emergency-response-checklist

目录

- emergency-response-checklist
  - 目录
  - 前言
  - 应急响应综合
    - 应急响应类型
    - 初步信息收集
    - 整体分析流程
    - 相关工具/资源
    - 可疑域名后缀
    - 常见动态域名提供商
    - misc
    - 相关项目
  - web应急响应
    - 各中间件/服务器日志默认存放位置
      - IIS
      - apache
      - tomcat
      - weblogic
      - jboss
    - webshell排查
    - 数据库排查
      - 数据库日志
        - mysql日志
        - mssql日志
      - misc
  - linux应急响应
    - 文件
    - 日志
    - 用户
    - 进程
    - 端口
    - 自启动
    - 计划任务
    - misc
  - windows应急响应
    - 文件
    - 日志
    - 帐号
    - 进程
    - 端口

        - 自启动
        - 计划任务
        - 注册表
        - 服务
        - misc
    - 网络层应急响应
        - DDOS
        - ARP欺骗
        - DNS劫持
        - HTTP劫持（内容劫持）
        - 参考资料
    - 交换机/路由器应急响应
        - 交换机负载过高（cpu100\x）
        - 交换机排查常用命令
        - 路由器常用命令
        - misc
        - 相关资料

前言

本项目旨在为应急响应提供全方位辅助，以便快速解决问题。

结合自身经验和网络资料，形成checklist，期待大家提供更多技巧，共同完善本项目，欢迎issue/pr。

愿大家应急之路一帆风顺

下载PDF

//图片皆来源于网络

应急响应综合

应急响应类型

web入侵：挂马、网页篡改（博彩/黑帽SEO等）、植入webshell，黑页，暗链等

主机入侵：病毒木马、勒索软件、远控后门、系统异常、RDP爆破、SSH爆破、主机漏洞、数据库入侵等

网络攻击：DDOS攻击、DNS/HTTP劫持、ARP欺骗等

路由器/交换机异常：内网病毒，配置错误等

初步信息收集

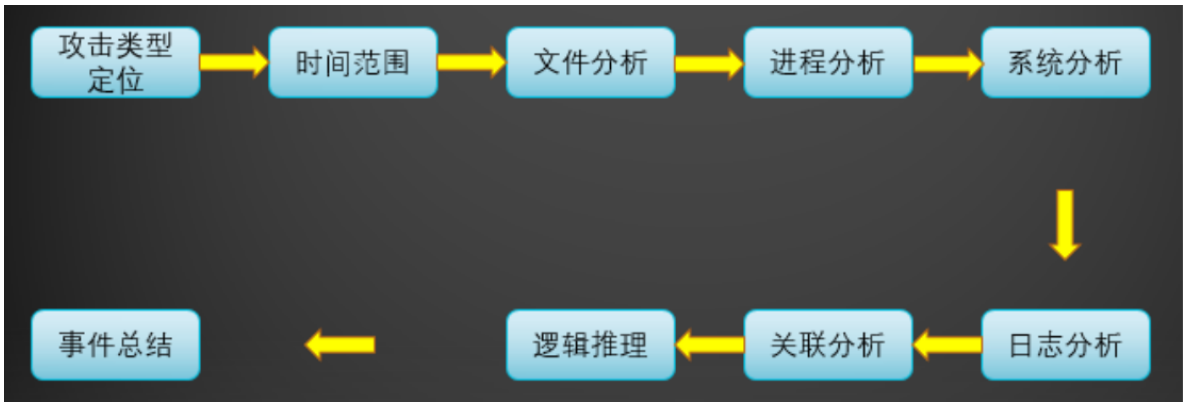
客户属性：如名称/区域/领域等

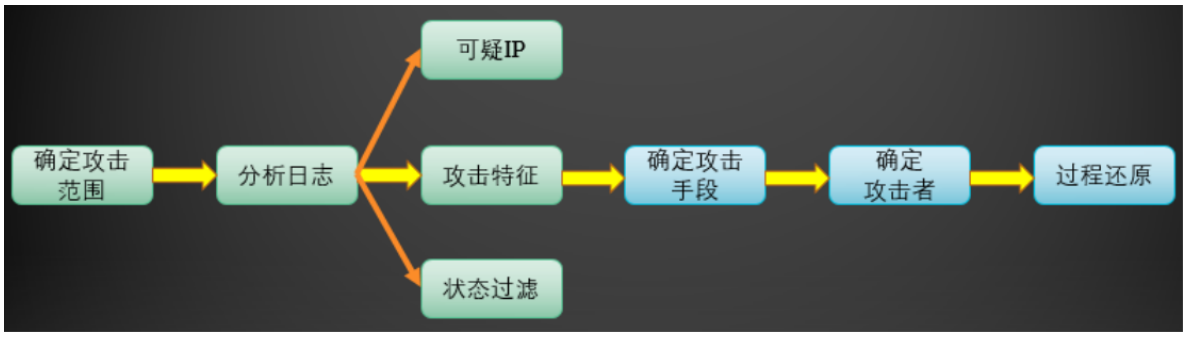
入侵范围：如主机数/网段等

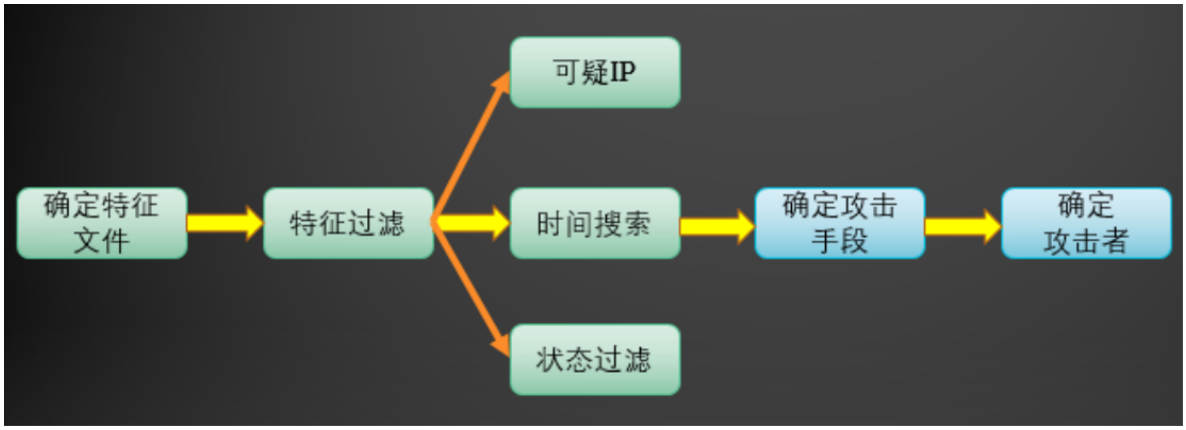
入侵现象：如cpu过高，勒索界面，异常网络链接，安全设备告警等

客户需求：是否要求溯源，是否要求协助修复等

整体分析流程







相关工具/资源

应急响应资源汇总：

https://github.com/theLSA/hack-er-tools

可疑域名后缀

> 顶级域名 申请地区或机构 为何重点关注
>
> .ru 俄罗斯 俄罗斯盛产黑客
>
> .ws 东萨摩亚 不知名国家，易申请，难追踪注册者
>
> .cc 科科斯群岛 不知名国家，易申请，难追踪注册者
>
> .pw 帕劳 不知名国家，易申请，难追踪注册者

> .bz 伯利兹 不知名国家，易申请，难追踪注册者
>
> .su 苏联 前苏联虽然解体了，顶级域名还在使用，且多与黑产有关
>
> .bw 伯兹瓦纳 不知名国家，易申请，难追踪注册者
>
> .gw 几内亚比绍 不知名国家，易申请，难追踪注册者
>
> .ms 蒙塞拉特岛 不知名国家，易申请，难追踪注册者
>
> .mz 莫桑比克 不知名国家，易申请，难追踪注册者

常见动态域名提供商

> 'f3322.net','3322.org','7766.org','8866.org', '9966.org','8800.org','2288.org','6600.org', 'f3322.org', 'ddns.net', 'xicp.net', 'vicp.net','wicp.net','oicp.net','xicp.net','vicp.cc','eicp.net','uicp.cn','51vip.biz','xicp.cn','uicp.net','vicp.hk','5166.info','coyo.eu','imblog.in','imzone.in','imshop.in','imbbs.in','imwork.net','iego.cn','vicp.co','iego.net','1366.co','1866.co','3utilities.com','bounceme.net','ddnsking.com','gotdns.ch','hopto.org','myftp.biz','myftp.org','myvnc.com','no-ip.biz','no-ip.info','no-ip.org','noip.me','redirectme.net','servebeer.com','serveblog.net','servecounterstrike.com','serveftp.com','servegame.com','servehalflife.com','servehttp.com','serveminecraft.net','servemp3.com','servepics.com','servequake.com','sytes.net','webhop.me','zapto.org','dynamic-dns.net','epac.to','longmusic.com','compress.to','wikaba.com','zzux.com','dumb1.com','1dumb.com','onedumb.com','wha.la','youdontcare.com','yourtrap.com','2waky.com','sexidude.com','mefound.com','organiccrap.com','toythieves.com','justdied.com','jungleheart.com','mrbasic.com','mrbonus.com','x24hr.com','dns04.com','dns05.com','zyns.com','my03.com','fartit.com','itemdb.com','instanthq.com','xxuz.com','jkub.com','itsaol.com','faqserv.com','jetos.com','qpoe.com','qhigh.com','vizvaz.com','mrface.com','isasecret.com','mrslove.com','otzo.com','sellclassics.com','americanunfinished.com','serveusers.com','serveuser.com','freetcp.com','ddns.info','ns01.info','ns02.info','myftp.info','mydad.info','mymom.info','mypicture.info','myz.info','squirly.info','toh.info','xxxy.info','freewww.info','freeddns.com','myddns.com','dynamicdns.biz','ns01.biz','ns02.biz','xxxy.biz','sexxxy.biz','freewww.biz','www1.biz','dhcp.biz','edns.biz','ftp1.biz','mywww.biz','gr8domain.biz','gr8name.biz','ftpserver.biz','wwwhost.biz','moneyhome.biz','port25.biz','esmtp.biz','sixth.biz','ninth.biz','got-game.org','bigmoney.biz','dns2.us','dns1.us','ns02.us','ns01.us','almostmy.com','ocry.com','ourhobby.com','pcanywhere.net','ygto.com','ddns.ms','ddns.us','gettrials.com','4mydomain.com','25u.com','4dq.com','4pu.com','3-a.net','dsmtp.com','mynumber.org','ns1.name','ns2.name','ns3.name','changeip.name','ddns.name','rebatesrule.net','ezua.com','sendsmtp.com','trickip.net','trickip.org','dnsrd.com','lflinkup.com','lflinkup.net','lflinkup.org','lflink.com','dns-dns.com','proxydns.com','myftp.name','dyndns.pro','changeip.net','mysecondarydns.com','changeip.org','dns-stuff.com','dynssl.com','mylftv.com','mynetav.net','mynetav.org','ikwb.com','acmetoy.com','ddns.mobi','dnset.com','authorizeddns.net','authorizeddns.org','authorizeddns.us','cleansite.biz'

misc

1）收集信息：操作系统版本，补丁，数据库版本，中间件/服务器，网络拓扑，受害范围，处置情况，提取日志（主机，安全设备，数据库等）

2) 务必亲自求证，眼见为实耳听为虚

相关项目

https://github.com/Bypass007/Emergency-Response-Notes

web应急响应

各中间件/服务器日志默认存放位置

IIS

C:\WINDOWS\system32\LogFiles

apache

Linux：/usr/local/apache/logs/
Windows：apache/logs/

tomcat

conf/logging.properties

logs/catalina.xx.log
logs/host-manager.xx.log
logs/localhost.xx.log
logs/manager.xx.log
主要记录系统启、关闭日志、管理日志和异常信息

