应急响应的基本流程(建议收藏)

系统安全运维 3天前

注意在整个过程中不要被客户或现场的运维人员误导。
操作前需先征得客户许可。
因实际的应急情况会比较复杂，因此需根据实际情况进行灵活处置。

1.了解情况

1. 发生时间：询问客户发现异常事件的具体时间，后续的操作要基于此时间点进行追踪分析。
2. 受影响系统类型：询问具体的操作系统类型及相关情况，以便后续的应急处置。
    - windows/linux
    - 财务系统/OA系统/官网，系统重要性，是否可关停
    - 是否有弱口令，远程管理端口是否开放
    - 都开放了什么端口，有什么服务，服务是否存在风险性
    - 必要的话现场检测，不要完全相信听来的东西
3. 异常情况：
    - 文件被加密
    - 设备无法正常启动
    - 勒索信息展示
    - CPU利用率过高
    - 网页挂马/黑链
    - 对外发送异常请求
    - 对外发送垃圾短信
    - 等非正常的情况
4. 已有的处置措施：
    - 之前是否存在此类问题
    - 是否在出现问题后配置了新的策略
    - 是否已有第三方已进行了应急处理，处理结果是什么
    - 是否有其他处置措施
5. 系统架构/网络拓扑：是否能提供网络拓扑图
6. 能否提供以下日志
    - 服务器日志
    - 应用日志，重点web日志

- 数据库日志

7. 已有的安全设备
   - 终端杀软
   - 防火墙
   - WAF
   - 流量分析设备
8. 基本的应急处置方案
   - 临时处置方案
   - 勒索病毒处置方案
   - 挖矿程序处置预案
   - 网页挂马处置预案
   - DDOS处置预案
   - 内部数据泄露处置预案
   - 其他处置预案
9. 应急报表：
   - 包含下述应急方法
   - 端口开放情况，及各个端口应用分析，处置建议

2. 遏制传播风险

- 禁止被感染主机使用U盘，移动硬盘。如必须使用做好备份
- 禁用所有无线/有线网卡或直接拔网线
- 关闭相关端口
- 划分隔离网络区域
- 封存主机，相关数据备份
- 被感染主机应用服务下线
- 被感染主机部分功能暂停
- 被感染主机相关账号降权，更改密码
- 勒索病毒处置 - 核心是止损,这点非常重要
  i. 通过各类检查设备和资产发现，确定感染面；
  ii. 通过网络访问控制设备或断网隔离感染区域，避免病毒扩散；
  iii. 迅速启动杀毒或备份恢复措施，恢复受感染主机的业务，恢复生产。（这点最重要，因为是保障业务的关键动作）
  iv. 启动或部署监测设备，针对病毒感染进行全面监测，避免死灰复燃。
  v. 在生产得到恢复并无蔓延之后，收集所有相关的样本、日志等，开展技术分析，并寻找感染源头，并制定整改计划。

3.已知高危漏洞排查

- 可与下面的步骤同时进行，扫描高危漏洞。但要注意扫描产生的大量日志不要影响漏洞排查

4.系统基本信息

- Windows

  1）查看当前系统的补丁信息 `systeminfo`

- Linux

  1）列出系统arp表，重点查看网关mac地址 `arp -a`
  2）文件搜索命令 `find / -name ".asp"`

- 重点关注

  1）系统内是否有非法账户
  2）系统中是否含有异常服务程序
  3）系统是否存在部分文件被篡改，或发现有新的文件
  4）系统安全日志中的非正常登陆情况
  5）网站日志中是否有非授权地址访问管理页面记录
  6）根据进程、连接等信息关联的程序，查看木马活动信息。
  7）假如系统的命令（例如netstat ls 等）被替换，为了进一步排查，需要下载一新的或者从其他未感染的主机拷贝新的命令。
  8）发现可疑可执行的木马文件，不要急于删除，先打包备份一份。
  9）发现可疑的文本木马文件，使用文本工具对其内容进行分析，包括回连IP地址、加密方式、关键字（以便扩大整个目录的文件特征提取）等。

5.异常连接排查

- Windows

  1）查看目前的网络连接，定位可疑的 ESTABLISHED `netstat -ano`

```
netstat -ano | findstr ESTABLISH

参数说明：
-a  显示所有网络连接、路由表和网络接口信息
-n  以数字形式显示地址和端口号
-o  显示与每个连接相关的所属进程 ID
```

```
-r   显示路由表
-s   显示按协议统计信息、默认地、显示 IP
LISTENING       侦听状态
ESTABLISHED     建立连接
CLOSE_WAIT      对方主动关闭连接或网络异常导致连接中断
```

