一、安全脚本

P1 安全脚本

HASH 值
HASH 值与文件名称、时间、大小等信息无关，仅与内容有关
查看/etc/passwd 文件 HASH 值

```
[root@svr5 ~]# md5sum /etc/passwd              #文件内容不改变校验结果一样
[root@svr5 ~]# cp /etc/passwd    /root/pass
[root@svr5 ~]# md5sum /root/pass               #校验结果和/etc/passwd 检验结果一样
[root@svr5 ~]# vim /root/pass                  #任意修改一行内容
[root@svr5 ~]# md5sum /root/pass               #校验结果和/etc/passwd 检验结果不同
[root@svr5 ~]# sha512sum /etc/passwd           #计算 hash 值的长度不同
[root@svr5 ~]# sha256sum /etc/passwd
```

数据安全监测脚本

```
[root@svr7 ~]# cd /root/shell/day06/
[root@svr7 day06]# vim data.sh
#!/bin/bash
for i in $(ls /etc/*.conf)
do
    md5sum $i >> /tmp/data.log
done
[root@svr7 day06]# chmod +x data.sh
[root@svr7 day06]# ./data.sh
```

通过脚本修改 SSH 配置文件
sshd 主配置文件: /etc/ssh/sshd_config

```
Port       3389                    //改用非标准端口
PermitRootLogin no                 //禁止 root 登录
UseDNS no                          //不解析客户机地址
AllowUsers  账户名                  //设置远程连接的白名单，多个用户空格分割
[root@svr7 day06]# cp /etc/ssh/sshd_config ./        #拷贝配置文件到当前目录
[root@svr7 day06]# vim ssh_config.sh
#!/bin/bash
conf="./sshd_config"
sed -i '/^#Port/s/22/1122/' $conf
sed -i '/^#PermitRootLogin/s/yes/no/' $conf
sed -i '/^#UseDNS/s/yes/no/' $conf
sed -i '$a AllowUsers tom' $conf
systemctl restart sshd
[root@svr7 day06]# chmod +x ssh_config.sh
[root@svr7 day06]# ./ssh_config.sh
```

二、格式化输入 passwd

P1 格式化输出数据

格式化输出 passwd

```
[root@svr5 ~]# awk -F:   'BEGIN{print "用户名   UID   家目录"}'
[root@svr5 ~]# awk -F:   'BEGIN{print "用户名   UID   家目录"}   {print $1 ,$3,$6}' /etc/passwd
| column -t                # column -t  主要作用使用 tab 键缩进排版
```

过滤系统账户中对应的密码

在 awk 中可以通过-v 选项调用 shell 中的变量

```
[root@svr5 ~]# hello="nihao"
[root@svr5 ~]# awk 'BEGIN{print hello}'                    #无输出结果
[root@svr5 ~]# awk 'BEGIN{print "hello"}'                  #打印字符串 hello
[root@svr5 ~]# awk 'BEGIN{hello=123;print hello}'
123
[root@svr5 ~]# hello="nihao"
[root@svr5 ~]# awk -v x=$hello 'BEGIN{print x}'
nihao
```

从/etc/passwd 中将所有能登陆的账户名提取出来

从/etc/shadow 中提取账户对应的密码

```
[root@svr7 day06]# vim userpass.sh
#!/bin/bash
USER=$(awk -F: '/bash$/{print $1}' /etc/passwd)
for i in $USER
do
    awk -F: -v x=$i '$1==x{print $1,$2}' /etc/shadow
done
[root@svr7 day06]# chmod +x userpass.sh
[root@svr7 day06]# ./userpass.sh
```

三、综合案例

P1 部署 PXE+kicstart 环境

DHCP 服务，TFTP 服务，HTTP 服务，kickstart 配置

```
[root@svr5 ~]# cat /root/shell/day06/pxe.sh
#!/bin/bash
DHCP_NET=192.168.4.0
DHCP_NETMASK=255.255.255.0
DHCP_MINIP=192.168.4.100
DHCP_MAXIP=192.168.4.200
```

```
DHCP_ROUTER=192.168.4.1
DHCP_NEXT_SERVER=192.168.4.7
HTTP_IP=192.168.4.7

#安装软件包.
yum -y install httpd dhcp tftp-server syslinux
#临时停用 SELinux
setenforce 0

#配置 DHCP 服务
cat > /etc/dhcp/dhcpd.conf << EOF
default-lease-time 600;
max-lease-time 7200;
subnet $DHCP_NET netmask $DHCP_NETMASK {
   range $DHCP_MINIP $DHCP_MAXIP;
   option routers $DHCP_ROUTER;
   next-server $DHCP_NEXT_SERVER;
   filename "pxelinux.0";
}
EOF
systemctl start dhcpd
systemctl enable dhcpd

#配置 httpd 共享服务器.
if [ ! -e /dev/cdrom ];then
     echo "未检测到系统光盘/dev/cdrom,请插入光盘后再试."
     exit
fi
[ -d /var/www/html/cdrom ] || mkdir /var/www/html/cdrom
mount /dev/cdrom /var/www/html/cdrom
systemctl start httpd

#配置 kickstart 文件.
cat > /var/www/html/ks.cfg << EOF
install
keyboard 'us'
rootpw --plaintext redhat
url --url="http://$HTTP_IP/cdrom"
lang en_US
firewall --disabled
auth    --useshadow    --passalgo=sha512
text
selinux --disabled
skipx
```

```
network    --bootproto=dhcp --device=eth0
reboot
timezone Asia/Shanghai
bootloader --location=mbr
zerombr
clearpart --all --initlabel
part /boot --fstype="xfs" --size=500
part / --fstype="xfs" --grow --size=1
%packages
@minimal
@core
%end
EOF

#配置 tftp 服务器.
cp /usr/share/syslinux/pxelinux.0 /var/lib/tftpboot/
cp /var/www/html/cdrom/isolinux/* /var/lib/tftpboot/
[ -d /var/lib/tftpboot/pxelinux.cfg ] || mkdir /var/lib/tftpboot/pxelinux.cfg/
cat > /var/lib/tftpboot/pxelinux.cfg/default <<EOF
default vesamenu.c32
timeout 600

label linux
   menu label ^Install CentOS 7
   kernel vmlinuz
   append initrd=initrd.img ks=http://$HTTP_IP/ks.cfg
EOF
systemctl start tftp

iptables -F
```