weblogic

domain_name/servers/server_name/logs/
server_name.log：server启停日志
access.log：安装在该server之上的应用http访问日志

jboss

LOG4J配置默认Deploy/conf/
如jboss/server/default/conf/jboss-log4j.xml

webshell排查

1) 整站打包用webshell扫描工具扫

2)
find /var/www/ -name "*.php" |xargs egrep 'assert|phpspy|c99sh|milw0rm|eval|(gunerpress|(base64_decoolcode|spider_bc|shell_exec|passthru|($_\POST[|eval(str_rot13|.chr(|${"_P|eval($_R|file_put_contents(.*$_|base64_decode'

3)
grep -i –r eval($_post /app/website/*

4)
find /app/website/ -type f|xargs grep eval($_post

数据库排查

数据库日志

mysql日志

1）错误日志：默认开启，hostname.err

2）查询日志：记录用户的所有操作。默认关闭，general_log_file（常见getshell手法）

3）慢查询日志：记录执行时间超过指定时间的查询语句，slow_query_log_file（慢查询getshell）

4）事务日志：ib_logfile0

5）二进制日志：记录修改数据或有可能引起数据改变的mysql语句，log_bin，默认在数据目录，如mysql-bin.000001

mssql日志

exec xp_readerrorlog

object Explorer-Management-SQL Server logs-view-logs

SQL Server 2008： R2\MSSQL10_50.MSSQLSERVER\MSSQL\Log\ERRORLOG

misc

1）mysql\lib\plugin目录的异常文件

2）select * from mysql.func的异常

3）mssql检查xp_cmdshell等存储过程

4）异常数据库登录

5）数据库用户弱口令

6）mysql相关命令

show global variables like '%log%';

show global variables like '%gene%';

show master status;

systemmore /mydata/data/stu18_slow.log;

showbinary logs;

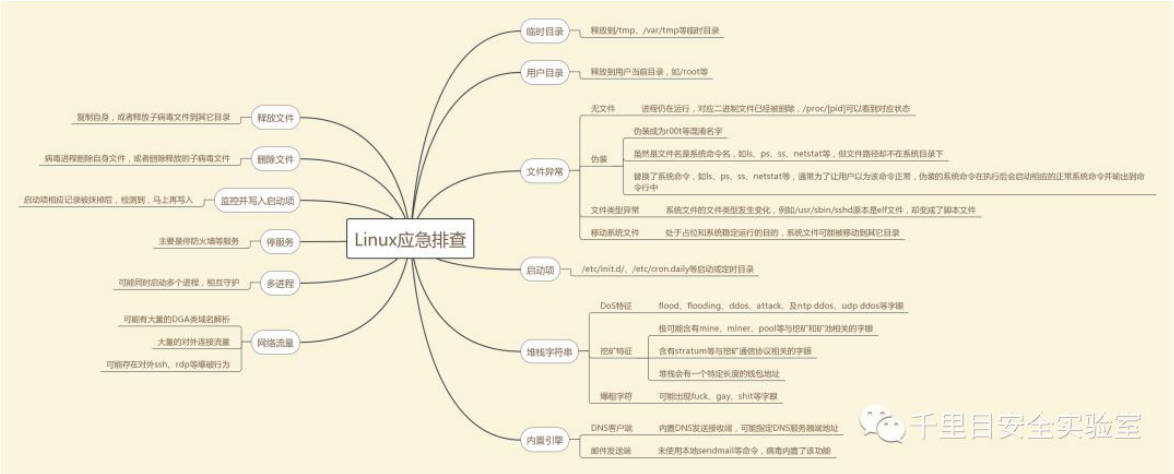
showmaster logs;

showbinlog events in 'mysql-bin.000011';

show processlist;

注意mysqld配置文件

linux应急响应



文件

ls -alt

查找72小时内新增的文件：

find / -ctime -2

文件日期、新增文件、可疑/异常文件、最近使用文件、浏览器下载文件

/var/run/utmp 有关当前登录用户的信息记录

/etc/passwd 用户列表

/tmp 临时目录

~/.ssh

/etc/ssh

查看文件：

ls -alt | head -n 10

查找24小时内被修改的JSP文件：

find ./ -mtime 0 -name "*.jsp"

根据确定时间去反推变更的文件：

ls -al /tmp | grep "Feb 27"

查找777的权限的文件：

find / *.jsp -perm 4777

隐藏文件.xxx

分析sshd 文件是否包括IP信息：

strings /usr/bin/.sshd | egrep '[1-9]{1,3}.[1-9]{1,3}.'

