
# Linux后门N种姿势

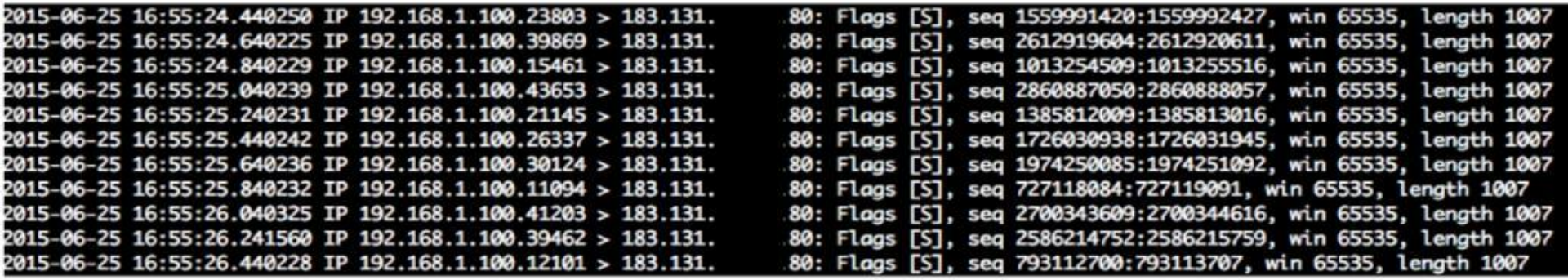
By:fuckadmin

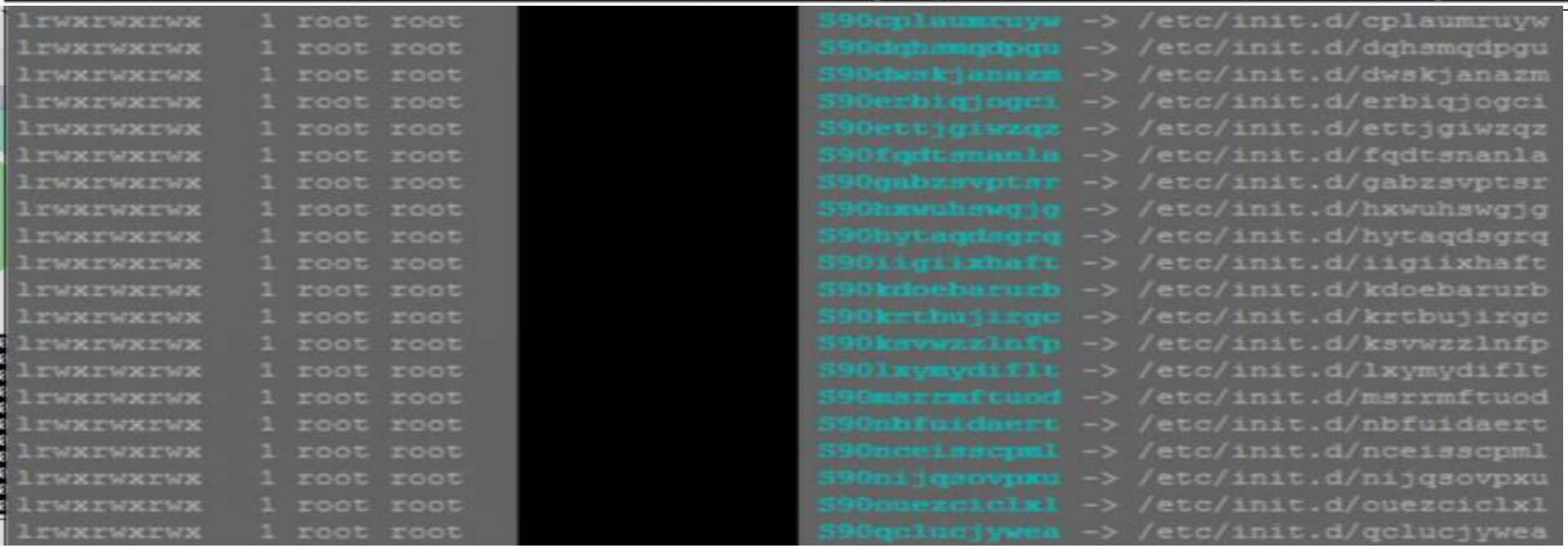
WhiteCellClub团队SRC负责人


1.前言
2.后门概述及种类
3.常见后门功能
4.Rootkit发现及检测
5.后续处理


- Linux服务器真的安全嘛？
- 真的百毒不侵？
- 存在哪些误解？

# 服务器“中毒”了?


2015-06-25 16:55:24.440250 IP 192.168.1.100.23803 > 183.131. .80: Flags [S], seq 1559991420:1559992427, win 65535, length 1007
2015-06-25 16:55:24.640225 IP 192.168.1.100.39869 > 183.131. .80: Flags [S], seq 2612919604:2612920611, win 65535, length 1007
2015-06-25 16:55:24.840229 IP 192.168.1.100.15461 > 183.131. .80: Flags [S], seq 1013254509:1013255516, win 65535, length 1007
2015-06-25 16:55:25.040239 IP 192.168.1.100.43653 > 183.131. .80: Flags [S], seq 2860887050:2860888057, win 65535, length 1007
2015-06-25 16:55:25.240231 IP 192.168.1.100.21145 > 183.131. .80: Flags [S], seq 1385812009:1385813016, win 65535, length 1007
2015-06-25 16:55:25.440242 IP 192.168.1.100.26337 > 183.131. .80: Flags [S], seq 1726030938:1726031945, win 65535, length 1007
2015-06-25 16:55:25.640236 IP 192.168.1.100.30124 > 183.131. .80: Flags [S], seq 1974250085:1974251092, win 65535, length 1007
2015-06-25 16:55:25.840232 IP 192.168.1.100.11094 > 183.131. .80: Flags [S], seq 727118084:727119091, win 65535, length 1007
2015-06-25 16:55:26.040325 IP 192.168.1.100.41203 > 183.131. .80: Flags [S], seq 2700343609:2700344616, win 65535, length 1007
2015-06-25 16:55:26.241560 IP 192.168.1.100.39462 > 183.131. .80: Flags [S], seq 2586214752:2586215759, win 65535, length 1007
