系统的密码不同

[root@server0 /]# useradd harry #linux 添加用户命令

[root@server0 /]# **pdbedit -a** harry #添加为 samba 帐号

new password:

```
retype new password:
[root@server0 /]# pdbedit -L          #查看所有的 samba 帐号
[root@server0 /]# pdbedit -x harry    #删除 samba 帐号 harry
[root@server0 /]# pdbedit -a harry
```

3.创建共享目录及配置共享

```
[root@server0 /]# mkdir /public
[root@server0 /]# echo haha > /public/1.txt
[root@server0 /]# vim /etc/samba/smb.conf
      [nsd]       #设置共享名
      path = /public   #设置实际共享的路径
[root@server0 /]# systemctl restart smb    //重启服务
```

4.修改 SELinux 策略: **布尔值策略**(服务功能的开关)

```
[root@server0 /]# getsebool -a | grep samba
[root@server0 /]# setsebool samba_export_all_ro on
[root@server0 /]# getsebool -a | grep samba
```

客户端:虚拟机 desktop0

1.安装软件包,支持 cifs 文件系统

```
[root@desktop0 ~]# yum -y install cifs-utils
```

2.进行挂载访问

```
]# mkdir /mnt/smb
```

格式: mount -o user=用户名,pass=密码

#服务器 IP 地址/共享名 挂载点目录

]# mount -o user=harry,pass=123

#172.25.0.11/nsd /mnt/smb/

]# df -h

]# ls /mnt/smb/

3.开机自动挂载/etc/fstab

#172.25.0.11/nsd /mnt/smb cifs

defaults,user=harry,pass=123,_netdev 0 0

[root@desktop0 ~]# umount /mnt/smb/

[root@desktop0 ~]# df -h

[root@desktop0 ~]# mount -a

[root@desktop0 ~]# df -h