Windows排查

万里

*

花名：万里

曾就职于奇安信集团，担任高级渗透测试工程师，从事网络安全工作7年，参与四届全国HW行动、北京冬奥重保等活动，担任CISP-PTE、CISP-IRE出题及监考，为CNCERT、SRC平台等提交数百漏洞。专注研究前沿网络安全技术，具有丰富的实战经验。擅长技术：Web渗透、内网渗透、代码审计、Kali、安全工具开发等。

中华人民共和国网络安全法

第二十七条

任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

课程内容仅用于以防御为目的的教学演示
请勿用于其他用途，否则后果自负

1、《中华人民共和国刑法》的相关规定：

第二百八十五条规定，非法侵入计算机信息系统罪;非法获取计算机信息系统数据、非法控制计算机信息系统罪;提供侵入、非法控制计算机信息系统程序、工具罪是指，违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金;情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

*

第一条

非法获取计算机信息系统数据或者非法控制计算机信息系统，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节严重”：

（一）获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上的；

（二）获取第（一）项以外的身份认证信息五百组以上的；

（三）非法控制计算机信息系统二十台以上的；

（四）违法所得五千元以上或者造成经济损失一万元以上的；

（五）其他情节严重的情形。

实施前款规定行为，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节特别严重”：

（一）数量或者数额达到前款第（一）项至第（四）项规定标准五倍以上的；

（二）其他情节特别严重的情形。

明知是他人非法控制的计算机信息系统，而对该计算机信息系统的控制权加以利用的，依照前两款的规定定罪处罚。

*

- 账号安全
- 历史命令
- 检查异常端口
- 检查异常进程
- 检查开机启动项
- 检查定时任务
- 检查服务
- 检查异常文件
- 检查系统日志

账号安全

1、用户信息文件/etc/passwd

root:x:0:0:root:/root:/bin/bash

account:password:UID:GID:GECOS:directory:shell

用户名：密码：用户ID：组ID：用户说明：家目录：登陆之后shell

注意：无密码只允许本机登陆，远程不允许登陆

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
```

账号安全

2、影子文件/etc/shadow

root:6oGs1PqhL2p3ZetrE$X7o7bzoouHQVSEmSgsYN5UD4.kMHx6qgbTqwNVC5oOAouXvcjQSt.Ft7ql1WpkopY0UV9ajBwUt1DpYxTCVvI/:16809:0:99999:7:::

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：密码修改到期到的警告天数：密码过期之后的宽限天数：账号失效时间：保留

```
avahi:*:18421:0:99999:7:::
nm-openvpn:*:18421:0:99999:7:::
nm-openconnect:*:18421:0:99999:7:::
pulse:*:18421:0:99999:7:::
saned:*:18421:0:99999:7:::
inetsim:*:18421:0:99999:7:::
colord:*:18421:0:99999:7:::
geoclue:*:18421:0:99999:7:::
lightdm:*:18421:0:99999:7:::
king-phisher:*:18421:0:99999:7:::
hack:$6$o683es5W8Ax0lcYC$JtfsPFQi8E5cquvJ8KkVZptEcmVj6X7VBKJqNk7cm10DVZ4V0BUdAZK.9/hP065sURTx5fWZ.BB9wh9MnAI7S/:18421:0:99999:7:::
systemd-coredump:!!:18421:::::
```

账号安全

1、查询特权用户特权用户(uid 为0)

[root@localhost ~]# awk -F: '$3==0{print $1}' /etc/passwd

2、查询可以远程登录的帐号信息

[root@localhost ~]# awk '/\$1|\$6/{print $1}' /etc/shadow

3、除root帐号外，其他帐号是否存在sudo权限。如非管理需要，普通帐号应删除sudo权限

[root@localhost ~]# more /etc/sudoers | grep -v "^#\|^$" | grep "ALL=(ALL)"

4、禁用或删除多余及可疑的帐号

usermod -L user　禁用帐号，帐号无法登录，/etc/shadow第二栏为!开头

userdel user　　删除user用户

userdel -r user　将删除user用户，并且将/home目录下的user目录一并删除

5、who　查看当前登录用户（tty本地登陆　pts远程登录）

w　　查看系统信息，想知道某一时刻用户的行为

uptime　查看登陆多久、多少用户，负载

历史命令

通过.bash_history查看帐号执行过的系统命令

1、root的历史命令

histroy

2、打开/home各帐号目录下的.bash_history，查看普通帐号的历史命令