2015-06-25 16:55:26.440228 IP 192.168.1.100.12101 > 183.131. .80: Flags [S], seq 793112700:793113707, win 65535, length 1007


lrwxrwxrwx 1 root root S90cplaumruyw -> /etc/init.d/cplaumruyw
lrwxrwxrwx 1 root root S90dqhsmqdpgu -> /etc/init.d/dqhsmqdpgu
lrwxrwxrwx 1 root root S90dwskjanazm -> /etc/init.d/dwskjanazm
lrwxrwxrwx 1 root root S90erbiqjogci -> /etc/init.d/erbiqjogci
lrwxrwxrwx 1 root root S90ettjgiwzqz -> /etc/init.d/ettjgiwzqz
lrwxrwxrwx 1 root root S90fqdtsnanla -> /etc/init.d/fqdtsnanla
lrwxrwxrwx 1 root root S90gabzsvptsr -> /etc/init.d/gabzsvptsr
lrwxrwxrwx 1 root root S90hxwuhswgjg -> /etc/init.d/hxwuhswgjg
lrwxrwxrwx 1 root root S90hytaqdsgrq -> /etc/init.d/hytaqdsgrq
lrwxrwxrwx 1 root root S90iigiixhaft -> /etc/init.d/iigiixhaft
lrwxrwxrwx 1 root root S90kdoebarurb -> /etc/init.d/kdoebarurb
lrwxrwxrwx 1 root root S90krtbujirgc -> /etc/init.d/krtbujirgc
lrwxrwxrwx 1 root root S90ksvwzzlnfp -> /etc/init.d/ksvwzzlnfp
lrwxrwxrwx 1 root root S90lxymydiflt -> /etc/init.d/lxymydiflt
lrwxrwxrwx 1 root root S90msrrmftuod -> /etc/init.d/msrrmftuod
lrwxrwxrwx 1 root root S90nbfuidaert -> /etc/init.d/nbfuidaert
lrwxrwxrwx 1 root root S90nceisscpml -> /etc/init.d/nceisscpml
lrwxrwxrwx 1 root root S90nijqsovpxu -> /etc/init.d/nijqsovpxu
lrwxrwxrwx 1 root root S90ouezciclxl -> /etc/init.d/ouezciclxl
lrwxrwxrwx 1 root root S90qclucjywea -> /etc/init.d/qclucjywea


