之前已经简单整理了应急响应中定位系统异常行为的常见命令，接下来简单整理下linux下的日志文件。

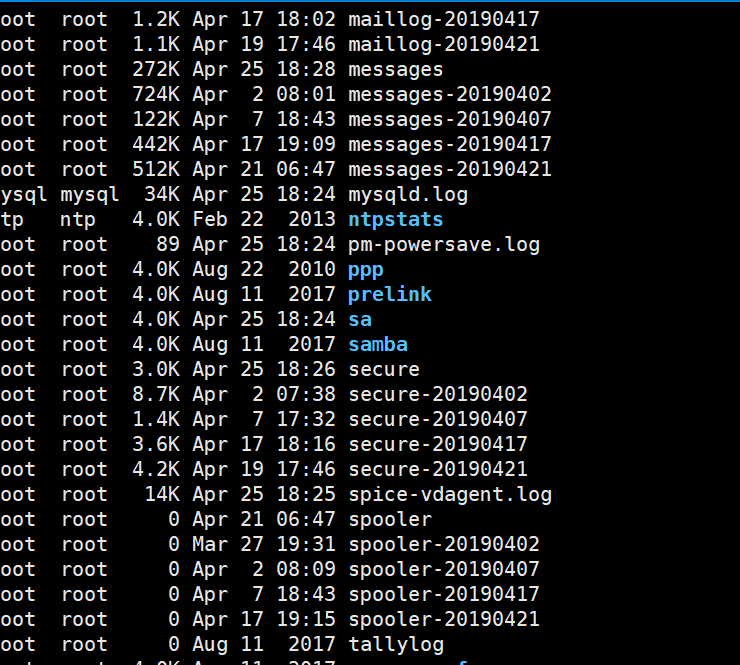
一、日志类型

内核及系统日志：这种日志由syslog统一管理，根据其主配置文件"/etc/syslog.conf"中的设置决定将内核消息及各种系统程序消息记录到什么位置。 用户日志：这种日志数据用于记录Linux系统用户登录及退出系统的相关信息，包括用户名、登录的终端、登录时间、来源主机、正在使用的进程操作等。 程序日志：有些应用程序运会选择自己来独立管理一份日志文件（而不是交给syslog服务管理），用于记录本程序运行过程中的各种事件信息。由于这些程序只负责管理自己的日志文件，因此不同的程序所使用的日志记录格式可能会存在极大差异。

通过查看 /etc/rsyslog.conf ，可查看相关系统日志配置情况。



linux系统日志一般存放在/var/log/目录下。



对于Linux系统中的一些常见日志文件，有必要熟悉其相应的用途，这样才能在需要的时候更快地找到问题所在，及时解决各种故障。

/var/log/messages：记录Linux内核消息及各种应用程序的公共日志信息，包括启动、IO错误、网络错误、程序故障等。对于未使用独立日志文件的应用程序或服务，一般都可以从该文件获得相关的事件记录信息。

