0.拿到mfc工程，先看Resource就是那些图形，结合其运行功能，双击控件一个个查看代码来理解。还要清楚大致有哪几个类。

1.log文件默认是位于：C:\Windows\System32\winevt\Logs下面。还有事件查看器可以查看事件日志。可以使用控制面板-》事件查看器查看。其中选中具体条目，右键属性中就能够清除日志。

学习网站：iverson5.lofter.com/post/1cc66689\_54e6035

默认下，通过“\\IP\盘符$”形式访问是不记录的？通过web之类的访问是在服务器上有记录的

2.默认下guest账户是被禁用的。

3.我把后缀名直接改成bmp，用WinHex查看发现内容完全没有变，包括文件头。我用在线的jpg转bmp，渣的一逼，能打开查看但是mfc中使用有问题，后来知道画图软件直接另存为转化，这个倒可以正常使用。简单地改后缀名只是简单地改后缀名。

5.IPC$:

IPC$(Internet Process Connection)是共享"命名管道"的资源，它是为了让进程间通信而开放的命名管道，通过提供可信任的用户名和口令，连接双方可以建立安全的通道并以此通道进行加密数据的交换，从而实现对远程计算机的访问。因为IPC是进程间通信。

　　以下是空会话中能够使用的一些具体命令：

　　1 首先先建立一个空连接（当然，这需要目标开放ipc$）

　　命令：net use \\ip\ipc$ "" /user:"" 空用户名和空密码

　　注意：上面的命令包括四个空格，net与use中间有一个空格，use后面一个，密码左右各一个空格。

　　2 查看远程主机的共享资源

　　命令：net view \\ip

　　解释：前提是建立了空连接后，用此命令可以查看远程主机的共享资源，如果它开了共享，可以得到如下面的结果，但此命令不能显示默认共享。

　　命令成功完成。

　　3 查看远程主机的当前时间

　　命令： net time \\ip

　　解释：用此命令可以得到一个远程主机的当前时间。

在 Windows NT 4.0 中是使用挑战响应协议与远程机器建立一个安全会话的，建立成功的会话将成为一个安全隧道，建立双方通过它互通信息，这个过程的大致顺序如下：

1 ）会话请求者（客户）向会话接收者（服务器）传送一个数据包，请求安全隧道的建立；

2 ）服务器产生一个随机的 64 位数（实现challenge）传送回客户；

3 ）客户取得这个由服务器产生的 64 位数，用试图建立会话的帐号的口令打乱它，将结果返回到服务器（实现响应）；

4 ）服务器接受响应后发送给本地安全验证（ LSA ）， LSA 通过使用该用户正确的口令来核实响应以便确认请求者身份。如果请求者的帐号是服务器的本地帐号，核实本地发生；如果请求的帐号是一个域的帐号，响应传送到域控制器去核实。当对挑战的响应核实为正确后，一个访问令牌产生，然后传送给客户。客户使用这个访问令牌连接到服务器上的资源直到建立的会话被终止。

可以知道，这是对称加密

空会话是在没有信任的情况下与服务器建立的会话（即未提供用户名与密码），但根据 WIN2000 的访问控制模型，空会话的建立同样需要提供一个令牌，可是空会话在建立过程中并没有经过用户信息的认证，所以这个令牌中不包含用户信息，因此，这个会话不能让系统间发送加密信息，但这并不表示空会话的令牌中不包含安全标识符SID （SSID它标识了用户和所属组），对于一个空会话， LSA 提供的令牌的 SID 是 S- 1-5-7 ，这就是空会话的 SID ，用户名是： ANONYMOUS LOGON （这个用户名是可以在用户列表中看到的，但是是不能在 SAM 数据库中找到，属于系统内置的帐号），这个访问令牌包含下面伪装的组：

Everyone

Network

在安全策略的限制下，这个空会话将被授权访问到上面两个组有权访问到的一切信息。

SMB:(Server Message Block) Windows 协议族，用于文件打印共享的服务；

NBT:(NETBios Over TCP/IP) 使用 137 （ UDP ） 138 （ UDP ） 139 （ TCP ）端口实现基于 TCP/IP 协议的 NETBIOS网络互联。

在 WindowsNT 中 SMB 基于 NBT 实现，即使用 139 （ TCP ）端口；而在 Windows2000 中， SMB 除了基于 NBT 实现，还可以直接通过 445 端口实现。

ipc$ 连接成功只能说明对方打开了 ipc$ 共享，并不能说明默认共享一定存在。 ipc$ 共享与默认共享是 两码 事， ipc$ 共享是一个命名管道，并不是哪个实际的文件夹，而默认共享却是实实在在的共享文件夹；普通共享是我们自己开启的可以设置权限的共享文件夹。

6.在bat文件里面可以有自删除命令，可以知道只要一向cmd输出完命令这个进程就关闭了，然后cmd调用del程序删除bat文件。

7.这个会直接把电脑卡死，一开始能做的只有动动鼠标，因为cmd一下子开了

start cmd其实单单用start或者cmd与命令行中也会开启一个新的命令行，但是这样就会使%0无效

%0

8.bat还可以执行一些语句，bat处理的是win32程序，不信你双击一个空的bat文件看报错

for /l %%i in (1,1,5) do start cmd这个是用dor循环开启5个cmd

解读这里的for循环：括号里面分别是起始值，每次增加值，终止值

for /r /d %a in (\*) do copy test.txt "%a" /y复制一个文件的磁盘的每个子文件夹当中：

for /l %a in (1,0,2) do net send 192.168.2.25 “Hi！"不停地执行同一条命令：

9.winlogon.exe就是按了Ctrl+Alt+Delete那个界面，管理着用户的登录与退出

ntsd -c q -pn winlogon.exe导致蓝屏

csrss.exe是windows最为核心的进程之一，负责图形管理。有的win7系统怎么有两个这个，看样子不像中毒，我是只有一个，我有两个估计就是中了。

ntsd -c q -pn csrss.exe导致死机

不过在我的win7系统上说：'ntsd' 不是内部或外部命令，也不是可运行的程序或批处理文件。那么就可以使用tasklist去杀，不知道是否要使用强制/f。

ntsd -c q -pn从Windows 2000就开始被附随在System32目录下。它能够结束除System、smss.exe、csrss.exe及各种rootkit程序外所有的程序。但在Windows Vista及以上版本的Windows中是不含ntsd的，[1] 必须手动下载至电脑中才可使用。

10.del命令对目录无效，所以要删除除了目录的所有文件：

del \* /s /q /f 虽然强制模式但是没有/q还是会有询问是否确认删除

11.按住Alt输入（必须以小键盘输入）10是换行，13是回车，160似乎是Alt的效果不过不能作为文件名。

12.文件名、目录名不能含有?、/等字符

13.3389是远程控制端口

14.让文件与硬件设备相关这时候文件不能删除，只有先去掉对应的硬件设备才可以删除。不知道linux下是不是也会这样？

15.我下载到U盘有一次就变成了先下载到电脑再传输到U盘。这应该是特例吧，用的是xp系统，网卡是可以与接口直接交互的。

16..msu是下过来的补丁的后缀名，双击直接安装

17.记事本的管理员打开，在打开要打开的文件。

18/If, by "the console" you mean a command prompt window ... whatever you set there

is only in effect for that process .. it is not global to the system, and is not

persistent to another process.

XX说：控制台是个即使命令窗口，在它里面的设置只是会对它影响，不会起到系统性的全局作用。

19.环境变量里面有PATHEXT，是默认后缀名。

20.替换dll文件，由于需要的权限是最高的信任安装者，其余的三个（管理员，用户，系统）都只是所以要右键，管理员取得所有权。

21.按住那个下VMware下面那条工具栏就变得好看了，不是win7Basic那种色调了

22.

mciSendString("set cdaudio door open", NULL, NULL, NULL);

mciSendString("set cdaudio door closed", NULL, NULL, NULL);

23.ping不通并不代表不能联系，因为可能是防火墙将ping包拦。

24.除了一般的磁盘文件格式外，还有管道、邮槽甚至是设备对象，在windows下也被当作文件来对待

25.大部分windows下的程序是基于消息机制的，而命令行下的不是消息机制的。

26.记事本程序的名字都是“文件名-记事本”，如果没有文件名，那就是“无标题-记事本”。

27.窗口程序都是消息机制的。没窗口自然就不是了。

28.Dos是单任务操作系统，所以在执行一个进程的时候会把控制权交出去。但是windows是多任务操作系统，所以他不能把控制权完全交出去。

29.鼠标右键加滚轮相当于Ctrl加滚轮，可以放大和缩小。

30.由于各种软件为了满足自身不同的需求，对注册表的信息进行读写，导致注册表存在了大量的冗余数据。

31.注册表五个

1、HKEY\_CURRENT\_USER

包含当前登录用户的配置信息的根目录。用户文件夹、屏幕颜色和“控制面板”设置均存储在此处。该信息被称为用户配置文件。

2、HKEY\_USERS

根键HKEY\_USERS根键包括默认用户的信息（Default子键）和所有以前登录用户的信息。。HKEY\_CURRENT\_USER 是 HKEY\_USERS 的子项。主要由.DEFAULT子项构成，新用户根据默认用户.DEFAULT子项的配置信息来生成自己配置文件，该配置文件包括环境、屏幕、声音等多种信息。信息。360SandBox注册在这里。

3、HKEY\_LOCAL\_MACHINE

此根键包含了当前计算机的配置数据，包括所安装的硬件以及软件的设置。这些信息是为所有的用户登录系统服务的。它是整个注册表中最庞大也是最重要的根键：

4、HKEY\_CLASSES\_ROOT

是HKEY\_LOCAL\_MACHINE\Software的子项。此处存储的信息可以确保当使用Windows 资源管理器打开文件时，将打开正确的程序。

HKEY\_CLASSES\_ROOT下的子项可分为两类：一类是已经注册的各类文件的扩展名，这类子项都是以“.”加上扩展名命名的；另一类是各种文件类型的有关信息，这类子项是以字母开头的。

5、HKEY\_CURRENT\_CONFIG

包含本地计算机在系统启动时所用的硬件配置文件信息，实际上是从两个注册表项创建而来的，即HKEY\_LOCAL\_MACHINE\System和HKEY\_LOCAL\_MACHINE\Software。因为此子树是动态创建的，因此修改它的内容没有什么实际意义。带CURRENT的都是动态创建的。确实是software和system，但是并不是说这两个和那两个就是完全一样的，HKEY\_\_CURRENT\_CONFIG\Software反而十分简洁，就一个键值项。

32.windows预装的，在注册表HKEY\_LOCAL\_MACHINE\Software\Microsoft\下，比如说IE主页的保存在它下面的Internet Explorer\Main。禁止磁盘驱动器自动运行的AutoRun功能所在注册表的HKEY\_CURRENT\_USER（HKEY\_CURRENT\_CONFIG下只有System和Software，不可能在这个里面了）\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer下的NoDriveTypeAutoRun。在HKEY\_LOCAL\_MACHINE下的windows这个系统子项下面还有Run用于设置自启项。

33.在本地策略组里面，用户配置->系统，在右边可以设置“只运行指定的Windows应用程序”、“只运行指定的Windows应用程序”、“Windows自动更新”也可在这里、“阻止访问注册表编辑工具”、“自定义用户界面”、“登录时不显示欢迎”。

运行“Regedit”打开注册表编辑器，展开HKEY\_CURRENT\_USER＼Software＼Microsoft＼Windows＼CurrentVersion＼Policies＼Explorer分支(如果没有就新建)，在右侧窗格中单击鼠标右键，选择“新建→Dword值”，输入子项名称“RestrictRun”，然后双击该项，在弹出的“编辑Dword值”对话框中输入键值“1”，确定后退出。 关闭注册表编辑器，重新登录系统，这时绝大部分程序已经被限制运行了，如果你想要打开某个程序时，会弹出一个警告窗口“本次操作由于这台计算机的限制而被取消。请与您的系统管理员联系”

不过，一旦运行就会说“本次操作由于这台计算机的限制而被取消”，这样一搜可能就会解决。所以要关闭错误提醒，还可以换上自己的言语。

33.SAM文件是windows的用户账户数据库,所有用户的登录名及口令等相关信息都会保存在这个文件中。SAM文件可以认为类似于unix系统中的passwd文件,不过没有unix的passwd文件那么直观，当我们忘记密码的时候，就可以通过删除SAM文件，快速地进入系统。

WinXP的SAM文件位于C:\Windows/system32/config/下，如果SAM文件损坏或丢失了，WinXP中的所有帐号就会丢失，而且还无法通过WinXP登录界面。要恢复SAM文件，你可以把Win XP安装光盘上的sam文件（H:\windows\repair\sam）复制到C:\Windows/system32/config/下即可。即打开命令行模式，输入copy H:\windows\repair\sam C:\windows\system32\config\sam回车，就大功告成了。

除了在C:\Windows\system32\config\下有，还有就是C:\Windows\system32\config\RegBack\这个应该是备份存储

34.