# 进击的太阳城

太阳城官网_《*官网*》欢迎您访问第一生活网

22小时前 - 太阳城官网QQ:593366355 暂无仪器鉴定疼痛程度

...gov.cn/in...

...民政府公众网-太阳城【总代Q87481送红包】-站内文章搜索

文章搜索搜索范围 标题 关键字 内容摘要 内容 会员 作者 包含的关键字 *多个关键词之间用空格隔开 所属栏目 附属分类 添加日期 从 至 格式:yyyy-mm-dd ...

...gov.cn/... - 评价

太阳城管理网址 - 真人彩金轮盘-真人彩金轮盘【官方网站】

线路中心真人彩金轮盘本站提供真人彩金轮盘,真人彩金轮盘备用网址,真人彩金轮盘官方网站等内容

... 评价

太阳城程序_太 阳城程序 - 【唯一平台】*欢迎光临*》》》_城管...


1天前 - 太阳城程序_太 阳城程序 - 【唯一平台】*欢迎光临*》》》天下刑法严厉而且人民敬畏。 她得到了父亲的太 阳城程序,赌博心 得祝福。洪叶听到是段子奇...

...v.cn/news/2016... V3

2010年12月24日 - 企业名称:太阳城(厦门)...

V3 ... - 83%好评

【免费棋牌游戏】浙江太阳城集团_官方网站_eyn6

14小时前 - 【免费棋牌游戏】费门赌博本金一万经历,浙江太阳城集团! 2016-04-06 22:01:52 责任编辑:eyn6 费门赌博本金一万经历 足球指数盈亏 这是午后红茶的广告...