/var/log/cron：记录crond计划任务产生的事件消息。

/varlog/dmesg：记录Linux系统在引导过程中的各种事件信息。

/var/log/maillog：记录进入或发出系统的电子邮件活动。

/var/log/lastlog：最近几次成功登录事件和最后一次不成功登录事件。

/var/log/rpmpkgs：记录系统中安装各rpm包列表信息。

/var/log/secure：记录用户登录认证过程中的事件信息。

/var/log/wtmp：记录每个用户登录、注销及系统启动和停机事件。

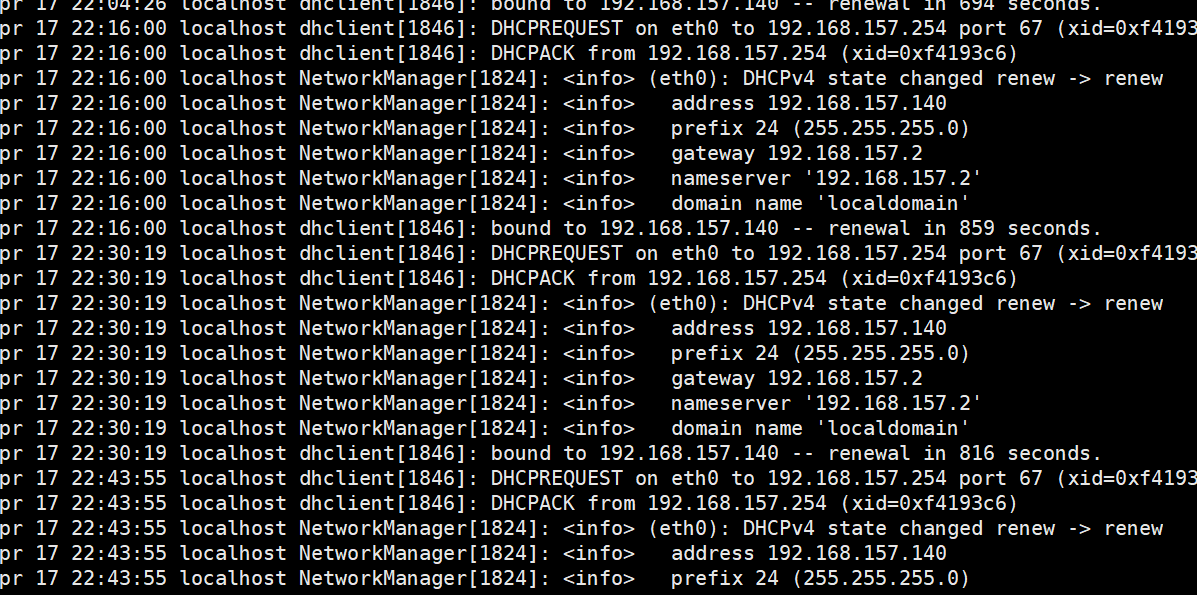
/var/log/utmp：记录当前登录的每个用户的详细信息

二、日志分析

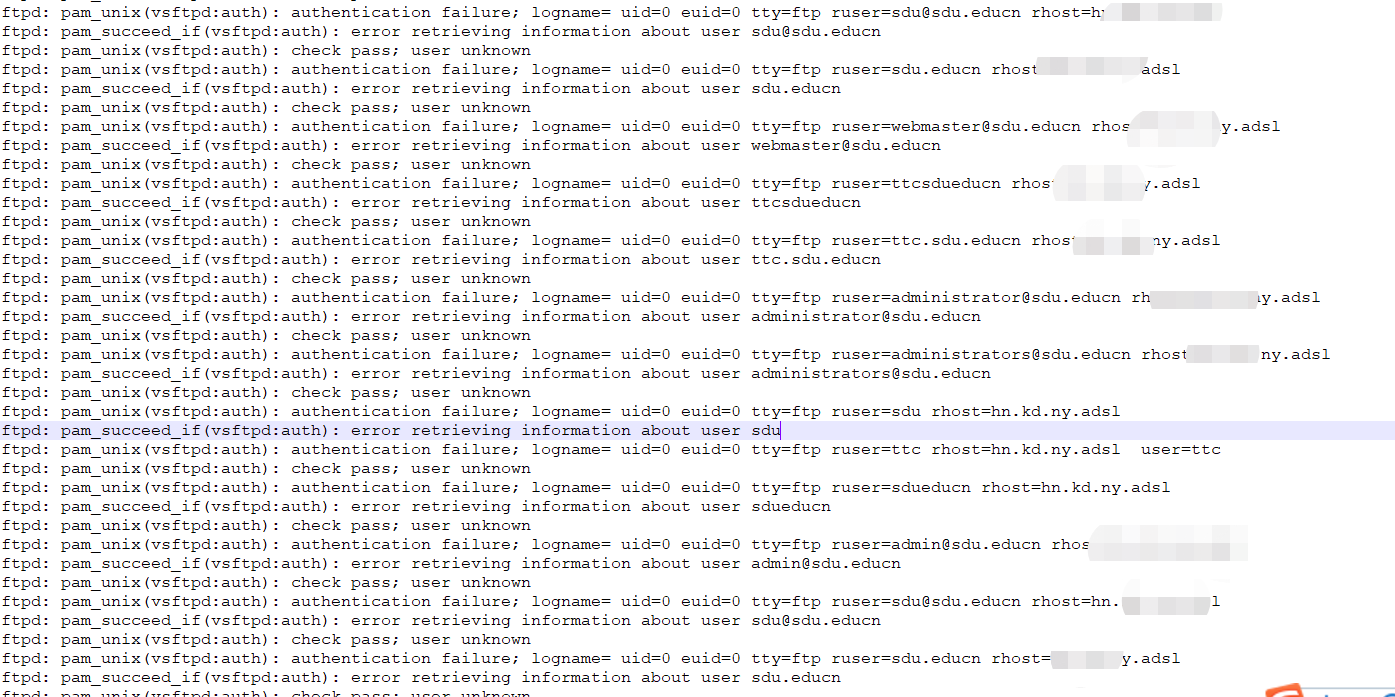
对于大多数文本格式的日志格式（如内核及系统日志、大多数的程序日志），只要使用tail、more、less、cat等文本处理工具就可以查看日志内容。而对于一些二进制格式的日志文件（eg：用户日志），则需要使用相应的查询命令。