更改：

find /etc/ /usr/bin/ /usr/sbin/ /bin/ /usr/local/bin/ -type f -mtime 0

访问：

find /tmp -iname "*" -atime 1 -type f

命令目录：/usr/bin /usr/sbin

日志

```
1.  /var/log/messages – 包括整体系统信息，其中也包含系统启动期间的日志。此外，mail，cron，daemon，kern和
    auth等内容也记录在var/log/messages日志中。
2.  /var/log/dmesg – 包含内核缓冲信息（kernel ring buffer）。在系统启动时，会在屏幕上显示许多与硬件有关的
    信息。可以用dmesg查看它们。
3.  /var/log/auth.log – 包含系统授权信息，包括用户登录和使用的权限机制等。
4.  /var/log/boot.log – 包含系统启动时的日志。
5.  /var/log/daemon.log – 包含各种系统后台守护进程日志信息。
6.  /var/log/dpkg.log – 包括安装或dpkg命令清除软件包的日志。
7.  /var/log/kern.log – 包含内核产生的日志，有助于在定制内核时解决问题。
8.  /var/log/lastlog – 记录所有用户的最近信息。这不是一个ASCII文件，因此需要用lastlog命令查看内容。
9.  /var/log/maillog /var/log/mail.log – 包含来着系统运行电子邮件服务器的日志信息。例如，sendmail日志信
    息就全部送到这个文件中。
10. /var/log/user.log – 记录所有等级用户信息的日志。
11. /var/log/Xorg.x.log – 来自X的日志信息。
12. /var/log/alternatives.log – 更新替代信息都记录在这个文件中。
13. /var/log/btmp – 记录所有失败登录信息。使用last命令可以查看btmp文件。例如，”last -f /var/log/btm
    p | more“。
14. /var/log/cups – 涉及所有打印信息的日志。
15. /var/log/anaconda.log – 在安装Linux时，所有安装信息都储存在这个文件中。
16. /var/log/yum.log – 包含使用yum安装的软件包信息。
17. /var/log/cron – 每当cron进程开始一个工作时，就会将相关信息记录在这个文件中。
18. /var/log/secure – 包含验证和授权方面信息。例如，sshd会将所有信息记录（其中包括失败登录）在这里。
19. /var/log/wtmp或/var/log/utmp – 包含登录信息。使用wtmp可以找出谁正在登陆进入系统，谁使用命令显示这个文
    件或信息等。
20. /var/log/faillog – 包含用户登录失败信息。此外，错误登录命令也会记录在本文件中。
21. 除了上述Log文件以外， /var/log还基于系统的具体应用包含以下一些子目录：
22. /var/log/httpd/或/var/log/apache2 – 包含服务器access_log和error_log信息。
23. /var/log/lighttpd/ – 包含light HTTPD的access_log和error_log。
24. /var/log/mail/ – 这个子目录包含邮件服务器的额外日志。
25. /var/log/prelink/ – 包含.so文件被prelink修改的信息。
26. /var/log/audit/ – 包含被 Linux audit daemon储存的信息。
27. /var/log/samba/ – 包含由samba存储的信息。
28. /var/log/sa/ – 包含每日由sysstat软件包收集的sar文件。
29. /var/log/sssd/ – 用于守护进程安全服务。
```


/var/log/

/var/log/wtmp 登录进入，退出，数据交换、关机和重启纪录，即last

/var/log/lastlog 文件记录用户最后登录的信息，即lastlog

/var/log/secure 记录登入系统存取数据的文件，如 pop3/ssh/telnet/ftp

/var/log/cron 与定时任务相关的日志信息

/var/log/message 系统启动后的信息和错误日志

/var/log/apache2/access.log apache access log

/var/log/message　　包括整体系统信息

/var/log/auth.log　　包含系统授权信息，包括用户登录和使用的权限机制等

/var/log/userlog　　记录所有等级用户信息的日志

/var/log/cron　　记录crontab命令是否被正确的执行

/var/log/xferlog(vsftpd.log)记录Linux FTP日志

/var/log/lastlog　　记录登录的用户，可以使用命令lastlog查看

/var/log/secure　　记录大多数应用输入的账号与密码，登录成功与否

var/log/faillog　　记录登录系统不成功的账号信息

history (cat /root/.bash_history)

查看爆破失败的IP：

grep 'Failed' /var/log/secure | awk '{print $11}' | sort | uniq -c | sort -nr

查看登录成功的IP：

grep 'Accepted' /var/log/secure | awk '{print $11}' | sort | uniq -c | sort -nr

more messages

定位有多少IP在爆破主机的root帐号：

grep "Failed password for root" /var/log/auth.log | awk '{print $11}' | sort | uniq -c | sort -nr | more

登录成功的IP：

grep "Accepted " /var/log/auth.log | awk '{print $11}' | sort | uniq -c | sort -nr | more

监控最后400行日志文件的变化 等价与 tail -n 400 -f （-f参数是实时）：

tail -400f demo.log

标记该行重复的数量，不重复值为1：

uniq -c demo.log

输出文件demo.log中查找所有包行ERROR的行的数量：

grep -c 'ERROR' demo.log

cat /var/log/secure |grep 'Accepted password'

查看登录成功的日期、用户名及IP：

grep "Accepted " /var/log/secure* | awk '{print $1,$2,$3,$9,$11}'

查看试图爆破主机的IP：

开启iptables：
grep "refused" /var/log/secure* | awk {'print $9'} | sort | uniq -c |sort -nr | more

未开启iptables：

grep "Failed password" /var/log/secure* | grep -E -o "(([0-9]{1,3}).([0-9]{1,3}).([0-9]{1,3}).([0-9]{1,3}))" | uniq -c

查看爆破主机的ROOT账号的IP：

grep "Failed password for root" /var/log/secure | awk '{print $11}' | sort

查看爆破用户名字典：

grep "Failed password" /var/log/secure | awk {'print $9'} | sort | uniq -c | sort -nr

grep -o "Failed password" /var/log/secure|uniq -c

grep "Accepted " /var/log/secure | awk '{print $1,$2,$3,$9,$11}

用户

last

/etc/shadow 密码登陆相关信息

uptime 查看用户登陆时间

/etc/sudoers sudo用户列表

/etc/passwd

查看UID为0的帐号：

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

查看能够登录的帐号：

cat /etc/passwd | grep -E "/bin/bash$"

awk '/$1|$6/{print $1}' /etc/shadow

lastlog 系统中所有用户最近一次登录信息

lastb 用户错误的登录列表

more /etc/sudoers | grep -v "^#|^$" | grep "ALL=(ALL)"

who 查询utmp文件并报告当前登录的每个用户

w 查询utmp文件并显示当前系统中每个用户和它所运行的进程信息

users 打印当前登录的用户，每个用户名对应一个登录会话。如果一个用户不止一个登录会话，其用户名显示相同次数

进程

lsof

ps aux | grep pid | grep –v grep

lsof -i:1677 查看指定端口对应的程序

lsof -p 1234 检查pid号为1234进程调用情况

strace -f -p 1234 跟踪分析pid号为1234的进程

lsof -g gid 找恶意文件关联的lib文件

ps -aux或ps -ef

pstree -a

获取进程pid后可cd到/proc/对应pid/fd

隐藏进程查看

```
ps -ef | awk '{print}' | sort -n | uniq >1
ls /proc | sort -n |uniq >2
diff 1 2
```

netstat -anptl

top

端口

netstat -anpt

自启动

~/.bashrc

rc.local

/etc/init.d

chkconfig

chkconfig --list | grep "3:on|5:on"