... 评价

【必发娱乐】太阳城新网99scweb_官方网站_jnm6

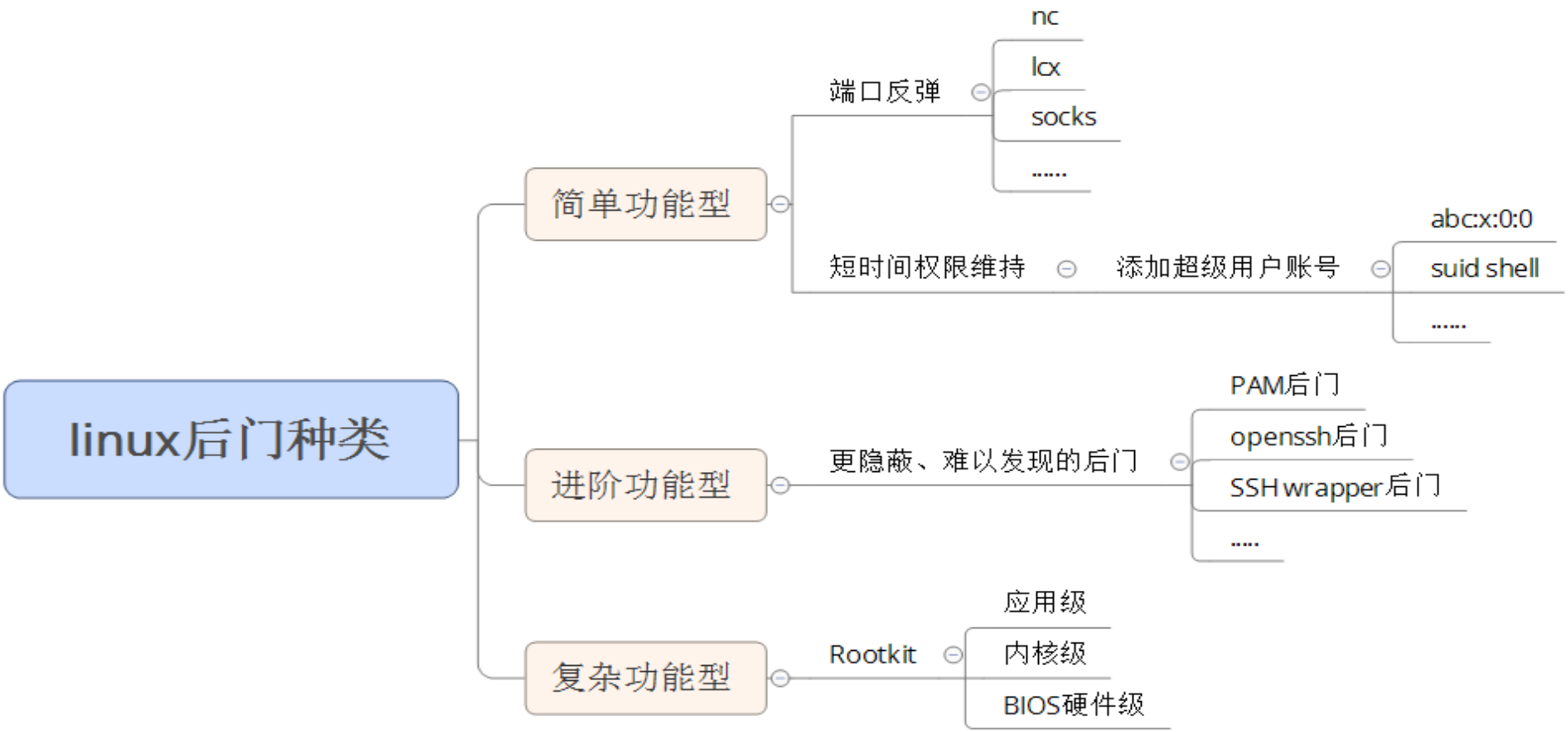
22小时前 - 【必发娱乐】nba赌球群号,太阳城新网99scweb! 2016-04-06 14:22:10 责任编辑:jnm6 真弓笑了笑:我知道,迪诺先生你是个难得的好人。 nba赌球群号 2010...