2）查看端口对应的pid `netstat -ano | findstr "port"`

3）`netstat -nb` 显示在创建每个连接或侦听端口时涉及的可执行程序，需要管理员权限，这条指令对于查找可疑程序非常有帮助。

- Linux

1）列出所有打开了网络套接字（TCP和UDP）的进程

```
lsof -i
lsof -i|grep -E "LISTEN|ESTABLISHED"
```

2）列出所有打开的端口及连接状态

```
netstat -antlp
netstat -an
```

```
说明
-a   显示所有连线中的 Socket。
-n   直接使用 IP 地址,而不通过域名服务器。
-t   显示 TCP 传输协议的连线状况。
-u   显示 UDP 传输协议的连线状况。
-v   显示指令执行过程。
-p    显示正在使用 Socket 的程序识别码和程序名称。
-s    显示网络工作信息统计表
```

6.正在运行的异常进程排查

- Windows

1）查看异常进程 任务管理器

2）显示运行在本地或远程计算机上的所有进程 `tasklist | findstr 11223`

```
根据netstat定位出的异常进程的pid，再通过tasklist命令进行进程定位
```

1）根据 wmic process 获取进程的全路径 `wmic process | findstr "xx.exe"`

2）查看进程的详细信息，比如进程路径，进程ID，文件创建日期，启动时间等

```
"开始->运行->msinfo32->软件环境 -> 正在运行任务"
```

1）关闭某个进程 `wmic process where processid="2345" delete`

- Linux

1）查找进程pid

```
netstat -antlp     先找出可疑进程的端口
lsof -i:port       定位可疑进程pid
```

2）通过pid查找文件

```
linux每个进程都有一个对应的目录
cd /proc/pid号     即可进入到该进程目录中
ls -ail    结果中exe对应的就是该pid程序的目录
ls -ail |grep exe
```

3）查看各进程占用的内存和cpu `top`

4）显示当前进程信息 `ps`

5）实现某个进程的精确查找 `ps -ef | grep apache`

6）结束进程 `kill -9 pid`

```
kill -9 4394
```

7）查看进程树 `pstree -p` 查找异常进程是否有父进程

8）也可以直接搜索异常进程的名程来查找其位置， `find / -name 'xxx'`

7.异常账号排查

- Windows

1）图形化界面查看当前的账户和用户组 `lusrmgr.msc`

2）查看当前账户情况 `net user`

3）查看某个账户的详细信息 `net user Guest`

4）查看当前组的情况 `net localgroup administrators`

5）查看当前系统会话，比如查看是否有人使用远程终端登陆服务器 `query user`

```
踢出该用户  `logoff ID`  ID是上面查询出来的。也可能是用户名
```

- Linux

1）查看utmp日志，获得当前系统正在登陆账户的信息及地址 `w`

2）获得系统前N次的登陆记录 `last | more`

3）查看账号情况 `cat /etc/passwd`

```
查找/etc/passwd 文件， /etc/passwd 这个文件是保存着这个 linux 系统所有 用户的信息
/etc/passwd中一行记录对应着一个用户，每行记录又被冒号(:)分隔为7个字段， 其格式和具
用户名:口令:用户标识号:组标识号:注释性描述:主目录:登录 Shell
注意：无密码只允许本机登陆，远程不允许登陆，某个版本之后好像因为安全问题，passwd文件
```

4）查看账号情况 `cat /etc/shadow`

```
root:$6$oGs1PqhL2p3ZetrE$X7o7bzoouHQVSEmSgsYN5UD4.kMHx6qgbTqwNVC5oOAouXvcjQSt.F
用户名：加密密码：密码最后一次修改日期：两次密码的修改时间间隔：密码有效期：密码修改到期

这里查账号感觉好一点，一般系统的账号都是没有密码的，所以找最长的那几个，那就是有密码的账
```

5）linux非root用户文件夹所在位置 `/home`

6）查看所有账户最后一次登陆时间 `lastlog`

7）显示用户登陆错误的记录 `lastb` 检查暴力破解

8）显示用户最近登陆信息 `last`

```
数据源为
/var/log/wtmp
/var/log/wtmp.1
```

```
/var/log/btmp
/var/log/btmp.1
```

9）查看当前登陆用户 `who` （tty本地登陆 pts远程登录）

10）查看当前时刻用户行为 `w`

11）查看登陆多久，多少用户，负载 `uptime`

12）禁用账户，账号无法登陆，/etc/shadow 第二栏为！开头 `usermod -L user`

13）删除user用户 `userdel -r user`

14）创建用户

```
useradd admin      #创建一个用户，在home目录下不创建文件夹
passwd admin       #修改之前创建的账号的密码
adduser admin2     #是一个比较完善的创建用户的命令，会在home目录下生成一个admin2的
```