1. 内核及系统日志

message日志，一般内核及大多数系统消息都被记录到公共日志文件"/var/log/messages"中，而其他一些程序消息被记录到不同的文件中，日志消息还能够记录到特定的存储设备中，或者直接向用户发送。具体根据rsyslog配置而定，日志如下



secure是应急中最常用的文件，主要记录系统存取数据的文件，如POP3、ssh、telnet、ftp等相关记录，从日志中可看出系统服务是否遭受到安全威胁，从如下日志中可看到ftp服务一直在被破解。



可通过grep命令查找文件里符合条件的字符串， 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

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}'

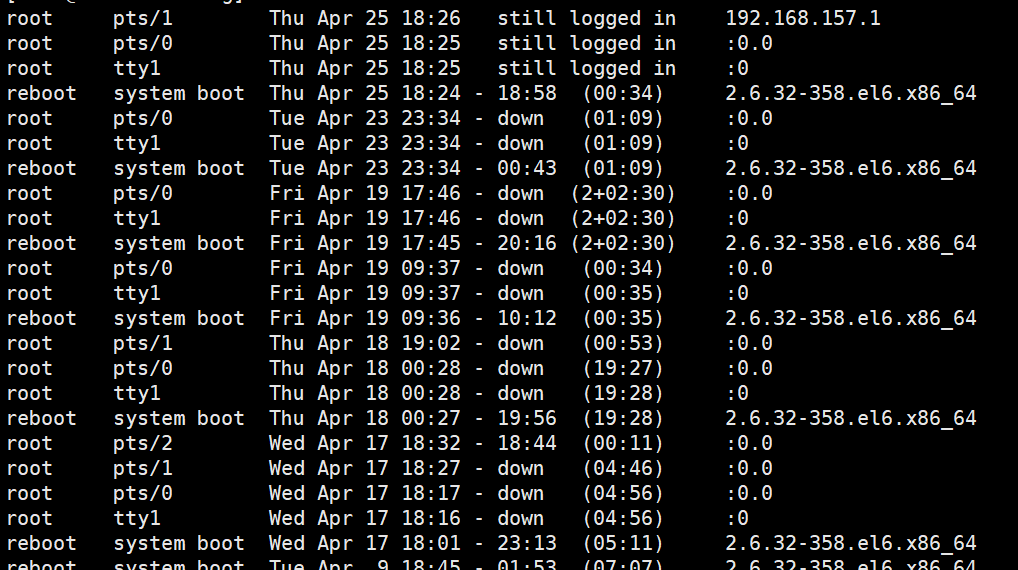
增加用户

grep "useradd" /var/log/secure 删除用户

grep "userdel" /var/log/secure

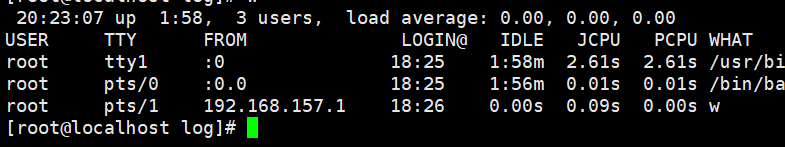
2.用户日志

wtmp日志记录了用户的登录、退出、重启等情况，可以查看系统是否存在异常用户登录，判断攻击者是否已经登录服务器，由于wtmp日志为二进制文件，所以利用用last命令查看，last -t 20190426120950 ,可查看这个时间之前的日志。



清除wtmp日志命令如下：# echo > /var/log/wtmp

utmp日志记录当前用户的一些信息，由于utmp日志文件同样为二进制文件，可通过w、who命令查看

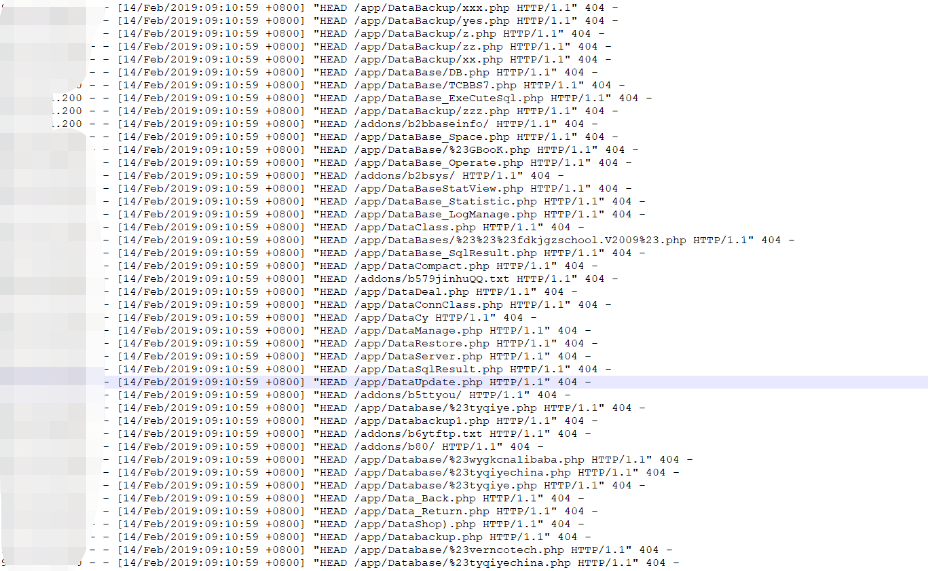


lastlog命令，用于显示系统中所有用户最近一次登录信息。lastlog文件在每次有用户登录时被查询。可以使用lastlog命令检查某特定用户上次登录的时间，并格式化输出上次登录日志/var/log/lastlog的内容。它根据UID排序显示登录名、端口号（tty）和上次登录时间。如果一个用户从未登录过，lastlog显示Never logged。注意需要以root身份运行该命令。

