

---

# Linux 主机入侵排查参考手册.md

## Linux 主机入侵排查参考手册

### 一、目录:

Linux 主机入侵排查参考手册

一、目录:

二、入侵事件分类

三、常规入侵排查步骤

1. 现场保留
2. 系统密码文件检查
3. 系统可疑进程查找
4. 检查系统守护进程
5. 检查网络连接和监听端口
6. 检查登录历史
7. 检查系统文件完整性
8. 清查 Webshell
9. 清查 Rootkit
10. 排查思路总结

---

## 二、入侵事件分类

### 1. 常见的安全事件

- Web 入侵: 挂马、篡改、Webshell
  - 系统入侵: 系统异常、RDP 爆破、SSH 爆破、主机漏洞
  - 病毒木马: 远控、后门、勒索软件
  - 信息泄漏: 脱裤、数据库登录 (弱口令)
  - 网络流量: 频繁发包、批量请求、DDOS 攻击
-

---

## 三、常规入侵排查步骤

### 1. 现场保留

- 在执行以下所有操作步骤之前，务必保留服务器相关现场文件；
- 备份下载所有业务代码，业务日志（包括 Nginx 访问日志），业务数据等文件至本地；若主机正在被入侵，可考虑暂停服务器业务之后通过云服务商操作台限制**出入流量**，仅供管理员或安全人员登录服务器进行操作；
- 备份下载服务器系统相关运行日志，包括：

- ~/.bash\_history
- /root/.bash\_history
- /var/log/messages\*
- /var/log/secure\*:
- /var/log/wtmp\*:
- /var/log/dmesg\*:
- /var/log/mail\*:
- /var/log/cron\*

- 日志用途简要解读：

/var/log/message	包括整体系统信息
/var/log/auth.log 等	包含系统授权信息，包括用户登录和使用的权限机制
/var/log/userlog	记录所有等级用户信息的日志。
/var/log/cron	记录 crontab 命令是否被正确的执行
/var/log/xferlog(vsftpd.log)	记录 Linux FTP 日志
/var/log/lastlog	记录登录的用户，可以使用命令 lastlog 查看
/var/log/secure	记录大多数应用输入的账号与密码，登录成功与否
var/log/wtmp	记录登录系统成功的账户信息，等同于命令 last
var/log/faillog	记录登录系统不成功的账号信息，一般会被黑客删除

### 2. 系统密码文件检查

1. 检查系统密码文件修改日期是否正常，着重观察 stat 命令中文件的修改时间及访问时间：
  - ls -ahl /etc/passwd

- 
- `stat /etc/passwd`
2. 查看文件修改的日期
    - `awk -F:'$3==0 {print $1}' /etc/passwd`
  3. 检查哪些特权用户存在（显示 uid 为 0 的用户），以及空口令账户：
    - `awk -F: 'length($2)==0 {print $1}' /etc/shadow`

### 3. 系统可疑进程查找

1. 查看系统所有进程，通过名称及所属权限组粗略判断是否存在可疑进程：
  - `ps aux`
  - 如果系统内核补丁健全且不存在可被利用的 root 级别业务漏洞，入侵者大概率无法获取 root 权限，可考虑执行 `ps aux | grep www` 或类似命令来识别可疑进程；
2. 重点查看如下进程：
  - `ps -aef | grep inetd`
  - `inetd` 是 UNIX 系统的守护进程，正常的 `inetd` 的 pid 都比较靠前，如果输出一个类似 `inetd -s /tmp/.xxx` 之类的进程，着重查看 `inetd -s` 之后的内容，在正常情况下，LINUX 系统中的 `inetd` 服务后面没有 `-s` 参数；
3. 进程执行路径：
  - 输入 `ps -aef` 查看输出信息，注意有无 `./xxx` 开头的进程。若发现异常的进程，经检查为入侵者留下的后门程序，可运行 `kill -9 pid` 关闭该进程，等待一至两分钟后，再次运行 `ps -aef`，确认进程是否终止执行；
  - 若进程出现杀死以后又重新启动的现象，则证明系统被人设置了自动启动恶意程序，执行 `find / -name "malware.elf.name" -print`，找到该文件，保存取证后从服务器上删除；
4. 检查是否存在异常占用资源的进程
  - `ps aux --sort=-pmem` `ps aux --sort=-pcpu`