15）删除用户

```
userdel admin2      #这样删除的话不完全，home目录下的admin2目录不会删除
userdel -rf admin   #-r 完全删除一个账户    -f强制删除
如果遇到账户删除显示已经删除，但创建同名的用户提示用户已存在的情况，尝试以下方法进行
手动删除passwd、shadow、group里面用户相关字段，以及用户相关的log和mail，并强制删
/home
/etc/passwd
/etc/group
/var/spool/mail
```

8.异常文件分析

- Windows

1）查看文件时间 右键查看文件属性，查看文件时间
2）Recent 是系统文件夹，里面存放着你最近使用的文档的快捷方式，查看用 户 recent 相关文件，通过分析最近打开分析可疑文件 `%UserProfile%\Recent`
3）通过文件时间属性来定位可疑文件:根据文件夹内文件列表时间进行排序，查找可疑文件。当然也可以搜索指 定日期范围的文件及文件 查看文件时间，创建时间、修改时间、

访问时间，黑客通过菜刀类工具改 变的是修改时间。所以如果修改时间在创建时间之前明显是可疑文件

- Linux

1）分析文件日期 `stat xx.asp`

2）返回最近24小时内修改过的文件 `find ./ -mtime 0`

```
返回的是前48~24小时修改过的文件   find ./ -mtime 1
返回10天内修改过的文件，可以把最近几天的数据一天天的加起来   find ./ -mtime 0 -o -
查找 24 小时内被修改的 php 文件   find ./ -mtime 0 -name "*.php"
```

3）敏感目录的文件分析 [类/tmp 目录，命令目录/usr/bin /usr/sbin 等], 查看 tmp 目录下的文件➜ `ls -alt /tmp/ | head -n 10` 这样是按时间顺序查出来的结果

4）特殊权限文件查找

```
find / *.jsp -perm 777
find / -perm 777 |more
find / *.sh -perm 777|grep .sh
```

5）隐藏的文,以 "."开头的具有隐藏属性的文件,当前目录查找 `ls -ar |grep "^\."`

6）i linux文件不可修改权限

```
chattr +I filename     给文件添加不可修改权限
chattr -I filename     将文件的不可修改权限去掉
lsattr filename      查看文件是否设置了相关权限
如果设置了该参数，则无论任何人想要删除改文件均需要将此权限去掉
```

7）a linux文件不可修改权限

```
chattr +a filename     给文件添加只追加权限
chattr -a filename     将文件的只追加权限去掉
lsattr filename      查看文件的相关权限设置
这个权限让目标只能追加，不能删除，而且不能通过编辑器追加
```

8）查看ssh相关目录有无可疑的公钥存在
Redis（6379） 未授权恶意入侵，即可直接通过redis到目标主机导入公钥

目录：/etc/ssh ./.ssh/

9.启动项排查

- Windows

1）查看开机启动有无异常文件 `msconfig`

2）win10开机启动文件夹

```
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp
快捷查找方法，找一个安装好的程序的快捷方式，右键打开文件位置，再进入该目录下的启动目
```

3）win7开机启动文件夹

```
C:\Users\rpkr\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
查找方式，开始>所有程序>启动 ,03查找同此方法
```

4）在注册表中查看开机启动项是否异常

```
开始->运行->regedit，打开注册表，查看开机启动项是否正常，特别注意如下三个注册表项：
HKEY_CURRENT_USER\software\micorsoft\windows\currentversion\run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce
检查右侧是否有启动异常的项目，如有请删除，并建议安装杀毒软件进行病毒查杀，清除残留病
```

- Linux

1）查看开机启动项内容

```
ls -alt /etc/init.d/
/etc/init.d 是 /etc/rc.d/init.d  的软连接
```

2）启动项文件 `more /etc/rc.local`

```
/etc/rc.d/rc[0~6].d
ls -l /etc/rc.d/rc3.d/
```

```
ll /etc |grep rc
```

