登录

【讨论】Linux应急响应

master / 2016-11-09 08:12:00 / 浏览数 7265 安全技术 技术讨论 顶(0) 踩(0)

最近工作中遇到了点Linux方面的应急响应问题，因为本人比较菜，所以掌握的知识点也不是很多。论坛既然开个讨论版块，那我就把我自己在响应过程中的一点排查思路发

1.bash_history记录
通常的Linux服务器在遭遇到入侵后，我的第一时间会去查看.bash_history文件，如图所示：
正常的操作系统里面有pentest(渗透测试)之类的字眼，一般来说，是黑客拿来做跳板机用的，便可以一目了然的知道这台服务器有没有被入侵，大大的提高了运维人员的排

当然，.bash_history能提供给我们的信息量很大，在这只是仅仅的一些举例。

2.last、lastb命令
具体命令详解，请参考百度：http://www.cnblogs.com/kerrycode/p/4223751.html
第一列：用户名
第二列：终端位置。pts/0 (伪终端) 意味着从诸如SSH或telnet的远程连接的用户.tty (teletypewriter) 意味着直接连接到计算机或者本地连接的用户
第三列：登录ip或者内核 。如果你看见:0.0 或者什么都没有，这意味着用户通过本地终端连接。除了重启活动，内核版本会显示在状态中。
第四列：开始时间
第五列：结束时间（ still login in 还未退出 down 直到正常关机 crash 直到强制关机 ）
第六列：持续时间

Last该命令用来列出目前与过去登录系统的用户相关信息，执行last指令时，它会读取位于/var/log目录下名称为wtmp的文件，并把该给文件的内容记录的登录系统的用户名
lastb显示登录失败的日志。

3.登录日志
系统日志：message、secure、cron、mail等系统日志；
应用程序日志：Apache日志、Nginx日志、FTP日志、MySQL等日志；
自定义日志：很多程序开发过程中会自定义程序日志，这些日志也是很重要的数据，能够帮我们分析入侵途径等信息；
bash_history：这是bash执行过程中记录的bash日志信息，能够帮我们查看bash执行了哪些命令(第一个提到过)。
其他安全事件相关日志记录
例如系统登录
该文件放在/var/logs/下边以secure.*为开头的文件，举例：

这里面存放着大量的ssh登录失败或者是成功的记录，这个文件可以很直观的看出哪些是爆破行为，哪些是正常的登录行为

4.Web_Access_log
为什么这个日志又起一个呢，因为现在很多的黑客都是通过web入侵，所以说要特别强调一下access_log
这个日志通常是我们在进行web反追踪的时候用到的日志，access log 监控每个 http request
的处理时间，以及方法、动作、相应等等操作，每一种不同的web容器存放的位置也不同，具体遇到要首先找配置文件，然后根据配置文件查找日志的存放信息，具体产生的

```
127.0.0.1 37 [05/Jun/2012:17:23:43 +0800] -- 200 2806 127.0.0.1 8080 GET/cdbleasing/message.listMessagePrompt.action?_dc=13388

127.0.0.1 533 [05/Jun/2012:17:26:31 +0800]- - 200 25994 127.0.0.1 8080 GET /cdbleasing/workflow.listTaskByCandidateUser.action
```

根据这些日志进行行为匹配和分析。

5.netstat
netstat 命令用于显示各种网络相关信息，如网络连接，路由表，接口状态 (Interface Statistics)，masquerade 连接，多播成员 (Multicast Memberships)
等等。
一般遇见服务器大量的发包或者是流量异常的时候，进行网络分析，具体操作参数很多，如有需要请自行百度
http://www.cnblogs.com/gqjucheng/archive/2012/01/08/2316661.html

可以一目了然的看到当前的连接情况，以及端口、ip使用情况，方便我们分析病毒外链等行为。

6.top or ps
top:命令是Linux下常用的性能分析工具，能够实时显示系统中各个进程的资源占用状况，类似于Windows的任务管理器。
ps:有时候系统管理员可能只关心现在系统中运行着哪些程序，而不想知道有哪些进程在运行。由于一个应用程序可能需要启动多个进程。所以在同等情况下，进程的数
量要比程序多的多。为此从阅读方面考虑，管理员需要知道系统中运行的具体程序。要实现这个需求的话，就需要利用命令ps来帮忙。
要对进程进行监测和控制，首先必须要了解当前进程的情况，也就是需要查看当前进程，而 ps
命令就是最基本同时也是非常强大的进程查看命令。使用该命令可以确定有哪些进程正在运行和运行的状态、进程是否结束、进程有没有僵死、哪些进程占用了过多
的资源等等。总之大部分信息都是可以通过执行该命令得到的。

7.Rootkit hunter
这个吧，不是专业的没有发言权，参见bird哥的私房菜
http://linux.vbird.org/linux_security/0420rkhunter.php
URL：http://www.rootkit.nl/projects/rootkit_hunter.html

8.Webshell kill tools
常规的webshell查杀是必须要进行的，可以使用seay以前写过的一个python版本的，也可以把源代码tar到本地进行解压，然后进行查杀。
或者是手动输入命令根据特征找webshell ,find / -name ".”

9.Corntab
Linux crontab定时执行任务,相当于Windows的开机启动项，命令格式与详细例子，大家可以参考下：
基本格式：
command 分 时 日 月 周
命令
第1列表示分钟1～59 每分钟用或者 /1表示
第2列表示小时1～23（0表示0点）
第3列表示日期1～31
第4列表示月份1～12
第5列标识号星期0～6（0表示星期天）
第6列要运行的命令

10.SUID/SGID
用下面的命令查找系统中所有的SUID和SGID程序，执行：

```
for PART in `grep -v ^# /etc/fstab | awk '($6 != "0") {print $2 }'`; do
find $PART ( -perm -04000 -o -perm -02000 ) -type f -xdev -print
done
```

11.隐藏进程查看
我没有代码

上一篇：自制攻击欺骗防御系统 下一篇：GitLab 任意文件读取漏洞 (...
1. 10 条回复


master 2016-11-09 09:04:14

求各抒己见

0 回复Ta


vskunkka 2016-11-09 10:51:07

我有代码

0 回复Ta


染血の雪 2016-11-09 11:20:16

这连总结都不算吧

0 回复Ta


虎哥 2016-11-09 11:28:13

能分享下代码么

0 回复Ta


hades 2016-11-09 12:23:09

欢迎踊跃总结

0 回复Ta


vskunkka 2016-11-10 03:31:08

进程隐藏的rootkit代码，内核级隐藏。。。。。。

0 回复Ta


master 2016-11-10 08:01:38

这是讨论啊，不是总结。

0 回复Ta


top 2017-01-12 14:40:35

大家就这样安静了。。。。。。

0 回复Ta


secscorpio 2017-01-22 03:31:36

基础的排查也就这么多了，http://secscorpio.top/?p=99

0 回复Ta


如风 2017-10-23 04:09:35

补充11:
检查隐藏进程
ps -ef | awk '{print }' | sort -n | uniq >1
ls /proc | sort -n |uniq >2
diff 1 2

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板