```
hack@kali:/home$ history
    1  ls
    2  airdecap-ng ctf.pcap -e ctf -p passworld1
    3  airdecap-ng ctf.pcap -e ctf -p password1
    4  aircrack-ng ctf.pcap
    5  aircrack-ng ctf.pcap -e ctf
    6  aircrack-ng ctf.pcap -e ctf -w
    7  aircrack-ng ctf.pcap -e ctf -p /usr/share/wordlists/fasttrack.txt
    8  aircrack-ng ctf.pcap -e ctf -p /usr/share/wordlists/fasttrack.txt
    9  aircrack-ng ctf.pcap -e ctf -p password1
   10  aircrack-ng ctf.pcap -e ctf -p password
   11  aircrack-ng ctf.pcap -e ctf
   12  aircrack-ng ctf.pcap
```

检查异常端口

netstat -antlp|more

查看下pid所对应的进程文件路径，
运行ls -l /proc/$PID/exe或file /proc/$PID/exe（$PID 为对应的pid 号）

```
hack@kali:/home$ netstat -antlp|more
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
```

检查异常进程

使用ps命令，分析进程

ps aux | grep pid

```
hack         950  0.0  3.1 280936 64308 ?        Sl   07:47   0:08 xfwm4
hack         953  0.0  0.3 237116  7660 ?        Ssl  07:47   0:00 /usr/libexec/gvfsd
hack         958  0.0  0.3 379852  8080 ?        Sl   07:47   0:00 /usr/libexec/gvfsd-fuse /run/user/1000/gvfs -f
hack         967  0.0  1.0 236212 21052 ?        Ssl  07:47   0:00 xfsettingsd
hack         968  0.0  2.9 344860 59896 ?        Sl   07:47   0:05 xfce4-panel
root         971  0.0  0.4 249488  9760 ?        Ssl  07:47   0:00 /usr/libexec/upowerd
hack         991  0.0  2.3 330112 48104 ?        Sl   07:47   0:03 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libwhiskermenu.so 1
hack         994  0.0  2.8 427796 58740 ?        Sl   07:47   0:11 Thunar --daemon
hack         999  0.0  6.9 552668 142372 ?       Sl   07:47   0:05 xfdesktop
hack        1002  0.0  1.1 201284 22744 ?        Sl   07:47   0:00 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libsystray.so 15 146
hack        1003  0.0  1.1 349016 22592 ?        Sl   07:47   0:00 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libstatusnotifier.so
hack        1004  0.0  2.0 519040 41340 ?        Sl   07:47   0:15 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libpulseaudio-plugin
hack        1005  0.0  1.9 251108 38796 ?        Sl   07:47   0:00 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libnotification-plug
hack        1006  0.0  1.9 252732 40048 ?        Sl   07:47   0:00 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libxfce4powermanager
hack        1009  0.0  1.7 251012 36660 ?        Sl   07:47   0:00 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libactions.so 21 146
hack        1024  0.0  1.9 326220 38972 ?        Ssl  07:47   0:00 /usr/lib/x86_64-linux-gnu/xfce4/notifyd/xfce4-notifyd
hack        1027  0.0  1.3 279760 27604 ?        Sl   07:47   0:00 light-locker
hack        1031  0.0  2.2 479644 45516 ?        Sl   07:47   0:00 nm-applet
```

检查开机启动项

系统运行级别示意图：

运行级别	含义
0	关机
1	单用户模式，可以想象为windows的安全模式，主要用于系统修复
2	不完全的命令行模式，不含NFS服务
3	完全的命令行模式，就是标准字符界面
4	系统保留
5	图形模式
6	重启动

查看运行级别命令 runlevel