空连接就是不用密码和用户名的IPC连接，在Windows 下，它是用 Net 命令来实现的． 　进入空连接 net use \\IP地址"密码" /user:"用户名" 　禁止空连接 开始-设置-控制面板-管理工具-服务 ，在服务中停止掉 server的服务就可以了。空连接就是空用户名与空密码的不信任连接

IPC$(Internet Process Connection) 是共享 " 命名管道 " 的资源，它是为了让进程间通信而开放的命名管道，通过提供可信任的用户名和口令，连接双方可以建立安全的通道并以此通道进行加密数据的交换，从而实现对远程计算机的访问。 IPC$ 是 NT/2000 的一项新功能，它有一个特点，即在同一时间内，两个 IP 之间只允许建立一个连接。 NT/2000 在提供了 ipc$ 功能的同时，在初次安装系统时还打开了默认共享，即所有的逻辑共享 (c$,d$,e$ …… ) 和系统目录 winnt 或 windows(admin$) 共享。所有的这些，微软的初衷都是为了方便管理员的管理，但在有意无意中，导致了系统安全性的降低。

1 ）会话请求者（客户）向会话接收者（服务器）传送一个数据包，请求安全隧道的建立；

2 ）服务器产生一个随机的 64 位数（实现挑战）传送回客户；

3 ）客户取得这个由服务器产生的 64 位数，用试图建立会话的帐号的口令打乱它，将结果返回到服务器（实现响应）；

4 ）服务器接受响应后发送给本地安全验证（ LSA ）， LSA 通过使用该用户正确的口令来核实响应以便确认请求者身份。如果请求者的帐号是服务器的本地帐号，核实本地发生；如果请求的帐号是一个域的帐号，响应传送到域控制器去核实。当对挑战的响应核实为正确后，一个访问令牌产生，然后传送给客户。客户使用这个访问令牌连接到服务器上的资源直到建立的会话被终止。

以上是一个安全会话建立的大致过程，那么空会话又如何呢？

空会话是在没有信任的情况下与服务器建立的会话（即未提供用户名与密码），但根据 WIN2000 的访问控制模型，空会话的建立同样需要提供一个令牌，可是空会话在建立过程中并没有经过用户信息的认证，所以这个令牌中不包含用户信息，因此，这个会话不能让系统间发送加密信息，但这并不表示空会话的令牌中不包含安全标识符SID （它标识了用户和所属组），对于一个空会话， LSA 提供的令牌的 SID 是 S- 1-5-7 ，这就是空会话的 SID ，用户名是： ANONYMOUS LOGON （这个用户名是可以在用户列表中看到的，但是是不能在 SAM 数据库中找到，属于系统内置的帐号），这个访问令牌包含下面伪装的组：

Everyone

Network

在安全策略的限制下，这个空会话将被授权访问到上面两个组有权访问到的一切信息。

在 Windows 2000 和以后版本中默认只有管理员和备份操作员有权从网络访问到注册表，而且实现起来也不方便，需借助工具。

这种非信任会话并没有多大的用处，但从一次完整的 ipc$ 入侵来看，空会话是一个不可缺少的跳板，因为我们从它那里可以得到用户列表，而大多数弱口令扫描工具就是利用这个用户列表来进行口令猜解的，成功的导出用户列表大大增加了猜解的成功率

35.

36.txt文件：

txt“文件头”（可以使用readfile获取）（不能算是文件头，只能算是编码）

txt文件的文件头跟编码有关。这个

ANSI没有文件头

Unicode文件头为0xFEFF

Unicode big endian 文件头为 0xFFFE（我电脑上txt另存为里面就是这种）(BIG ENDIAN：最低位地址存放高位字节，可称高位优先，内存从最低地址开始按顺序存放（高数位数字先写）。最高位字节放最前面。LITTLE ENDIAN：最低位地址存放低位字节，可称低位优先，内存从最低地址开始按顺序存放（低数位数字先写）。最低位字节放最前面。)

UTF-8 文件头为 0xBFBBEF

看来winhex看到的是一个文件的完整内容了，文件的其他信息是由操作系统的某个对象进行管理。

37.命令行与使用它打开的程序之间并不是子父进程的关系，因为一旦命令行被关闭了，这个进程也会被关闭，除非打开的是服务。更像是调试的关系。

38.当windows的桌面启动的时候，Explorer.exe就会出现在进程列表。windows资源管理器

39.几十Kb的txt占掉了几MB内存，2.3MBrtf占掉了30MB内存。这些文本文件原来占内存都是十分恐怖的。一个浏览器标签页也会占掉几十MB内存。

40.windows的putty和linux的nc客户端有点像。

41.SID也就是安全标识符（Security Identifiers），是标识用户、组和计算机帐户的唯一的号码。在第一次创建该帐户时，将给网络上的每一个帐户发布一个唯一的 SID。如果存在两个同样SID的用户，这两个帐户将被鉴别为同一个帐户，原理上如果帐户无限制增加的时候，会产生同样的SID。

SID在注册表中，最后一个连字符后的数字被称为RID： 第一个000001F4（16进制），换算成十进制是500，说明是系统建立的内置管理员帐号administrator，000001F5换算成10进制是501，也就是GUEST帐号了。自己建立的都是1000开始。 所以通过SID我们可以获取改成任何名字的管理员名字。通过用户的名字就能得到对应的sid，然后自己将sid改成管理员的sid等等。

42.复制与剪切都会把数据放到剪切板里面。

43.使用注册表对可执行文件镜像劫持IFEO。

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\cmd.exe]

"debugger"="explorer.exe"

把cmd.exe劫持为explorer.exe,也就是不让cmd.exe运行。

reg add "hklm\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\cmd.exe" /f

reg add "hklm\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\cmd.exe" /v debugger /d explorer.exe /f

44.你需要一个 admin 权限的 shell ，比如 telnet ，木马， cmd 重定向等

45.在 xp 的默认安全选项中，任何远程访问仅被赋予来宾权限，也就是说即使你是用管理员帐户和密码，你所得到的权限也只是 Guest ，因此大部分操作都会因为权限不够而失败，而且到目前为止并没有一个好的办法来突破这一限制。所以如果你真的得到了 xp 的管理员密码，我建议你尽量避开 ipc 管道

46.NetBIOS是Network Basic Input/Output System的简称，一般指用于局域网通信的一套API。在Windows操作系统中，默认情况下在安装TCP/IP协议后会自动安装NetBIOS。

47.PentestBox由印度人开发，运行在windows下的渗透测试环境

48.打开

inetmgr IIS

mstsc 远程桌面

dxdiag DirectX修复工具，但是可以看到系统具体版本什么的信息。

49.windows里面应该是..\，win10里面../是没有用的。

50.一直有stdout输出到shell界面，我选中一块地方，就停止显示了。不过之后右键一下就继续了。

51.windows XP里面桌面在C:\Documents and Settings\Administrator下的“桌面”，中文版xp必须用中文。

52.控制面板-》本地安全策略-》IP安全策略。首先创建一个筛选目标（IP筛选器），再在管理筛选器里面对其进行操作。我的意思就是介绍一下windows7里面就有IP筛选器这个东西，类似于iptables。

53.由STSTEM用户创建的进程都是系统进程。

csrss.exe 处理图形相关任务

explorer.exe windows资源管理器（windows图形界面外壳程序）。结束后会看不到任务栏与桌面等。可以被新建。重载explorer.exe可以用来安全地卸载U盘（如果一般方式做不到的话）。

lsass.exe 用于windows的安全机制、本地安全和登录策略

services.exe 服务管理进程，被终止之后还会被重启

smss.exe 会话管理器（用户与操作系统之间的会话）

svchost.exe 从dll中运行的服务的通用主机进程名称，所以任务管理器会有一大堆都叫这个的进程。

system 内存页面管理程序

system idle process 在cpu空闲的时候发出指令让它暂停工作以降低温度，在任务管理器里面它的CPU占用率就约是100%减去实际占用率

winlogon.exe 管理用户登录和退出的用户登录程序

54.Windows做DNS解析时有如下步骤：

1.local hosts file - C:\Windows\System32\drivers\etc\hosts

2.DNS

3.NBNS那么当访问者输入一个不存在的域名，而LOCAL HOST FILE、DNS服务器均无法给出解析时，我们可爱又人性化的Windows就会发送NBNS请求进行查询。 NBNS请求它是一个广播包！那么通过回复NBNS响应，从而转移流量进行欺骗（Metasploit，使用nbns\_response模块，然后设置欺骗IP）。NetBios Spoofing利用方法目前来说有两种：HTTP和SMB（SMB通信，如：\\thanks1132124324）。 然后分别使用metasploit的use auxiliary/server/capture/http\_ntlm和use auxiliary/server/capture/smb可以获取hash，通过破解、HASH传递等进一步渗透。

防御：使用高版本的WINDOWS系统，使用高强度的密码，以加大HASH破解难度

55.NetBios入侵：

有扫描器可以扫描出来共享资源，或者可以直接尝试Pqwak 破解密码

NBTSTAT命令可以用来查询涉及到NetBIOS信息的网络机器，这里面有机器用户名（空连接也可以做到）

\\10.0.13.191”（或带C＄，D＄等查看默认共享）这种地址是可以在IE中输入，或者运行中

关闭NetBIOS协议漏洞

1. 解开文件和打印机共享绑定

鼠标右击桌面上[网络邻居]→[属性] →[本地连接] →[属性]，去掉“Microsoft网络的文件和打印机共享”前面的勾，解开文件和打印机共享绑定。这样就会禁止所有从139和445端口来的请求，别人也就看不到本机的共享了。

2. 利用TCP/IP筛选

鼠标右击桌面上[网络邻居] →[属性]→[本地连接] →[属性]，打开“本地连接属性”对话框。选择[Internet协议(TCP/IP)]→[属性]→[高级]→[选项]， 在列表中单击选中“TCP/IP筛选”选项。单击[属性]按钮，选择“只允许”，再单击[添加]按钮(如图2)，填入除了139和445之外要用到的端口。这样别人使用扫描器对139和445两个端口进行扫描时，将不会有任何回应。

3. 使用IPSec安全策略阻止对端口139和445的访问

选择[我的电脑]→[控制面板]→[管理工具]→[本地安全策略]→[IP安全策略，在本地机器]，在这里定义一条阻止任何IP地址从TCP139和TCP445端口访问IP地址的IPSec安全策略规则，这样别人使用扫描器扫描时，本机的139和445两个端口也不会给予任何回应。

4. 停止Server服务

选择[我的电脑]→[控制面板]→[管理工具]→[服务]，进入服务管理器，关闭Server服务。这样虽然不会关闭端口，但可以中止本机对其他机器的服务，当然也就中止了对其他机器的共享。但是关闭了该服务会导致很多相关的服务无法启动，如机器中如果有IIS服务，则不能采用这种方法。

5. 使用防火墙防范攻击

在防火墙中也可以设置阻止其他机器使用本机共享。如在“天网个人防火墙”中，选择一条空规则，设置数据包方向为“接收”，对方IP地址选“任何地址”，协议设定为“TCP”，本地端口设置为“139到139”，对方端口设置为“0到0”，设置标志位为“SYN”，动作设置为“拦截”，最后单击[确定]按钮，并在“自定义IP规则”列表中勾选此规则即可启动拦截139端口攻击了。

55.运行 Windows 的计算机启动时，将执行检查以确定计算机是否已正常关机。 如果计算机未正常关机，则生成内核电源事件 41 消息

56.今天刚重装了台服务器，配站时候遇到了权限问题，多了几个未知帐户，账户名是“未知帐户(S-1-5-21-682003330-2139871995-725345543-500)”。挺惹眼的。于是删除，出现错误提示：【因为未知帐户(S-1-5-21-682003330-2139871995-725345543-500)”从其父系继承权限，您无法删除此对象。要删除“未知帐户(S-1-5-21-682003330-2139871995-725345543-500)”，您必须阻止对象继承权限。只需要在权限的高级设置里面设置好“禁用继承以后就可以删除了”。