#### 4. 检查系统守护进程

1. 检查/etc/inetd.conf 文件，输入如下命令来确认系统所开启的远程服务：

- `cat /etc/inetd.conf | grep -v "^#"`
- 入侵者可以通过直接替换 in.xxx 程序来创建一个后门，比如用 /bin/sh 替换掉 in.telnetd，然后重新启动 inetd 服务，那么 telnet 到服务器上的所有用户将不需要输入用户名和密码而直接获得一个 rootshell；

#### 5. 检查网络连接和监听端口

1. 执行 `netstat -anp` 列出本机所有的连接和监听的端口，查看是否有非法连接；

2. 执行 `netstat -anp | grep -i listen` 检查正在监听的端口和进程，查看是否有明显异常；

- 执行结果一般如下图所示：

```
root@sm0nk:~# netstat -anlp | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2624/sshd
tcp6       0      0 :::22                  :::*                    LISTEN      2624/sshd
udp        0      0 0.0.0.0:68              0.0.0.0:*               7
raw6       0      0 :::58                  :::*                    534/NetworkManager


Active UNIX domain sockets (servers and established)
Proto RefCnt Flags   Type       State       I-Node     PID/Program name      Path
unix  2      [ ACC ]     Stream    LISTENING   20477      2177/gnome-session-@/tmp/.ICE-unix/2177
unix  2      [ ACC ]     Stream    LISTENING   15622      868/pulseaudio        /run/user/132/pulse/native
unix  3      [ ]       DGRAM     11272       1/init          /run/systemd/notify
unix  2      [ ]       DGRAM     11274       1/init          /run/systemd/cgroups-agent
unix  2      [ ACC ]     Stream    LISTENING   11276      1/init          /run/systemd/private
unix  2      [ ACC ]     SeqPacket LISTENING   11281      1/init          /run/udev/control
unix  2      [ ACC ]     Video     LISTENING   22323      631/gdm3            @/tmp/dbus-7NyFWPXE
unix  2      [ ACC ]     Stream    LISTENING   11295      1/init          /run/systemd/journal/stdout
unix  2      [ ACC ]     Stream    LISTENING   20412      2171/Xorg            @/tmp/.X11-unix/X0
unix  7      [ ]       DGRAM     11298      1/init          /run/systemd/journal/socket
unix  15     [ ]       DGRAM     11303      1/init          /run/systemd/journal/dev-log
unix  2      [ ACC ]     Stream    LISTENING   11307      1/init          /run/lvm/lvmetad.socket
unix  2      [ ACC ]     Stream    LISTENING   11313      1/init          /run/lvm/lvmpolld.socket
unix  2      [ ACC ]     Stream    LISTENING   14625      662/gnome-session-b /tmp/.ICE-unix/662
```

- 如果系统存在可疑连接，例如：

- 如图可看出 pid 为 1742, 1677 及 1683 的进程为可疑进程，可通过 ps 命令来查找相应路径：

- 
3. 执行 `netstat -A inet -p` 检查是否存在异常连接;
  4. 在执行之后, 可通过执行 `lsof` 及 `ss` 命令交叉检查命令执行结果, 防止 `netstat` 命令被替换或者系统装有 `rootkit`;

## 6. 检查登录历史

1. 在主机上执行 `last -f wtmp` 查看近期 SSH 登陆历史:
  -  注意: `last` 命令依赖于 `/var/log/wtmp` 的完整性, 若入侵者通过入侵运行在高权限的业务系统, 可以执行 `root` 命令时, 可能会修改该文件, 或者执行 `sudo systemctl stop rsyslog` 来停止运行相关日志服务, 此时入侵应为严重入侵事故;
  - 执行 `stat /var/log/messages` 及 `stat /var/log/wtmp` 来查看相关日志修改日期是否正常;
2. 检查 SSH 相关配置文件是否被修改:
  - 检查 `~/.ssh/authorized_keys` 是否包含被恶意添加的 `ssh` 登陆公钥;
  - 检查 `/etc/ssh/sshd_config` 是否包含额外 `pam.d` 文件, 恶意 `pam` 文件可用于窃取 `ssh` 用户登陆密码;
  - 检查 `/usr/sbin/sshd` 的修改时间, 确定该可执行文件的完整性。