3）定时任务-基本使用

```
1.利用crontab创建计划任务
crontab -l 列出某个用户 cron 服务的详细内容
2.删除每个用户cront任务（慎重：删除所有的计划任务）
crontab -r
3.使用编辑器编辑当前的crontab文件
crontab -e
如：*/1 * * * * echo ""hello word"" >> /tmp/test.txt 每分钟写入文件
4.利用anacron实现异步定时任务调度
每天运行 /home/bacup.sh 脚本
vi /etc/anacrontab
#daily 10 example.daily /bin/bash /home/backup.sh
当机器在backup.sh期望被运行时是关机的，anacron会在机器开机十分钟后运行它，而不用再
ls -al /var/spool/cron/     查看隐藏的计划任务
Tips：默认编写的crontab文件会保存在（/var/spool/cron/用户名 例如：/var/loop/cr
5.查看分析任务计划
crontab -u <-l, -r, -e>
-u 指定一个用户
-l 列出某个用户的任务计划
-r 删除某个用户的任务
-e 编辑某个用户的任务（编辑的是/var/spool/cron下对应用户的cron文
件，也可以直接修改/etc/crontab文件）
```

10.计划任务排查(定时任务)

- Windows

1）查看Windows 计划任务 `taskschd.msc`

```
或者 【程序】→【附件】→【系统工具】→【任务计划程序】
```

- Linux

1）查看当前计划任务有哪些 `crontab -l` 是否有后门木马程序启动相关信息

2）查看分析计划任务 `crontab -u <-l, -r, -e>`

```
解释
-u 指定一个用户
-l 列出某个用户的任务计划
-r 删除某个用户的任务
-e  编辑某个用户的任务（编辑的是/var/spool/cron 下对应用户的 cron 文件，也可以直接
/etc/crontab 文件）
```

3）查看 etc 目录任务计划相关文件 `ls -al /etc/cron*  cat /etc/crontab`

4）此处要注意隐藏的计划任务，在linux中以 . 开头的文件为隐藏文件，要使用 `ls -al` 来查看

5）定时任务 - 入侵排查
重点关注以下目录中是否存在恶意脚本
/var/spool/cron/*
/etc/crontab
/etc/cron.d/*
/etc/cron.daily/*
/etc/cron.hourly/*
/etc/cron.monthly/*
/etc/cron.weekly/
/etc/anacrontab
/var/spool/anacron/*
小技巧：more /etc/cron.daily/* 查看目录下所有文件

11.日志排查

- Windows
  i. 查看防护设备的日志
  ii. 打开日志管理器 `eventvwr.msc`
  iii. 查看暴力破解问题，筛选事件ID，win2008 4625
- Linux

1）查看历史命令记录文件 `cat /root/.bash_history |more` ,每个账户对应的文件夹下都有这样一个日志文件，但感觉记录的不是特别全。可以直接在root下搜索 .bash_history 这个文件。

2）如有 `/var/log/secure` 日志，可观察其进行暴力破解溯源

3）ubuntu 建议使用 lastb 和 last 进行暴力破解溯源

```
/var/log/message 系统启动后的信息和错误日志，
/var/log/secure 与安全相关的日志信息
/var/log/maillog 与邮件相关的日志信息
/var/log/cron 与定时任务相关的日志信息
/var/log/spooler UUCP和news设备相关日志信息
/var/log/boot.log 进程启动和停止相关的日志消息
```

4）linux系统日志相关配置文件为/etc/rsyslog.conf（syslog.conf） 主要找wget\ssh\scp\tar\zip 添加账户修改密码一类的

- web服务器

1）无论任何web服务器，都需要关注以下的日志
access_log
error_log
access.log
error.log

2）apache日志位置

```
应通过httpd.conf配置来判断。
在httpd.conf中搜索未被注释的、以指令字CustomLog为起始的行，该行即指定了日志的存储位
搜索可使用文本搜索，也可使用grep进行：grep -i CustomLog httpd.conf | grep -v ^#
搜索结束后会获得类似如下的搜索结果：
CustomLog /var/mylogs/access.log common
其中 /var/mylogs/access.log即为客户日志的路径。
若此处未指明日志的完整路径而只是列举日志的文件名（如：access.log），
则意指该文件存储与默认的日志存储目录下（即，/var/log/httpd 或 /var/httpd 目录）。
```

3）IIS日志位置

```
IIS日志默认存储于 %systemroot%\system32\LogFiles\W3SVC目录中，
日志命名方式为exYYMMDD.log（YYMMDD指：年 月 日）。
但IIS日志路径也可通过用户配置来指定，通过WEB站点配置可确认其位置：
WEB站点 — 属性 — 网站 — W3C扩展日志文件格式 — 属性 — 日志文件目录
```

- 数据库

1）mysal - cat mysql.log|grep union

12.恢复阶段

- 此阶段以客户为主，仅提供建议

1. webshell/异常文件清除
    - 相关样本取样截图留存
2. 恢复网络
3. 应用功能恢复
4. 补丁升级
5. 提供安全加固措施，推荐切合的安全产品

