安全应急

应急响应目标

在第一时间采取响应的措施，恢复业务到正常，调查安全事件发生的原因，避免同类事件发生，提供数字证据

应急响应范围

邮件钓鱼，黑客入侵，APT 攻击，漏洞利用，网络攻击，数据外泄，时间通报，攻击溯源，网络异常，网站被黑，网站挂马，网站暗链，网站篡改

应急响应的目的

判断这次应急是否是被成功入侵的安全事件
找到攻击者入口点
提取恶意样本
帮助客服梳理攻击者的攻击路线，提供漏洞修复方案

Linux 系统基础知识

Etc/sysconfig/network-script/ 网卡配置
目录结构
/bin 放置系统命令目录，/bin 目录可以在维护模式下还可以被操作
/boot 放置开机使用的文件，包括 linux 核心文件以及开机选单与开机所需设定文件
/dev 放置装置与周边设备都是以文件的形态，存在于这个目录当中
/etc 系统主要的设定文件几乎都放置在这个目录内，列如人员的账户密码文件，各种服务的起始文件等等
/home 系统预设的使用者家目录(home,directory) 你新增的用户家目录都会规范进来
/lib 和/lib64 系统的函试库非常的多，而.lib 或者/lib64 放置常用的函数
/opt 存放第三方软件和位置目录
/root root 用户的家目录
/sbin linux 有非常多指令是用来设定系统环境的，这些指令只有 root 才能够利用来设置系统，里面包括了开机，修复，还原系统所需要的指令
/tmp 任何人都可以读写的目录，重新启动目录中存放的文件会被删除

用户组
所有者，所在组，其它组
文件普通权限
Rwx r=4 w=2 x=1
文件特殊权限
SUID：s 出现在文件所有者的 X 权限上
SGID：s 出现在文件所属群组的 X 权限上
SBIT：t 出现在文件其他用户的 x 权限上

Linux 常用命令

Stat 跟文件
会显示文件 UID，文件名，文件属性，文件访问时间，文件内容修改时间，文件元数据变化时间
Access time 访问时间：文件中的内容最后被访问的最后时间
Modified time 修改时间：文件内容被修改的最后时间
Change time 变化时间：文件的元数据发生变化，写入文件，更改所有者，权限修改

Ls 命令 列出文件
-a 显示隐藏文件，-L 详细显示，-R 递归显示

Netstat 命令
-a 显示所有链接中的 soket -n 使用 ip，而不是域名显示 -t 显示 TCP 链接
-p 显示每个网络链接对应的进程和用户 -l 显示处于监听中的 socket
-e 显示拓展信息，inode 等信息
-u 显示 UDP 连接

Lsof 命令 列出来当前系统打开文件
Lsof -c sshd 显示 sshd 进程现在打开的文件
Lsof -p pid 显示进程号为 pid 的进程情况
Lsof +d /tmp 显示目录下被进程打开的文件
Lsof +D /tmp 递归显示显示目录下被进程打开的文件
Lsof -i:80 查看端口为 80 的 tcp 或者 udp 进程

Ps 命令 常用进程
Ps -a 显示当前终端下的进程
Ps -u 以用户为主的显示方式
Ps -x 显示所有进程

Grep 命令 检索命令
Grep -I 忽略大小写
Grep -v 不包含特殊字符

Tcpdump 命令 抓流量
Tcpdump -I eth0 抓取网卡为 eth0 的流量
Tcpdump tcp 抓取 tcp 流量
Tcpdump port 53 抓取端口为 53 的流量，源端口或者目的端口
Tcpdump host 1.1.1.1 抓取和主机 1.1.1.1 有关的流量
Tcpdump -w wireshark。Pcap 流量保存为图形化分享软件可识别的数据包

Find 命令 目录文件列出来，也可以查找文件
Find path -name filename 在 path 路径下查找文件名为 filename 的文件

Find path -perm 777 在 path 路径下查找文件权限为 777 的文件
Find path -perm -700 在 path 路径下查找文件权限为 700 以及 700 以上权限的文件

Md5 计算文件 Md5
Rz 接收文件
Sz 传输文件
Strings 字符串显示文件

Linux 常规检查项-关键文件，关键目录等

文件检测-历史命令

Root 用户执行过的历史命令
/root/.bash_history
对应 username 执行过的历史命令
/home/{username}/.bash_history
当前用户执行过的历史命令
History

文件检测-系统关键文件

/etc/passwd 包含系统用户和用户的主要信息
/etc/shadow 用于储存系统中用户的密码，又称为影子文件
/etc/group 记录组 ID 和组名的对应文件

写到 profile 里面的命令都是会被调用执行的
/etc/profile 此文件涉及系统的环境，变量，会从中调用 shell 变量
/root/.bash_profile 变量
/home/{username}/.bash_profile 变量

/root/.bashrc 此文件为系统的每个用户设置的环境信息，用户第一次登陆时，该文件被执行
/home/{username}/.bashrc
/root/.bash_logout 用户退出的时候的操作
/home/{username}/.bash_logout
/root/.ssh/authorized_keys 存放 ssh 公私钥的地方
/home/{username}/.ssh/authorized_keys

文件检测—系统关键目录

/root/
/home/{username}
/tmp
/var/tmp
/dev/shm

命令检测，防止恶意命令替换

/usr/bin/ps
/usr/bin/netatat
/usr/bin/ps
/usr/sbin/lsof
/usr/sbin/ss
/usr/bin/stat

