1.配置一个认证服务器：

station1为domain2.example.com的客户端根据下列要求提供认证服务：

1）Kerberos realm是DOMAIN2.EXAMPLE.COM

2）administrative或者其他的密码设置为postroll

3）认证服务提供的ID范围为：4500-14500

认证服务启动后，在web页面管理中心创建如下帐号：

（1）

name:Lukesh Rao

Username:lukesh

UID:4501

Group:lukesh

GID:4501

Home directory:/home/remoteusers/lukesh

Initial password:postroll

（2）

name：Elana Bianchi

User:elana

UID:4502

Group:elana

GID:4502

Home directory:/home/remoteusers/elana

Initial password:postroll

（3）

Name:Midori Inoue

Username:midori

UID:4503

Group:midori

GID:4503

Home directory:/home/remoteusers/midori

Initial password:postroll

答案：

Station1安装的时候IP地址是DHCP的，需要改成静态的，这是IDM的必须，禁用NetworManager，iptables -F,更改主机名为题中给出的名字，注意时间必须一致，如果不一致需要先调试ntp时间同步再安装IPA

安装IPA的时候用命令行模式安装，添加用户的时候用图形界面安装防止出错

dns需要手动配置172.24.1.250

# /etc/init.d/NetworkManager stop or # service NetworkManager status; service NetworkManager stop

# chkconfig NetworkManager off

# vim /etc/sysconfig/network-scripts/ifcfg-eth0

NM\_CONTROLLED=no

IPADDR=192.168.0.250 -> 通过ifconfig 得到

NETMASK=255.255.255.0

GATEWAY=192.168.0.254 -> 通过route -vn 得到

DNS1=192.168.0.254 -> 通过cat /etc/resolv.conf得到

# vim /etc/sysconfig/network 改主机名

# chkconfig network on; service network restart

# iptables -F

# /etc/init.d/iptables save

配yum

# yum install ipa-server -y

# ipa-server-install --help

# ipa-server-install --hostname=station1.domain2.example.com -n domain2.example.com -r DOMAIN2.EXAMPLE.COM -p postroll -a postroll --idstart=4500 --idmax=14500 -N -U

2.配置认证客户端：

配置station2使用station1提供的认证服务。

Configure station2 to use the centralized authentication services providey by station1. Note that station2 has been configured to automount home directories for centralized user accounts that are exported by host.domain1.example.com

答案：

# /etc/init.d/NetworkManager stop or # service NetworkManager status; service NetworkManager stop

# chkconfig NetworkManager off

# vim /etc/sysconfig/network 改主机名

# iptables -F

# /etc/init.d/iptables save or # service iptables save

# yum install ipa-client

# ipa-client-install --domin=doman1.example.com --server=station1.domin1.example.com --realm=DOMAIN2.EXAMPLE.COM -p admin -w flectrag --no-ntp --mkhomedir -U

# id hurry

3.安装安全相关更新：

考试系统已经配置了yum资源库[http://rhgls.domain1.example.com/updates](http://rhgls.domain1.example.com/updates.This)，该资源库包括本次考试所需更新。

在station1和station2上完成：

1）用适合的命令列出可用的安全更新并将结果输出到/root/rhsa.txt;注意必须在更新系统前、和完成所有考试后进行。

2）安装相关安全更新。

答案：

配置yum源，在2台虚拟机上都要配置并把要求查找的文件导出来，以下的操作需要2台虚拟机上都操作一遍

# yum updateinfo

# yum updateinfo list | grep RHSA >> /root/rhsa.txt or, # yum updateinfo list security >> /root/rhsa.txt

# yum -y update --security

4.安装软件包：

在http://rhgls.domain7.example.com/materials/qtined上已经下载了两个不确定源的服务软件包。这些包都没有签名，每个包的安装都会对station2的用户请求写文档。检查哪一个包是安全的，并且安装在station2，不安全的包不能安装。

答案：

把第二个rpm包排除，第一和第三的rpm包显示都是正常无威胁的，把第一和第三个包进行rpm安装即可

# rpm -qpl --scripts rpm包

# rpm -qp --triggers rpm包

5.创建加密卷：

在station2上创建加密块设备，有如下要求：

1）该块设备必须是逻辑卷

2）该卷的名称必须是wallet

3）该设备必须属于已经存在的卷组treasure

4）该设备必须使用treasure的所有可用空间

5）该设备的加密短语必须是sk0nkw0rkz+

6）该加密设备应该被格式化为ext4

7）该设备不需要自动挂载到/private但是挂载点必须创建

8）该加密文件系统，当挂载在/private时应该包含复制的http://rghls.domain7.example.com/materials/maypreciousss.sh

