linux 应急响应

一、前期交互（同 windows 应急响应）

二、linux 应急响应

1)操作系统信息

a) Uname -a 查看操作系统信息、内核版本
b) cat /proc/version
c) lsb_release -a(需要安装 lsb:yum install lsb):可以用来获取发行版本的信息
d) 枚举主机的所有服务：service --status-all
e) 查看历史命令：history 或 cat ~/.bash_history
f) 查看主机的驱动程序：lsmod
g) 查看是否添加了 ssh 私钥：ll ~/.ssh

2)登录排查

a) 查看当前登录的用户：who
b) 查看上一次登陆成功的用户：last
c) 查看最近登录失败的用户：lastb
d) 查看所有用户最近登录的时间：lastlog
e) 查看用户信息：cat /etc/passwd，注意查看可登录 shell 的用户，shell 为/bin/bash
f) 检测 Uid=0 的用户（超级用户，拥有 root 权限）：
   awk -F: '$3==0 {print $1}' /etc/passwd
g) 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
h) /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

3)启动项排查

a) 列出所有的开机启动项：chkconfig --list
b) 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)

4)进程排查

a) ps[参数]
   i. -e 显示所有进程
   ii. -f 全格式
   iii. -h 不显示标题

iv. -a 显示所有进程，包括其他用户的进程

v. -x 显示所有程序

vi. -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]

5)计划任务

a) crontab -l 查看计划任务

b) Crontab -r 删除计划任务

c) /var/log/cron 查看计划任务日志

d) 查看隐藏计划任务：crontab -e 或 cat -A /var/spool/cron/root

6)日志

a) /var/log/cron 计划任务

b) /var/log/lastlog 登录的用户

c) massage 系统信息

d) secure 记录用户输入的账号密码

e) wtmp 登陆成功的用户信息

f) faillog 登录失败的用户信息

7)文件排查

a) 查看 tmp 目录下的文件 /tmp /var/tmp

b) Ls -alt | head -n 10 按时间顺序排列
c) 查看文件的时间戳 stat *
d) 查看权限为 777 的文件 find / -perm 777 | more
e) 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