```
hack@hack:~$ runlevel
N 5
```

检查定时任务

1、利用crontab创建计划任务

基本命令

crontab -l 列出某个用户cron服务的详细内容

Tips：默认编写的crontab文件会保存在 (/var/spool/cron/用户名 例如:/var/spool/cron/root

crontab -r 删除每个用户cront任务(谨慎：删除所有的计划任务)

crontab -e 使用编辑器编辑当前的crontab文件

如：*/1 * * * * echo "hello world" >> /tmp/test.txt 每分钟写入文件

检查定时任务

2、利用anacron实现异步定时任务调度

使用案例

每天运行 /home/backup.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之后运行它，而不用再等待 7天

检查定时任务

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

检查服务

第一种修改方法：

chkconfig [--level 运行级别] [独立服务名] [on|off]
chkconfig –level 2345 httpd on 开启自启动
chkconfig httpd on （默认level是2345）

第二种修改方法：

修改/etc/re.d/rc.local 文件
加入 /etc/init.d/httpd start

第三种修改方法：

使用ntsysv命令管理自启动，可以管理独立服务和xinetd服务。

检查服务

1、查询已安装的服务：

RPM包安装的服务

chkconfig --list 查看服务自启动状态，可以看到所有的RPM包安装的服务
ps aux | grep crond 查看当前服务

系统在3与5级别下的启动项
中文环境
chkconfig --list | grep "3:启用\|5:启用"
英文环境
chkconfig --list | grep "3:on\|5:on"

源码包安装的服务

查看服务安装位置，一般是在/user/local/
service httpd start
搜索/etc/rc.d/init.d/ 查看是否存在

检查异常文件

1、查看敏感目录，如/tmp目录下的文件，同时注意隐藏文件夹，以“..”为名的文件夹具有隐藏属性

2、得到发现WEBSHELL、远控木马的创建时间，如何找出同一时间范围内创建的文件?

可以使用find命令来查找，如 find /opt -iname "*" -atime 1 -type f 找出 /opt 下一天前访问过的文件

3、针对可疑文件可以使用stat进行创建修改时间。

检查系统日志

日志默认存放位置：/var/log/
查看日志配置情况：more /etc/rsyslog.conf)

日志文件	说明
/var/log/cron	记录了系统定时任务相关的日志
/var/log/cups	记录打印信息的日志
/var/log/dmesg	记录了系统在开机时内核自检的信息，也可以使用dmesg命令直接查看内核自检信息
/var/log/mailog	记录邮件信息
/var/log/message	记录系统重要信息的日志。这个日志文件中会记录Linux系统的绝大多数重要信息，如果系统出现问题时，首先要检查的就应该是这个日志文件
/var/log/btmp	记录错误登录日志，这个文件是二进制文件，不能直接vi查看，而要使用lastb命令查看
/var/log/lastlog	记录系统中所有用户最后一次登录时间的日志，这个文件是二进制文件，不能直接vi，而要使用lastlog命令查看
/var/log/wtmp	永久记录所有用户的登录、注销信息，同时记录系统的启动、重启、关机事件。同样这个文件也是一个二进制文件，不能直接vi，而需要使用last命令来查看
	记录当前已经登录的用户信息，这个文件会随着用户的登录和注销不断变

检查系统日志

1、定位有多少IP在爆破主机的root帐号：
grep "Failed password for root" /var/log/secure | awk '{print $11}' | sort | uniq -c | sort -nr | more

定位有哪些IP在爆破：
grep "Failed password" /var/log/secure|grep -E -o "(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)"|uniq -c

爆破用户名字典是什么?
grep "Failed password" /var/log/secure|perl -e 'while($_=<>){ /for(.*?) from/; print "$1\n";}'|uniq -c|sort -nr

2、登录成功的IP有哪些：
grep "Accepted " /var/log/secure | awk '{print $11}' | sort | uniq -c | sort -nr | more

登录成功的日期、用户名、IP：
grep "Accepted " /var/log/secure | awk '{print $1,$2,$3,$9,$11}'

检查系统日志

3、增加一个用户kali日志：
Jul 10 00:12:15 localhost useradd[2382]: new group: name=kali, GID=1001
Jul 10 00:12:15 localhost useradd[2382]: new user: name=kali, UID=1001, GID=1001, home=/home/kali
, shell=/bin/bash
Jul 10 00:12:58 localhost passwd: pam_unix(passwd:chauthtok): password changed for kali
#grep "useradd" /var/log/secure

4、删除用户kali日志：
Jul 10 00:14:17 localhost userdel[2393]: delete user 'kali'
Jul 10 00:14:17 localhost userdel[2393]: removed group 'kali' owned by 'kali'
Jul 10 00:14:17 localhost userdel[2393]: removed shadow group 'kali' owned by 'kali'
grep "userdel" /var/log/secure

5、su切换用户：
Jul 10 00:38:13 localhost su: pam_unix(su-l:session): session opened for user good by root(uid=0)

sudo授权执行:
sudo -l
Jul 10 00:43:09 localhost sudo: good : TTY=pts/4 ; PWD=/home/good ; USER=root ;
COMMAND=/sbin/shutdown -r now

Linux事件日志简介

日志默认存放位置：/var/log/

查看日志配置情况：more /etc/rsyslog.conf

日志文件	说明
/var/log/cron	记录了系统定时任务相关的日志
/var/log/cups	记录打印信息的日志
/var/log/dmesg	记录了系统在开机时内核自检的信息，也可以使用dmesg命令直接查看内核自检信息
/var/log/mailog	记录邮件信息
/var/log/message	记录系统重要信息的日志。这个日志文件中会记录Linux系统的绝大多数重要信息，如果系统出现问题时，首先要检查的就应该是这个日志文件
/var/log/btmp	记录错误登录日志，这个文件是二进制文件，不能直接vi查看，而要使用lastb命令查看
/var/log/lastlog	记录系统中所有用户最后一次登录时间的日志，这个文件是二进制文件，不能直接vi，而要使用lastlog命令查看
/var/log/wtmp	永久记录所有用户的登录、注销信息，同时记录系统的启动、重启、关机事件。同样这个文件也是一个二进制文件，不能直接vi，而需要使用last命令来查看
/var/log/utmp	记录当前已经登录的用户信息，这个文件会随着用户的登录和注销不断变化，只记录当前登录用户的信息。同样这个文件不能直接vi，而要使用w,who,users等命令来查询
/var/log/secure	记录验证和授权方面的信息，只要涉及账号和密码的程序都会记录，比如SSH登录，su切换用户，sudo授权，甚至添加用户和修改用户密码都会记录在这个日志文件中

Linux事件日志简介

- 比较重要的几个日志：
- 登录失败记录：/var/log/btmp /---lastb
- 最后一次登录：/var/log/lastlog /----lastlog
- 登录成功记录: /var/log/wtmp /---last
- 登录日志记录：/var/log/secure
- 目前登录用户信息：/var/run/utmp /---w、who、users
- 历史命令记录：history 仅清理当前用户： history -c

日志分析技巧

Linux下常用的shell命令如：find、grep 、egrep、awk、sed

1、grep显示前后几行信息:

标准unix/linux下的grep通过下面参数控制上下文：

grep -C 5 foo file 显示file文件里匹配foo字串那行以及上下5行

grep -B 5 foo file 显示foo及前5行

grep -A 5 foo file 显示foo及后5行

查看grep版本号的方法是

grep -V

日志分析技巧

Linux下常用的shell命令如：find、grep 、egrep、awk、sed

1、grep显示前后几行信息:

标准unix/linux下的grep通过下面参数控制上下文：

grep -C 5 foo file 显示file文件里匹配foo字串那行以及上下5行

grep -B 5 foo file 显示foo及前5行

grep -A 5 foo file 显示foo及后5行

查看grep版本号的方法是

grep -V

日志分析技巧

3、如何显示一个文件的某几行：