答案：

# vgdisplay treasure

PE Size 32.00 MiB

Free PE / Size 12 / 384 MiB

# lvcreate -n wallet -l 12 treasure

# cryptsetup luksFormat /dev/treasure/wallet #写错了删除crysetup remove wallet

# cryptsetup luksOpen /dev/treasure/wallet wallet

# mkfs.ext4 /dev/mapper/wallet

# mkdir /private; mount /dev/mapper/wallet /private

# cd /private && wget http://X.X.X.X

6.追踪错误登录：

station1和station2上配置，3次登录失败后锁定帐号3分钟；不管通过SSH还是本地控制台登录都能生效。

答案：

# vim /etc/pam.d/system-auth

auth required pam\_tally2.so deny=3 unlock\_time=120

account required pam\_tally2.so

# vim /etc/pam.d/password-auth

auth required pam\_tally2.so deny=3 unlock\_time=120

account required pam\_tally2.so

7.配置一个日志服务：

在station1配置日志服务，有如下要求：

1）station1必须开启远程日志

2）station2的日志消息存放到/var/log/station2.log中

答案

# yum install rsyslog

# vim /etc/rsyslog.conf

打开514 tcp udp

# vim /etc/syslog.d/station2.conf

:fromhost, isequal,”station2.example.com” /var/log/station2.log

# /etc/init.d/rsyslog restart

# chkconfig rsyslog on

Station2操作

# vim /etc/rsyslog.conf

\*.\* @@station1.domain1.example.com

将RULES下面的/var/log/的日志全部注释掉，将station2上面的日志文件指向station1，本地不留任何log

测试logger hah(station2)

# tailf /var/log/station2.log

9.禁用root通过SSH访问：

在station1和station2上配置root用户不能登录，但是其他的非root用户必须要能访问

答案：

# vim /etc/ssh/sshd\_config

PermitRootLogin no

10.设置密码过期策略：

设置station2上所有新建的本地用户密码过期（expire）为6天。

答案：

# vim /etc/login.defs

PASS\_MAX\_DAYS 6

11.设置默认权限：

要求wario用户在station2上创建文件的权限是—w-r-----,创建目录的权限是d-wxr-x--x

答案： (文件夹 777， 文件666，然后减去umask的值，得到的就是文件夹和文件的默认权限)

# cd → 切换到wario用户的家目录下

# vim .bash\_profile

umask 0426

12.配置软件包的签名检查：

http://rhgls.domain7.example.com/materials包含几个不同的公共keys，其中有一个可以用来给demo\_package签名，软件包demo\_package在http://rhgls.domain7.example.com/materials/signed, 根据以下要求在station2给demo\_package签名：

1）用户key签名后的包能用rpm校验

2）包可以用yum安装

3）从该资源库中的安装默认使用该key进行签名

4）除了有效的key外其他的key不能用来签名和检查

答案：

# rpm -qa gpg-pubkey 查看本机有哪些个key

# rpm -K 包名 查看rpm包是否签名

# rpm --import rpm-gpg-key 导入下载下来的key查看是由哪个key给软件包签的名

# rpm -vvK 包名

# rpm -e key名 删除key

查到是由哪个key加密后，配置yum源:

gpgcheck=1

gpgkey=file:///tmp/RPM-GPG-KEY-EX413-1

13.删除文件：

删除station2上的/root/removeme.txt文件。

答案：

# lsattr 查看文件的权限有-i参数

# chattr -i removeme.txt 将-i参数取消

# rm -rf remove.txt

14.查找文件：

在station1上查找有特殊权限的文件并且将结果保存到/root/specialfiles.txt中。

答案：

# find /usr/bin -perm -4000 >>/root/specialfiles.txt

# find /usr/bin -perm -2000 >>/root/specialfiles.txt

# find /usr/bin -perm -1000 >>/root/specialfiles.txt

or

# find /usr/bin -type f -perm /7000 > /root/specialfiles.txt

15.配置入侵检测：

根据如下要求使用AIDE监控station1

1）下载文件http://rhgls.domain7.example.com/pub/materials/ex413.cfg到/etc/目录。

2）AIDE只监控文件/etc/ex413.cfg的权限（permission）和所有权（ownership）的变化。

3）AIDE的数据库文件放在/etc/lib/aide/aide.db.gz

答案：

# yum install aide –y

# cd /etc/

# wget http://rhgls.domain7.example.com/pub/materials/ex413.cfg

# vim /etc/aide.conf

NEW = p+u+g

/etc/ex413.cfg NEW

剩下的配置文件可以全部删除

# vim /etc/aide.conf

@@define DBDIR /etc/lib/aide → 将var 改为 etc

database=file:@@{DBDIR}/aide.db.gz

# aide --init

# mv /etc/lib/aide/aide.db.new.gz /etc/lib/aide/aide.db.gz

# aide --check

16.配置文件的访问：

根据下列要求，在station1下为/marketing 目录设置权限控制：

1）原始文件不能修改也不能删除。

2）即使不在 /etc/fstab 里提供选项，也要求能够实现文件的访问控制 (用 tune2fs 定义默认挂载选项)

3）文件系统中的目录是/marketing/data .

