**Morning：**

1、Linux基本防护

**-修改账户有效期**

chage -l gjq #查看账户有效期

chage -E 2018-12-01 gjq #修改账户有效期  
 chage -d 0 gjq #将密码设为最近日期(过期)

Tips：将有效期设为过去的某个时间，可以禁用账户

查看账户的默认配置（无需修改）

[root@proxy ~]# cat /etc/login.defs

PASS\_MAX\_DAYS 99999 #密码最长有效期

PASS\_MIN\_DAYS 0 #密码最短有效期

PASS\_MIN\_LEN 5 #密码最短长度

PASS\_WARN\_AGE 7 #密码过期前几天提示警告

UID\_MIN 1000 #UID最小值

UID\_MAX 60000 #UID最大值

CREATE\_HOME yes #自动创建家目录

ENCRYPT\_METHOD SHA512 #密码加密算法

**-临时锁定账户**

passwd -l gjq 或 usermod -L gjq #锁定账户

passwd -u gjq 或 usermod -U gjq #解锁账户

passwd -S gjq #查看锁定状态

**-隐藏tty登陆信息**

[root@proxy ~]# vim /etc/issue #登陆时显示信息

Welcome, IT world !

**-文件系统安全**

1）文件系统额外属性

[root@proxy ~]# cat /etc/fstab

/dev/vda1 /boot xfs defaults,noexec 0 0

/dev/vda3 /home xfs defaults,noatime 0 0

#noexec让分区下所有程序都不可执行

#noatime不再更新atime时间（建议所有分区都加，降低CPU占用）

atime(访问时间)、mtime(修改内容时间)、ctime（修改权限时间）

2）文件隐藏属性

chattr +i /etc/hosts #锁定文件(无法修改、删除)

chattr -i /etc/hosts #解锁

chattr +a /etc/hosts #锁定文件仅可追加(只能>>追加)

chattr -a /etc/hosts #解锁

lsattr /etc/hosts #查看隐藏属性

2、sudo分配管理权限

**-使用su命令**

su - [账户名称]

su - [账户名称] -c “命令”

[gjq@proxy ~]$ whoami #查看登陆用户名

[gjq@proxy ~]$ su - -c 'touch /tmp/test.txt'

[root@proxy ~]# ll /tmp/test.txt

-rw-r--r--. 1 root root 0 12月 7 10:50 /tmp/test.txt

**-使用sudo提权**

管理员授权命令 -> 普通用户sudo执行命令 -> 输入自己的密码

1）修改/etc/sudoers配置

[root@proxy ~]# vim /etc/sudoers 或 visudo

gjq ALL=(ALL) /usr/bin/systemctl

用户名 登陆主机=(用户身份) 命令列表

2）切换用户，验证sudo

[gjq@proxy ~]$ sudo -l #查看sudo权限列表

[gjq@proxy ~]$ systemctl start httpd #不用sudo时启动服务失败

Authentication is required

[gjq@proxy ~]$ sudo systemctl start httpd #输入密码，启动成功

[sudo] gjq 的密码：

3）授权多个命令

[root@proxy ~]# man sudoers

[root@proxy ~]# vim /etc/sudoers

Host\_Alias 别名=主机1,主机2 #定义主机别名

User\_Alias 别名=用户1,用户2 #定义用户别名

Runas\_Alias 别名=用户1,用户2 #定义目的用户别名

Cmnd\_Alias 别名=文件绝对路径1,路径2 #定义命令别名

gjq ALL=(ALL) NETWORKING #使用别名

gjq ALL=(ALL) /usr/bin/passwd [A-Za-z]\*,!/usr/bin/passwd root

#允许用户修改密码，不可修改root密码

4）给用户组提权

[root@proxy ~]# vim /etc/sudoers

%wheel ALL=(ALL) ALL

#%wheel ALL=(ALL) NOPASSWD: ALL #允许无密码sudo

[root@proxy ~]# usermod -a -G wheel gjq

5）启用日志记录

[root@proxy ~]# vim /etc/sudoers

Defaults logfile="/var/log/sudo" #指定日志文件

**Afternoon：**

1、提高SSH服务安全

**-配置基本安全策略**

[root@proxy ~]# vim /etc/ssh/sshd\_config

Protocol 2 #SSH协议

PermitRootLogin no #禁止root用户登录

PermitEmptyPasswords no #禁止密码为空的用户登录

UseDNS no #不解析客户机地址(提高登陆速度)

LoginGraceTime 1m #登录限时(超过1m不输密码超时)

MaxAuthTries 3 #每连接最多认证次数(n-1次)

**-配置SSH黑白名单**

[root@proxy ~]# vim /etc/ssh/sshd\_config

AllowUsers lisi gjq@192.168.4.0/24 #定义账户白名单

#DenyUsers USER1 #账户黑名单

#AllowGroups GROUP1 #组白名单

#DenyGroups GROUP1 #组黑名单

注意： 只定义黑名单时，默认其他都可以访问；

只要定义了白名单，其他拒绝访问。

**-使用密钥登陆**

[root@room12pc2 ~]# ssh-keygen -N '' -f /root/.ssh/id\_rsa

#非交互式生成密钥对

[root@room12pc2 ~]# ssh-copy-id root@192.168.4.5

#发送公钥到/root/.ssh/authorized\_keys

[root@proxy ~]# vim /etc/ssh/sshd\_config

AuthorizedKeysFile .ssh/authorized\_keys #指定公钥接收文件

PasswordAuthentication no #禁止使用口令登陆

注意：Windows使用远程工具可以直接生成密钥对，然后把公钥内容拷贝到远程主机**~/.ssh/authorized\_keys**文件中

2、SELinux安全防护

传统的权限针对用户（Linux，使用root执行命令，自动降级为普通用户）

SELinux控制程序（什么程序，可以读什么文件）

[root@proxy ~]# vim /etc/selinux/config

SELINUX=disabled #设置模式

SELINUXTYPE=targeted #保护策略

#targeted，控制主要的网络服务安全；mls，控制所有程序

[root@proxy ~]# ls -Z /var/ftp/ #查看文件的安全上下文

drwxr-xr-x. root root system\_u:object\_r:public\_content\_t:s0 /var/ftp/

[root@proxy ~]# ps aux -Z #查看进程的安全上下文

[root@proxy ~]# chcon -t public\_content\_t /root/test.txt

#修改文件的安全上下文

[root@proxy ~]# chcon -R --reference=/var/ftp /root

#以/var/ftp为模板递归修改/root安全上下文