**第二十二章 nc扫描端口-curl手动查杀木马过程之生成木马程序病原体并自动运行**

**本节所讲内容：**

**22.1 使用nc扫描端口**

**22.2 curl 查看web服务器类型**

**22.3 手动查杀木马过程之生成木马程序病原体**

**22.4 手动查杀木马过程之让木马程序自动运行**

**22.1 使用nc扫描端口**

**nc 被称为linux下的瑞士军刀 短小精悍**

**22.1.1 安装：**

**Rhel 6**

**[root@xuegod64 init.d]# rpm -qf `which nc`**

**nc-1.84-24.el6.x86\_64**

**如果同安装的话 可使用yum -y install nc 进行安装**

**Rhel 7**

**[root@xuegod63 ~]# rpm -qf `which nc`**

**nmap-ncat-6.40-7.el7.x86\_64**

**2.1.2 语法及示例**

**语法：# nc  -v  -w 10   -z  IP地址 端口号**

**-v  显示指令执行过程。  
 -w  <超时秒数>   设置等待连线的时间。  
 -u  表示使用UDP协议  
 -z  使用0输入/输出模式，只在扫描通信端口时使用。**

**注意：在rhel 7版本中nc 命令的 -z选项取消掉了，既与rhel 6 的使用方法相同，使用时略掉 -z 即可，在rhel 7 版本中 nc 6.40版本，nc执行时 不会主动退出，需要ctrl+d 或 ctrl+c 或直接回车**

**例1：扫描指定的22端口**

**Rhel 6**

**[root@xuegod64 ~]# nc -v -w 10 -z 192.168.1.63 22**

**Connection to 192.168.1.64 22 port [tcp/ssh] succeeded!**

**Rhel 7**

**[root@xuegod63 ~]# nc -v -w 10 192.168.1.64 22**

**Ncat: Version 6.40 ( http://nmap.org/ncat )**

**Ncat: Connected to 192.168.1.64:22.**

**SSH-2.0-OpenSSH\_7.4**

**Ncat: 0 bytes sent, 21 bytes received in 3.13 seconds.**

**例2：扫描1到65535的端口范围，只输出打开的端口**

**[root@xuegod63 ~]#nc -v -w 1 -z 192.168.1.63 1-65535  
 ....**

**nc: connect to 192.168.1.64 port 6635 (tcp) failed: Connection refused**

**nc: connect to 192.168.1.64 port 6636 (tcp) failed: Connection refused**

**nc: connect to 192.168.1.64 port 6637 (tcp) failed: Connection refused**

**注： 加-v 会把每个端口扫描结果都显示出来。显示消息比较长。**

**[root@xuegod63 ~]# nc -w 1 -z 192.168.1.63 1-65535**

**#去掉-v参数即可，这样只显示可用的端口  
 Connection to 192.168.0.100 80 port [tcp/http] succeeded!  
 Connection to 192.168.0.100 2121 port [tcp/scientia-ssdb] succeeded!  
 Connection to 192.168.0.100 4004 port [tcp/pxc-roid] succeeded!  
 Connection to 192.168.0.100 8081 port [tcp/tproxy] succeeded!  
 Connection to 192.168.0.100 11211 port [tcp/\*] succeeded!**

