实验 08：安全加固

一、实验目的

1、掌握防火墙服务的配置管理；

2、掌握防火墙规则的设计与配置；

3、掌握基于防火墙的业务安全防护配置。

二、实验学时

2 学时

扫码看操作演示

三、实验类型

设计研究

四、实验需求

1、硬件

每人配备计算机 1 台。

2、软件

安装 VMware WorkStation Pro 或 Oracle VM VirtualBox 软件，安装 Mobaxterm 软件。

3、网络

本地主机与虚拟机能够访问互联网，虚拟机网络不使用 DHCP 服务。

4、工具

无。

五、实验任务

1、完成防火墙服务的管理；

2、完成防火墙日志的配置；

3、完成使用防火墙提升服务的安全性。

六、实验内容及步骤

1、本实验需要 VM 1 台。

2、本实验 VM 配置信息如下表所示。

虚拟机配置	操作系统配置
虚拟机名称：VM-Lab-08-Task-01-172.31.0.181 内存：2GB CPU：1 颗，1 核心 虚拟磁盘：20GB 网卡：1 块，NAT	主机名：Lab-08-Task-01 IP 地址：172.31.0.181 子网掩码：255.255.255.0 网关：172.31.0.254 DNS：172.31.0.254

3、本实验拓扑图。

无。

4、本实验操作演示视频。

本实验操作演示视频为视频集的第 8 集：

https://www.bilibili.com/video/BV1iH4y1c7ft?p=8

七、实验考核

1、使用 SELinux 提升系统的安全性

1.1 配置 SELinux

（1）管理 SElinux 的工作模式

使用 getenforce 命令查看当前的工作模式，使用 setenforce 命令在强制模式和宽容模式间进行切换。

```
# 查看当前 SELinux 的工作模式
[root@Lab-08-Task-01 ~]# getenforce
# 默认为强制模式
Enforcing

# 修改 SELinux 的工作模式为宽容模式
[root@Lab-08-Task-01 ~]# setenforce 0
# 查看修改后模式
[root@Lab-08-Task-01 ~]# getenforce
Permissive

# 恢复 SELinux 的运行模式为强制模式
[root@Lab-08-Task-01 ~]# setenforce 1
# 查看修改后模式
[root@Lab-08-Task-01 ~]# getenforce
Enforcing
```

（2）更改 SELinux 的工作模式和运行状态

永久修改工作模式或者关闭 SELinux，需对 SELinux 的配置文件进行修改，修改完成后重新启动操作系统方可生效。

```
# 查看系统当前 SELinux 的运行状态
[root@Lab-08-Task-01 ~]# cat /etc/selinux/config | grep '^SELINUX=
'
SELINUX=enforcing

# 修改配置文件实现 SELinux 为关闭状态
[root@Lab-08-Task-01 ~]# sed -i 's/SELINUX=enforcing/SELINUX=dis
```

```
abled/g' /etc/selinux/config
# 重启操作系统
[root@Lab-08-Task-01 ~]# reboot
# 检验状态修改是否生效
[root@Lab-08-Task-01 ~]# getenforce
Disabled
# 修改配置文件实现 SELinux 为开启状态
[root@Lab-08-Task-01 ~]# sed -i 's/SELINUX=disabled/SELINUX=enf
orcing/g' /etc/selinux/config
# 重启操作系统
[root@Lab-08-Task-01 ~]# reboot
# 检验状态修改是否生效
[root@Lab-08-Task-01 ~]# getenforce
Enforcing
```

1.2 安装 SELinux 管理工具

SELinux 常用的管理工具有 chcon、semange 等，本实验步骤选用 semange 工具。semange 工具集成在 policycoreutils-python-utils 软件中，可使用 yum 工具安装。

```
# 使用 yum 工具安装 policycoreutils-python-utils
[root@Lab-08-Task-01 ~]# yum install -y policycoreutils-python-utils
```

1.3 依据场景设计 SELinux

通过 SELinux 提升用户操作的安全性。

需求描述：

修改系统用户映射到 SELinux 内核用户的类型，实现创建用户时 SELinux 用户类型为 user_u。

```
# 查看系统默认用户类型
[root@Lab-08-Task-01 ~]# semanage login -l
登录名                  SELinux 用户            MLS/MCS 范围
    服务
# 系统默认用户的 SELinux 用户类型为 unconfined_u（未限制）
__default__             unconfined_u            s0-s0:c0.c1023       *
root                    unconfined_u            s0-s0:c0.c1023       *

# 修改系统默认用户的 SELinux 用户类型
[root@Lab-08-Task-01 ~]# semanage login -m -s user_u -r s0 __def
ault__

# 修改后重新验证查看是否配置成功
[root@Lab-08-Task-01 ~]# semanage login -l
登录名                  SELinux 用户            MLS/MCS 范围
    服务
# 查看系统默认用户的 SELinux 用户类型已经更改为 user_u(普通用户类型)
__default__             user_u                  s0                   *
root                    unconfined_u            s0-s0:c0.c1023       *

# 创建新的用户，并使用新用户进行登录验证
[root@Lab-08-Task-01 ~]# adduser testuser
#设置密码
```

```
[root@Lab-08-Task-01 ~]# passwd testuser

# 切换为新用户进行登录，查看该用户的安全上下文信息
[testuser@Lab-06-Task-01 ~]# id -Z
user_u:user_r:user_t:s0
```