## 7. 检查系统文件完整性

1. 检查几处重点目录, 查看相关二进制可执行文件是否被更改:
  - 查看 `tmp` 目录下的文件: `ls -alt /tmp/`
  - 查看开机启动项内容: `ls -alt /etc/init.d/`, `ls -alt /etc/rc.d/`, `sudo systemctl list-unit-files --state=enabled`
  - 查看可执行文件目录: `ls -alt /usr/bin`, `ls -alt /usr/sbin`
  - 查看 `crontab` 记录: `cat /etc/crontab` 以及 `crontab -l`
  - 使用 `stat` 命令着重查看 `ls`, `cat`, `netstat`, `ss`, `lsof`, `grep` 等二进制文件的更改时间, 例如:

```
stat install.sh
File: "install.sh"
Size: 1340 Blocks: 8 IO Block: 4096 普通文件
Device: 27h/39d Inode: 111285830 Links: 1
```

---

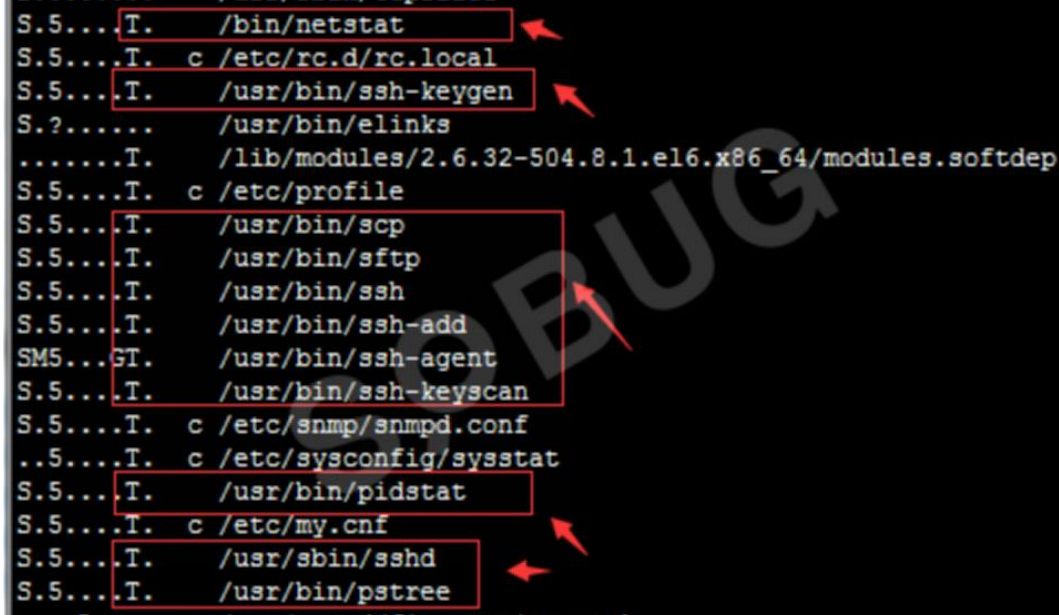
```
Access: (0644/-rw-r--r--) Uid: ( 504/ www) Gid: ( 502/ www)
Access: 2013-07-24 14:46:35.071180026 +0800
Modify: 2013-07-24 12:52:18.721961569 +0800
Change: 2013-07-24 12:52:18.722961608 +0800
```

## 2. Centos 系统下 RPM 检查

- 为防止关键可执行二进制文件被篡改，可通过 rpm 自带的-Va 来校验所有的 rpm 软件包，为防止 RPM 文件本身被篡改，可上传稳定安全的 RPM 至服务器后，执行./rpm -Va > rpm.log 进行检查；
- 如果一切均校验正常将不会产生任何输出。
- 如果有不一致的地方，就会显示出来；输出格式是 8 位长字符串,c 用以指配置文件，接着是文件名。8 位字符的每一个 用以表示文件与 RPM 数据库中一种属性的比较结果 。.(点) 表示测试通过。下面的字符表示对 RPM 软件包进行的某种测试失败：

```
5 MD5 校验码
S 文件尺寸
L 符号连接
T 文件修改日期
D 设备
U 用户
G 用户组
M 模式 e (包括权限和文件类型)
```

- 以下图为例，可知 ps, pstree, netstat, sshd 等等系统关键可执行文件已被篡改：



```
S.5....T. /bin/netstat
S.5....T. c /etc/rc.d/rc.local
S.5....T. /usr/bin/ssh-keygen
S.2..... /usr/bin/links
.....T. /lib/modules/2.6.32-504.8.1.el6.x86_64/modules.softdep
S.5....T. c /etc/profile
S.5....T. /usr/bin/scp
S.5....T. /usr/bin/sftp
S.5....T. /usr/bin/ssh
S.5....T. /usr/bin/ssh-add
SM5...GT. /usr/bin/ssh-agent
S.5....T. /usr/bin/ssh-keyscan
S.5....T. c /etc/snmp/snmpd.conf
..5....T. c /etc/sysconfig/sysstat
S.5....T. /usr/bin/pidstat
S.5....T. c /etc/my.cnf
S.5....T. /usr/sbin/sshd
S.5....T. /usr/bin/pstree
```