57.Windows RT是Windows家族的一个新成员，代表的是ARM下的版本。

58.win10之前的系统都是明显存在漏洞的，不知道你在担心什么！

59.在windows里面services.msc里面服务的依存关系都是可以看到的。

60.在“控制面板”-》“程序和功能”-》“启用或关闭windows功能”中关闭无关功能。

控制面板\所有控制面板项\管理工具-》高级安全 Windows 防火墙 这里面可以详细设置windows 防火墙的入站出站规则

61.win10的终端支持C-v粘贴内容，复制也比win7终端方便（默认选中就是复制）

62.网络右键属性，里面可以控制共享开关。然后指定文件夹，通过文件夹属性-》高级共享，来实现网上邻居的扩展。只能以文件夹为单位进行共享。

63.windows XP与windows Server 2003采用了相同的内核。

64.打开Cmder目录下的config文件夹，里面的aliases文件就是我们可以配置的别名文件，只需将里面ls命令的别名按下列方式修改就可以在ls命令下显示中文。mini版与full版本差别就是是否内建git-for-windows。

“因为这个系统已经停用命令码执行，所以无法载入xxxx”是因為目前 Cmder 預設會啟動 PowerShell 主控台 (Console)，但 Windows 內建的 PowerShell 預設的 ExecutionPolicy 是 AllSigned，也就是任何沒有簽章的 PowerShell 指令檔都是不允許執行的。Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser

通常習慣開啟「命令提示字元」主控台，所以我都會修改 Cmder 的預設值，讓每次開啟 Cmder 都直接進入傳統的「命令提示字元」主控台，其設定方式如下：

按下 Win+Alt+P 開啟選項設定。

切換到 Startup 頁籤，設定 Specified named task 並選取 {cmd} ，然後儲存設定

因為 Cmder 預設將 Ctrl+W 設定為關閉目前主控台，不過我們在 Linux 環境下 Ctrl+W 主要是用來刪除一段文字用的，這功能被拿掉就真的礙手礙腳了，所以建議將此快速鍵關閉。

Win+Alt+P 開啟選項設定。

Alt+F4 ： 關閉所有頁籤

Alt+Shift+1 ： 管理员权限開啟 cmder.exe

Alt+Shift+2 ： 一般权限开启cmder.exe

Alt+Shift+3 ： 開啟 powershell.exe (系統管理員權限)

Ctrl+1 ： 快速切換到第 1 個頁籤 Ctrl + 2 ： 快速切換到第 2 個頁籤

Ctrl+n ： 快速切換到第 n 個頁籤 ( n 值無上限 )

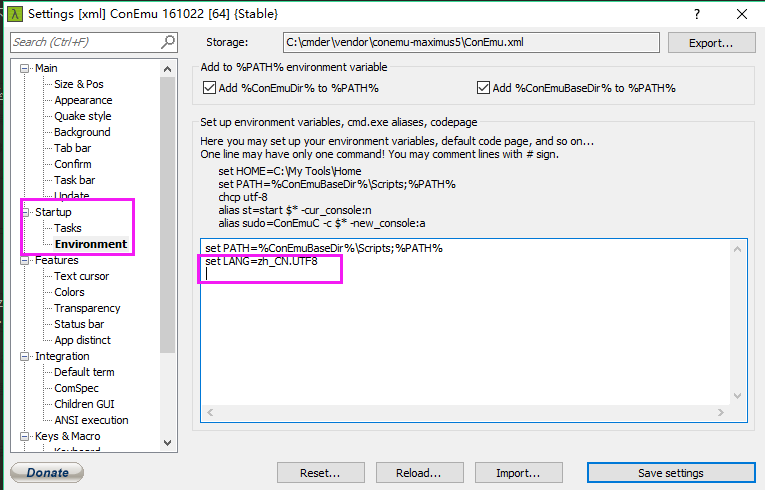
ESC ：清除目前輸入的整行

powershell可执行ls命令（但不支持所有linux命令，比如reset），可以通过ls来查看权限。

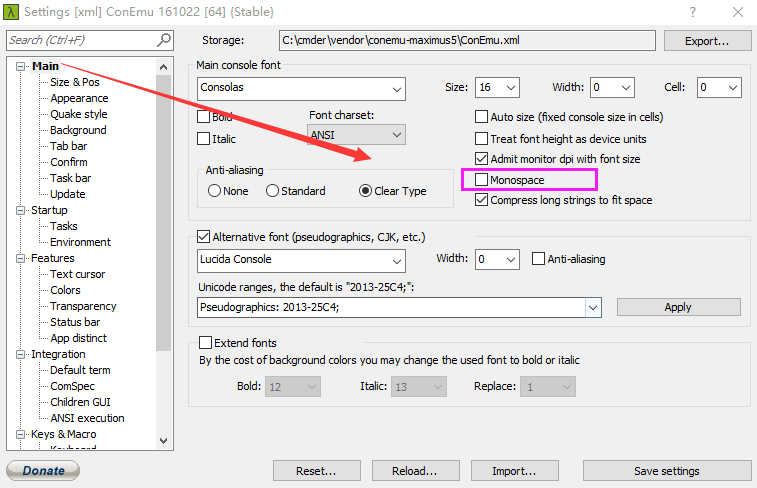
1、Cmder ls目录中文显示编码的问题

 因为没有了 aliases 文件，所以，不能使用原来的方式来的方式来修改中文显示编码的问题

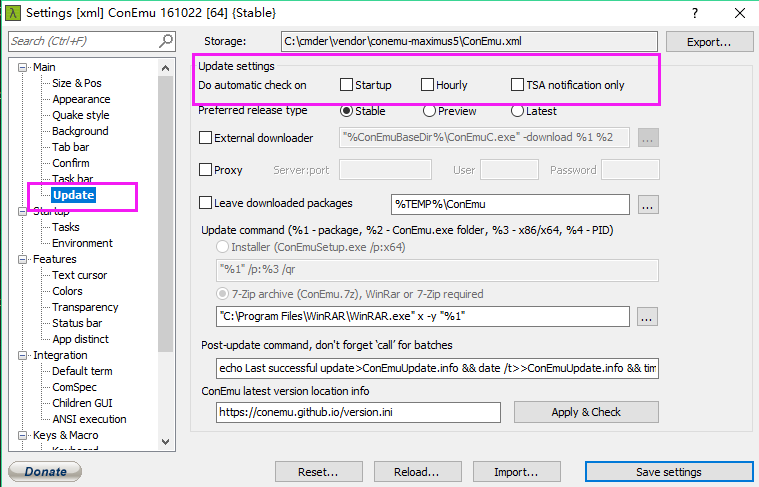
 新版本的设置方法如下图：**[set LANG=zh\_CN.UTF8]**



2、中文文字乱码重叠的问题

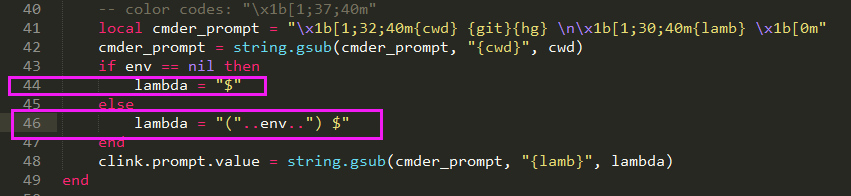


3、关闭启动时自动检查更新



4、修改 **λ**  提示符为 **$**

 修改安装包目录 vendor 下的 **clink.lua** 文件



65.VPN连接

在本地建立一个“连接到我的工作场所”用于拨号或者进行VPN连接的连接。VPN连接还有种功能就是拨这个前可以设置自动拨某个连接，从而连上Internet先。如果使用了VPN却无法访问Internet，那就在属性-》高级里面去掉“在远程网络上使用默认网关”的选项。

开始-》程序-》管理工具-》路由和远程访问 {

需要在服务中禁用“Windows Firewall/Internet Connection Sharing (ICS)”

创建VPN一般上如果服务器只有一个IP，那还要加上NAT。创建的时候选择“自定义配置”，创建之后要在NAT的设置中“新增接口”也就是使用已有的哪个网络适配器来连出去。然后还要在属性上设置接口启用NAT才能成功开启NAT。

设置VPN服务器的属性可以被远程访问，且仅用于局域网路由选择不作为请求拨号路由选择。在属性的日志设置中选不记录任何事件。不过我认为这只是VPN服务器的日志设置，还有系统日志...

}通过上面的步骤已经建立了VPN服务器，最后要做的就是对用户的授权：我的电脑-》管理-》本地用户和组-》用户 给用户可以进行远程访问的权限（拨入或VPN）

66.此电脑-》属性-》远程设置 可以设置是否允许远程协助连接这台计算机。属性里面还有设置性能最强还是效果最强还是windows自己做出选择。

67.

68.很多下载程序会自动修改防火墙从而允许其通过。手动的添加，防火墙点开以后，高级设置或者添加例外

69.目前知道windows的可执行有exe、vbs、dll。开启3389端口除了用注册表隐蔽开启或者软件模拟人的行为开启，还可以通过其他进程，比如SQL数据库就提供了对系统的不少操作。

70. type c:\boot.ini windows2000有这个文件，里面存着操作系统的信息。

71.共享盘上的autorun.inf也会被执行

72.文件夹木马:

自定义文件夹向导-》选择或编辑该文件夹的HTML模板-》

在Folder.htt中设置vbs代码<script language=vbscript>xxx</scipt>

文件夹一旦被打开就会执行脚本

73.

#include "stdafx.h" #include<windows.h> int \_tmain(int argc, \_TCHAR\* argv[])

{

HANDLE hFile =CreateFile(L"a.txt ",GENERIC\_WRITE|GENERIC\_READ, 0, //注意a.txt后有一个空格 NULL, OPEN\_EXISTING, // 打开存在的文件 FILE\_ATTRIBUTE\_NORMAL, NULL); if (hFile ==INVALID\_HANDLE\_VALUE)

{

printf("openfailed!");

} else {

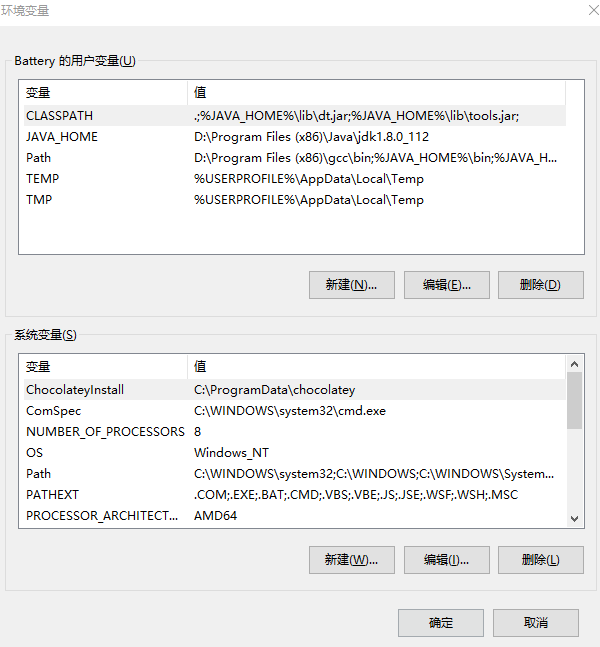
printf("fileopened");

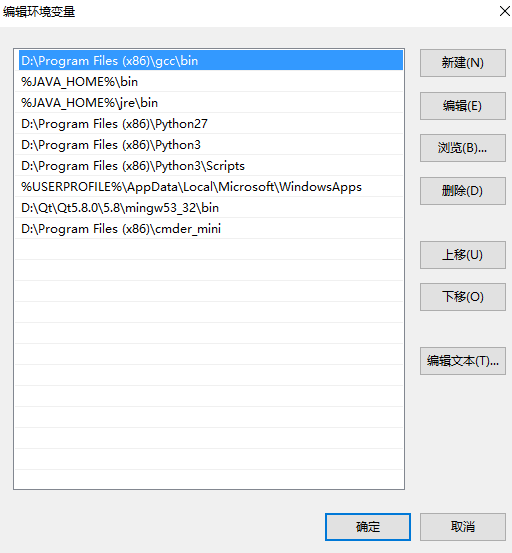
}

CloseHandle(hFile); return 0;

}

通过此代码可知道，即使我们传入参数是”a.txt ”带空格，最后访问到却确是”a.txt”不带空格





74.Windows RT 是移动平台版

75.Windows10的搜索已经支持文本文件的内容搜索了。

76.远程桌面的开启： 还是旗舰版的好

启用Win8/10(中文版/核心版/家庭版)中被阉割的远程桌面服务端 ：

https://github.com/stascorp/rdpwrap/releases

双加install.bat就好，RDPConf查看状态。

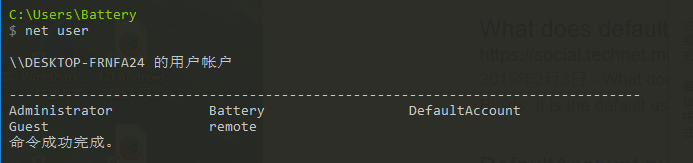
远程桌面协助的开启需要新建一个加入远程桌面用户组的账户。

还需要注意计算机防火墙的阻挡以及此电脑-》属性-》远程设置-》是否允许进行远程协助，远程桌面（允许的用户也在这里进行添加）

PS：Windows10同一时间只允许有一个用户在线，如果其他用户登陆，那么已登录的用户就会被踢（如上图），所以需要通过破解，来达到多用户同时在线的目的。我还没有进行验证。给的方法是安装RDP Wrapper Library，https://github.com/stascorp/rdpwrap/releases 。