2、使用防火墙进行系统安全防护

2.1 配置防火墙

（1）管理防火墙服务

对防火墙服务的管理包括查看防火墙 Firewalld 服务状态、开启、关闭、重启、重新载入防火墙策略等。

```
# 查看防火墙 Firewalld 服务状态
[root@Lab-08-Task-01 ~]# systemctl status firewalld

# 关闭防火墙服务
[root@Lab-08-Task-01 ~]# systemctl stop firewalld

# 开启防火墙服务
[root@Lab-08-Task-01 ~]# systemctl start firewalld

# 重启防火墙服务
[root@Lab-08-Task-01 ~]# systemctl restart firewalld

# 设置防火墙为开机不自启
[root@Lab-08-Task-01 ~]# systemctl disable firewalld

# 设置防火墙为开机自启动
[root@Lab-08-Task-01 ~]# systemctl enable firewalld

# 重新载入防火墙规则
[root@Lab-08-Task-01 ~]# firewall-cmd --reload
```

（2）配置防火墙日志策略

对防火墙日志的配置有全局日志配置和规则日志配置两部分。全局日志配置是对防火墙日志规则进行配置，防火墙日志服务由系统 rsyslog 服务进行管理，日志默认存放在/var/log/firewalld 日志文件中，日志文件基于日期时间自动归档。规则日志配置是设置防火墙触发特定防火墙规则时记录日志的方式。

```
# 全局日志配置
# 实现防火墙对单播网络通信的日志记录。
# 防火墙日志存放目录变更为/var/log/firewalldlog。
# 防火墙日志记录等级调整为所有等级的日志均记录。

# 使用 vi 命令编辑/etc/firewalld/firewalld.conf 文件
[root@Lab-08-Task-01 ~]# vi /etc/firewalld/firewalld.conf
# ----------/etc/firewalld/firewalld.conf 文件----------
# firewalld.conf 配置文件内容较多，本部分仅显示与防火墙日志配置有关的内容
# 将 LogDenied=off 改为 LogDenied=unicast，实现对单播网络通信的日志
```

```
记录
LogDenied=unicast
# --------------------/etc/firewalld/firewalld.conf 文件--------------------
# 创建防火墙日志存放目录
[root@Lab-08-Task-01 ~]# mkdir /var/log/firewalldlog
# 重新载入配置文件
[root@Lab-08-Task-01 ~]# systemctl reload firewalld

# 使用 vi 命令编辑/etc/rsyslog.conf 文件
[root@Lab-08-Task-01 ~]# vi /etc/rsyslog.conf
# --------------------/etc/rsyslog.conf 文件--------------------
# 在配置文件中增加以下内容，kern.*表示记录所有等级的系统内核产生的日志信息
kern.*                                                  /var/log/firewalldlog/loginfo
# --------------------/etc/rsyslog.conf 文件--------------------
# 重启日志相关服务
[root@Lab-08-Task-01 ~]# systemctl restart rsyslog

# 规则日志配置
# 允许本地主机（172.20.1.40）通过 httpd 服务访问服务器。
# 实现触发规则的通信的日志记录。
# 设置日志记录的频率为每秒最多 3 条。
# 根据防火墙规则要求配置
[root@Lab-08-Task-01 ~]# firewall-cmd --permanent --add-rich-rule='rule family=ipv4 source address=172.20.1.40 service name="http" log level=notice prefix="HTTP" limit value="3/s" accept'

# 重新载入防火墙配置使其生效
[root@Lab-08-Task-01 ~]# firewall-cmd --reload
```

2.2 依据场景设计防火墙

（1）通过防火墙指定端口和协议允许访问。

需求描述：

第一：打开 443/TCP 端口。

第二：永久打开 3690/TCP 端口。

第三：永久打开 100-500/TCP 端口（指定范围内端口全部打开）。

```
# 打开 443/TCP 端口
[root@Lab-08-Task-01 ~]# firewall-cmd --add-port=443/tcp

# 永久打开 3690/TCP 端口
[root@Lab-08-Task-01 ~]# firewall-cmd --add-port=3690/tcp --permanent

# 永久打开 100-500/TCP 端口（指定范围内端口全部打开）
[root@Lab-08-Task-01 ~]# firewall-cmd --add-port=100-500/tcp --permanent

# 重新载入防火墙配置
```

```
[root@Lab-08-Task-01 ~]# firewall-cmd --reload
```

