2_Engineer02 防火墙 selinux

案例: 编写一个判断脚本,在 server0 上创建 /root/foo.sh 脚本

1)当运行/root/foo.sh redhat,输出为 fedora

2)当运行/root/foo.sh fedora,输出为 redhat

3)当没有任何参数或者参数不是 redhat 或者 fedora 时,

4)其错误输出产生以下信息: /root/foo.sh redhat|fedora

```
[root@server0 ~]# vim  /root/foo.sh
    #!/bin/bash
    # 判断$1 参数的脚本
    if [ $#  -eq  0 ];then      #判断用户是否输入参数
    echo '/root/foo.sh  redhat|fedora' >&2   #变成错误输出
    exit 3                      #脚本退出返回的状态值
    elif [ $1 == redhat ];then #判断是否为 redhat
    echo fedora
    elif [ $1 == fedora ];then #判断是否为 fedora
    echo redhat
    else
    echo '/root/foo.sh  redhat|fedora' >&2  #变成错误输出
    exit 4   #脚本退出返回的状态值
    fi
```

案例: 编写一个批量添加用户脚本,在 server0 上创建 /root/batchusers 脚本

1)此脚本要求提供用户名列表文件作为参数

2)如果没有提供参数,此脚本应该给出提示

Usage: /root/batchusers,退出并返回相应值

3)如果提供一个不存在的文件,此脚本应该给出提示 Input file not found,退出并返回相应值

4)新用户的登录 Shell 为/bin/false,无需设置密码

5)用户列表测试文件: http:#classroom/pub/materials/userlist

```
[root@server0 ~]# vim /root/userlist
     duanwu
     zhongqiu
     zhsan
     lisi
     dc
[root@server0 ~]# vim  /root/batchusers
     #!/bin/bash
     if  [ $# -eq 0 ];then              #判断是否有参数
          echo  'Usage: /root/batchusers' >&2
          exit 2
     elif [ -f  $1  ];then              #判断文件是否存在
```

```
        for  a  in $(cat $1)
        do
        useradd -s /bin/false  $a  &> /dev/null
        echo $a 创建成功
        done
    else
        echo 'Input file not found' >&2
        exit 3
    fi
[root@server0 ~]# /root/batchusers  /root/userlist
```

一 系统安全保护

1.1 SELinux 安全机制

Security-**E**nhanced **Linux**

美国 NSA 国家安全局主导开发,一套增强 Linux 系统安全的强制访问控制体系

集成到 Linux 内核(2.6 及以上)中运行

RHEL7 基于 SELinux 体系针对用户、进程、目录和文件提供了预设的保护策略,以及管理工具

1.2 SELinux 的运行模式

enforcing(强制)、permissive(宽松)、disabled(彻底禁用)

任何模式切换成 **disabled** 模式,都要经历重启

1.3 切换运行模式

临时切换: setenforce 1|0

永久设置: 修改**/etc/selinux/config** 文件

SELINUX=permissive #在文件中将此处设置为需要的模式

虚拟机 server0

```
[root@server0 ~]# getenforce      #查看当前的状态
[root@server0 ~]# setenforce  0   #临时修改为宽松模式
[root@server0 ~]# getenforce
[root@server0 ~]# vim /etc/selinux/config
SELinux=permissive    #修改配置文件,永久设置运行模式
```

虚拟机 desktop0

```
[root@desktop0 ~]# getenforce
[root@desktop0 ~]# setenforce  0
[root@desktop0 ~]# getenforce
[root@desktop0 ~]# vim /etc/selinux/config
SELinux=permissive
```

二 配置用户环境

2.1 alias 别名设置

查看已设置的别名

alias [别名名称]

定义新的别名

alias 别名名称='实际执行的命令行'

取消已设置的别名

unalias [别名名称]

影响指定用户的 bash 解释环境

~/.bashrc,每次开启 bash 终端时生效

影响所有用户的 bash 解释环境

/etc/bashrc,每次开启 bash 终端时生效

```
[root@server0 ~]# vim /root/.bashrc
alias hello='echo hello'
[root@server0 ~]# vim  /home/student/.bashrc
alias hi='echo hi'
[root@server0 ~]# vim /etc/bashrc
alias dc='echo tc'
```