/etc/init.d/rc.local

/etc/rc.local

/etc/init.d/ 开机启动项

/etc/cron* 定时任务

计划任务

crontab -l

crontab /etc/cron*

crontab -u root -l

cat /etc/crontab

ls /etc/cron.*

/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/*

/var/log/cron*

misc

stat

echo $PATH

./rpm -Va > rpm.log

kill -9

chattr –i

rm

setfacl

getfacl

lsattr

ssh

chmod

find / -perm -004000 -type f

chattr +i

去执行权限：

chmod 000

查看预加载库：

echo $LD_PRELOAD

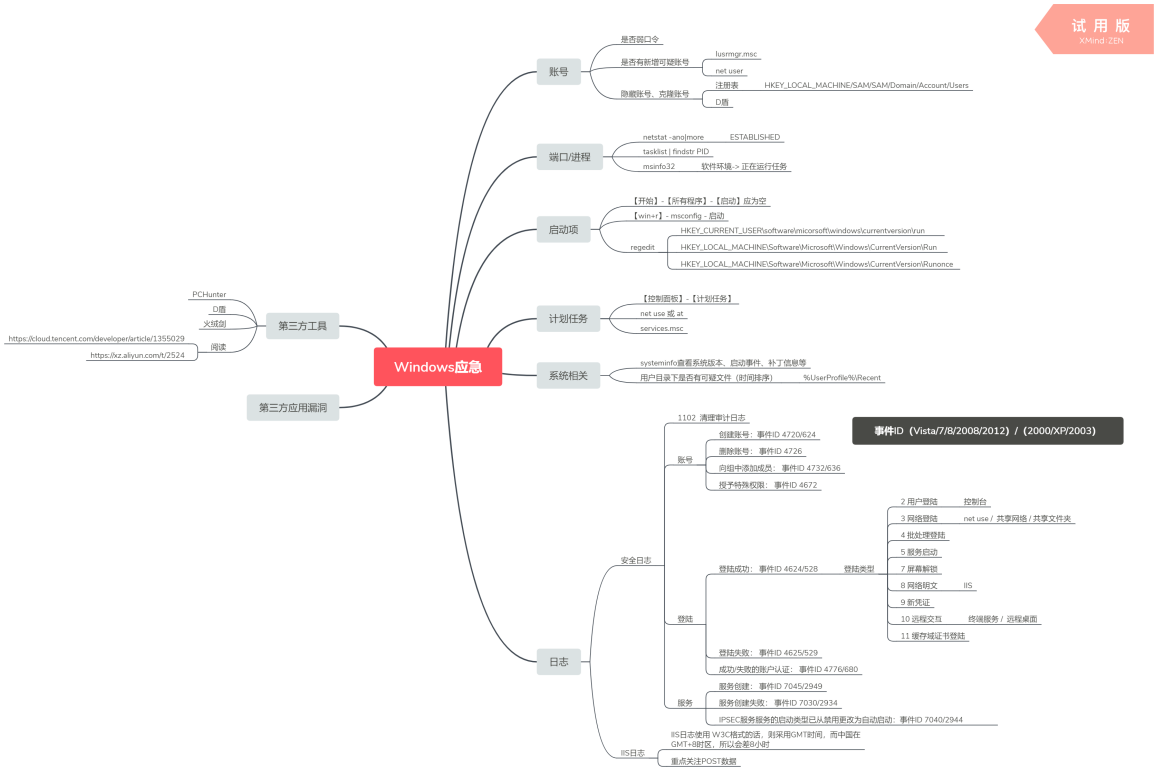
ssh后门快速判断：

strings /usr/bin/.sshd | egrep '[1-9]{1,3}.[1-9]{1,3}.'

> 检查SSH后门：
>
> 1）比对ssh的版本
>
> ssh -V

> 2）查看ssh配置文件和/usr/sbin/sshd的时间：
>
> stat /usr/sbin/sshd
>
> 3）strings检查/usr/sbin/sshd，是否有邮箱信息
>
> 4）通过strace监控sshd进程读写文件的操作
>
> 一般的sshd后门都会将账户密码记录到文件，可以通过strace进程跟踪到ssh登录密码文件。
>
> ps axu | grep sshd | grep -v grep
>
> root 65530 0.0 0.1 48428 1260 ? Ss 13:43 0:00 /usr/sbin/sshd
>
> strace -o aa -ff -p 65530
>
> grep open aa* | grep -v -e No -e null -e denied| grep WR
>
> aa.102586:open("/tmp/ilog", O_WRONLY|O_CREAT|O_APPEND, 0666) = 4

windows应急响应



//图片来源：https://www.cnblogs.com/0x4D75/p/9838098.html

文件

C:\Documents and Settings\Administrator\Recent

C:\Documents and Settings\Default User\Recent

%UserProfile%\Recent

文件日期、新增文件、可疑/异常文件、最近使用文件、浏览器下载文件

下载目录

回收站文件

程序临时文件

历史文件记录

应用程序打开历史

搜索历史

快捷方式（LNK）

c:\windows\temp\

Window 2003 C:\Documents and Settings

Window 2008R2 C:\Users\

Temp/tmp目录

开始-运行，输入%UserProfile%\Recent

时间排序文件

日志

开审核策略

系统日志，程序日志，安全日志

eventvwr.msc

1）服务器日志：

FTP连接日志和HTTPD事务日志：%systemroot% \system32\LogFiles\

IIS日志默认存放在System32\LogFiles目录下，使用W3C扩展格式

2）操作系统日志：

登录成功的所有事件：

LogParser.exe -i:EVT –o:DATAGRID “SELECT * FROM c:\Security.evtx where EventID=4624"