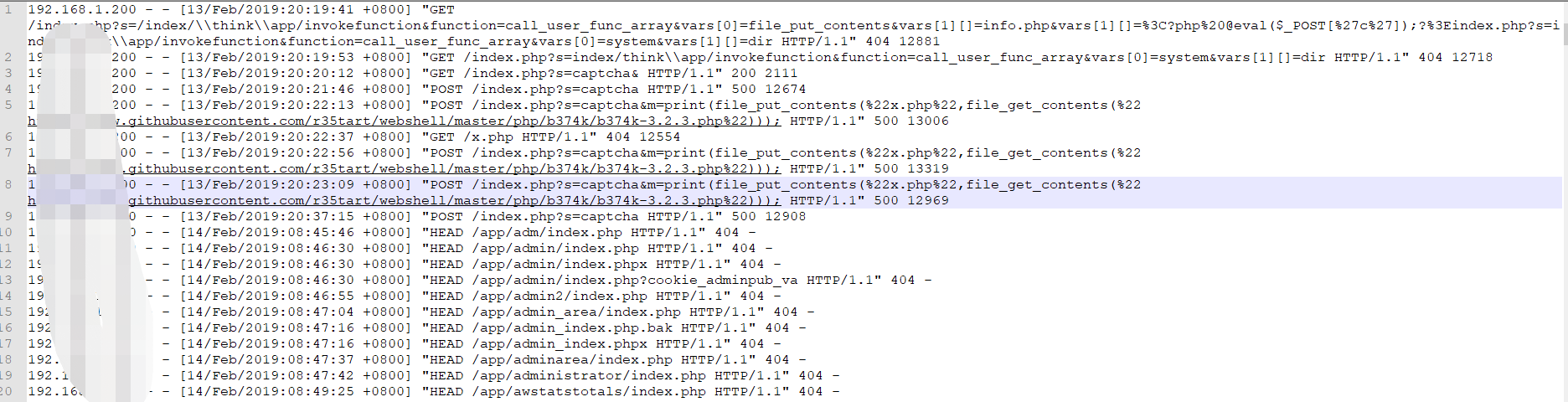
3.程序日志

在Linux系统中，还有相当一部分应用程序并没有使用syslog服务来管理日志。而是由程序自己维护日志记录。例如，httpd网站服务程序使用两个日志文件access\_log和error\_log。

由于多数攻击都是发布在互联网的漏洞被利用导致，留存程序日志对于日后的溯源还是很有必要的，常见的中间件有weblogic、jboss、iis、tomcat，web日志记录攻击者的行为，可通过web日志知道攻击者通过什么方式进入系统。