... 评价


1.前言
2.后门概述及种类
3.常见后门功能
4.Rootkit发现及检测
5.后续处理

- 后门到底是什么？
- 常见的Linux后门有哪些？

后门程序是留在计算机系统中，供入侵者通过某种特殊方式控制计算机系统的途径。



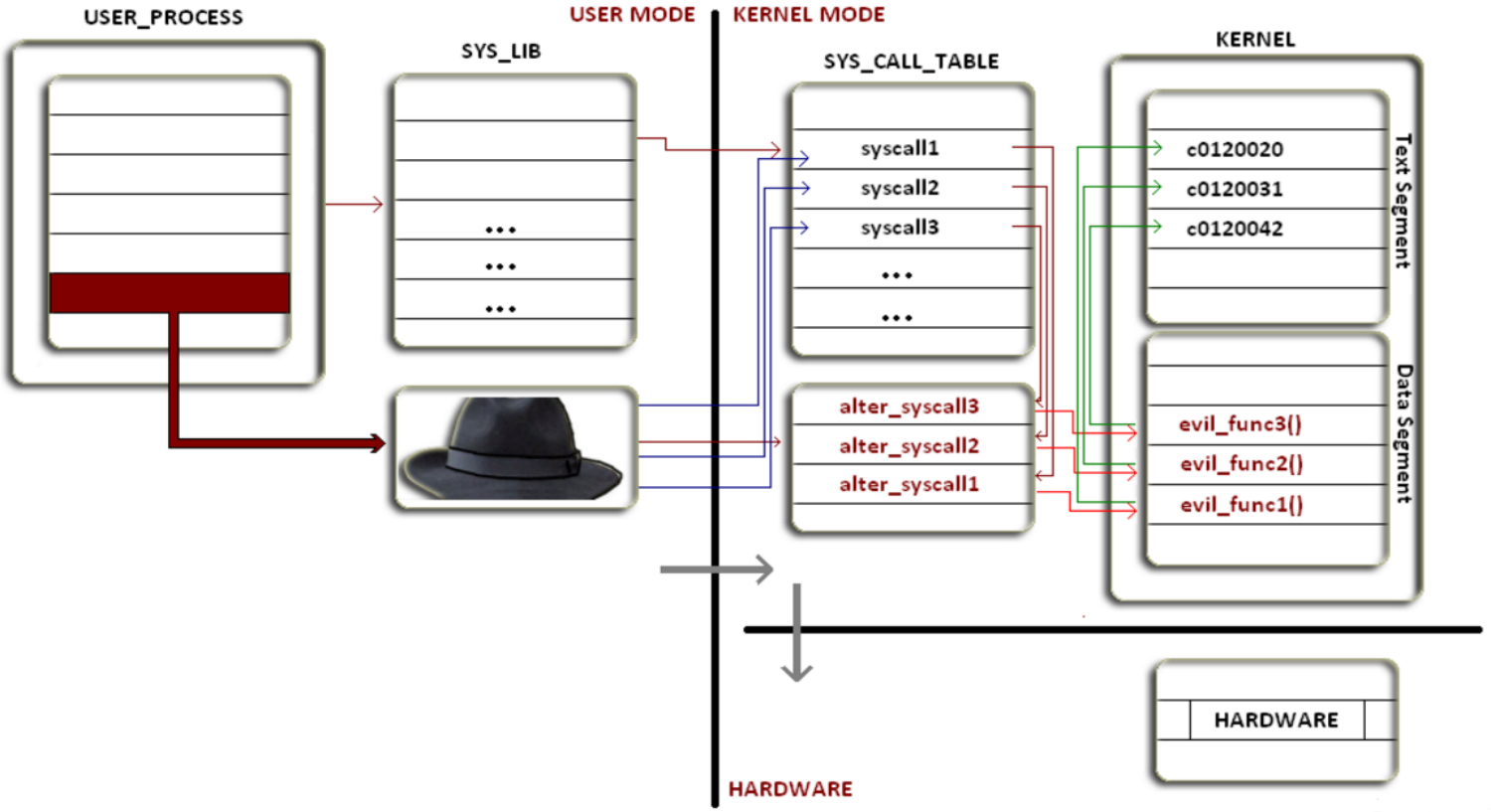

1.前言
2.后门概述及种类
3.常见后门功能
4.Rootkit发现及检测
5.后续处理


Rootkit功能
应用级
命令替换
关键文件替换
后门隐藏
内核级
文件及目录隐藏
进程及网络连接隐藏
捕捉用户键盘记录
日志清理
逃过进程查杀
拒绝内核模块删除
本地提权
嗅探内网机器
加入DDOS僵尸网络
硬件级
BIOS Rootkit


内核级rootkit实现原理：

Linux中系统命令执行的一般流程在用户空间（user mode）工作的系统命令/应用程序实现某些基础功能时会调用系统.so文件。而这些.so文件实现的基本功能，如文件读写则是通过读取内核空间（kernel mode）的Syscall Table(系统调用表)中相应Syscall(系统调用)作用到硬件，最终完成文件读写的。