（2）通过防火墙指定服务允许/禁止访问。

需求描述：

第一：允许访问本机的 http、https 服务。

第二：允许访问本机的 zabbix-server 服务。

第三：禁止访问本机的 cockpit、dhcpv6-client 服务。

第四：启用 SYN、ICMP 洪泛攻击保护。

```
# 允许访问本机的 http、https 服务
[root@Lab-08-Task-01 ~]# firewall-cmd --permanent --add-service=http
[root@Lab-08-Task-01 ~]# firewall-cmd --permanent --add-service=https

# 允许访问本机的 zabbix-server 服务
[root@Lab-08-Task-01 ~]# firewall-cmd --permanent --add-service=zabbix-server

# 禁止访问本机的 cockpit、dhcpv6-client 服务
[root@Lab-08-Task-01 ~]# firewall-cmd --permanent --remove-service=cockpit
[root@Lab-08-Task-01 ~]# firewall-cmd --permanent --remove-service=dhcpv6-client

# 重新载入防火墙配置
[root@Lab-08-Task-01 ~]# firewall-cmd --reload
```

（3）通过防火墙指定 IP 地址允许/禁止访问。

需求描述：

第一：允许来自 IP 地址为 172.31.0.111 的主机的流量通过防火墙。

第二：禁止来自 IP 地址为 172.31.1.121 的主机的流量通过防火墙。

```
# 允许来自 IP 地址为 172.31.0.111 的主机的流量通过防火墙
[root@Lab-08-Task-01 ~]# firewall-cmd --permanent --add-source=172.31.0.111

# 禁止来自 IP 地址为 172.31.1.121 的主机的流量通过防火墙
[root@Lab-08-Task-01 ~]# firewall-cmd --permanent --remove-source=172.31.0.121

# 重新载入防火墙配置
[root@Lab-08-Task-01 ~]# firewall-cmd --reload
```

（4）通过防火墙提升远程管理服务安全性。

需求描述：

第一：允许地址范围 172.20.1.40/24 内的客户端远程连接服务器，进行远程管理维护。

第二：客户端远程连接服务器时，每分钟最多允许 5 次远程连接，禁止频繁请求。

```
# 使用 firewall-cmd 命令删除默认 ssh 服务规则
[root@Lab-08-Task-01 ~]# firewall-cmd --permanent --remove-service=ssh
```

```
# 使用 firewall-cmd 命令添加指定地址能够远程访问的规则
[root@Lab-08-Task-01 ~]# firewall-cmd --permanent --add-rich-rule
='rule family=ipv4 source address=172.20.1.40/24 service name="ssh
" limit value="5/s" accept'

# 重新载入防火墙配置
[root@Lab-08-Task-01 ~]# firewall-cmd --reload
```

（5）通过防火墙提升数据库服务安全性。

需求描述：

第一：本地客户端（172.20.1.40）能够使用 MySQL WorkBench 连接 MariaDB 数据库。

第二：本地客户端（172.20.1.40）能够通过浏览器访问 phpMyAdmin 管理界面，进行数据库管理。

配置方法：

```
# 使用 firewall-cmd 命令添加本地客户端允许远程连接数据库
[root@Lab-08-Task-01 ~]# firewall-cmd --permanent --add-rich-rule
='rule family=ipv4 source address=172.20.1.40 port port=3306 proto
col=tcp accept'

# 使用 firewall-cmd 命令添加本地客户端允许访问 phpMyAdmin
[root@Lab-08-Task-01 ~]# firewall-cmd --permanent --add-rich-rule
='rule family=ipv4 source address=172.20.1.40 port port=80 protoco
l=tcp accept'

# 重新载入防火墙配置
[root@Lab-08-Task-01 ~]# firewall-cmd --reload
```

八、实验考核

实验考核分为【实验随堂查】和【实验线上考】两个部分。

实验随堂查：每个实验设置 2-5 考核点。完成实验任务后，任课教师随机选择一个考核点，学生现场进行演示和汇报讲解。

实验线上考：每个实验设置 10 道客观题。通过线上考核平台（如课堂派）进行作答。

1、实验随堂查

本实验随堂查设置 2 个考核点，具体如下：

考核点 1：禁止来自 IP 地址为 172.31.0.100~115 的主机的流量通过防火墙

考核点 2：实现禁止服务器的远程连接服务

2、实验线上考

本实验线上考共 10 题，题型为单选、多选、判断、填空等题型。