# 服务器被攻击了该怎么办？

整理了一份企业服务器安全防范笔记以及应急方案，需要的朋友可以直击点击领取。

# 一、处理服务器遭受攻击的一般思路

## 1.切断网络

所有的攻击都来自于网络，因此，在得知系统正遭受HK的攻击后，首先要做的就是断开服务器的网络连接，这样除了能切断攻击源之外，也能保护服务器所在网络的其他主机。

## 2.查找攻击源

可以通过分析系统日志或登录日志文件，查看可疑信息，同时也要查看系统都打开了哪些端口，运行哪些进程，并通过这些进程分析哪些是可疑的程序。这个过程要根据经验和综合判断能力进行追查和分析。下面的章节会详细介绍这个过程的处理思路。

## **3.分析入侵原因和途径**

既然系统遭到入侵，那么原因是多方面的，可能是系统漏洞，也可能是程序漏洞，一定要查清楚是哪个原因导致的，并且还要查清楚遭到攻击的途径，找到攻击源，因为只有知道了遭受攻击的原因和途径，才能删除攻击源同时进行漏洞的修复。

## **4.备份用户数据**

在服务器遭受攻击后，需要立刻备份服务器上的用户数据，同时也要查看这些数据中是否隐藏着攻击源。如果攻击源在用户数据中，一定要彻底删除，然后将用户数据备份到一个安全的地方。

## **5.重新安装系统**

永远不要认为自己能彻底清除攻击源，因为没有人能比HK更了解攻击程序，在服务器遭到攻击后，最安全也最简单的方法就是重新安装系统，因为大部分攻击程序都会依附在系统文件或者内核中，所以重新安装系统才能彻底清除攻击源。

## **6.修复程序或系统漏洞**

在发现系统漏洞或者应用程序漏洞后，首先要做的就是修复系统漏洞或者更改程序bug，因为只有将程序的漏洞修复完毕才能正式在服务器上运行。

## **7.恢复数据和连接网络**

将备份的数据重新复制到新安装的服务器上，然后开启服务，最后将服务器开启网络连接，对外提供服务。

# 二、检查并锁定可疑用户

当发现服务器遭受攻击后，首先要切断网络连接，但是在有些情况下，比如无法马上切断网络连接时，就必须登录系统查看是否有可疑用户，如果有可疑用户登录了系统，那么需要马上将这个用户锁定，然后中断此用户的远程连接。

## **1.登录系统查看可疑用户**

通过root用户登录，然后执行“w”命令即可列出所有登录过系统的用户，如下图所示。

通过这个输出可以检查是否有可疑或者不熟悉的用户登录，同时还可以根据用户名以及用户登录的源地址和它们正在运行的进程来判断他们是否为非法用户。

## **2.锁定可疑用户**

一旦发现可疑用户，就要马上将其锁定，例如上面执行“w”命令后发现nobody用户应该是个可疑用户（因为nobody默认情况下是没有登录权限的），于是首先锁定此用户，执行如下操作：

[root@server ~]# passwd -l nobody

锁定之后，有可能此用户还处于登录状态，于是还要将此用户踢下线，根据上面“w”命令的输出，即可获得此用户登录进行的pid值，操作如下：

[root@server ~]# ps -ef|grep @pts/3531 6051 6049 0 19:23 ? 00:00:00 sshd: nobody@pts/3

[root@server ~]# kill -9 6051

这样就将可疑用户nobody从线上踢下去了。如果此用户再次试图登录它已经无法登录了。

## **3.通过last命令查看用户登录事件**

last命令记录着所有用户登录系统的日志，可以用来查找非授权用户的登录事件，而last命令的输出结果来源于/var/log/wtmp文件，稍有经验的入侵者都会删掉/var/log/wtmp以清除自己行踪，但是还是会露出蛛丝马迹在此文件中的。

# 三、查看系统日志

查看系统日志是查找攻击源最好的方法，可查的系统日志有/var/log/messages、/var/log/secure等，这两个日志文件可以记录软件的运行状态以及远程用户的登录状态，还可以查看每个用户目录下的.bash\_history文件，特别是/root目录下的.bash\_history文件，这个文件中记录着用户执行的所有历史命令。

# 四、检查并关闭系统可疑进程

检查可疑进程的命令很多，例如ps、top等，但是有时候只知道进程的名称无法得知路径，此时可以通过如下命令查看：

首先通过pidof命令可以查找正在运行的进程PID，例如要查找sshd进程的PID，执行如下命令：

[root@server ~] # pidof sshd

13276 12942 4284

然后进入内存目录，查看对应PID目录下exe文件的信息：

[root@server ~] # ls -al /proc/13276/exe

lrwxrwxrwx 1 root root 0 Oct 4 22:09 /proc/13276/exe -> /usr/sbin/sshd

这样就找到了进程对应的完整执行路径。如果还有查看文件的句柄，可以查看如下目录：

[root@server ~]# ls -al /proc/13276/fd

通过这种方式基本可以找到任何进程的完整执行信息，此外还有很多类似的命令可以帮助系统运维人员查找可疑进程。例如，可以通过指定端口或者tcp、udp协议找到进程PID，进而找到相关进程：