指定登录时间范围的事件：

LogParser.exe -i:EVT –o:DATAGRID “SELECT * FROM c:\Security.evtx where TimeGenerated>’2018-06-19 23:32:11' and TimeGenerated<’2018-06-20 23:34:00' and EventID=4624"

提取登录成功的用户名和IP：

LogParser.exe -i:EVT –o:DATAGRID “SELECT EXTRACT_TOKEN(Message,13,’ ‘) as EventType,TimeGenerated as LoginTime,EXTRACT_TOKEN(Strings,5,’|') as Username,EXTRACT_TOKEN(Message,38,’ ‘) as Loginip FROM c:\Security.evtx where EventID=4624"

登录失败的所有事件：

LogParser.exe -i:EVT –o:DATAGRID “SELECT * FROM c:\Security.evtx where EventID=4625"

提取登录失败用户名进行聚合统计：

LogParser.exe -i:EVT “SELECT EXTRACT_TOKEN(Message,13,’ ‘) as EventType,EXTRACT_TOKEN(Message,19,’ ‘) as user,count(EXTRACT_TOKEN(Message,19,’ ‘)) as Times,EXTRACT_TOKEN(Message,39,’ ‘) as Loginip FROM c:\Security.evtx where EventID=4625 GROUP BY Message”

系统历史开关机记录：

LogParser.exe -i:EVT –o:DATAGRID “SELECT TimeGenerated,EventID,Message FROM c:\System.evtx where EventID=6005 or EventID=6006"

帐号

新增用户

弱口令

管理员对应键值

lusrmgr.msc 查看账户变化

net user 列出当前登录账户

wmic UserAccount get 列出当前系统所有账户

C:>net localgroup administrators

隐藏/克隆帐号：

LD_check

注册表-管理员键值：

HKEY_LOCAL_MACHINE/SAM/SAM/Domains/Account/Users

D盾查杀

日志-登录时间/用户名

进程

tasklist /svc | findstr pid

netstat -ano

tasklist /svc

findstr

wmic process | find "Proccess Id" > proc.csv

Get-WmiObject -Class Win32_Process

Get-WmiObject -Query "select * from win32_service where name='WinRM'" -ComputerName Server01, Server02 | Format-List -Property PSComputerName, Name, ExitCode, Name, ProcessID, StartMode, State, Status

> 没有签名验证信息的进程
>
> 没有描述信息的进程

> 进程的属主
>
> 进程的路径是否合法
>
> CPU或内存资源占用长时间过高的进程

msinfo32

wmic process get caption,commandline /value

wmic process where caption=”svchost.exe” get caption,commandline /value

wmic service get name,pathname,processid,startname,status,state /value

wmic process get CreationDate,name,processid,commandline,ExecutablePath /value

wmic process get name,processid,executablepath| findstr "7766"

端口

netstat -ano

CLOSED：无连接活动或正在进行

LISTEN：监听中等待连接

SYN_RECV：服务端接收了SYN

SYN_SENT：请求连接等待确认

ESTABLISHED：连接建立数据传输

FIN_WAIT1：请求中止连接，等待对方FIN

FIN_WAIT2：同意中止，请稍候

ITMED_WAIT：等待所有分组死掉

CLOSING：两边同时尝试关闭

TIME_WAIT：另一边已初始化一个释放

LAST_ACK：等待原来的发向远程TCP的连接中断请求的确认

CLOSE-WAIT：等待关闭连接

自启动

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx

(ProfilePath)\Start Menu\Programs\Startup 启动项

msconfig 启动选项卡

gpedit.msc 组策略编辑器

开始>所有程序>启动

msconfig-启动

计划任务

C:\Windows\System32\Tasks\

C:\Windows\SysWOW64\Tasks\

C:\Windows\tasks\

schtasks

taskschd.msc

at

开始-设置-控制面板-任务计划

注册表

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList，
HKLM\SAM\Domains\Account\

hklm:\Software\Microsoft\Windows\CurrentVersion\policies\system

hklm:\Software\Microsoft\Active Setup\Installed Components

hklm:\Software\Microsoft\Windows\CurrentVersion\App Paths

hklm:\software\microsoft\windows nt\CurrentVersion\winlogon

hklm:\software\microsoft\security center\svc

hkcu:\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths

hkcu:\Software\Microsoft\Windows\CurrentVersion\explorer\RunMru

hklm:\Software\Microsoft\Windows\CurrentVersion\explorer\Startmenu

hklm:\System\CurrentControlSet\Control\Session Manager

hklm:\Software\Microsoft\Windows\CurrentVersion\explorer\ShellFolders

hklm:\Software\Microsoft\Windows\CurrentVersion\ShellExtensions\Approved

hklm:\System\CurrentControlSet\Control\Session Manager\AppCertDlls

hklm:\Software\Classes\exefile\shell\open\command

hklm:\BCD00000000

hklm:\system\currentcontrolset\control\lsa

hklm:\Software \Microsoft\Windows\CurrentVersion\Explorer\BrowserHelper Objects

hklm:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects

hkcu:\Software\Microsoft\Internet Explorer\Extensions

hklm:\Software\Microsoft\Internet Explorer\Extensions

hklm:\Software\Wow6432Node\Microsoft\Internet Explorer\Extensions

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
HKEY_CLASSES_ROOT\exefile\shell\open\command