提升为管理权限，也不一定能登录远程终端，因为远程终端的登录还需要指定允许的用户。

远程终端日志功能会记录几个操作（登录、消息、、断开、注销等）自己记得根据系统版本百度到方法关了。还要注意，还可能被设置在用户登录的时候执行xxx.bat什么的从而制作自己的日志。管理工具-》终端服务配置…

remote是我自己加的

新建remote账户发现环境变量全部是空的，虽然软件那些都还是存在，这就要重新配置。

windows的任务管理器里面可以看到用户对资源的占用情况从而判断是否有其他用户已经登录。

但是发现有Remote Management Users，没有Remote Desktop Users这个组，我remote没有权限登录，之前我记得此账户中填写[\\xxxx](file:///\\\\xxxx)就可以回到默认设置但是笔记不知道哪里去了，不过还好能直接打字“网络服务”，然后密码为空。

将remote账户加到Remote Management Users组以后开机就会有这个账户选择，登录以后访问的内容完全是一样的就是缺少windows的系统设置比如说环境变量。

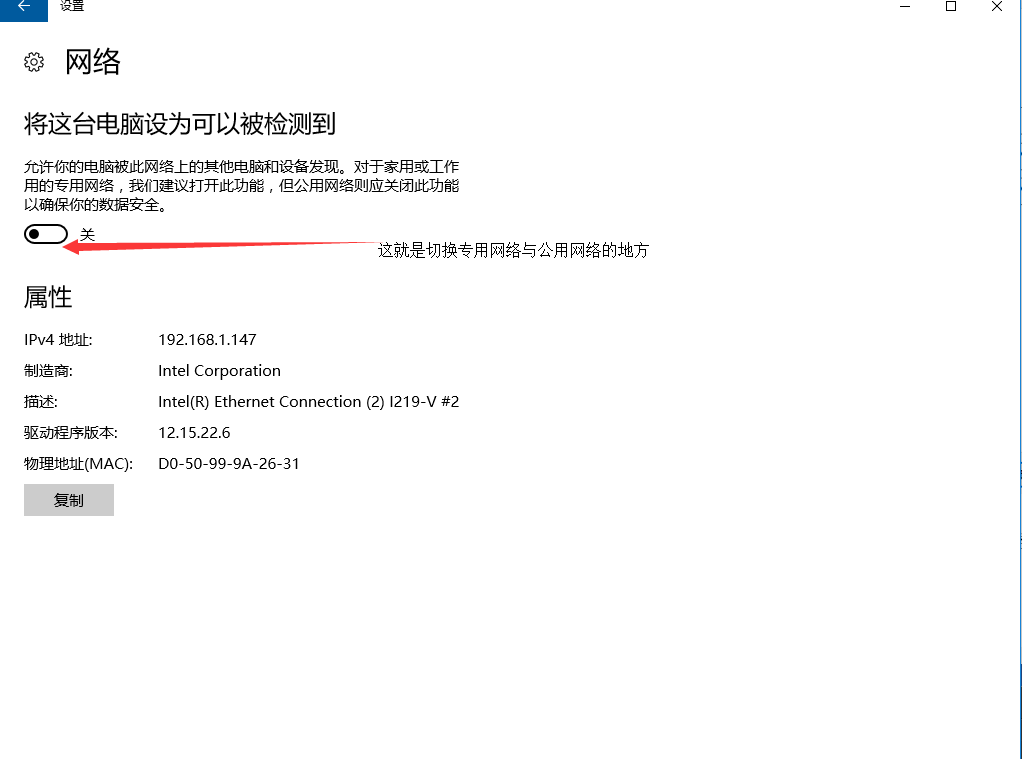


推荐软件：向日葵远程控制，VNC

QQ共享屏幕倒是没问题，但是尝试远程桌面连接就直接拒绝。

如果支持的话，可以修改注册表就能开启远程桌面（包括修改防火墙对RDP的支持），RegSnap可以进行对注册表的快照，然后进行比较。

连接账户可以在用户名后面加上一个@域名。

77、

78. 内存地址：

1.文件偏移地址 (File Offest)  
数据在PE文件中的地址叫文件偏移地址,个人认为叫做文件地址更加准确.这是文件在磁盘上存放时相对文件开头的偏移.  
2.装载地址 (Image Base)  
PE装入内存时的基地址.默认情况下,EXE文件在内存中的基地址是0x00400000,DLL文件是0x10000000.这些位置可以通过修改编译选项更改.  
3.虚拟内存地址 (Virtual Address,VA)  
PE文件中的指令被装入内存后的地址.  
4.相对虚拟地址 (Relative Virtual Address,RVA)  
相对虚拟地址是内存地址相对于映射基质的偏移量.  
虚拟内存地址,映射基质,相对虚拟内存地址三者之间有如下关系.  
VA=Image Base + RVA

PE文件中的数据按照磁盘数据标准存放，以0x200字节为基本单位进行组织。 代码装入内存后，将按照内存数据标准存放，以0x1000字节为基本单位进行组织。

79.PE文件中的数据段：

.data  = writable data   
.rdata =  readonly data

.data当然保存的是数据了。比如程序中的全局变量。在data数据段储存为全局变量或静态数据，在应用程序初始化的时候该段的全部变量归0，有全局静态数据静态数据常量保存。

.rdata有时候会部分保存IAT数据。部分保存的是一些结构。比如MFC程序就有一些vptr相关的信息。.rdata 保存函数指针或是间接调用的虚拟函数指针或虚拟表对象/类指针等，不同的编译器可能对该段有所处理不同吧。传入函数的字符串常量也存储在这里。

.data:00404000 ; Section 2. (virtual address 00004000)

.data:00404000 ; Virtual size : 00000050 ( 80.)

.data:00404000 ; Section size in file : 00000200 ( 512.)

.data:00404000 ; Offset to raw data for section: 00002C00

.data:00404000 ; Flags C0300040: Data Readable Writable

.data:00404000 ; Alignment : 4 bytes

4000是基地址。

.rdata:00405000 ; Section 3. (virtual address 00005000)

.rdata:00405000 ; Virtual size : 00000E48 ( 3656.)

.rdata:00405000 ; Section size in file : 00001000 ( 4096.)

.rdata:00405000 ; Offset to raw data for section: 00002E00

.rdata:00405000 ; Flags 40600040: Data Readable

.rdata:00405000 ; Alignment : 32 bytes

.idata:00408358 ; Imports from Qt5Core.dll

.idata:00408358 ;

.idata:00408358 ; Section 6. (virtual address 00008000)

.idata:00408358 ; Virtual size : 00001C80 ( 7296.)

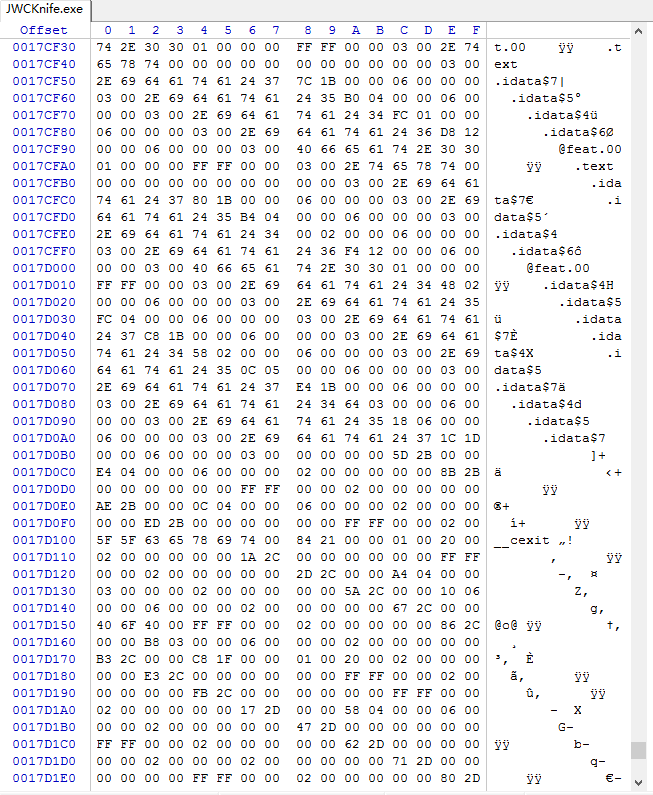
.idata:00408358 ; Section size in file : 00001E00 ( 7680.)

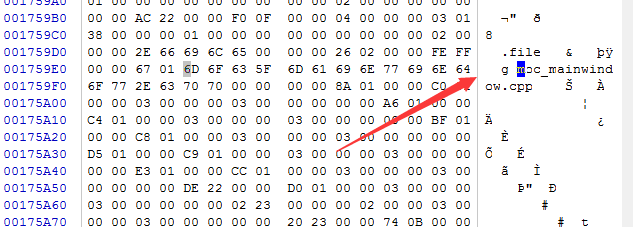
.idata:00408358 ; Offset to raw data for section: 00004C00

.idata:00408358 ; Flags C0300040: Data Readable Writable

.idata:00408358 ; Alignment : 4 bytes

一个某个类函数中局部变量的增加，都会引起全局变量地址的改变。下面的图片是debug模式生成的eexe使用WinHex打开：





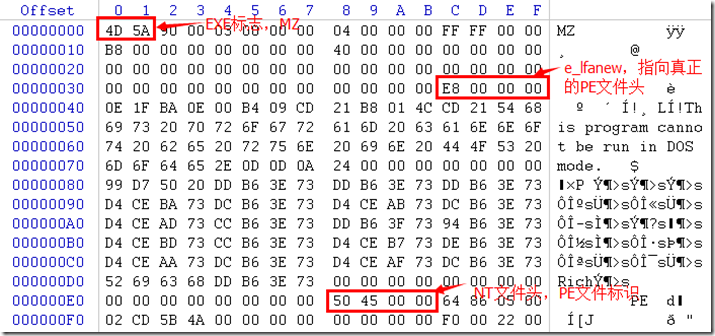
而在文件的最后：



PE：

DOS MZ header 开头两个字必须是MZ。  
DOS Stub “This program cannot run in DOS mode”， 它简单调用中断21h服务9来显示字符串  
PE header  
Section table  
Section 1  
Section 2  
Section...  
Section n

下面是PE文件的文件头：



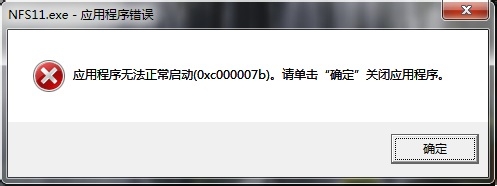
QIODevice 是一个抽象类，所以不能被实例化，是所有IO类的基类。

79、exe文件自我操作的实现：

1.底层硬盘读写

2. 绕过文件不能操作自己的机制

3.调用另一个文件，该文件中有操作自己的代码

80. **也许大家会问了：我玩的游戏都有DirextX 11的特效了，还会和DirectX 9有关系吗？**

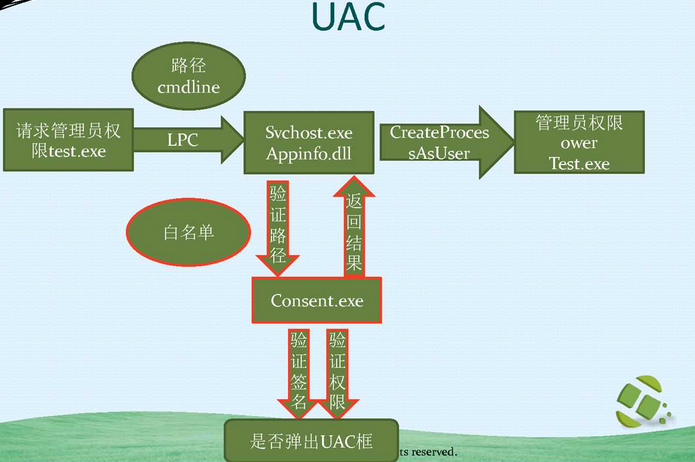
事实上，游戏公司为了游戏的兼容性，往往都是基于DirectX 9.0的API开发游戏，然后加上DirectX 10和DirectX 11的特效，这样的话，不管什么样的显卡都可以玩游戏。也正是如此，DirectX 9.0有问题会影响目前最新的游戏。请大家一定要牢记一点，不管是32位操作系统还是64位操作系统，一定要安装32位版本的DirectX文件，这是关键。