新开一个终端验证

三 http

虚拟机 server0:搭建 Web 服务器

Web 服务:提供网页内容

实现 Web 服务的软件: httpd Nginx Tomcat

实现 **Web** 通信的协议: **http(**超文本传输协议**)**

3.1 安装 **httpd** 软件

[root@server0 ~]# yum -y install httpd

3.2 重启程序**(**重启服务**)**开机自启

[root@server0 ~]# **systemctl restart httpd** #服务名称 httpd

[root@server0 ~]# **systemctl enable httpd** #设置开机自启

3.3 本机测试访问

[root@server0 ~]# firefox 172.25.0.11

3.4 书写自己的页面文件

默认存放路径: /var/www/html

默认首页文件名称: index.html

[root@server0 ~]# vim /var/www/html/index.html

<marquee><font color=red><h1>NSD1906 haha

滚动 字体颜色 标题字体

[root@server0 ~]# firefox 172.25.0.11 #测试

四 **FTP**

虚拟机 server0:搭建 FTP 服务

FTP 服务:传输数据 FTP 协议:文件传输协议

实现 FTP 服务软件:vsftpd 默认共享路径:/var/ftp

4.1 安装 **vsftpd** 软件

[root@server0 ~]# yum -y install vsftpd

4.2 重启程序(重启服务)\开机自起

[root@server0 ~]# **systemctl restart vsftpd** #服务名称 vsftpd

[root@server0 ~]# **systemctl enalbe vsftpd** #设置开机自启

[root@server0 ~]# firefox ftp://172.25.0.11

五 防火墙策略管理

5.1 防火墙作用: 隔离 众多的策略,允许出站,严格控制入站

5.2 防火墙分类: 硬件防火墙 软件防火墙

5.3 firewalld 服务基础

系统服务:firewalld

管理工具:firewall-cmd、firewall-config

5.4 预设安全区域

根据所在的网络场所区分,预设保护规则集

public: 仅允许访问本机的 ssh dhcp ping 服务

trusted: 允许任何访问

block: 阻塞任何来访请求(明确拒绝,有回应客户端)

drop: 丢弃任何来访的数据包(没有回应,节省服务端资源)

根据数据包的源 IP 地址

数据包组成: 源 IP 地址 目标 IP 地址 数据

5.5 防火墙判定原则:

查看数据包的源 IP 地址,然后查看自己所有的区域,那个区域中有该源 IP 地址的规则,则进入该区域

5.6 区域查看\设置\服务增删\永久设置\拒绝访问\端口映射

5.6.1 查看默认区域

]# firewall-cmd --get-default-zone

5.6.2 查看区域规则

]# firewall-cmd --zone=public --list-all

#zone 等于 trusted\public\drop\block 中任意一种时,代表查看该区域的规则

]# firewall-cmd --list-all

--zone=XXXX 被省略时,代表查看系统当前生效的防火墙区域的区域规则

5.6.3 设置默认区域

]# firewall-cmd --set-default-zone=trusted\public\drop\block

5.6.4 区域服务增删

]# firewall-cmd --zone=public **--add-service=ftp\http**

]# firewall-cmd --zone=public **--remove-service=ftp\http**

]# firewall-cmd **--add-service=ftp\http**

]# firewall-cmd **--remove-service=ftp\http**

--zone=XXXX 被省略时,代表在系统当前生效的防火墙区域内添加\删除服务

5.6.5 永久设置防火墙规则

]# firewall-cmd **--permanent** --zone=public --add-service=http

]# firewall-cmd **--permanent** --zone=public --add-service=ftp

5.6.6 单独拒绝\修改拒绝某 IP 地址的访问

虚拟机 server:将虚拟机 desktop 的 IP 地址写入 block

]# firewall-cmd --zone=block **--add-source=172.25.0.10**

]# firewall-cmd --zone=block **--remove-source=172.25.0.10**

#在 block 区域内添加\删除 IP 地址

5.6.7 端口映射

端口: 协议或程序或服务的编号

利用 root 可以改变端口,而且一个程序可以具备多个端口

]# **firewall-cmd --permanent --zone=public --add-forward-port**

=port=5423:proto=tcp:toport=80

[root@desktop0 ~]# firefox 172.25.0.11**:5423**

#端口映射后访问时需要添加端口号

5.6.8 重新加载防火墙设置

]# **firewall-cmd --reload**

#所有设置在设置完成后,都最好重新加载防火墙设置

六 互联网常见的协议及默认端口:

http:	超文本传输协议	端口:80
https:	安全的超文本传输协议	端口:443
DNS:	域名解析协议	端口:53
FTP:	文件传输协议	端口:21
tftp:	简单的文件传输协议	端口:69
telnet:	远程管理协议(明文传输)	端口:23
ssh:	远程管理协议(加密传输)	端口:22
SMTP:	邮件协议(用户发邮件)	端口:25
pop3:	邮件协议(用户收邮件)	端口:110
snmp:	简单的网络管理协议	端口:161