服务

services.msc

misc

查看指定时间范围包括上传文件夹的访问请求：

findstr /s /m /I “UploadFiles” *.log

关键信息是x.js

findstr /s /m /I “x.js” *.asp

根据关键字搜索：

for /r d:\ %i in (*shell*.asp) do @echo %i

set

systeminfo

((?:(?:25[0-5]|2[0-4]\d|((1\d{2})|([1-9]?\d))).){3}(?:25[0-5]|2[0-4]\d|((1\d{2})|([1-9]?\d))))

安装安全软件：360/小A/瑞星/腾讯管家/金山/火绒

网络层应急响应

DDOS

> SYN 类攻击判断
>
> 1.服务器 CPU 占用率很高。
>
> 2.出现大量的 SYN_RECEIVED 的网络连接状态。
>
> 3.网络恢复后，服务器负载瞬时变高。网络断开后瞬时负载下将。

> UDP 类攻击判断
>
> 1.服务器 CPU 占用率很高。
>
> 2.网卡每秒接受大量的数据包。
>
> 3.网络 TCP 状态信息正常。

> CC 类攻击判断
>
> 1.服务器 CPU 占用率很高。
>
> 2.Web 服务器出现类似 Service Unavailable 提示。
>
> 3.出现大量的 ESTABLISHED 的网络连接状态且单个 IP 高达几十个甚至上百个连接。
>
> 4.用户无法正常访问网站页面或打开过程非常缓慢，软重启后短期内恢复正常，几分钟后又无法访问。

> 参考资料：https://www.hi-linux.com/posts/50873.html

常见攻击类型：

icmp flood：

> 此攻击属于大流量攻击，其原理就是不断发送不正常的 ICMP 包（所谓不正常就是 ICMP 包内容很大），导致目标带宽被占用。但其本身资源也会被消耗，并且目前很多服务器都是禁 ping 的（在防火墙里可以屏蔽 ICMP 包），因此这种方式已经落伍。

syn flood：

原理就是伪造大量不存在的IP地址，阻断TCP三次握手的第三次ACK包，即不对服务器发送的SYN+ACK数据包做出应答。由于服务器没有收到客户端发来的确认响应，就会一直保持连接直到超时，当有大量这种半开连接建立时，即造成SYN Flood攻击。

特征：syn+ack
netstat -n -p TCP | grep SYN_RECV

防御：

在Linux上可以修改以下配置提高TCP半开连接队列大小的上限：

/proc/sys/net/ipv4/tcp_max_syn_backlog

可以减少半开状态下等待ACK消息的时间或者重试发送SYN-ACK消息的次数：

/proc/sys/net/ipv4/tcp_synack_retries

SYN Cookies

SYN Cache

IPS规则

开启防火墙，限制单ip的syn包的频率

udp flood：

> 由于 UDP 是一种无连接的协议，因此攻击者可以伪造大量的源 IP 地址去发送 UDP 包，此种攻击属于大流量攻击。正常应用情况下，UDP 包双向流量会基本相等，因此在消耗对方资源的时候也在消耗自己的资源。

CLDAP协议 Reflection DDoS：

> 在CLDAP中只提供三种操作：searchRequest、searchResponse（searchResEntry和searchResDone）、abandonRequest，在不提供身份验证功能的情况下，客户端可以使用UDP数据报对LDAP服务器389端口发起操作请求。由于客户端发起searchRequest后服务端将返回searchResEntry和searchResDone两条应答消息，一般情况下执行该操作将具有较小数据包反射出较大数据包的效果，这一缺陷随即被利用进行反射放大DDoS攻击

ACK flood：

> ACK Flood 攻击是在 TCP 连接建立之后进行的。所有数据传输的 TCP 报文都是带有 ACK 标志位的，主机在接收到一个带有 ACK 标志位的数据包的时候，需要检查该数据包所表示的连接四元组是否存在。如果存在则检查该数据包所表示的状态是否合法，然后再向应用层传递该数据包。如果在检查中发现该数据包不合法（例如：该数据包所指向的目的端口在本机并未开放），则主机操作系统协议栈会回应 RST 包告诉对方此端口不存在。

> 当发包速率很大的时候，主机操作系统将耗费大量的精力接收报文、判断状态，同时要主动回应 RST 报文，正常的数据包就可能无法得到及时的处理。这时候客户端的表现就是访问页面反应很慢，丢包率较高。

Connection Flood：

> 典型的并且非常有效的利用小流量冲击大带宽网络服务的攻击方式。这种攻击的原理是利用真实的 IP 地址向服务器发起大量的连接，并且建立连接之后很长时间不释放。长期占用服务器的资源，造成服务器上残余连接 (WAIT 状态) 过多，效率降低，甚至资源耗尽，无法响应其它客户所发起的连接。

DNS 放大攻击：

原理：伪造DNS数据包，向DNS服务器发送域名查询报文了，而DNS服务器返回的应答报文则会发送给被攻击主机。放大体现在请求DNS回复的类型为ANY，攻击者向服务器请求的包长度为69个字节，而服务器向被攻击主机回复的ANY类型DNS包长度为535字节，大约放大了7倍（放大倍数视具体情况）。
构造受害者IP为源IP
大量DNS服务器实现DDoS

特征：大量dns请求

防御：IPS规则、关闭递归查询，DNS解析器应仅向源自受信任域的设备提供其服务，acl。

增大带宽、联系ISP上游阻断。

CC攻击：

> 原理就是借助代理服务器针对目标系统的消耗资源比较大的页面不断发起正常的请求，造成对方服务器资源耗尽，一直到宕机崩溃。因此在发送 CC 攻击前，我们需要寻找加载比较慢，消耗资源比较多的网页。比如：需要查询数据库的页面、读写硬盘的文件等。

慢速连接攻击：

> 针对HTTP协议，先建立起HTTP连接，设置一个较大的Conetnt-Length，每次只发送很少的字节，让服务器一直以为HTTP头部没有传输完成，这样连接一多就很快会出现连接耗尽。