4）目录的属主是 root 属组是 guests .

5）guests 组对 data 下目前和将来的文件及子目录有所有权限且新建的文件或目录要能继承该权限(设置 acl 和默认 acl ) .

6）marley 和piaf不是guests的成员

7）用户marley 对目录有读和写的权限且新建的文件或目录继承该权限。

8）除了guests的成员，其他用户不能访问/marketing/data目录(设置 acl 和默认 acl )。

答案：

第一问应该通过chattr +i 来实现

# df -h

# vim /etc/fstab

defaults,acl → 不应该通过加acl这种方式来实现，应该通过tune2fs -o acl ...

# tune2fs -l /dev/vda1 | grep "mount options"

Default mount options: (none)

# tune2fs -o acl /dev/vda1

# cd /marketing; mkdir data

# chown root. guests data/

# chmod g+w data/; chmod g+s data/ or # setfacl -R -m g:guests:rwx data/; setfacl -R -m d:g:guests:rwx data/

# id marley; id piaf

# setfacl -dR -m u:marley:rw- data/ or # setfacl -R -m u:marley:rw- data/ ; # setfacl -R -m d:u:marley:rw- data/

# setfacl -dR -m u:piaf:rw- data/ or # setfacl -R -m u:piaf:rw- data/ ; # setfacl -R -m d:u:piaf:rw- data/

# chmod o-r data/; chmod o-x data/ 应该是通过后面这种方式来实现 # setfacl -R -m o:--- data/; setfacl -R -m d:o:--- data/

17.配置应用程序：

在station2上已经安装/usr/local/bin/db\_setpass，当一个用户运行该程序时，可以输入一些字符串并且将用户信息和字符串以加密的方式存储到一个文件中，如果不加任何参数将显示一些额外用法信息。

额外信息（要求）：

1）db\_setpass使用/usr/local/etc/dbusers.dat.如果该文件不存在则将被程序首次运行是创建。

2）db\_setpass和/usr/local/etc/dbusers.dat的属主为dbmgr，属组为dbmgr.

3）station2上的其他用户能读取/usr/local/etc/dbusers.dat但只有dbmgr和root可以修改或写入。

4）station2的所有（已有或新建）用户能运行db\_setpass且能存储一个密码短语到/usr/local/etc/dbusers.dat

答案：

# /usr/local/bin/db\_setpass root -p redhat

# id dbmgr

# useradd dbmgr

# chown dbmgr.dbmgr /usr/local/bin/db\_setpass

# chown dbmgr.dbmgr /usr/local/etc/dbuser.dat

# chmod 744 /usr/loca/bin/dbuser.dat

# chmod u+s /usr/local/bin/db\_setusers

# chmod u+s /usr/local/etc/dbuser.dat

18.审计文件活动（activity）：

在station2的/root/rockentries.txt设置审计,key :“ex413”,审计的事件read,write,excute,appends; 将审计日志发送到station1.

答案：

# service auditd start

# vim /etc/audisp/plugins.d/syslog.conf

active=yes

# vim /etc/audit/audit.rules

-w /root/rockentries.txt -p rwxa -k ex413

# service auditd restart

# chkconfig auditd --list; chkconfig auditd on

19.配置防火墙：

根据以下要求，在station1和station2配置防火墙：

1）所有本地主机的访问都允许

2）除下列服务外其他都blocked（阻塞）

（1）所有的主机都可以访问 ipa-server 的 ssh 端口

（2）所有的主机都可以访问 ipa-server 的 80 端口

（3）同网段（domain7.example.com）可以访问任意的服务，因这涉及到服务端要收集日志

答案：

注意：防火墙在两台虚拟机上都需要开启514端口，用于rsyslog的日志推送

# iptables -L --line-number 将防火墙的条目用数字进行标记

# iptables -F

# iptables -A INPUT -s 127.0.0.1 -j ACCEPT

# iptables -A INPUT -p tcp --dport 22 -j ACCEPT

# iptables -A INPUT -p tcp --dport 80 -j ACCEPT（station1 加）

# iptables -A INPUT -p tcp --dport 514 -j ACCEPT

# iptables -A INPUT -p udp --dport 514 -j ACCEPT

# iptables -A INPUT -s !172.24.1.0/24 -j REJECT 必须指定IP地址，不能用域名

# /etc/init.d/iptables save or # service iptables save

20.CPU限制:

在station1上，设置devels组内成员的每个登录会话使用CPU时间为2分钟（minutes）

答案：

# vim /etc/security/limits.conf

@qutest hard cpu 2