81. UAC（User Access Control）

由于vista在启用uac时貌似平等对待不管是Windows系统的还是第三方应用获得uac权限都要弹框获得用户许可（管理账户登陆以后会有两个令牌，默认是被过滤掉任何特权的令牌，只有当运行的程序被标记为“要求提升权限”，才会使用管理员权限的令牌）。所以在win7上微软启用了白名单机制，对于某些系统应用可以直接获得uac权限：

1. 该可执行文件必须经过 Windows Publisher 的数字签名，Windows Publisher 是用于对 Windows 附带的所有代码进行签名的证书（仅由 Microsoft 进行签名是不够的，因此 Windows 未附带的 Microsoft 软件不包括在内？表示不能理解居然不因为这个不包括在内）；
2. 在程序的manifest文件中申明成类似这个样子的<autoElevate>true</autoElevate>
3. 该可执行文件必须位于其中一个为数不多的“安全”目录中。安全目录是指标准用户无法修改的目录，并且它们包括 %SystemRoot%\System32（例如，\Windows\System32）及其大多数子目录、%SystemRoot%\Ehome，以及 %ProgramFiles% 下的少许目录（其中包括 Windows Defender 和 Windows 日记本）

Windows 系统的一些白名单进程中调用某些 COM 接口(IFileOperation)来实现向受保护的目录复制文件是不会触发 UAC 提示框的。不过最高权限即便是windows自家的程序都会弹出UAC，并不使用白名单机制了，需要使用本地漏洞提权。

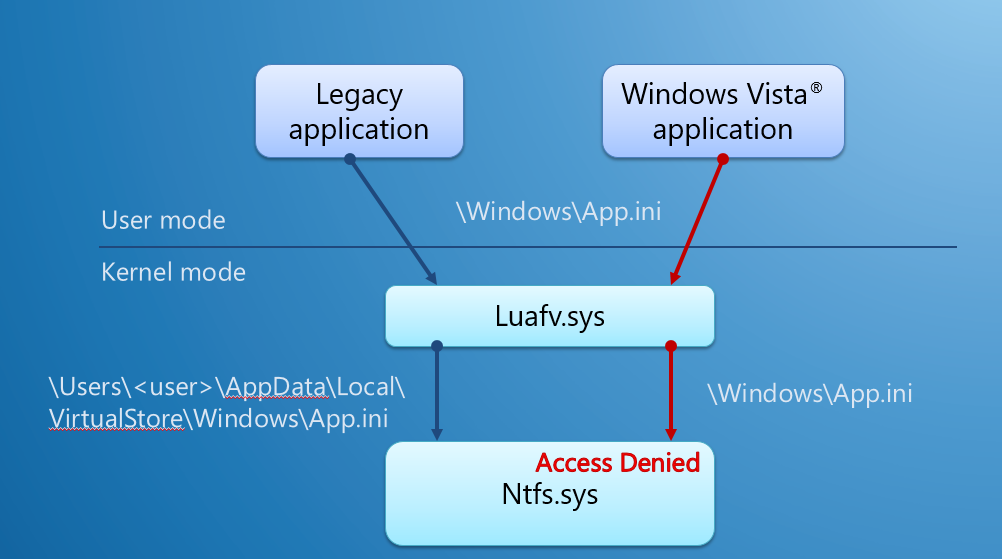


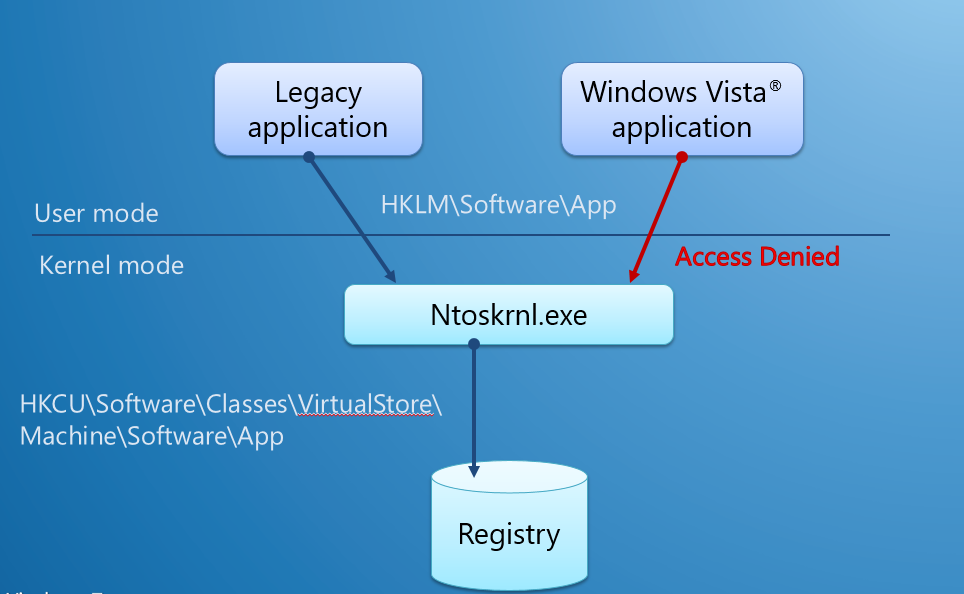


windows用于系统更新的TrustedInstaller权限很大。

UAC 虚拟化（Virtualization）也被称为重定向（Data Redirection）。在权限判定的过程中，如果用户的权限没有达到程序所需的权限，UAC 就会重定向该文件夹。例如，如果程序试图写入到 C:\Program Files\Contoso\Settings.ini目录下，但用户没有写入权限，这个写操作就会被重定向C:\Users\Username\AppData\Local\VirtualStore\Program Files\contoso\settings.ini。UAC 虚拟化分为两个部分，文件虚拟化和注册表虚拟化。在以下情况虚拟化不可用：

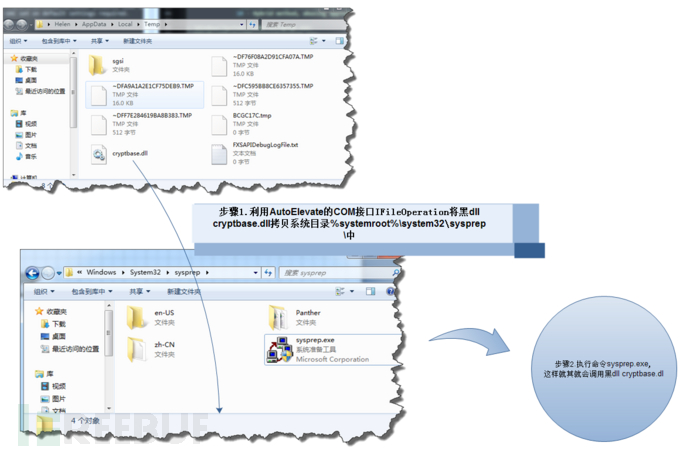
* 64 位程序
* 非交互式程序
* 模拟令牌的进程 (Processes that impersonate)
* 内核模式调用方
* 带有 requestedExecutionLevel（请求执行等级）的可执行程序





UAC 主要的实现文件在于 appinfo.dll 这个文件，这个 dll 是通过注册LPC接口进行调用的。触发UAC，系统会创建consent.exe进程，通过白名单与用户选择来进行判断以RAiLuanchAdminProcess是否创建管理员进程。

使用dll劫持的bypassUAC：



将dll弄到敏感目录也会弹出一个UAC框表示“您需要提供管理员权限才能移动到词文件夹”，这时候使用的是使用windows系统中国一些白名单进程中调用文件操作接口来进行复制或者移动，因为可以很方便地注入explorer.exe进程创建IFileOperation object。在exe的NT PE部分的FLAG加上了IMAGE\_FILE\_DLL。后来使用过哦dll劫持migwiz.exe，最近的是使用ntwdblib.dll来劫持cliconfig.exe

使用白名单：

遍历系统目录（%systemroot%\system32\或者%systemroot%\syswow64\）找出所有白名单程序：strings.exe  -s \*.exe | findstr /i "autoElevate">"D: \UacFuzzer\autoevate.txt" -s就是为了在输出的时候打印程序的名字，win10里面已经是-f。

Wusa.exe是从windows vista开始的更新独立安装程序，cmd中有wusa这个命令，可以安装或者卸载补丁，常使用的参数就是/quiet来安装或者卸载，/extract来进行任意目录的写（wusa.exe exploit.cab /extract:c:\windows\system32\sysgrep）。之前是通过exploer.exe的autoelevate的COM接口IfileOperation来讲dll送入需要权限的目录中，现在可以用wusa或者其他方式。

infDefault.exe exploit.inf来做到任意目录的写入与任意注册表的添加

PkgMgr.exe等

2016年8月we found that a scheduled task named “SilentCleanup” is configured on stock Windows 10 installations to be launchable by unprivileged users but to run with elevated/high integrity privileges。然后分析进程的行为，找到了dll劫持的地方。这个程序会在%TEMP%中新建文件夹并释放exe和一系列dll给exe，然后高权限执行。

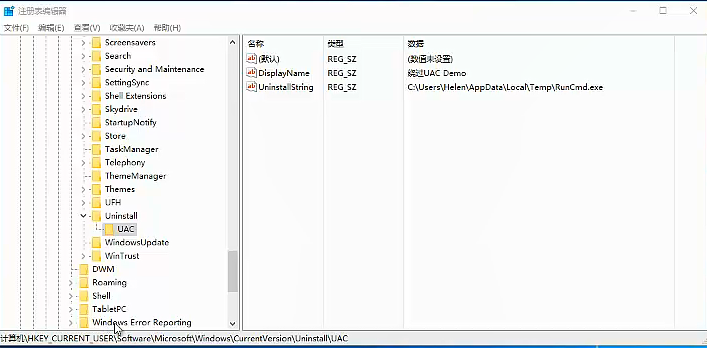
2016年8月，可以通过注册表中的eventvwr绕过：因为eventvwr.exe 或者CompMgmtLauncher.exe HKCU\Software\Classes\mscfile\shell\open\command中的键值直接定成我们的exe路径，然后执行两个中一个exe就好。

曾经qq pinyin以为想要预留一部分0xExx-0xExx作为windows用户的造字空间，然后被借助用于bypass了。

使用com object：-

控制面板中卸载过程序大兄弟应该知道,卸载哪些带小盾牌的程序,是不会触发 UAC 提示框的,这也是属于白名单的范畴.那么上面这位大兄弟的做法就是遍历卸载程序列表,替换第三方的带小盾牌的程序,然后模拟鼠标点击控制面板中的项来卸载程序,从而实现 BYPASS

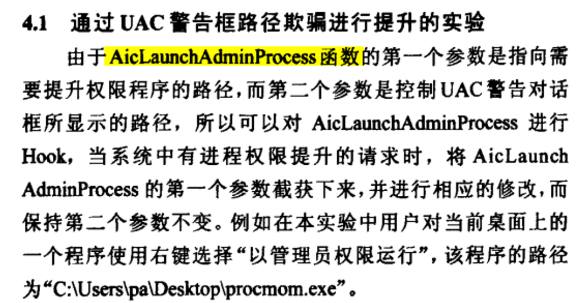
2015年卸载面板升级绕过方法：注册表CURRENT\_USER的Uninstall下新建一个值然后UninstallString只想要要bypass 的exe，还有个DisplayName 其键值是卸载面板中显示的名字（WMI里面有卸载接口，win32\_product只能列举出通过windows instalkler安装的产品也就是安装包以msi结尾的安装程序。注册表UnisntallString 的值就会是msiexec.exe带上产品编号）。卸载的主要功能在appwiz.cpl这个COM组件实现。



使用IARPUninstallStringLaunche未公开接口过UAC：



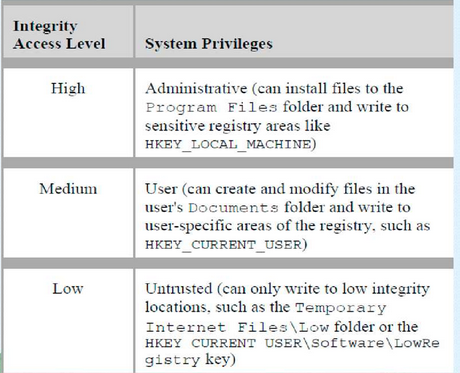
调用COM接口需要类型库，但是OLE/COM object viewer并没有给出类型库，于是我们就自己访问虚表获取卸载方法的指针。x86 下 LaunchUninstallStringAndWait 这个虚函数的地址在偏移 12 的位置,x64 下在偏移 24 的位置.并且发现windows内部也是借助虚表中指针的获取来使用这个接口。



code inject bypass uac：

这种行为容易被行为查杀





High上面还有个System

各个权限等级之间进行了隔离，这种隔离叫做UIPI。如果应用有TokenUIAccess 这个token，就能通过这种隔离，这种token主要出现在windows的辅助程序。要提升权限的发起进程必须要具有完整的中等权限。