```
cat input_file | tail -n +1000 | head -n 2000
#从第1000行开始，显示2000行。即显示1000~2999行
```

4、find /etc -name init

//在目录/etc中查找文件init

日志分析技巧

5、只是显示/etc/passwd的账户

`cat /etc/passwd |awk  -F ':'  '{print $1}'`
//awk -F指定域分隔符为':'，将记录按指定的域分隔符划分域，填充域，$0则表示所有域,$1表示第一个域,$n表示第n个域。

6、sed -i '153,$d' .bash_history

删除历史操作记录，只保留前153行

日志分析技巧

A、/var/log/secure

1、定位有多少IP在爆破主机的root帐号：
grep "Failed password for root" /var/log/secure | awk '{print $11}' | sort | uniq -c | sort -nr | more

定位有哪些IP在爆破：
grep "Failed password" /var/log/secure|grep -E -o "(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)"|uniq -c

爆破用户名字典是什么?
grep "Failed password" /var/log/secure|perl -e 'while($_=<>){ /for(.*?) from/; print "$1\n";}'|uniq -c|sort -nr

2、登录成功的IP有哪些：
grep "Accepted " /var/log/secure | awk '{print $11}' | sort | uniq -c | sort -nr | more

登录成功的日期、用户名、IP：
grep "Accepted " /var/log/secure | awk '{print $1,$2,$3,$9,$11}'

日志分析技巧

3、增加一个用户kali日志：
Jul 10 00:12:15 localhost useradd[2382]: new group: name=kali, GID=1001
Jul 10 00:12:15 localhost useradd[2382]: new user: name=kali, UID=1001, GID=1001, home=/home/kali
, shell=/bin/bash
Jul 10 00:12:58 localhost passwd: pam_unix(passwd:chauthtok): password changed for kali
#grep "useradd" /var/log/secure

4、删除用户kali日志：
Jul 10 00:14:17 localhost userdel[2393]: delete user 'kali'
Jul 10 00:14:17 localhost userdel[2393]: removed group 'kali' owned by 'kali'
Jul 10 00:14:17 localhost userdel[2393]: removed shadow group 'kali' owned by 'kali'
grep "userdel" /var/log/secure

5、su切换用户：
Jul 10 00:38:13 localhost su: pam_unix(su-l:session): session opened for user good by root(uid=0)

sudo授权执行:
sudo -l
Jul 10 00:43:09 localhost sudo: good : TTY=pts/4 ; PWD=/home/good ; USER=root ;
COMMAND=/sbin/shutdown -r now