Day 07 综合串讲 综合练习

一、HTTPS网站加密

HTTP是明文协议，网络中传输的任何数据都是明文，包括用户和密码，如果有人抓包，所有数据都可以获得

加密算法：

对称算法（AES,DES）

非对称算法（RSA,DSA）

信息摘要（md5,sha512,sha265）

对称加密（加密和解密是一把钥匙）适合单机加密

非对称密码（加密和解密不是一把钥匙）：

公钥和私钥

信息摘要：

# md5sum 文件名

数据完整性校验（检查数据是否被人修改过）

在server主机操作

# yum -y install mod\_ssl

//安装该软件包让httpd支持加密网站

· 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（与相应公钥匹配）vim

去classroom下载公钥（证书）

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

去classroom下载私钥

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

去classroom下载根证书（上面的私钥和公钥是谁提供的）

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

修改配置文件：/etc/httpd/conf.d/ssl.conf，修改证书位置，端口号等

# systemctl restart httpd

客户机访问：

https://server0.example.com:443

自己新建加密格式

<VirtualHost \*:443>

sslengine on

SSLCaCertificateFile /

SSLCertificateFile /

SSLCertificateKeyFile /

</VirrualHost>

二、邮件系统（postfix）可以做类似于163的邮件系统

# vim /etc/postfix/main.cf

76:myhostname = server0.example.com

//主机名

83Lmydomain = example.com

//域名的后缀，邮箱的后缀

99:myorigin = $mydomain

//发件人的后缀

116:inet\_interfaces = 主机名/all

//允许主机/所有人给自己发邮件，默认仅接受本机发的邮件

164：mydestination = $myhostname,localhost.$mydomain,localhost

//什么邮件我才收

# systemctl restart postfix

# mail -s 标题 收件人

内容

内容

. //独立的点回车表示邮件内容结束

# mail //收取邮件，q退出

三、分区工具fdisk,parted

fdisk分区只能分4个主分区

fdisk分区每个分区最大只能是2T

parted可以分超过4个主分区（128），分区大小可以大于2T

parted分区首先要选择分区的类型msdos,gpt模式

msdos就是fdisk使用的模式

gpt模式：

# parted /dev/vdb mklabel gpt

//选择分区模式，可以使msdos或是gpt

# parted /dev/vdb mkpart primary 1 2G

//对/dev/vdb分区(kpart)，分主分区（primary）

//从硬盘的第1M到1G之间的容量分一个分区

# parted /dev/vdb mkpart primary 2G 5G

# parted /dev/vdb mkpart primary 5G 6G

# parted /dev/vdb/print

# mkfs/xfs /dev/vdb1

# mkswap /dev/vdb2 //创建交换分区

//交换分区是把硬盘当内存使用的分区

# vim /etc/fstab

/dev/vdb2 swap swap defaults 0 0

# mount -a

# swapon -a

//启用swap分区

# swapon -s

//查看已启用的分区