Engineer03

SELinux 安全机制

• 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)**

变成disabled状态,必须经历重启

• 切换运行模式

– 临时切换:**setenforce 1|0** **1代表强制模式 0代表宽松模式**

– 查看当前模式**:getenforce**

– 固定配置:**/etc/selinux/config** 文件

防火墙策略基本使用

一 搭建基本web服务

1.安装httpd软件包

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

2.重起httpd服务

[root@server0 ~]# systemctl restart httpd

[root@server0 ~]# systemctl enable httpd

3.本机访问测试

[root@server0 ~]# firefox 172.25.0.11

4.书写网页文件

**默认存放网页文件路径：/var/www/html**

**默认网页文件名称：index.html**

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

<marquee><font color=red><h1>NSD1811 阳光明媚

滚动 字体颜色 红色 最大字体

[root@server0 ~]# firefox 172.25.0.11

二、搭建基本FTP服务

1.安装vsftpd软件包

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

2.重起httpd服务

[root@server0 ~]# systemctl restart vsftpd

[root@server0 ~]# systemctl enable vsftpd

1. 本机访问测试

**默认共享数据的路径:/var/ftp**

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

防火墙策略管理

作用:隔离过滤

硬件防火墙

软件防火墙

firewalld服务基础

RHEL7的防火墙体系

系统服务:firewalld服务

管理工具:firewall-cmd、 firewall-config

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sshd、dhcp、ping等少数几个服务

– **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（没有回应，直接丢弃，节省资源）

数据包:源IP地址 目标IP地址 数据

防火墙判定的规则:

1. 查看客户端请求中源IP地址,然后查阅自己哪个区域,有该IP地址的规则,则进入该区域
2. 进入默认区域public

默认区域的修改

虚拟机Server0：

]# **firewall-cmd --get-default-zone**  #查看默认区域

虚拟机Desktop0：

]# ping -c 2 172.25.0.11 #可以通信

虚拟机Server0：

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

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

虚拟机Desktop0：

]# ping -c 2 172.25.0.11 #不可以通信，有回应

虚拟机Server0：

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

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

虚拟机Desktop0：

]# ping -c 2 172.25.0.11 #不可以通信，没有回应

public区域的服务的协议添加

虚拟机Server0：

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

]# firewall-cmd --get-default-zone #查看公共区域

]# firewall-cmd --zone=public --list-all #查看区域规则

虚拟机Desktop0：

]# firefox 172.25.0.11 #不可以访问

虚拟机Server0：在public区域添加规则,添加服务访问协议http,ftp

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

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

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

虚拟机Desktop0：

]# firefox 172.25.0.11 #可以访问

]# firefox ftp://172.25.0.11 #可以访问

常见互联网应用协议：

**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：简单文件传输协议 默认端口：69**

**DNS：域名解析协议 默认端口：53**

**telnet：远程管理协议 默认端口：23**

**SMTP：邮件协议（用户发邮件） 默认端口：25**

**pop3：邮件协议（用户收邮件） 默认端口：110**

**SNMP：网络管理协议 默认端口：161**

永久在public区域中添加协议

• 配置规则的位置

– 永久(permanent)

虚拟机Server0：

]# firewall-cmd --reload #重新加载防火墙所有规则

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

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

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

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

]# firewall-cmd --reload #重新加载防火墙所有规则

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

临时删除

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

永久删除

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

]# firewall-cmd --reload

源IP地址规则的添加

虚拟机Server0：单独拒绝Desktop0访问

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

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

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

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:

<http://172.25.0.11:5423/>

http://172.25.0.11

端口:协议或服务或程序编号 标识作用

IP地址:在互联网寻找到相应的主机

端口:在主机上标识 协议或服务或程序

数据包:源IP地址 目标IP地址 数据 目标端口

虚拟机desktop:

[root@desktop0 ~]# firefox 172.25.0.11:5423 #访问失败

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:

[root@desktop0 ~]# firefox 172.25.0.11:5423 #访问成功S