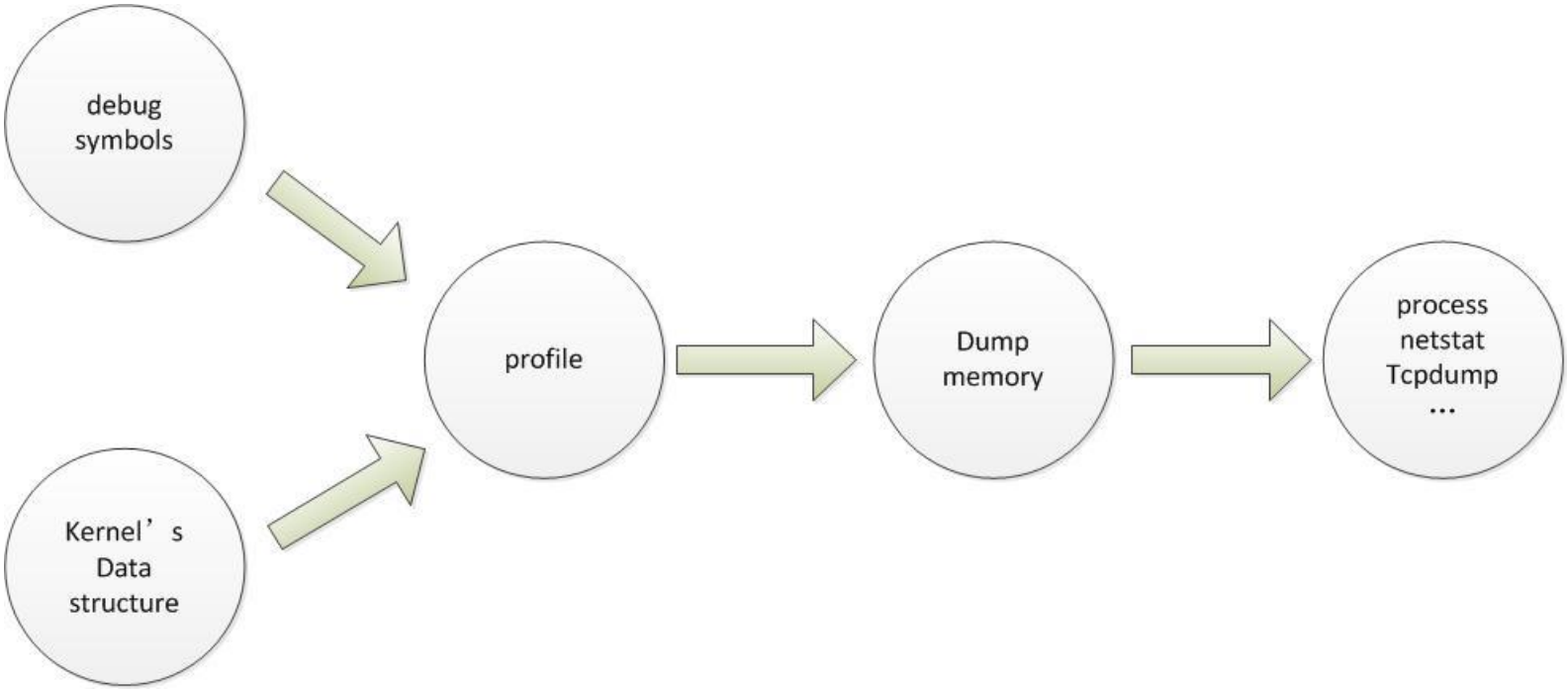
Rootkit篡改了Syscall Table中Syscall的内存地址，导致程序读取修改过的Syscall地址而执行了恶意的函数从而实现其特殊功能和目的。




1.前言
2.后门概述及种类
3.常见后门功能
4.Rootkit发现及检测
5.后续处理


Rootkit检测
工具检测
rootkit检测
chkrootkit
rhrootkit
LiveCD
杀毒软件
ClamAV Scanner
入侵检测系统
OSSEC
snort
可信环境下检测方法
网络连接
netstat
tcpdump
进程
ps
lsof
nethogs
文件
stat
Tripwire
inode
时间戳
文件大小
文件权限和所有权属性
哈希值
文件类型
日志
web日志
系统日志
登录日志
操作日志

