linux应急响应

1. 前期交互（同windows应急响应）
2. linux应急响应
3. 操作系统信息
   1. Uname -a查看操作系统信息、内核版本
   2. cat /proc/version
   3. lsb\_release -a(需要安装lsb:yum install lsb):可以用来获取发行版本的信息
   4. 枚举主机的所有服务：service --status-all
   5. 查看历史命令：history或cat ~/.bash\_history
   6. 查看主机的驱动程序：lsmod
   7. 查看是否添加了ssh私钥：ll ~/.ssh
4. 登录排查
   1. 查看当前登录的用户：who
   2. 查看上一次登陆成功的用户：last
   3. 查看最近登录失败的用户：lastb
   4. 查看所有用户最近登录的时间：lastlog
   5. 查看用户信息：cat /etc/passwd，注意查看可登录shell的用户，shell为/bin/bash
   6. 检测Uid=0的用户（超级用户，拥有root权限）：

awk -F: '$3==0 {print $1}' /etc/passwd

* 1. 检测空口令用户：在日志文件夹下执行cat secure\* | grep none |grep test 如果有空口令用户登录，那么执行结果中会有accepted none字样
  2. /etc/sudoers文件是sudo的配置文件，当用户执行sudo命令时，系统会自动寻找sudoers文件，判断用户是否有执行sudo的权限，如果发现配置文件中有跟root权限相同的其他用户，编辑此配置文件，将用户删除即可

1. 启动项排查
   1. 列出所有的开机启动项：chkconfig --list
   2. 开机自启检查项：/etc/rc.d(存放的是各个级别的启动脚本) /etc/init.d /etc/profile.d(linux环境变量)
2. 进程排查
   1. ps[参数]
      1. -e显示所有进程
      2. -f全格式
      3. -h不显示标题
      4. -a显示所有进程，包括其他用户的进程
      5. -x显示所有程序
      6. -u以用户为主的格式显示程序

ps -ef

·UID用户id

·PID进程id

·PPID父进程id

·C CPU占用率

·STIME 开始时间

·TTY开始此进程的终端设备

·TIME 进程运行的总时间

·CMD命令名

ps -aux

·%cpu进程占用的cpu百分比

·%mem 进程占用的内存百分比

·vsz 进程使用的虚拟内存量

·rss 进程使用的固定内存量

b) top(动态查看进程)

c) pstree(树形结构显示进程)

d) kill -9 [进程id] 杀死进程

e) 查看进程运行路径 ll /proc/[进程id]

f) ps -p [pid] -o lstart查看进程开放时间

g) pstree -h [pid] -p -a查看某个进程的进程树

h) 查看开放的端口：netstat -antpl，通过端口判断进行排查，排查有没有异常端口正 在进行网络连接（看state状态）

i) 查看正在进行的网络连接：lsof -i

j) 查看进程打开的文件：lsof -p [pid] lsof -c [进程名]

h) 查看端口对应的进程：fuser -n tcp [端口号]

1. 计划任务
   1. crontab -l查看计划任务
   2. Crontab -r删除计划任务
   3. /var/log/cron 查看计划任务日志
   4. 查看隐藏计划任务：crontab -e 或cat -A /var/spool/cron/root
2. 日志
   1. /var/log/cron计划任务
   2. /var/log/lastlog登录的用户
   3. massage系统信息
   4. secure记录用户输入的账号密码
   5. wtmp登陆成功的用户信息
   6. faillog登录失败的用户信息
3. 文件排查
   1. 查看tmp目录下的文件 /tmp /var/tmp
   2. Ls -alt | head -n 10 按时间顺序排列
   3. 查看文件的时间戳 stat \*
   4. 查看权限为777的文件 find / -perm 777 | more
   5. 查看指定文件夹下7天之内修改过的文件：find /var/log -type f -mtime +7 |xargs ls -alh