**22.2 使用curl 查看web服务器类型**

**22.2.1 查看web服务器类型：**

**[root@xuegod63 ~]# curl -I www.taobao.com**

**HTTP/1.1 200 OK**

**Server: Tengine # 根据nginx开发的**

**Date: Tue, 30 Dec 2014 13:35:47 GMT**

**Content-Type: text/html; charset=gbk**

**Connection: keep-alive**

**Vary: Accept-Encoding**

**Set-Cookie: CAT=deleted; expires=Mon, 30-Dec-2013 13:35:46 GMT**

**Expires: Tue, 30 Dec 2014 14:35:47 GMT**

**Cache-Control: max-age=3600**

**22.3 手动查杀木马过程之生成木马程序病原体**

**22.3.1 生成木马程序病原体**

**[root@xuegod63 ~]# vim /usr/bin/fregonnzkq**

**#!/bin/bash**

**touch /tmp/aaa.txt**

**while true**

**do**

**#echo hello world**

**#如何知道我的木马有没有实时运行？ 怎么做？**

**echo `date` >> /tmp/date.txt**

**sleep 1**

**done**

**[root@xuegod63 ~]# chmod +x /usr/bin/fregonnzkq**

**测试：**

**[root@xuegod63 ~]#fregonnzkq & #可以执行**

**[root@xuegod63 ~]# ps -axu | grep freg**

**Warning: bad syntax, perhaps a bogus '-'? See /usr/share/doc/procps-3.2.8/FAQ**

**root 4900 0.1 0.1 106152 1252 pts/1 S 16:29 0:00 /bin/bash /usr/bin/fregonnzkq**

**[root@xuegod63 bin]# kill -9 4900**

**22.4 手动查杀木马过程之让木马程序自动运行**

**22.5.1 让木马自动运行**

**如何让木马自动运行？ 有几种方法？**

**实战：黑客如何让脚本定时执行**

**1、计划任务： crontab**

**2、开机启动**

**3、系统命令被人替换，定一个触发事件**

**接下来，老师是黑客，你是网警。**

**22.5.2 计划任务： crontab**

**[root@xuegod63 ~]# crontab -e #写入**

**1 2 \* \* \* /usr/bin/fregonnzkq &**

**#分 时 天 月 周**

**#每天2点1分，执行命令/usr/bin/fregonnzkq &**

**\* 表每X， 比如： 每天，每月，每周**

**排查：**

**[root@xuegod63 ~]# crontab -l #查看root用户的计划任务**

**黑客：以非root用户添加计划任务。 最好使用已经存在系统用户添加。这里使用bin用户来添加**

**例：**

**[root@xuegod63 ~]# crontab -u bin -e**

**1 \* \* \* \* echo "aaaaaaa" >> /tmp/bin.txt**

**排查：**

**[root@xuegod63 ~]# crontab -u bin -l**

**1 \* \* \* \* echo "aaaaaaa" >> /tmp/bin.txt**

**排查：所有用户的计划任务？**

**做黑客要有一个很扎实的基础，还要有很好的思维**

**[root@xuegod63 ~]# ll /var/spool/cron/**

**total 8**

**-rw------- 1 root root 42 Nov 12 10:11 bin**

**-rw------- 1 root root 19 Nov 12 10:06 root**

**注：所有用户的计划任务，都会在/var/spool/cron/下产生对应用户名的文件。**

**22.4.2 黑客：高级crontab ，篡改一个系统级别的计划任务**

**[root@xuegod63 bin]# ls /etc/cron #按两下tab键**

**cron.d/ cron.deny cron.monthly/ cron.weekly/**

**cron.daily/ cron.hourly/ crontab**

**注：**

**crontab #写具体时间的统级别的定时任务**

**cron.d/ #系统级别的定时任务**

**cron.daily/ #系统每天要执行计划任务**

**cron.hourly/ #系统每小时要执行计划任务**

**cron.monthly/ #系统每月要执行计划任务**

**cron.weekly/ #系统每周要执行计划任务**

**[root@xuegod63 ~]# find /etc/cron\* #查看可以添加系统级别的计划任务**

**例1：系统级别的计划任务**

**[root@xuegod63~]# vim /etc/crontab #在最后追加**

**01 3 \* \* \* root /bin/workstat &**

**例2：添加系统级别的木马程序。 