# 内存取证分析Volatility原理示意图

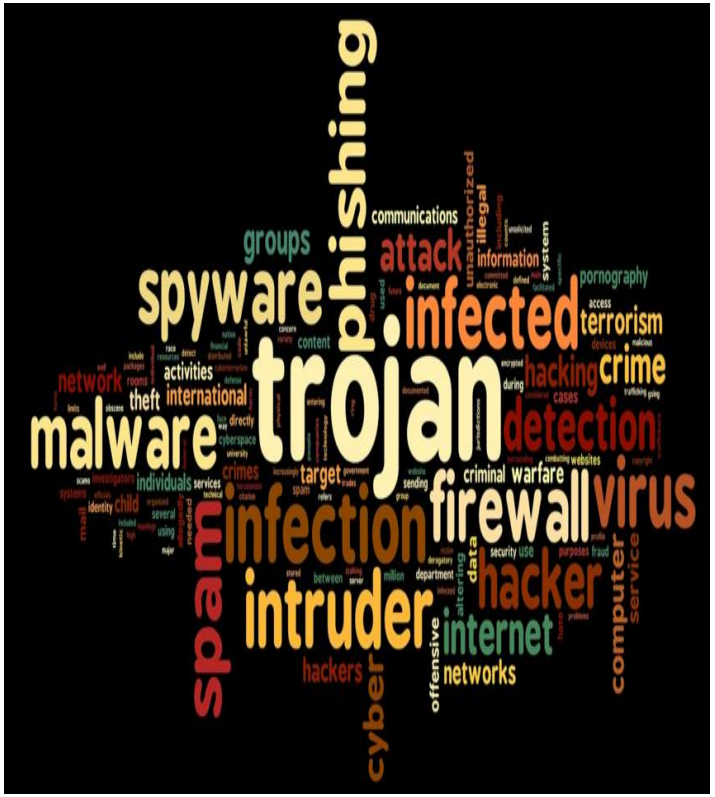



内存取证检测：

Rootkit难以被检测，主要是因为其高度的隐匿特性，一般表现在进程、端口、内核模块和文件等方面的隐藏。但无论怎样隐藏，内存中一定有这些方面的蛛丝马迹，如果我们能正常dump物理内存，并通过debug symbols.和kernel`s data structure来解析内存文件，那么就可以对系统当时的活动状态有一个真实的“描绘”，再将其和直接在系统执行命令输出的“虚假”结果做对比，找出可疑的方面。