IE就运行在Low-IL。

控制面板\用户帐户\用户帐户 中可以对UAC的提醒触发等级进行更改。不过这歌更改本身就会触发一次UAC。

83.在win7里面出现了服务进程与用户进行会话隔离，这个现在在win10中没有



84.WMI里面有卸载接口，win32\_product只能列举出通过windows instalkler安装的产品也就是安装包以msi结尾的安装程序。注册表UnisntallString 的值就会是msiexec.exe带上产品编号。

85.win10 中进程是不是特权程序，可以在任务管理器中查看。

86.只要是个错误码就能使用VS中的Error Lookup来查看

87.注入的进程有exploer.exe进程，notepad、calc进程

88. 如果用户是标准用户， Windows 会给用户分配一个标准 Access Token.  
如果用户以管理员权限登陆，会生成两份访问令牌，一份是完整的管理员访问令牌（Full Access Token），一份是标准用户令牌。一般情况下会以标准用户权限启动 Explorer.exe 进程。

89. RPC Functions（Remote Procedure Call），使得一个程序可以调用另一计算机的子程序，顺便一提，本地过程调用（LPC，Local Procedure Call）则是在本机进程间进行通讯。

90. 64位系统文件重定向导致的，我们32位程序访问%systemroot%\system32\的时候，被重定向到了%systemroot%\syswow64\这个目录

91.可以使用PowerShell脚本注册一个WMI时间去监视文件/文件夹的变化

92.没有托盘图标的话就不会有托盘通知

93.UACME这个UAC工具中提到：如果能将windows Debugging Tools中的dbghelp.dll、symsrv.dll文件放入就能获取更多的信息，这两个dll不能来自windows自带。

94.移动媒介的自动播放设置：控制面板\硬件和声音\自动播放

95. C盘多出了一个$WINDOWS.~BT的隐藏文件夹，一般带$的文件一般都是临时文件，这个文件夹是临时windows的安装文件。

96.PE可执行文件都可以作为模块

97.配置信息保存：存成自定义文件、写入注册表、用配置文件。

98.自启动：用快捷方式放到startup目录、windows服务、注册表的run项

99. windows下tab有补全和范围内选择的作用

100.CLSID

clsid是指windows系统对于不同的应用程序，文件类型，OLE对象，特殊文件夹以及各种系统组件分配一个唯一表示它的ID代码，用于对其身份的标示和与其他对象进行区分。下载dll以后，使用regsvr32在注册表中加上clsid。

101.NT 包含NT、2K、XP、2K3、Vista、7、Server 2008

DOS平台 DOS、windows 1.x/3.x/9x/Me

102.原来services.msc里面有酷狗服务

103.网上邻居支持设置：

文件夹共享： [\\xxx\xx](file:///\\\\xxx\\xx) 出现在Internet中

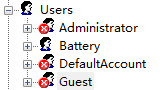
http共享 <http://xxx/xx>

ftp共享 <ftp://xx.xx>

通过文件夹右键属性开启的共享，出现在“本地网络”中。

最终出现在net use中的仅仅设置了文件夹共享的。

104. Wake-On-LAN简称WOL，是一种电源管理功能；如果存在网络活动，则允许设备将操作系统从待机或休眠模式中唤醒。该标准允许网络管理员远程打开PC机电源，以便进行文件升级、资源跟踪和设备清点等工作。 通过SMB控制。

105.win10默认关闭的账户有

（使用dumpsec中的Hyena） 先安装一个破解版的注册里以后，再安装最新版的就会直接是破解的。这说明破解和注册表的一些事情有关系。

106.windows 2017年秋季的更新才开始禁用SMBv1。同时建议不要禁用 SMBv2 或 SMBv3

107.注册表跟新完毕以后，**可以gpupdate /force，**不过务必重启。

108.启用和关闭windows功能里面可以关闭“IE”。

109.windows上有些命令和linux下是一样的，这是因为windows services for unix SFU的存在，提供了一些模仿Unix的平台。

110.原来我基本在使用的工具都在“控制面板\系统和安全\管理工具”。组策略就是其中的本地安全策略。其中的账户策略里面设定账户被锁定的阈值。

111. Windows具有一个传统的坏习惯，就是除了在主用户密码数据库之外，还在多个地方缓存密码信息。Local Security Authority（LSA） Secrets缓存处于注册表里的HKEY\_LOCAL\_MACHINE\SECURITY\Policy\Secrets子键下，收录以下信息：服务帐户的明文口令。

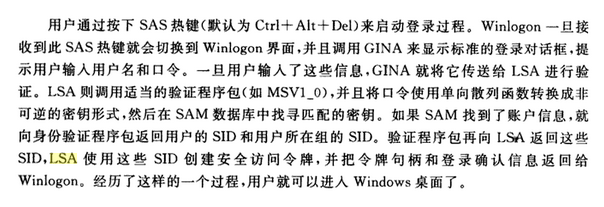
112.windows server 2008 并没有在SAM中存储LM，但是windows server 2012 又出现了。

113.windows对密码有缓存：NTLM缓存（存储在内存中）、LSA Security缓存（HKLM\SECURITY\Policy\Secrets，这里甚至有部分口令是明文，登录自己机器的到全是hash）、Cache缓存（存储以前登录域的用户登录信息，存储在HKLM\SECURITY\CAHCE\NL$n，一般NT系统$n默认为1-10。这个数字在HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon中设置）。

114.LSA：

进程名lsass

Windows 2000将从KDC获得的票证和密钥存储在凭据缓存中，这是由LSA保护的易失性内存区域。 只有在LSA的安全环境中运行的进程才能访问缓存。 它的内存从来没有被分页到磁盘。 当安全主体注销或系统关闭时，存储在其中的所有对象都将被销毁。在windows2003中：



115.开机启动：

凡是有允许发生开机自启动的地点被称为自启动扩展点ASEP。

界面调整：msconfig

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 详细规定自启动的exe，没想到看到鼠标的驱动是一个exe，也是这里同意了Windows Defender的开机自启动。

116.定时启动任务的队列叫做Schedule，使用at命令可以查看。

AT 命令已弃用。请改用 schtasks.exe

不支持该请求。

117.组策略：Policy

本地策略组：专业版才有 gpedit.msc

DC会有一个群组策略控制台。群组策略对象（group policies objects，GPO）被保存在活动目录中（AD）或一台计算机上。规则又优先级、继承。在其安全配置中的内容最有趣。群组策略生效有延迟：secedit /refreshpolicy MACHINE\_POLICY

同时激活本地和域的组策略就会有意想不到的问题发生

118.EMET Enhanced Mitigation Experience Toolkit

增强的减灾体验工具包 (EMET) 是一种可以帮助阻止软件中的漏洞被利用的实用程序。win10中更名为Windows Defender Exploit Guard WDEG就是windows defender的设置。是依托系统（windows）本身的防御机制来阻止对各类软件漏洞的利用。其防御手段包括DEP、SEHOP、EAF、ASLR等。

DEP：数据执行保护 CPU上设置了一个代表内存页执行权限的NX/XD标志位 不允许CS：IP的地址在堆栈中 堆栈只能作为参数 BIOS中可以设置是否使用这个位，没启动会导致CPU与Hyper-v不兼容

ASLR： 内存地址空间基址随机化 在可执行文件和动态链接库中启用，加大了缓冲区溢出攻击的难度 但是可能可以实现DOS攻击 我们自己编写的程序或者链接库，可以通过设置一个链接选项，Project Property -> Configuration Properties -> Linker -> Advanced -> Randomized Base Address，来设置是否支持ASLR。

SEHOP：结构异常处理程序覆盖保护 发生异常的时候就记录异常处理链，调用异常程序时就验证

EAF: 导出地址表访问过滤 都会阻止尝试从模块读取导出和导入目录。通常，一个shellcode使用IAT解析其他函数前会先获取[GetModuleHandle](http://wordpress.redirectingat.com/?id=725X1342&site=modexp.wordpress.com&xs=1&isjs=1&url=https%3A%2F%2Fmsdn.microsoft.com%2Fen-us%2Flibrary%2Fwindows%2Fdesktop%2Fms683199%28v%3Dvs.85%29.aspx&xguid=af1c229770783c0d21eeb9ff0b7752a7&xuuid=26a5c8a10a811eabfe96ba0)和[GeProcAddress](http://wordpress.redirectingat.com/?id=725X1342&site=modexp.wordpress.com&xs=1&isjs=1&url=https%3A%2F%2Fmsdn.microsoft.com%2Fen-us%2Flibrary%2Fwindows%2Fdesktop%2Fms683212%28v%3Dvs.85%29.aspx&xguid=af1c229770783c0d21eeb9ff0b7752a7&xuuid=26a5c8a10a811eabfe96ba0)的地址。如果PE文件从其他模块导入API，这个导入目录将包含导入描述符的数组，每个代表一个模块。

windows的防护机制还有ACL。

Service Resource Isolation：许多服务都工作做在同一个账户中，如果一个被攻破就会导致其他服务也会受到控制。windows server 2008中的处理方法就是服务资源隔离，可以独立运行的服务就基于service-specific SID 服务专属SID，服务的资源只能被自己改动，用户的SID没有这个权限。对于必须在相同环境中工作的服务，给予了正常的SID和Restricted SID（s-1-5-33），都会被加到服务进程的限制SID列表中，但是有的只有Restricted SID，当受限制的进程或线程对某一个对象进行操作的时候，只有当两个SID都存在的时候，对资源的操作才会被批准，权限SID代表个人，受限制SID代表group。可以使用M$的PsTool工具包中的psgetsid 通过sid来查询服务的名字。sc showsid 则能从服务名字查询出sid。

session 0被隔离：应用服务和系统进程保持在session 0中，用户会话从session 1开始。如果都在session 0，那么就能发送消息到任何高权限应用，从而借此执行任意命令。这就是从前的“Shatter Attack”。

119.windows下的两种加密：

EFS: Encrypting File System 随机产恒一个文件加密密钥FEK，对保证速度，使用对称加密。但是对FEK再使用文件所属主账户的公钥 和来自恢复代理的公钥进行加密。但问题是对“为了预防对免肝数据进行加密的用户离开了公司或丢失加密密钥”，强制要求这种加密爱系统必须要有一个数据恢复代理。 因为与用户账户关联，所以可以直接通过另一个操作系统进行重设。

Bitlocker Drive Encyption BDE：是对整个卷的加密，使用的时候会产生一个密钥恢复文件。但是有研究人员，通过cold boot ：对DRAM芯片降温，延长了从内存导入操作系统的时间，并在这个足够的时间内对系统进行扫描并保留一个镜像文件。从文件中解密出BDE密钥。研究者甚至绕过了采用了TPM（trusted Platform Module）芯片的系统，这是一个单独的芯片用来存储BDE，从而使得BDE几乎不可能被绕过。

120.windows的文件保护功能会将关键内容被修改以后还会恢复，目前知道的有iis的标语dll。

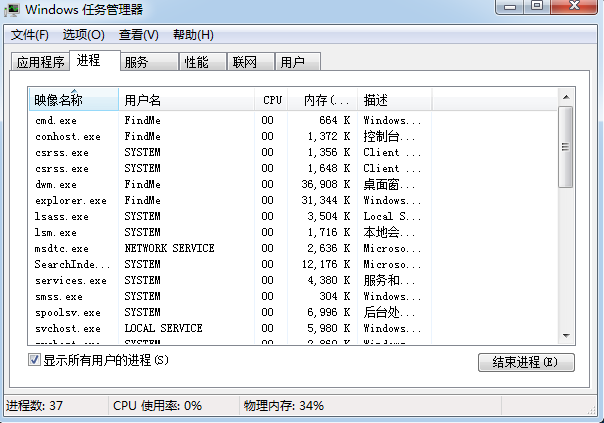
不过从前在2000和xp中也有windows 文件保护WFP，后来再vista中更新为windows资源保护 WRP， 不再是侦测对关键文件的修改，而开始使用ACL。

121. 计算机使用 SID 来跟踪每个帐户： 如果重命名管理员帐户，计算机仍然知道哪个帐户是管理员帐户。 这是因为 SID 不同于名称，它永远不会更改。IL（integrity level）安全等级就可以作为SID实施。

122.svchost.exe

是从动态链接库 (DLL) 中运行的服务的通用主机进程名称。而作为一个共享的进程服务，它的进程令牌将包含组中每个服务所需要的所有权限的合集。windows设置了几个scvhost来用作对服务权限的锁定。

123.通过任务管理器可以知道windows里面还隐藏这一些用户名：


124. 信号用来改变一个程序的执行流。比如说结束还是中断挂起。

125.删除windows.old需要System权限，不过可以通过磁盘清理工具执行，说明这个工具能有这么高的权限。

126.一般黑客藏的都是系统进程：

部分系统进程被关闭会自动重启。

conime.exe 与输入法编辑器有关系

ctfmon.exe 也是与输入法有关系，该进程能保证输入法状态栏出现在任务栏  
csrss.exe 该进程是微软客户端/服务端的运行时子进程。该进程管理windows图形相关任务。

explorer.exe windows的资源管理器，是windows图形界面的外壳程序，该进程的运行能确保显示windows的图标以及任务栏。如果出现错误，常常需要我们从任务管理器关闭后，手动创建（通过任务管理器的新建就能够创建）

lsass.exe 用于windows的安全机制、本地安全与登录策略

services.exe 用于管理进程,

smss.exe 管理子系统，负责用户与操作系统之间的对话

svchost.exe 从动态链接库中运行的服务的通用名称

system windows的内存管理进程

system idle process 在CPU空闲的时候，发出命令，使CPU挂起（暂停工作），从而能够降低CPU的温度

winlogon.exe 管理用户的登录与退出

rundll32.exe 执行32/64位dll文件中的内部函数，不会有一个个dll执行进程，实现了进程的隐藏。位于c:\windows\system32

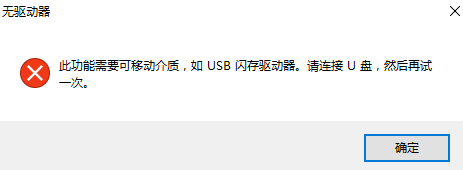
127.superscan以及wireshasrk这种程序都需要 管理员 权限才能运行。

128. 注册表里面有一个“阿里旺旺接受到的可疑文件”.

