##################安全DAY03#################

**一.Linux基本防护**

1. 用户账户安全

设置账号有效期

chage -E yyyy-mmm-dd #指定效日期

配置文件/etc/login.defs

账号的锁定与解锁

passwd -l 用户名 #锁定用户密码

passwd -S 用户名 #查看状态

passwd -u 用户名 #解锁

强制定期修改密码

配置文件/etc/login.defs

1. 文件系统安全

锁定/解锁保护文件

lsattr 查看 chattr 添加

控制的三种方式:+ - =

两种属性:i(不可变) a(仅可追加)

1. **用户切换与提取**
2. su切换用户身份

切换与提权的应用场景

su - 用户　　＃同时切换到该用户的系统环境

su 用户　　＃只切换身份，不进入该用户的环境

1. su提升执行权限

用户提权：让普通用户登录系统后，有

主配置文件：／etc/sudoers　　格式:用户 主机列表=命令列表

配置为sudo提权

添加Mike localhost,pxcnode71=/sbin/\*,!/sbin/ifconfig

eth0,/bin/rpm,/bin/yum,/bin/systemctl\*

httpd,/bin/vim,/etc/httpd/conf/httpd.conf

查看提权命令 sudo -l

启动日志文件: 在配置文件里添加 Defaults logfile=”/var/log/sudo”

Sudo 别名设置(别名名称必须要用大写)

用户别名 User\_Alias

主机别名 Host\_Alias

命令别名 Cmnd\_Alias

例如:User\_Alias MUUSER=yaya,ying,ly

Host\_Alias MYSER=localhost,pxcnode71

Cmnd\_Alias MYSOFT=/bin/rpm,/bib/yum,/sbin/fdisk

MYUSER MYSER=MYCMD , MYSOFT

bob MYSER=MYSOFT

1. ssh访问控制

Ssh基本保护

Sshd基本安全配置

修改配置文件 /etc/ssh/sshd\_config中的 端口和地址

黑白名单

黑名单:不允许使用名单里的用户链接ssh服务

DenyUsers USER1 USER2

DenyGroup GROUP1 GROUP2...

白名单:仅允许使用.....

AllowUsers

Ssh密钥对验证

公钥

私钥

1. SElinux安全概述
2. Selinux介绍
3. 相关的软件包
4. 查看当前系统selinux是否启用
5. 临时禁用和启用selinux命令
6. 永久启用selinux要修改那个文件

Selinux应用

1.查看上下文

Ls -lZ /etc/passwd

Ls -ldz /etc

Ps aux -Z

Ps aux -Z | grep httpd

2.一般操作规律

创建新文件或目录 自动继承父目录的上下文

移动的文件时,保持原有的上下文属性不变

复制的文件,自动继承目标位置的上下文

1. 安全上下文

属性构成：用户：角色：访问类型：选项：

1. 修改安全上下文

　 -t 指定修改类型

-R 递归修改

1. 重置安全上下文(restorecon)