从上图日志中可看到攻击者对系统做了大量目录枚举，尝试找到合适可用的目录。 枚举到可用目录后，恶意攻击者尝试通过漏洞上传后门文件

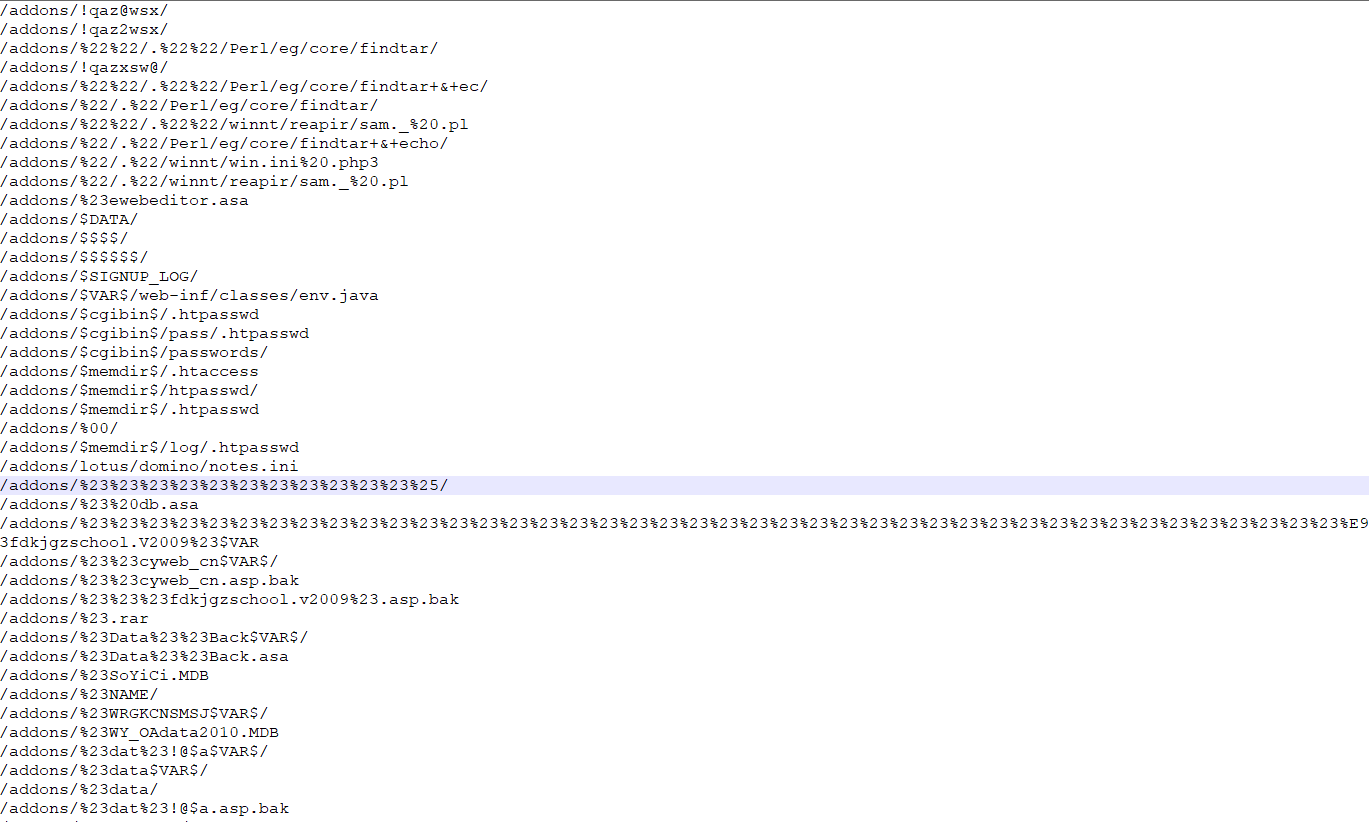


通过对日志的分析可对恶意用户的行为进行简单分析，明确攻击行为，确定攻击来源。

4.常见日志分析方法

由于日志文件通常是很大，如果单纯用命令去分析日志当然可以，但会不会很累呢，让工具来帮我们分析日志不失为好的办法。

自己写脚本，根据关键字去提取有用信息，比如根据ip地址、网站路径等，下图从日志中提取的攻击者用的网站目录。



工具：

<https://security.tencent.com/index.php/opensource/detail/15>

<http://www.freebuf.com/sectool/126698.html>

<http://www.freebuf.com/sectool/110644.html>

<http://www.freebuf.com/sectool/8982.html><http://www.freebuf.com/articles/web/96675.html>

平台（商业项目）：

360 >> 360星图

Splunk >> 机器数据引擎

赛克蓝德 >> SeciLog

优特捷信息技术 >> 日志易

HanSight瀚思 >> 安全易

百泉众合数据科技 >>LogInsight

江南天安 >> 彩虹WEB攻击溯源平台

开源项目：

elk <https://www.elastic.co>

scribe<https://github.com/facebook/scribe>

chukwa<http://incubator.apache.org/chukwa/>

kafka <http://sna-projects.com/kafka/>

Flume<https://github.com/cloudera/flume/>

三、 结束语

通过分析日志，感知可能正在发生的攻击，还原攻击者的攻击路径， 从较大的角度观察攻击者更“关心”哪些系统，发现已知或位置攻击方法，从日志中发现应用0day、Nday。数据库、操作系统、安全设备等日志都可做联动，借助大数据进行分析。日志分析本质为数据分析，而数据驱动安全必定是未来的趋势。