129. 一种重置开机密码的方式： 重置密码的时候没有验证



如果没有使用这个功能，那么在开机进入用户选择界面的时候，虽然有一个重置密码，但是点击就会提示



其实创建的时候也会有这个

130. 在“打开或关闭windows功能”的地方，开启了telnet以后。然后就会多了一个tlntadmn命令等，并在服务中多出对Telnet服务的控制。可以使用tlntadmn config sec = - ntlm 关闭ntlm认证。我们在受害机上面这么做。

131.注册表-》文件-》连接网络注册表 如果对方开起了远程注册表服务，就能直接更改，但是这样子好麻烦。

在注册表里面可以进行修改：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictanonymous

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer

132.此电脑右键管理-》操作-》连接到另外一台计算机，这里使用的是IPC$连接。《黑客·攻防》上面演示了通过这种方式开启对方的远程注册表服务。

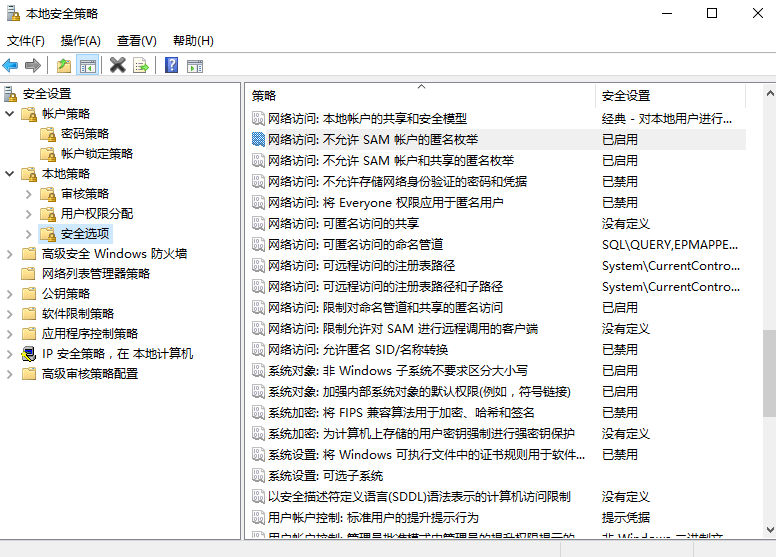
133.

适配器的属性里关闭

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictanonymous 修改值为1

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer 修改值为0

控制面板-》管理工具-》本地安全策略-》不允许SAM账户的匿名枚举 默认已经启用

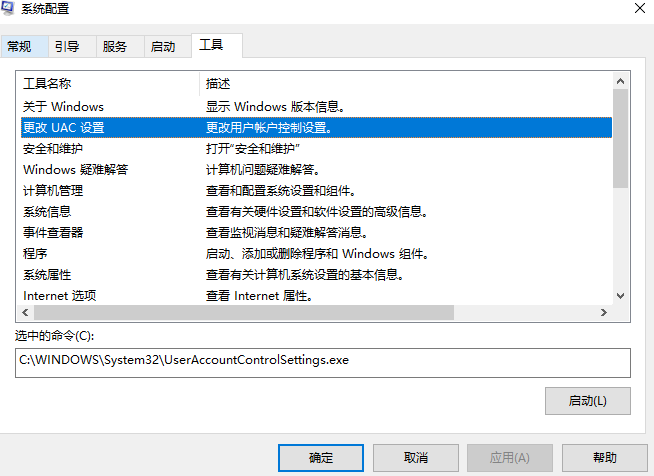


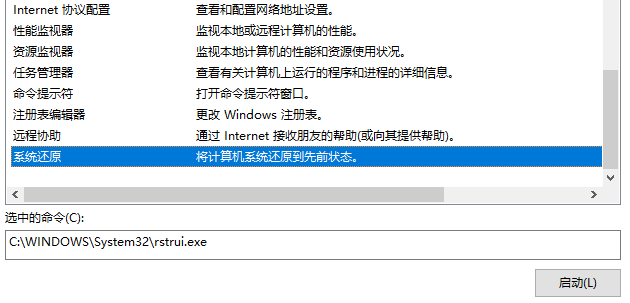
134. msconfig

主要是控制开启启动的相关内容：

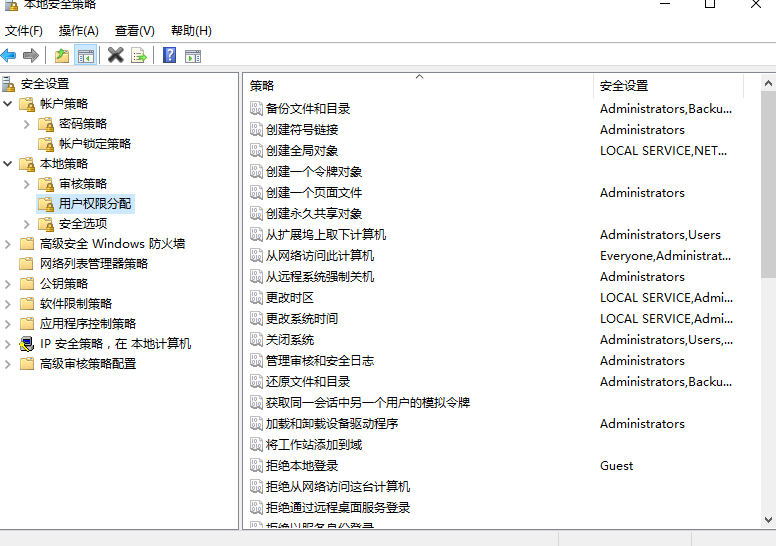


并且能找到一系列关键工具的路径：

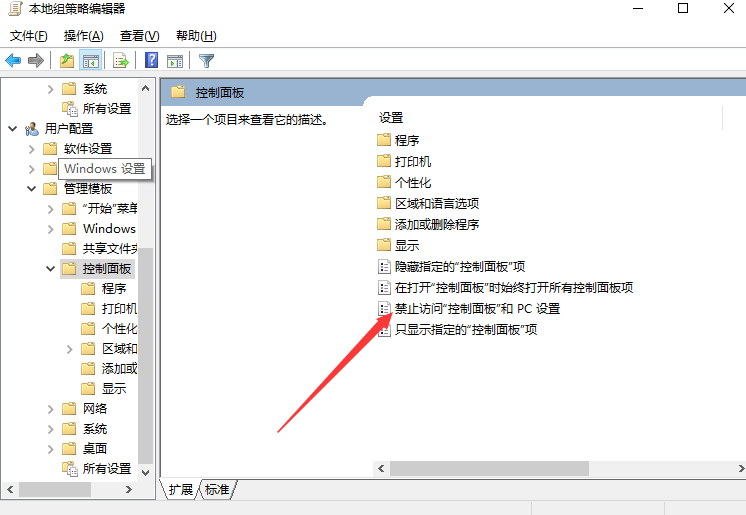




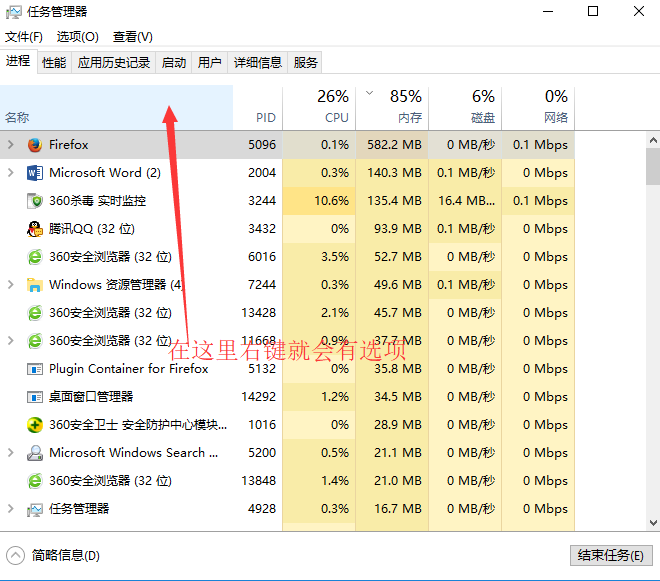
135.



136.gpedit.msc中



137.资源管理器里面可以设置显示的内容：



指定进程右键，还可以打开文件所在的位置。需要注意的是进程管理器中显示的是映象名称。

任务管理器里面也是可以开关服务的、控制启动、查看用户。

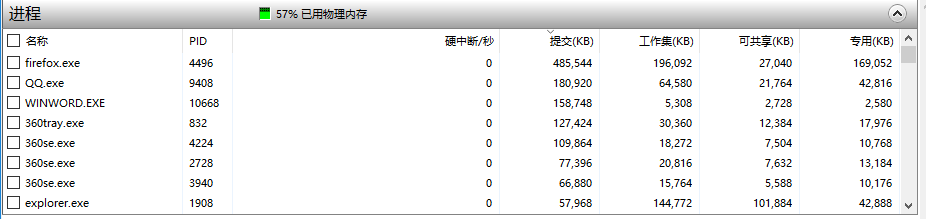
在详细信息里面可以“转到服务”以及“设置优先级”。

138.Memory Compression

微软的一个内存管理机制进程。严肃哦不经常访问的内存页面，降低内存的紧张程度，减少置换次数，以减少对硬盘的读写，提升性能。但是这个进程对内存的占用太可怕了，一直在增加，感觉并不会自己释放。于是

进入管理员的powershell，执行Disable-MMAgent –mc 并重启。执行Get-MMAgent可以查看当前的状态。

139.资源管理器中内存的介绍：



硬中断/秒：最后一分钟内出现的每秒平均硬盘页中断数

提交：操作系统为进程保留的虚拟内存量

工作集：进程当前正在使用的内存的物理量

可共享：进程与其他进程共享使用的物理量

专用：….

140.