检测系统安装包

列出系统所有按照的 rpm 包
Rpm -qa
校验系统所有 rpm 包
Rpm -V -a
校验特定文件或者命令
Rpm -V -f /etc/sysconfig

Which ps 查看 ps 命令的变量路径

Linux 应急计划任务

Crontab 计划任务：系统自带的定时执行脚本或者命令的系统服务

Systemctl status crond 查看 crond 服务状态
Systemctl start crond 启动 crond 服务
Systemctl stop crond 停止 crond 服务
Systemctl enable crond 开机启动 crond 服务
Systemctl disable crond 关闭开机启动 crond 服务

Crontab
-l 列出 crontab
-u 指定用户用户
-e 编辑 crontab
从左到右依次为：
[分钟] [小时] [每月的某一天] [每年的某一月] [每周的某一天] [执行的命令]

/etc/cron.deny /etc/cron.allow

Crontab 的限制文件，用户名存在 cron.deny，且 cron.allow 不存在，或者用户名不存在 cron.allow 的时候，不允许此用户创建 crontab

Cron.allow 优先级高于 cron.deny

系统默认不存在 cron.allow

系统默认 crontac 相关配置文件目录
/etc/cron.d/
/etc/cron.hourly/
/etc/cron.daily/
/etc/cron.monthly/
/etc/cron.weekly/
/etc/crontab
/var/spool/cron/
/var/log/cron crontab 日志
/etc/systemd/system/multi-user.target.wants/crond.service

Linux-系统日志

配置文件

/etc/rsyslog.conf
/etc/rsyslog.d/*

登陆相关日志

/var/log/下

Secure 记录于安全相关的信息
Lastlog 当前登陆的用户日志
Wtmp 永久记录每个用户登陆，注销及系统的启动，停机的事件，last 命令查看
Btmp 尝试登陆且失败日志

其他日志
Messages 各种系统守护进程，用户程序和内核相关信息
Cron c rontab 日志
Audit/* audit 日志，监控系统调用
Boot.log 启动信息相关日志
Yum.log 通过 yum 安装 rpm 相关日志
Httpd/* httpd 服务访问日志和错误日志
Firewalld 防火墙相关日志
Mail 邮件相关日志
Dmesg 核心启动日志

Windows 常见命令

Regedit 查看策略表
Msconfig 查看系统配置
Taskmgr 启动任务管理器

Eventvwr,msc　打开日志的命令
Gpedit.msc　　打开本地组策略
Compmgmt.msc　计算机管理
Lusrmgr.msc　　打开用户与组
Taskschd　　打开计划任务
Net user xxx /add 添加用户
Net localgroup administrators xxxx /add 把某用户放到管理员组里面
Net session 查询当前会话
Net start 查看当前运行的服务
Net use 查看当前共享连接
Net share 查看共享映射的盘符，连接状态
Net share xxx /del 删除共享的链接
查看隐藏用户可以去，用户管理

Findstr /s /l “hellow” **
查询包含 hellow 的关键字

Wmic pross

Attrib 查看文件属性
Attrid 1.txt
Attrid -R

系统日志收集工具
Sglad_ir
Gather_log

系统变量敏感文件路径

%WINDIR%　　C 盘 windows
%WINDIR%\system32\%　c 盘 windows system32
%TEMP% 临时目录
%APPDATA% 软件程序
%LOCALAPPDATA% 软件程序
Windows 系统日志
C:\Windows\System32\winevt\Logs\system.evtx
Windows 系统安全日志
C:\Windows\System32\winevt\Logs\ Security.evtx
4624id 是登陆成功的 id
Windows 应用程序日志
C:\Windows\System32\winevt\Logs\ Application.Evtx

主要关注安全日志，里面记录账户登陆，注销，等等的日志

系统日志中的 id

Id 12 系统启动
6005ID 事件日志服务启动
6004ID 事件日志服务停止
Id 13 系统关闭

安全日志中的 id

4732 添加用户启动安全性的本地组中
4722 启动用户的 id
4720 创建用户
4624 登陆成功
4625 失败登陆
4726 删除用户
4634 注销
4776 成功/失败的账户认证
1102 清理日志

安全日志中的 登陆日志类型

2 交互登陆
3 网络登陆(通过 net use，访问共享网络）
4 批处理(为批处理程序保留)
5 服务器启动
6 不支持
7 解锁（带密码保护的屏幕保护程序）
8 网络明文，iis 服务器登陆验证
10 远程交互(终端服务，远程桌面，远程辅助)
11 缓存域证书登陆

常用的抓包工具

wireshark
Tcp.port eq 25
查询 tcp 端口为 25 的
Ip.addr == 127.0.0.1 包含 127.0.0.1 的

Linux 抓包用的比较多
Tcpdump

Tcpdump host ip
抓这个 ip

Tcpdump host ip1 and ip2
抓
Tcpdump -I eth0 监听这个网卡

Tcpdump tcp port 445 and src host ip
源 ip 端口为 445 的

这个 windows 用的比较多，比较简单好用，用 Micrsosoft Network Monitor

安全分析工具
PChunter

Autoruns
Process explorer

https://www.anquanke.com/post/id/182858

Web 日志分析

Apache
在 httpd.conf 里面记录 log 的访问日志的路径
/etc/httpd/logs
Access.log
Nginx

现在主要的日志格式是 NCSA 拓展格式
访问主机(remotehost)
日期时间(date)
请求(request)
请求类型(METHOD)
请求资源(RESOURCE)
协议版本号(PROTOCOL)
状态码(status)
传输字节数(bytes)
来源页面(referrer)
浏览器信息(agent)