可以追加到原系统的脚本中，也可以自己新创建一个脚本，放到对应的目录下**

**[root@xuegod63 ~]# vim /etc/cron.daily/tmpwatch #在最后添加**

**/usr/bin/fregonnzkq &**

**[root@xuegod63 ~]# chmod +x /etc/cron.daily/tmpwatch**

**测试执行：**

**[root@xuegod63 ~]# /etc/cron.daily/tmpwatch**

**[root@xuegod63 ~]# ps -aux |grep freg**

**root 2445 0.6 0.1 113132 1428 pts/0 S 21:24 0:00 /bin/bash /usr/bin/fregonnzkq**

**root 2466 0.0 0.0 112676 980 pts/0 S+ 21:25 0:00 grep --color=auto freg**

**注：说明添加的木马成功了。**

**排查：**

**方法1：利用md5sum ，来检验文件的完整性**

**例：**

**语法：md5sum 文件**

**[root@xuegod63 ~]# md5sum /etc/cron.daily/tmpwatch**

**17856453d7325d7750309910aa64e5ca /etc/cron.daily/tmpwatch**

**[root@xuegod63 ~]#vim /etc/cron.daily/tmpwatch #在最后，添加一些内容**

**[root@xuegod63 ~]# md5sum /etc/cron.daily/tmpwatch #再次查看md5值不一样**

**6152bd26fc26d623eaf9dd551b9faed8 /etc/cron.daily/tmpwatch**

**注：系统级别的计划任务，从安装好系统后， 就固定下来，不变了。**

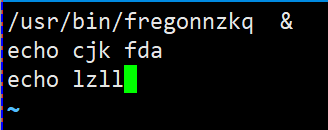
**如何排查/etc/cron\*下所有文件有没有被黑客修改或追加？ 不知道：1 会：6**

**例2： 对/etc/cron\*下所有文件都生成md5值，并存一个md5值**

**[root@xuegod63 ~]# find /etc/cron\* -type f -exec md5sum {} \; > /usr/share/file\_md5.v1**

**测试：**

**[root@xuegod63 ~]# vim /etc/cron.daily/tmpwatch #在最后添加以下内容：**



**做对比：**

**[root@xuegod63 ~]# find /etc/cron\* -type f -exec md5sum {} \; >/usr/share/file\_md5.v2**

**[root@xuegod63 ~]# diff /tmp/file\_md5.v1 /tmp/file\_md5.v2 #对比**

**< 6152bd26fc26d623eaf9dd551b9faed8 /etc/cron.daily/tmpwatch**

**---**

**> a34bbcd2c63889ad2a1ab48d751dc974 /etc/cron.daily/tmpwatch**

**22.5.3 扩展**



**为什么 “快速查杀”比较快？？？ 它是怎么查杀的？？**

**hosts c:\system 等**

**先生成dm5值库，然后对比，找出不一样的文件，再认真查一下**

**注：如果忘提前生成/usr/share/file\_md5.v1？**

**找一台正常和你服务器系统版本号一样的虚拟机，在虚拟机中生成md5值数据库文件。复制到咱们服务器上，再对比。**

**思路：很重要**

**总结：过通过计划任务运行木马程序**

**1、普通计划任务： crontab**

**2、高级crontab ，篡改一个系统级别的计划任务**

**22.5.4 通过开机启动来运行进程**

**黑客：/etc/rc.local 这个是开机启动脚本**

**[root@xuegod63 ~]# vim /etc/rc.local #在文档中插入以下红色内容**

**echo aaaa**

**[root@xuegod63 ~]# /etc/rc.local #测试执行**

**aaaaa**

**注：在rhel7当中 /etc/rc.d/rc.local 文件被去掉了执行权限，所以需要加上执行权限**

**[root@xuegod63 ~]# chmod +x /etc/rc.d/rc.local**

**注：/etc/rc.local 是个链接文件**

**特例： 黑客在/etc/rc.local 中添加很多空行，然后在文档最后添加木马程序， 再把光标移动到行首，保存退出。**

**排查：过滤掉空行**

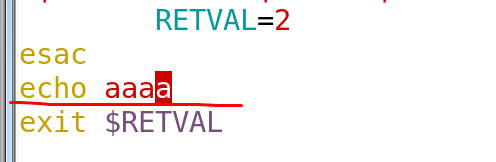
**[root@xuegod63 ~]# grep -v ^$ /etc/rc.local # ^$ #以$结束符开头的行，就是空行。 -v #表示取反，显示**