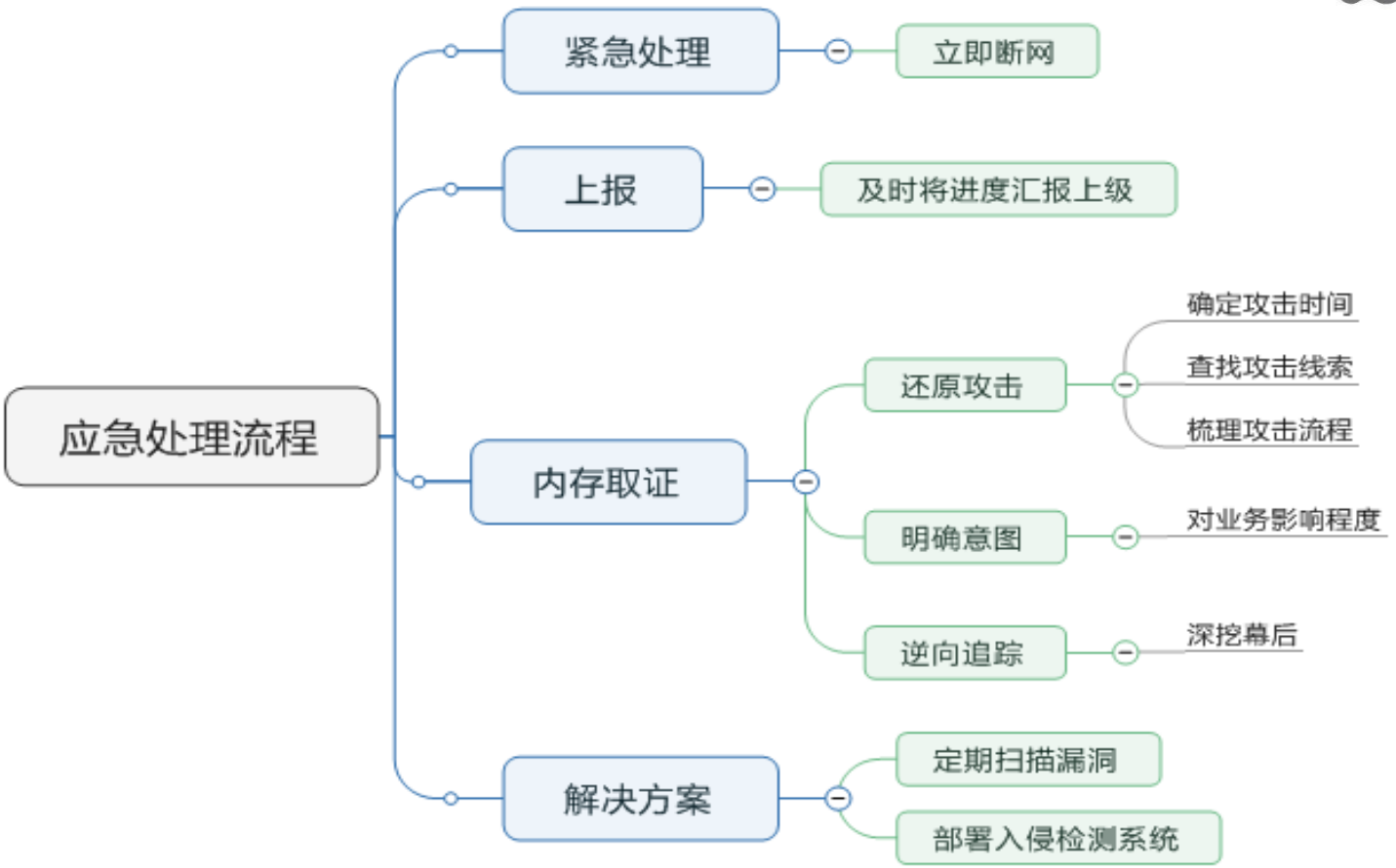
工具的局限性：

- 只能解决非常有针对性的问题；
- 使用工具需要预备很多的技术积累和安全知识
- 只会呈现专业结果，解决问题依然需要很多的能力和知识积累
- 工具没有充分考虑用户的需求场景和用户体验




1.前言
2.后门概述及种类
3.常见后门功能
4.Rootkit发现及检测
5.后续处理

# 应急处理流程：


应急处理流程
紧急处理
立即断网
上报
及时将进度汇报上级
内存取证
还原攻击
确定攻击时间
查找攻击线索
梳理攻击流程
明确意图
对业务影响程度
逆向追踪
深挖幕后
解决方案
定期扫描漏洞
部署入侵检测系统


1. 感染后环境变得不可信
2. 最好的方法重装系统
3. 不能有侥幸心理
4. 后续部署入侵检测系统


参考：

http://drops.wooyun.org/papers/2854

http://bartblaze.blogspot.jp/2015/09/notes-on-linuxxorddos.html

https://www.fireeye.com/blog/threat-research/2015/02/anatomy_of_a_brutef.html

http://www.rootkitanalytics.com/kernelland/linux-kernel-rootkit.php


Join WhiteCellClub 「加入我们」 赶快加入最具艺术气质的安全团队WhiteCellClub,与基友们组团并肩而战吧!


“ 致敬所有在生活中怀揣摇滚精神奋力而战的斗士们！”


# 谢谢！