Slowloris 攻击：

> Slowloris 是一种慢速连接攻击，Slowloris 是利用 Web Server 的漏洞或设计缺陷，直接造成拒绝服务。其原理是：以极低的速度往服务器发送 HTTP 请求，Apache 等中间件默认会设置最大并发链接数，而这种攻击就是会持续保持连接，导致服务器链接饱和不可用。Slowloris 有点类似于 SYN Flood 攻击，只不过 Slowloris 是基于 HTTP 协议。

NTP Flood

SSDP Flood

DOS通用防御：

砸钱，上抗d设备，流量清洗，高防，硬防，cdn，隐藏真实ip

> 网络层 DDoS 防御
>
> 1.限制单 IP 请求频率。
>
> 2.网络架构上做好优化，采用负载均衡分流。
>
> 3.防火墙等安全设备上设置禁止 ICMP 包等。
>
> 4.通过 DDoS 硬件防火墙的数据包规则过滤、数据流指纹检测过滤、及数据包内容定制过滤等技术对异常流量进行清洗过滤。
>
> 5.采用 ISP 近源清洗，使用电信运营商提供的近源清洗和流量压制，避免全站服务对所有用户彻底无法访问。这是对超过自身带宽储备和自身 DDoS 防御能力之外超大流量的补充性缓解措施。

> 应用层 DDoS 防御
>
> 1.优化操作系统的 TCP/IP 栈。
>
> 2.应用服务器严格限制单个 IP 允许的连接数和 CPU 使用时间。
>
> 3.编写代码时，尽量实现优化并合理使用缓存技术。尽量让网站静态化，减少不必要的动态查询。网站静态化不仅能大大提高抗攻击能力，而且还给骇客入侵带来不少麻烦，至少到现在为止关于 HTML 的溢出还没出现。
>
> 4.增加 WAF（Web Application Firewall）设备，WAF 的中文名称叫做 Web 应用防火墙。Web 应用防火墙是通过执行一系列针对 HTTP / HTTPS 的安全策略来专门为 Web 应用提供保护的一款产品。
>
> 5.使用 CDN / 云清洗，在攻击发生时，进行云清洗。通常云清洗厂商策略有以下几步：预先设置好网站的 CNAME，将域名指向云清洗厂商的 DNS 服务器；在一般情况下，云清洗厂商的 DNS 仍将穿透 CDN 的回源的请求指向源站，在检测到攻击发生时，域名指向自己的清洗集群，然后再将清洗后的流量回源。
>
> 6.CDN 仅对 Web 类服务有效，针对游戏类 TCP 直连的服务无效。这时可以使用 DNS 引流 + ADS (Anti-DDoS System) 设备来清洗，还有在客户端和服务端通信协议做处理（如：封包加标签，依赖信息对称等）。

> 参考资料：https://www.hi-linux.com/posts/50873.html

ARP欺骗

> ARP攻击，是针对以太网地址解析协议（ARP）的一种攻击技术，通过欺骗局域网内访问者PC的网关MAC地址，使访问者PC错以为攻击者更改后的MAC地址是网关的MAC，导致网络不通。
>
> ---百度百科

在网络中产生大量的ARP通信

arp -a

防御：

防火墙，mac地址绑定

DNS劫持

控制域名解析权限，比如访问google.com解析到了baidu.com的IP，比如通过iframe打开google.com

防御：

换DNS服务器，采用https，向工信部/运营商投诉

HTTP劫持（内容劫持）

在和网站交互过程中的劫持了请求，比如在右下角出现广告弹窗（插入js或dom）

防御：

采用https，向工信部/运营商投诉

参考资料

https://www.hi-linux.com/posts/50873.html

https://www.cnblogs.com/zdz8207/p/10729294.html

交换机/路由器应急响应

交换机负载过高（cpu100%）

常见原因：

线路老化，端口接错（千兆/百兆/环路），内网病毒蠕虫，业务变动导致流量剧增，PBR，广播风暴

现象：

丢包，延时较大

交换机排查常用命令

show process cpu

show platform health

sh int | i protocol | rate | broadcasts 哪个端口收发包较多

show ip traffic

Monitor session 1 soure interface cpu

Monitor session 1 des interface 具体接口

sh platform cpu packet statistics

路由器常用命令

enable 进入特权模式

config terminal 进入全局配置模式

router（config）#line console 0 进入控制台口

router（config-line）#line vty 0 4 进入虚拟终端（Ctrl+z）返回特权模式

int s0/0 进入Serail接口

no shutdown 激活当前接口

ip address 设置IP地址

int f0/0.1 进入子接口

copy running-config startup-config 保存配置

show version 显示路由器的版本信息

show running-config 显示整个路由器的配置

show run interface serial 0 显示端口s0的配置

show int serial 0 显示端口s0的状态

show contr serial 0 显示端口s0是DTE还是DCE

show cdp neighbor 显示连接了哪些邻居

show cdp entry * 显示连接的路由的具体信息

show cdp interface s0 显示s0口连接的邻居

show ip route

show run 查看当前配置

misc

> HiPri代表是处理高优先级的进程，LoPri代
> 表处理低优先级的进程，LoPri 值比较大原因是因为进程超过了HiPri给定的Target，然后交给了LoPri来处理

> Cat4k Mgmt HiPri和Cat4k Mgmt LoPri两个进程的原理。当某个进程占用CPU时间超过规定的CPU分配时间时，Cat4k Mgmt HiPri进程便会接管这个进程; 而当Cat4k平台上某项进程占用CPU超出了应分配的CPU时间时，Cat4k Mgmt LoPri进程会接管这项进程，使其他进程能够得到CPU时间。

相关资料

https://www.cisco.com/c/zh_cn/support/docs/switches/catalyst-3750-series-switches/68461-high-cpu-utilization-cat3750.html

https://blog.51cto.com/2825930/2286871

https://blog.51cto.com/2825930/2286867

www.voidcn.com/article/p-ynqudrjf-wr.html

blog.sina.com.cn/s/blog_4ca83f8301015357.html