**方法1： 木马程序脚本写到已经存在的开机启动服务中，例如: httpd (apache web服务器启动脚本)**

**[root@xuegod63 ~]# ls /etc/init.d/ #这个目录下的脚本文件，都是可以开机启动的脚本文件**

**abrt-ccpp halt netstat rpcidmapd**

**[root@xuegod63 ~]# vim /etc/init.d/httpd # 在倒数第二行添加**



**测试：**

**[root@xuegod63 ~]# service httpd restart**

**Stopping httpd: [ OK ]**

**Starting httpd: [ OK ]**

**aaaaa**

**方法2：更强的黑客：自己写一个开机启动程序**

**[root@Xd9BdoAkG ~]# vim /etc/rc.d/init.d/fregonnzkq**

**#!/bin/sh**

**# chkconfig: 12345 90 90**

**# description: fregonnzkq**

**### END INIT INFO**

**case $1 in**

**start)**

**/usr/bin/fregonnzkq &**

**;;**

**stop)**

**;;**

**\*)**

**/usr/bin/fregonnzkq &**

**;;**

**esac**

**1、赋予启动脚本执行权限，并启动**

**[root@xuegod63 ~]# chmod +x /etc/init.d/fregonnzkq**

**[root@xuegod63 ~]# service fregonnzkq start**

**[root@xuegod63 ~]# ps -axu | grep freg #查看，可以运行**

**Warning: bad syntax, perhaps a bogus '-'? See /usr/share/doc/procps-3.2.8/FAQ**

**root 6725 0.0 0.1 11392 1248 pts/1 S 16:32 0:00 /bin/bash /usr/bin/fregonnzkq**

**2、添加到开机自动启动服务列表**

**[root@xuegod63 ~]# chkconfig --add fregonnzkq**

**[root@xuegod63 ~]# chkconfig --list fregonnzkq**

**fregonnzkq 0:off 1:on 2:on 3:on 4:on 5:on 6:off**

**3、重启测试服务有没有开机启动**

**[root@xuegod63 ~]# ps -axu | grep freg**

**Warning: bad syntax, perhaps a bogus '-'? See /usr/share/doc/procps-3.2.8/FAQ**

**root 2213 0.1 0.1 108256 1344 ? S 16:35 0:00 /bin/bash /usr/bin/fregonnzkq**

**4、排查**

**[root@xuegod63 ~]# cd /etc/rc3.d/**

**[root@xuegod63 rc3.d]# ls \*fre\* #开机启动，表示系统级别3下开机启动**

**S90fregonnzkq**

**5、查看每个系统别下的启动脚本**

**[root@xuegod63 etc]# ll /etc/rc\*/\* | grep fre**

**lrwxrwxrwx 1 root root 20 Oct 25 16:33 /etc/rc0.d/K90fregonnzkq -> ../init.d/fregonnzkq**

**lrwxrwxrwx 1 root root 20 Oct 25 16:33 /etc/rc1.d/S90fregonnzkq -> ../init.d/fregonnzkq**

**lrwxrwxrwx 1 root root 20 Oct 25 16:33 /etc/rc2.d/S90fregonnzkq -> ../init.d/fregonnzkq**

**lrwxrwxrwx 1 root root 20 Oct 25 16:33 /etc/rc3.d/S90fregonnzkq -> ../init.d/fregonnzkq**

**lrwxrwxrwx 1 root root 20 Oct 25 16:33 /etc/rc4.d/S90fregonnzkq -> ../init.d/fregonnzkq**

**lrwxrwxrwx 1 root root 20 Oct 25 16:33 /etc/rc5.d/S90fregonnzkq -> ../init.d/fregonnzkq**

**lrwxrwxrwx 1 root root 20 Oct 25 16:33 /etc/rc6.d/K90fregonnzkq ->**

**6、删除木马方法**