　 恢复所在位置的默认安全上下文属性　　restorecon　文件名

重启后全部重置　　touch /.autorelabel ; reboot

1. 调整selinux布尔值bool 真　／假

服务的功能开关

查看布尔值　getsebool -a 可列出所有的布尔值

设置布尔值　setsebool -P 永久更改

案例：运行ftp服务，允许匿名用户对/var/ftp/share 目录上传和下载文件的 权限

Yum - y install vsftpd

Vim +29 /etc/vsftpd/vsftpd.conf

Mkdir /var/lib/share

Chmod 0+w /var/lib/share

Systemctl restart vsftpd

Netstat -ntulp | grep :21

Cp /etc/passwd /var/lib/share

Setenforce 1

设置bool值setsebool -P ftpd\_anon\_write　on　ftpd\_full\_access

客户端命令行链接ftp--回车--ls--cd共享文件夹---下载get--- 上传put

错误日志：/var/log/messages

Setenforce 0 可以启动httpd 　1 不可以启动httpd

##################DAY 04监控与服务安全##########

1. **加密与解密**
2. 加密的目的及方式

机密性：对称加密（同一个秘钥）

　非对称加密（不同秘钥）

完整性：信息摘要

1. 常见的加密算法

对称　加密：DES AES

非对称加密：RSA　DSA

Hash散列技术：MD5 SHA（内容发生变化　值则发生变化）

1. **数据加解密实验**

Gpg --version gnupg2支持命令的软件

1.Gpg对称加密与解密

发送方 加密文件　gpg -c 文件名----移动到/tmp/下

接收方 解密文件 gpg -d ／tmp/文件名　＞　～／其他名

2.Gpg非对称加密与解密（密钥对加密）

公钥文件　加密

私钥文件　解密

非对称加解密的工作过程：

解密方创建密钥对　gpg --gen-key（ls ~/.gnupg存放公私钥）

导出公钥 gpg --export -a (-a使导出的文件不乱码)

gpg --export -a >　／tmp/userb.pub

共享公钥给加密方　scp

加密方导入公钥 gpg--import

gpg --import /tmp/userb.pub

使用公钥加密文件 gpg -e -r 用户名

gpg -e -r userb a.txt

共享加密文件给解密方：文件．gpg移动到／tmp／下

加密方私钥解密文件gpg -d /tmp/a.txt.gpg > 新名字

1. **Gpg数字签名**(用于验证文件的完整性)　md5

继续上一个实验：拥有私钥的用户对文件做数字签名

Gpg -b 文件名　（文件名．sig　是签名文件）

拥有公钥的用户验证文件签名

gpg --verify　/tmp/文件名．Sig

**二．aide入侵检测系统**

初始化系统：安装软件包aide

　修改配置文件

sed -i '99,312s/^/#/' /etc/aide.conf

Vim +98 /etc/aide.conf

写入内容 /roto/ FIPSR

　初始化检查：aide --init

查看文件：ls /var/lib/aide/

备份数据库

mv /var/lib/aide/aide.db.new.gz /opt/

cp /opt/aide.db.new.gz

/var/lib/aide/aide.db.gz

入侵检查：aide --check

1. **扫描与抓包**

**安全概述分析**

典型的扫描方式： Scan 主动监测

Sniff 被动监听

Capture 数据包捕获

常见的安全分析工具：NMAP(扫描器)

Tcpdump命令 　wireshark图形(协议分析)

**扫描nmap**

安装nmap

命令格式：nmap 扫描类型　选项　扫描目标

扫描类型包括:-sS TCP扫描

　-sT TCP链接扫描

　-sU UDP扫描

　-sP ICMP扫描

　-A 目标系统全部扫描

选项：-A 目标系统全面分析

-p　指定端口是否开启

-n　扫描时不做主机名解析，加快速度

**抓包tcpdump**

安装软件tcpdump

基本用法：tcpdump 选项　过滤条件

选项包括: -i 指定监控的网络接口

-c 定义抓包的个数

-A 转换为ACSII码　以方便阅读

-w 将数据包信息保存到指定文件

-r　从指定文件读取数据包的信息

过滤条件：类型：host

方向：src

协议: tcp arp....