13.跟踪总结

1. 分析事件原因
    - 攻击来源，IP
    - 攻击行为分析，弱口令、可以导致命令执行的漏洞等
2. 输出应急报告
3. 事后观察
4. 提供加固建议

附1 有毒没毒还是要自己分辨的

- windows下常用的安全工具

工具	主要功能	下载地址
360杀毒	306全家桶就不用说了吧	http://sd.360.cn/download_center.html
河马	webshell查杀	http://www.shellpub.com/
microsoft network monitor	轻量级的无线抓包	https://www.microsoft.com/en-us/download/details.aspx?id=4865
深信服检测工具	类似于360	https://edr.sangfor.com.cn/#/introduction/all_tools
PCHunter	可查看进程、内核、服务等	http://www.xuetr.com/
火绒剑	可查看进程、内核、服务等	https://www.huorong.cn/
D盾	查找恶意文件以及webshell	http://www.d99net.net/News.asp?id=47
ProcessExplorer	Windows系统和应用程序监视工具	https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer
processhacker	类似ProcessExplorer	https://processhacker.sourceforge.io/downloads.php
autoruns	可查看windows在启动或登陆时启动的程序	https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns
卡巴斯基	病毒扫描，没用过	http://devbuilds.kaspersky-labs.com/devbuilds/KVRT/latest/full/KVRT.exe
VirSCAN.org	在线病毒分析平台	http://www.virscan.org/language/zh-cn/
腾讯哈勃分析系统	在线病毒分析平台	https://habo.qq.com/
Jotti恶意软件分析系统	在线病毒分析平台	https://virusscan.jotti.org/
ScanVir	在线病毒分析平台	http://www.scanvir.com/

linux下常用的安全工具-linux下不方便，可以把文件拷出来，用windows的工具去检测

工具	主要功能	下载地址
Chkrootkit	查找检测rootkit后门的工具	http://www.chkrootkit.org/
rootkit hunter	查找检测rootkit后门的工具	http://rkhunter.sourceforge.net/

附2

1. 处理前先kill掉病毒进程，避免插入的U盘被加密
2. 如果日志分析阶段遇到困难，可对代码进行webshell查杀，可能会有惊喜
3. PC Hunter 数字签名颜色说明：
   黑色：微软签名的驱动程序；
   蓝色：非微软签名的驱动程序；
   红色：驱动检测到的可疑对象，隐藏服务、进程、被挂钩函数；
4. ProcessExplorer (1).子父进程一目了然；
   (2).属性中的关键信息:
   [映像]->[路径/命令行/工作目录/自启动位置/父进程/用户/启动时间];[TCP/IP];[安全]->[权限]；
   (3).想了解不同颜色意思？[选项]->[配置颜色]；
   (4).打开procexp，在标题栏右键，可以勾选其它一些选项卡

(5).进程标识颜色不同是用于区分进程状态和进程类型，进程开始启动时为绿色，结束时为红色

可对某个进程进行操作，右键单击即可

5. chkrootkit主要功能
   检测是否被植入后门、木马、rootkit/检测系统命令是否正常/检测登录日志
   chkrootkit安装：rpm -ivh chkrootkit-0.47-1.i386.rpm
   检测，#chkrootkit –n；如果发现有异常，会报出“INFECTED”字样
6. rkhunter主要功能：系统命令（Binary）检测，包括Md5 校验 Rootkit检测 本机敏感目录、系统配置、服务及套间异常检测 三方应用版本检测
7. RPM check检查 ./rpm -Va > rpm.log 下图可知ps, pstree, netstat, sshd等等系统关键进程被篡改了：

```
原文链接：https://github.com/1120362990/Paper/blob/master/%E5%BA%94%E6%80%A5%E5%
公众号排版：系统安全运维
```

好文推荐

渗透测试面试近期热门题

干货|安全工程师面试题汇总

渗透工程师常用命令速查手册

Web常见漏洞描述及修复建议

流量分析与日志溯源的个人理解

规范报告中的漏洞名称以及修复建议

应急响应 | 7款WebShell扫描检测查杀工具

11个步骤完美排查Linux机器是否已经被入侵

欢迎关注 系统安全运维

系统安全运维

未知攻 焉知防 攻防兼备

17篇原创内容

公众号

每日坚持分享，麻烦各位师傅文章底部给点个“再看”，感激不尽🤭

喜欢此内容的人还喜欢

应急响应之windows入侵排查篇

系统安全运维

10种网站常见安全隐患及防御方法

系统安全运维

Windows 应急响应思路及技巧

系统安全运维