## 8. 清查 Webshell

### 1. 服务器上新增文件分析：

- 查找 24 小时内被修改的 JSP 文件: `find ./ -mtime 0 -name "*.jsp"`, (最后一次修改发生在距离当前时间 n24 小时至(n+1)24 小时)
- 查找 72 小时内新增的文件 `find / -ctime -2`, 采用-ctime 时, 内容未改变权限改变时候也可以查出
- 根据确定时间去反推变更的文件, `ls -al /tmp | grep "Feb 27"`
- 查找 777 的权限的文件, `find / *.jsp -perm 4777`

### 2. 打包下载业务代码, 本地使用 D 盾进行扫描;

- 在查找 webshell 时, 不推荐在服务器上直接 `grep` 可疑函数进行查找, 在 webshell 通常都会进行变形加密的今天, 容易产生遗漏;
- 可将业务代码所在目录所有文件同步会本地, 进行后续分析, 推荐下载 D 盾进行 webshell 的扫描查杀:
- 下载地址: <http://www.d99net.net/>

- 使用截图:



## 9. 清查 Rootkit

1. 在入侵者获取 root 权限的情况下, 可能会对主机进行 rootkit 的安装, 一般采用驱动劫持的形式, 在业务机器被安装 rootkit 的情况下, 恶意进程、流量、文件都可能被隐藏, 无法发现, 可通过安装 chkrootkit 或 rkhunter 进行 rootkit 的识别查找;

### 2. chkrootkit

- 主要功能:

- 检测是否被植入后门、木马、rootkit
- 检测系统命令是否正常
- 检测登录日志

- 下载地址: <http://www.chkrootkit.org/>

- 使用示例:



```
root@sm0nk:~/Desktop/PenTest/chkrootkit-0.52# ./chkrootkit -h
Usage: ./chkrootkit [options] [test ...]
Options:
  -h          show this help and exit
  -V          show version information and exit
  -l          show available tests and exit
  -d          debug
  -q          quiet mode
  -x          expert mode
  -r dir      use dir as the root directory
  -p dir1:dir2:dirN path for the external commands used by chkrootkit
  -n          skip NFS mounted dirs
root@sm0nk:~/Desktop/PenTest/chkrootkit-0.52# ./chkrootkit -l
./chkrootkit: tests: aliens asp bindshell lkm rexedcs sniffer w55808 wted scalper slapper z2 chkutmp OSX RSPLUG amd basenane biff chfn chsh cron cron
tab date du dirname echo egrep env find fingerd gpm grep hdparm su ifconfig inetd inetdconf identd init killall ldsopreload login ls lsof mail minge
tty netstat named passwd pidof pop2 pop3 ps pstree rpcinfo rlogind rshd slogin sendmail sshd syslogd tar tcpd tcpdump top telnetd timed traceroute vd
ir w write
root@sm0nk:~/Desktop/PenTest/chkrootkit-0.52#
```

### 3. rkhunter

- 主要功能
  - 系统命令（Binary）检测，包括 Md5 校验
  - Rootkit 检测
  - 本机敏感目录、系统配置、服务及套间异常检测
  - 三方应用版本检测
- 下载地址: <http://rkhunter.sourceforge.net/>
- 使用示例:

```
root@sm0nk:~# rkhunter --checkall --sk
[ Rootkit Hunter version 1.4.2 ]

Checking system commands...

Performing 'strings' command checks
  Checking 'strings' command [ OK ]

Performing 'shared libraries' checks
  Checking for preloading variables [ None found ]
  Checking for preloaded libraries [ None found ]
  Checking LD_LIBRARY_PATH variable [ Not found ]

Performing file properties checks
  Checking for prerequisites [ Warning ]
  /usr/local/bin/rkhunter [ OK ]
  /usr/sbin/adduser [ Warning ]
  /usr/sbin/chroot [ OK ]
  /usr/sbin/cron [ OK ]
  /usr/sbin/groupadd [ OK ]
  /usr/sbin/groupdel [ OK ]
  /usr/sbin/groupmod [ OK ]
  /usr/sbin/grpck [ OK ]
```

10. 排查思路总结

1. 下图为常规入侵事件后的系统排查思路，以供参考：