多个条件组合　and or

WireShark协议分析器

图形抓包软甲

##############安全第五天################

1. **系统审计**

相关概述： 什么是审计

审计的案例

部署audit　（服务为auditd）

主配置文件：/etc/audit/auditd.conf

配置审计服务

Auditctl 命令: -l查看　　-s查询状态　　-D 删除所有规则

定义临时规则：auditctl -w /etc/passwd -p wa -k passwd\_change

-w为写的权限　（r x a）

-k(key\_name)为可选项　方便识别哪些规则生成特定 　　　　　　　的日志项

定义永久规则：/etc/audit/rules.d/audit.rules

审计日志

系统提供的ausearch命令可以搜索日志

该程序默认搜索：/var/log/audit/audit.log

搜索日志：ausearch -k fidisk\_change

1. **服务安全**

▲前提部署nginx环境

**1.Nginx服务安全（包括三种以下分别写出）**

删除不需要的模块:./configure --without-http\_autoindex\_module

隐藏软件版本信息：修改文件

src/http/ngx\_http\_header\_filter\_module.c

重新加载模块编译安装

/configure --without-http\_autoindex\_module

测试：curl -I <http://192.168.4.72>

限制并发：ngx\_http\_limit\_req\_module为默认模块

（该模块可降低ddos攻击风险）

配置文件：limit\_req\_zone $binary\_remote\_addr

zone=one:10m rate=1r/s；（http部分）

limit\_req zone=one burst=5;（server部分）

拒绝非法请求：配置文件server部分加入if ($request\_method

!~ ^(GET|POST)$){return 444;}

测试　curl -i -X GET <http://192.168.4.72>

防止buffer溢出：防止客户端请求数据溢出

有效降低机器Dos攻击风险

1. **数据库服务安全(mariadb)（五个方面）**

初始化安全脚本: mysql\_secure\_installation

修改数据库密码（三种方式）

mysqladmin -hlocalhost -uroot -p password "新密码"

set password for root@"localhost"=password("新密码");

update mysql.user set password=password("新密码");

清楚历史命令：删除保存历史命令的配置文件　.mysql\_history

.bash\_history

设置防火墙规则：从TCp层开始设置ACL策略

数据备份与还原方式：mysqldump binlog innobackupex 主从同步

数据安全：创建可以远程登陆的账户

可以通过nmap或tcpdump获取数据库服务器的状态

1. **Tomcat服务安全（java语言编写的网站）**

隐藏版本信息

修改文件　/usr/local/tomcat/lib/org/apache/catalina/util/S

修改文件　+69 /usr/local/tomcat/conf/server.xml

添加server=”名”

测试：curl -I http://网址：端口／文件名

降权启动

创建用户

修改所属组和所属主　/usr/local/tomcat

su - -c '/usr/local/tomcat/bin/startup.sh' tomcat

查看测试：ps aux | grep java

删除默认的测试页面：rm -rf /usr/local/tomcat/webapps/\*

1. **Linux安全之打补丁**

1.相关概念

2.创建补丁文件：diff -u 旧文件 新文件 > bd.patch（新文件名）

-u是创建补丁文件必须要添加的选项（打补丁使用）

-r 递归对比目录中的所有资源（可以对比目录）

-a 所有文件视为文本（包括二进制程序）

-N 无文件视为空文件（空文件怎么变成第二个文件）

1. 打补丁(讲补丁文件传给客户端)

Patch命令需要安装patch软件来提供

命令格式：patch -p数字　＜　补丁文件名

数字：表示删除重复目录的个数

(补丁文件里路径和被补丁文件路径比较)

撤销补丁：patch -RE < 补丁文件　#进入到补丁文件的目录进行撤销

################安全第六天###############

iptables -t filter -nL --line-numbers 查看防火墙规则

iptables-save > /etc/sysconfig/iptables　保存

**主机型防火墙(自己保护自己)(有iptables服务的机器)**

Iptables -t filter -F 清空防火墙规则

iptables -t filter -A INPUT -p tcp --dport 22 -j ACCEPT　添加规则

iptables -t filter -P INPUT DROP　清除默认规则

iptables -t filter -nL INPUT --line-numbers

限制对指定服务端口的访问

Iptables -A INPUT -s 192.168.4.52 -p tcp --dport 22 -j ACCEPT

别人ping不到自己但自己ping得到自己

iptables -t filter -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT

网络型防火墙(控制数据包是否允许经过自己)

环境要求：客户端设置网关 route add default gw 192.168.2.51

服务端echo 1 > /proc/sys/net/ipv4/ip\_forward　#临时设置

echo 'net.ipv4.ip\_forward=1' >> /etc/sysctl.conf永久设置

Sysctl -a 查看

清空防火墙规则之前要把DROP改成INPUT

客户端设置:iptables -t filter -P FORWARD DROP

iptables -t filter -A FORWARD -p tcp --dport 80 -j ACCEPT

iptables -t filter -A FORWARD -p tcp --sport 80 -j ACCEPT

扩展匹配条件

MAC地址匹配 -m mac

多端口匹配 -m multiport

IP范围匹配 -m iprange

iptables -t filter -A FORWARD -p icmp -j ACCEPT

iptables -t filter -I FORWARD 5 -p icmp -m iprange --src-range 192.168.4.50-192.168.4.60 -j DROP

客户端

iptables -t filter -I FORWARD 5 -p icmp -m mac --mac-source 52:54:00:81:78:3a