**方法1：[root@xuegod63 etc]# chkconfig --del fregonnzkq**

**或：**

**方法：2：[root@xuegod63 etc]# ll /etc/rc5.d/S90fregonnzkq #删除/etc/init.d/fregonnzkq 就可以了，因为其他级别下都是这个文件软链接**

**lrwxrwxrwx 1 root root 20 Oct 25 16:33 /etc/rc5.d/S90fregonnzkq -> ../init.d/fregonnzkq**

**排查： 对比法**

**[root@xuegod63 ~]# find /etc/init.d/ -type f -exec md5sum {} \; > /usr/share/init.d.v1**

**[root@xuegod63 ~]# find /etc/init.d/ -type f -exec md5sum {} \; > /usr/share/init.d.v2**

**[root@xuegod63 ~]# diff /usr/share/init.d.v1 /usr/share/init.d.v2**

**22.5.6 排查方法总结：**

**方法1：对比其他服务器好的配置文件 ，利用MD5值做对比**

**方法2： 查看被黑当天生成或被修改的文件**

**[root@xuegod63 ~]# find /etc/init.d/ -mtime -1 #查看被前一天到现在被修改的文件**

**/etc/init.d/**

**/etc/init.d/netstat**

**/etc/init.d/httpd**

**22.5.7 使用 rpm检查文件的完整性**

**语法：rpm -V 软件包的名字 #使用 rpm检查文件的完整性**

**语法：rpm -Vf 命令的绝对路径 #使用 rpm检查命令的完整性**

**例1、[root@xuegod63 ~]# rpm -V httpd**

**S.5....T. /etc/rc.d/init.d/httpd**

**注：**

**S file Size 大小不一致**

**M Mode 模式不一致 (包括许可和文件类型)**

**5 MD5 sum 校验和不一致**

**D Device 主从设备号不匹配**

**L readLink(2) 路径不匹配**

**U User 属主不一致**

**G Group 所属组不一致**

**T mTime 修改时间不一致**

**例2、查看命令有没有被修改**

**[root@xuegod63 rc3.d]# which zic**

**/usr/sbin/zic**

**[root@xuegod63 rc3.d]# rpm -Vf /usr/sbin/zic**

**[root@xuegod63 rc3.d]# echo aaa >> /usr/sbin/zic**

**[root@xuegod63 rc3.d]# rpm -Vf /usr/sbin/zic**

**prelink: /usr/sbin/zic: prelinked file size differs**

**S.?....T. /usr/sbin/zic**

**系统中有很多命令和软件包，如何校对所有的命令和包？**

**实战：查看所有rpm安装的软件包，生成命令或文件是否被改过？**

**例：rpm -Va > rpm\_check.txt**

**22.4.8 系统命令被人替换**

**例1：黑客修改/替换系统命令 , 查看命令有没有被修改**

**[root@xuegod63 ~]# which find**

**/usr/bin/find**

**[root@xuegod63 ~]# cp /usr/bin/find /usr/bin/ffind**

**[root@xuegod63 ~]# rm -rf /usr/bin/find #删除原来的find**

**[root@xuegod63 ~]# vim /usr/bin/find #插入以下内容**

**#!/bin/bash**

**/usr/bin/ffind**

**echo aaaaa**

**[root@xuegod63 ~]# chmod +x /usr/bin/find**

**[root@xuegod63 ~]#**

**测试：**

**[root@xuegod63 ~]# find /boot #说明木马执行成功。**

**...**

**aaaaa**

**总结：**

**黑客如何让脚本定时执行，以下三种方法：**

**1、计划任务： crontab 和系统级别的计划任务**

**2、开机启动rc.local和开机启动脚本**

**3、系统命令被人替换，定一个触发事件**

**排查：**

**方法1：通过生成md5值数据库，查询文件系统的完整性**

**方法2: 利用find命令查找下最近被修改过的文件：一般情况下命令文件都很久之前被修改的。**

**方法3: 被入侵后，检测检测所有rpm -Va 生成的文件是否被改动过**