案例5: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

echo 'Usage: /root/batchusers' >&2

exit 3

elif [ -f $1 ];then

for a in $(cat $1)

do

useradd -s /bin/false $a &> /dev/null

echo $a用户创建成功

done

else

echo Input file not found >&2

exit 4

fi

####################################################

系统安全保护

SELinux概述

• Security-Enhanced 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

SELinux运行模式的切换

• SELinux的运行模式

– enforcing(强制)、permissive(宽松)

– disabled(彻底禁用)

任何模式切换到disabled(彻底禁用),都必须经历重启系统

• 切换运行模式

– 临时切换:setenforce 1|0

– 固定配置:/etc/selinux/config 文件

虚拟机Server0:

[root@server0 ~]# getenforce #查看当前系统SELinux状态

Enforcing

[root@server0 ~]# setenforce 0 #当前修改SELinux状态

[root@server0 ~]# getenforce

Permissive

[root@server0 ~]# vim /etc/selinux/config #永久配置文件

SELINUX=permissive

虚拟机desktop0:

[root@desktop0 ~]# setenforce 0

[root@desktop0 ~]# getenforce

Permissive

[root@desktop0 ~]# vim /etc/selinux/config

SELINUX=permissive

###################################################

配置用户环境

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]

用户个性化配置文件

• 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

虚拟机Server:

[root@server0 ~]# vim /home/student/.bashrc

alias hi='echo hi'

[root@server0 ~]# vim /root/.bashrc

alias hello='echo hello'

[root@server0 ~]# vim /etc/bashrc

alias haxi='echo xiha'

###################################################

防火墙策略管理

虚拟机server构建Web服务:提供一个页面内容

1.安装软件包httpd

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

[root@server0 ~]# rpm -q httpd

2.重启httpd程序

[root@server0 ~]# systemctl restart httpd #重启

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

ln -s '/usr/lib/systemd/system/httpd.service' '/etc/systemd/system/multi-user.target.wants/httpd.service'

[root@server0 ~]#

3.本机测试访问:

[root@server0 ~]# firefox 172.25.0.11

4.书写页面文件

存放网页文件位置:/var/www/html/

网页文件名字:index.html

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

<marquee><font color=red><h1>NSD1905阳光明媚

滚动 字体颜色 标题字体

[root@server0 ~]# firefox 172.25.0.11

####################################################

虚拟机server构建FTP服务:文件传输

1.安装软件vsftpd

[root@server0 ~]# yum info vsftpd

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

2.重启服务

[root@server0 ~]# systemctl restart vsftpd

[root@server0 ~]# systemctl enable vsftpd

ln -s '/usr/lib/systemd/system/vsftpd.service' '/etc/systemd/system/multi-user.target.wants/vsftpd.service'

3.本机测试验证

默认共享路径:/var/ftp/

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

####################################################

防火墙: 隔离

严格过滤入站,允许出站

硬件防火墙

软件防火墙:本机防护

firewalld服务基础

• 系统服务:firewalld

• 管理工具:firewall-cmd、firewall-config

• 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 sshd dhcp ping服务

– trusted:允许任何访问

– block:阻塞任何来访请求(明确拒绝)

– drop:丢弃任何来访的数据包(直接丢弃,不给客户端回应,节省资源)

数据包: 源IP地址 目标IP地址 数据

防火墙匹配原则:匹配及停止

1.查看数据包中源IP地址,然后查询所有区域中规则,哪一个区域中有该源IP地址的规则,则进入哪一个区域

2.进入默认区域(public)

####################################################

虚拟机server:

]# firewall-cmd --get-default-zone #查看防火墙默认区域

虚拟机desktop

]# ping 172.25.0.11 #可以通信

虚拟机server:

]# firewall-cmd --set-default-zone=block #修改默认区域

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

虚拟机desktop

]# ping 172.25.0.11 #不可以通信,有回应

虚拟机server:

]# firewall-cmd --set-default-zone=drop

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

虚拟机desktop

]# ping 172.25.0.11 #不可以通信,没有回应

####################################################

互联网常见协议:

http:超文本传输协议 默认端口80

https:安全超文本传输协议 默认端口443

FTP:文件传输协议 默认端口21

TFTP:简单的文件传输协议 默认端口69

telnet:远程管理协议 默认端口23

DNS:域名解析协议 默认端口53

snmp:简单的网络管理协议 默认端口161

smtp:邮件协议(发邮件) 默认端口25

pop3:邮件协议(收邮件) 默认端口110

区域中添加协议

虚拟机server:

]# firewall-cmd --set-default-zone=public

]# firewall-cmd --get-default-zone #查看防火墙默认区域

]# firewall-cmd --zone=public --list-all #查看区域策略

虚拟机desktop:

]# firefox 172.25.0.11 #失败

]# firefox ftp://172.25.0.11 #失败

虚拟机server:

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

]# firewall-cmd --zone=public --list-all #查看区域策略

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

]# firewall-cmd --zone=public --list-all #查看区域策略

虚拟机desktop:

]# firefox 172.25.0.11 #成功

]# firefox ftp://172.25.0.11 #成功

#################################################

• 配置规则的位置

– 永久(permanent)

]# firewall-cmd --reload #重新加载防火墙所有配置

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

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

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

]# firewall-cmd --reload

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

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

]# firewall-cmd --reload

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

###################################################

了解:区域中添加源IP地址

单独拒绝虚拟机desktop,所有的访问

将虚拟机desktop的源IP地址,写入区域block

虚拟机server:

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

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

虚拟机desktop

]# firefox 172.25.0.11

]# firefox ftp://172.25.0.11

]# ping 172.25.0.11

################################################

宽松:默认区域为trsuted,单独拒绝的源IP地址写入block

严格:默认区域为block,单独允许的源IP地址写入trsuted

#################################################

什么是端口: 协议或程序的编号

数据包: 源IP地址 目标IP地址 数据 目标端口

实现本机的端口映射

• 本地应用的端口重定向(端口1 --> 端口2)

– 从客户机访问端口1的请求,自动映射到本机端口2

– 比如,访问以下两个地址可以看到相同的页面:

客户端: 172.25.0.11:5423---->172.25.0.11:80

虚拟机server

]# firewall-cmd --permanent --zone=public

--add-forward-port=port=5423:proto=tcp:toport=80

]# firewall-cmd --reload

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

虚拟机desktop:

]# firefox 172.25.0.11:5423

##################################################