[root@server ~] # fuser -n tcp 111111 /tcp : 1579[root@server ~] # fuser -n tcp 2525 /tcp : 2037[root@server ~] # ps -ef|grep 2037root 2037 1 0 Sep23 ? 00:00:05 /usr/libexec/postfix/masterpostfix 2046 2037 0 Sep23 ? 00:00:01 qmgr -l -t fifo -upostfix 9612 2037 0 20:34 ? 00:00:00 pickup -l -t fifo -uroot 14927 12944 0 21:11 pts /1 00:00:00 grep 2037

在有些时候，攻击者的程序隐藏很深，例如rootkits后门程序，在这种情况下ps、top、netstat等命令也可能已经被替换，如果再通过系统自身的命令去检查可疑进程就变得毫不可信，此时，就需要借助于第三方工具来检查系统可疑程序，例如前面介绍过的chkrootkit、RKHunter等工具，通过这些工具可以很方便的发现系统被替换或篡改的程序。

# 五、检查文件系统的完好性

检查文件属性是否发生变化是验证文件系统完好性最简单、最直接的方法，例如可以检查被入侵服务器上/bin/ls文件的大小是否与正常系统上此文件的大小相同，以验证文件是否被替换，但是这种方法比较低级。此时可以借助于Linux下rpm这个工具来完成验证，操作如下：

[root@server ~] # rpm -Va....L... c /etc/pam .d /system-authS.5..... c /etc/security/limits .confS.5....T c /etc/sysctl .confS.5....T /etc/sgml/docbook-simple . catS.5....T c /etc/login .defsS.5..... c /etc/openldap/ldap .confS.5....T c /etc/sudoers..5....T c /usr/lib64/security/classpath .security....L... c /etc/pam .d /system-authS.5..... c /etc/security/limits .confS.5..... c /etc/ldap .confS.5....T c /etc/ssh/sshd\_config

对于输出中每个标记的含义介绍如下：

**S 表示文件长度发生了变化**

**M 表示文件的访问权限或文件类型发生了变化**

**5 表示MD5校验和发生了变化**

**D 表示设备节点的属性发生了变化**

**L 表示文件的符号链接发生了变化**

**U 表示文件/子目录/设备节点的owner发生了变化**

**G 表示文件/子目录/设备节点的group发生了变化**

**T 表示文件最后一次的修改时间发生了变化**

如果在输出结果中有“M”标记出现，那么对应的文件可能已经遭到篡改或替换，此时可以通过卸载这个rpm包重新安装来清除受攻击的文件。

不过这个命令有个局限性，那就是只能检查通过rpm包方式安装的所有文件，对于通过非rpm包方式安装的文件就无能为力了。同时，如果rpm工具也遭到替换，就不能通过这个方法了，此时可以从正常的系统上复制一个rpm工具进行检测。

对文件系统的检查也可以通过chkrootkit、RKHunter这两个工具来完成，关于chkrootkit、RKHunter工具的使用，如果感兴趣下篇将展开介绍。

<https://baijiahao.baidu.com/s?id=1707598878558001256&wfr=spider&for=pc>

<https://baijiahao.baidu.com/s?id=1714830469112128633&wfr=spider&for=pc>

[https://zhuanlan.zhihu.com/p/425794729](https://baijiahao.baidu.com/s?id=1714830469112128633&wfr=spider&for=pc)

# [Linux入侵排查时安全工具整理](https://baijiahao.baidu.com/s?id=1714830469112128633&wfr=spider&for=pc)

[https://cloud.tencent.com/developer/article/1816436](https://baijiahao.baidu.com/s?id=1714830469112128633&wfr=spider&for=pc)

[https://github.com/grayddq/GScan](https://baijiahao.baidu.com/s?id=1714830469112128633&wfr=spider&for=pc)

# 入侵检测系统

<https://www.jianshu.com/p/a43774aa4600>

AIDE(Adevanced Intrusion Detection Environment,高级入侵检测环境)是个入侵检测工具，主要用途是检查文本的完整性。我们可以通过配置AIDE的配置文件aide.conf选择我们想要加密目录，并且选择我们想加密的策略

# 搭建Linux入侵检测系统(ids)

<http://t.zoukankan.com/kyooo-p-13232478.html>

# Lyins

程序定位为安全人员日常使用的一款用于主机基线和审计的工具，可辅助漏洞扫描和配置管理，也可部分用于入侵检测。

<https://github.com/CISOfy/lynis>

git clone https://github.com/CISOfy/lynis

cd lynis && ./lynis audit system

<https://www.jb51.net/article/192374.htm>

### **开始审计并查找漏洞**

执行本地安全扫描，所以使用‘audit system’参数来扫描整个系统。运行下面的命令来启动对整个系统的审计：

[root@localhost lynis]# ./lynis audit system

或者

[root@localhost lynis]# ./lynis audit system --wait

--wait选项：等待用户按回车键显示下一节的报告。

有时我们不想扫描或审计整个系统的应用程序或服务，所以我们可以按类别审计自定义应用程序。我们可以先列出所有的组，然后选择需要审计或扫描的组。

[root@localhost lynis]# ./lynis show groups

<https://zhuanlan.zhihu.com/p/262871136>

在报告的底部，Lynis 根据报告的发现提出了建议。每项建议后面都有一个 “TEST-ID”（为了下一部分方便，请将其保存起来）。

Lynis 提供了一个选项来查找关于每个建议的更多信息，你可以使用 show details 命令和 TEST-ID 号来访问：

./lynis show details TEST-ID

这将显示该测试的其他信息。例如，我检查了 SSH-7408 的详细信息：

$ ./lynis show details SSH-7408