FTP服务器、IIS服务器：

控制面板-》添加删除程序-》IIS-》文件传输协议FTP服务 老版本需要插入光盘，虚拟机里面使用iso文件. win10里面直接开启。

控制面板-》程序与功能-》启动或关闭windows功能-》information server

win10中可以开启tftp客户端：

控制面板-》程序与功能-》启动或关闭windows功能

还有NFS、SNMP都是在这里开启。

特殊功能： 适用于linux的windows子系统

控制面板-》程序与功能-》启动或关闭windows功能-

141.windows 默认并没有启用内置的管理员账户

原来从Win8开始到Win10，administrator内置管理员权限和modern应用就不能共存。所以只要用内置管理员（不是普通管理员），就不能登录Microsoft也不能使用modern应用（包括应用商店、edge浏览器等等）。而用其他普通用户和一般管理员（不是内置administrator）权限的用户登录就没有问题。

142.复制不会开启管理员权限，所以复制一些敏感的内容，一旦需要管理员权限就会不能复制，只好选择跳过。所以推荐在cmd管理员模式下，使用copy命令。

143. user profile service 用户登录以后配置文件加载服务。

注册表中配置文件: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

就是注册表中出了问题，原来的文件夹变成了.bak。不能乱删账户啊，每一次账户的ID在注册表中都是增加的啊。

使用了激活工具，看它安装了一个xxx，于是windows一开机就不能登录，如果登录就会说无法登录到当前的用户账号，相当于用户配置文件与账户脱离，这应该是注册表中的事情，可惜没有好好弄，我直接删除，想看看用户账户的配置能不能替换，都怪自己考虑不足。

144.更改注册表之前进行备份，但是使用导入功能的时候，都快结束了来个报错。说访问出错。应该是因为我拿从前的注册表进行导入，其中有一些项已经不一样了。不过看样子还是恢复了一部分。

145.有些人登录到windows的账户是‘远程’的，配置文件存储在Microsoft的云端。

146. Ralink RT5370 网卡直接插上去，只能被作为一个USB3.0识别，360驱动大师也没有辙。只有插着重启一次电脑才能有用。netsh wlan show drivers可以看到使用的是windows自带的WLAN驱动。毕竟芯片是Ralink。

147.在user目录下发现Default文件夹，这是个隐藏文件夹，上一次因为用户账户不能登录的灾难中，似乎临时账户都是从这个文件夹中创建而来的。还有一个Default.migrated 文件夹。

Default.migrated文件夹是微软系统更新后，在用户文件夹中自动生成的文件夹，包含用户帐户路径和设置的迁移数据，一般位于C:\Users目录下。它的作用包括：

　　作用一：创建新用户时，使用相同的设置

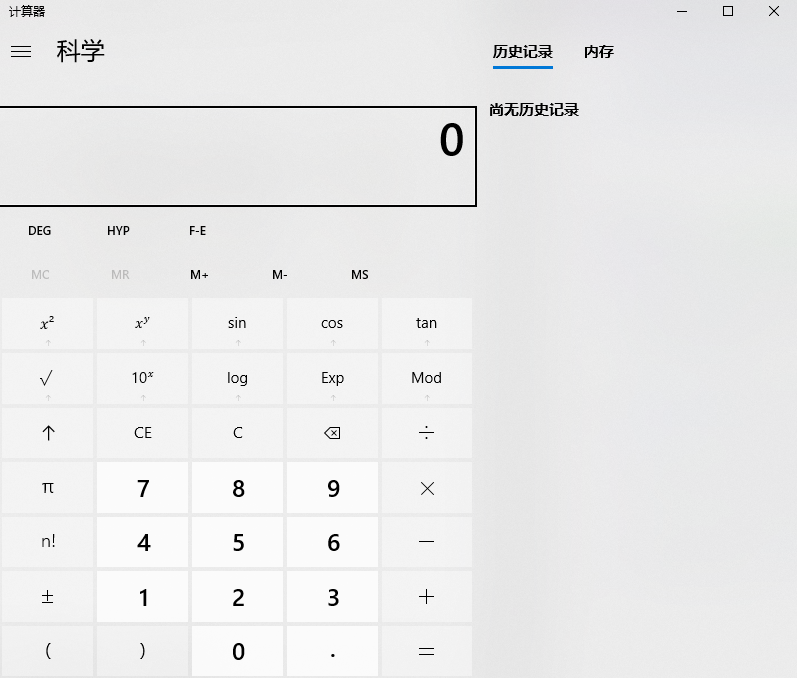
　　作用二：用来恢复系统用户配置。

148.使用windows自带的图片查看器，是有缓存的，在查看的时候不影响对照片的删除或者移动。

149.计算器

不要使用标准计算器，算不准，坑

科学计算器变大可以改变界面



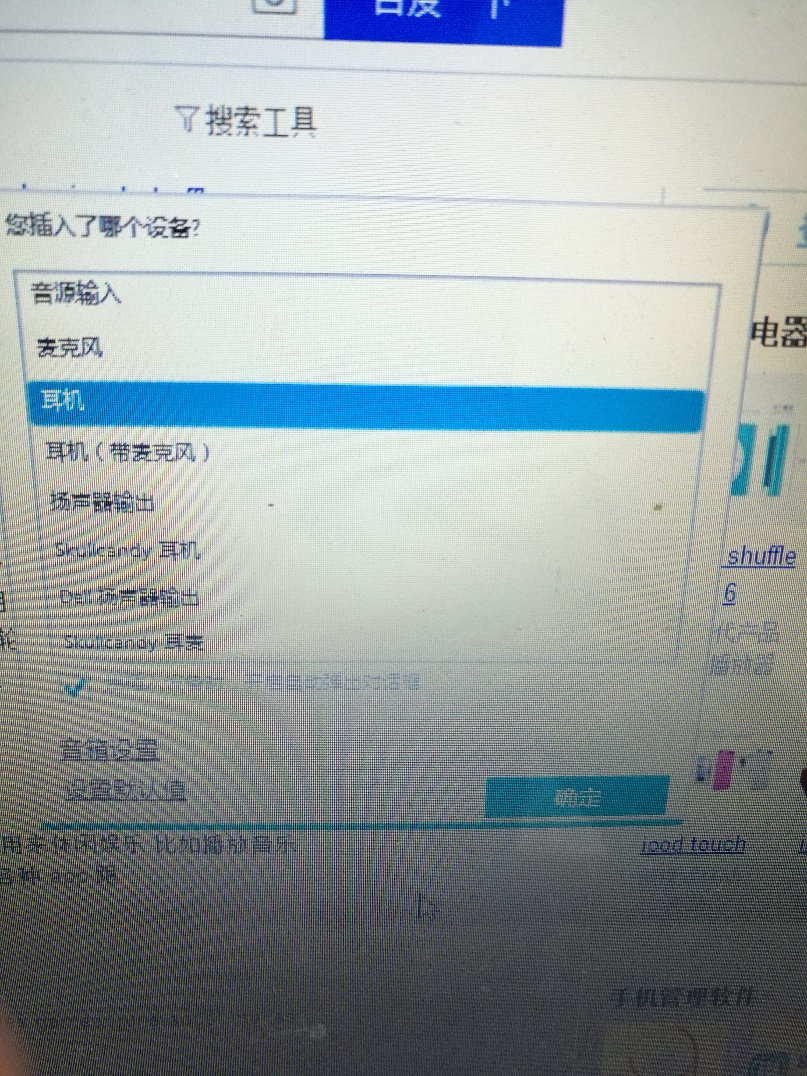
150.C盘瘦身：



C:\\ProgramData\\Package Cache该目录是Visual Studio的安装源目录。删除后可以节俭5个G左右的C盘空间空间。

151. windows登录界面的时候通过五次敲击Shift，触发粘滞键的询问，同时因为文件替换（被替换文件c:\windows\system32\sethc.exe）的原因，能触发自己指定的程序，可以是一个shell（稍后自己执行explorer.exe），也可以直接是explorer。exe从而进入界面。这个后门可以被远程桌面利用。

152. 当向dell电脑中插入耳机的时候会给出提示：



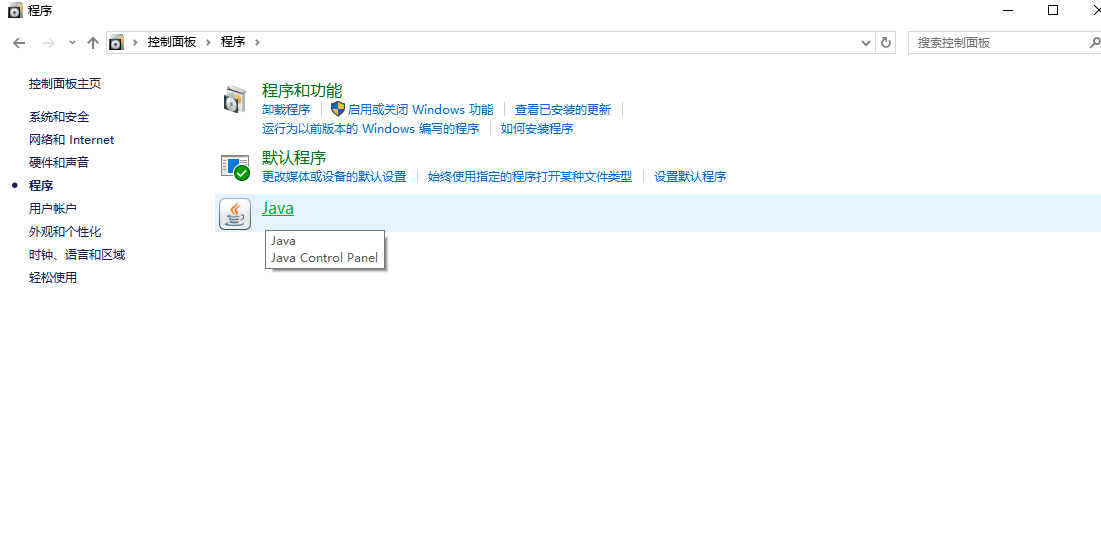
我认为是可以像震网病毒一样攻击

153.U盘不能显示盘符（不能被挂载）：

右下角的U盘符号表示U盘驱动的加载，加载成功了也并不意味着U盘的盘符出现。有一段时间就是没有出现，同时设备管理器里面存在一个“未知设备”。解决办法是在“设备管理器”-》“通用串行总线控制器”-》“USB大容量存储设备” 卸载设备，我卸载了3次左右就好了。

试过将U盘插入其他的电脑上，倒是都可以成功出现盘符。

154. Java程序被阻止运行：



在安全标签中添加例外网站，不是80端口的需要加上端口号。

155.终端中的字符串 与 带空格路径 ：

C:\Program Files\Google\Chrome>cd "C:\Documents and Settings\计算机学院专业实验

室\桌面"

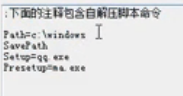
C:\Documents and Settings\计算机学院专业实验室\桌面>

156.在用户的根目录下，存在一个NTUSER.DAT的隐藏文件，被解析为视频文件。Ntuser.ini、Ntuser.dat及LOG日志文件都属于用户配置文件，就是系统用户的一些记录和配置，你不要删除！不过病毒也有时候会伪装成此文件。

157.自解压文件：

解压前运行文件Presetup= 用于创建目录，如果已经存在需要进一步处理

解压后运行文件Setup= 运行解压以后的内容



158.捆绑器：

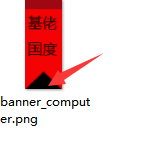
执行一个exe以后会执暗中执行预先设定好的exe文件

159.没有显示文件扩展名的windows，在图标被更改的情况下，对于电脑小白就会很奇怪，双击一个图片文件以后但是没有显示图片，什么都没有（实际上这是一个exe文件被你执行了）。

还有一部分常用文件可以在正常打开的时候执行程序，比如office文档。

对于windows的部分扩展名默认启动软件漏洞的利用也可以做到这一步。

160.windows显示png的部分有时候就会显示成为黑色。



161.点击win+F的时候会触发反馈中心，这时候就会自动截屏在“图片”-》FeedBack文件夹中。

162.services.msc 里面每一个服务双击以后都能看到关于这个服务作用的描述。可以不必到网上查阅。

163. **windows内核：**

**windows操作系统基本结构：**

分为运行于处理器特权模式的操作系统内核，以及运行在处理器非特权模式的用户空间代码。采用宏内核模式来进行构架，这使得任意的内核模块或设备驱动程序都可能破坏其他内核模块数据，这种宏内核机制也使得Windows操作系统容易遭受以驱动方式植入内核的Rootkit的危害，为了避免这类攻击，最新的Windows7缺省要求所以请求安装进入内核执行的设备驱动程序都需要经过数字签名，这能够有效地提升内核的安全性。同时，由于用户态程序对操作系统内核特权代码和数据没有直接访问的权利，因此Windows内核模块对恶意的用户态程序具备完善的防御能力。

**Windows操作系统内核的基本模块包括如下：**

Windows执行体、Windows内核体、设备驱动程序、硬件抽象层、Windows窗口与图形界面接口内核实现代码。

Windows执行体：提供了基本的[操作系统](https://www.baidu.com/s?wd=%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Y4PHR3m1cLPhDvujDYPAR10ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EPHm4rH0krjDL" \t "_blank)服务，包括内存管理，进程和线程管理，安全性，I/O，网络和扩进程通信等等。

设备驱动层驱动层一般由硬件抽象层(HAL)、板级支持包(BSP)和驱动程序组成

**Windows内核中实现的机制：**

Windows进程和线程管理机制、Windows内存管理机制（Windows的虚拟内存空间分为系统核心内存区与用户内存区间两部分，系统核心内存用于映射内核、HAL、Win32k.sys等内核执行模块，并存储内核内存对象，对于内核中运行的特权代码，则可通过DKOM技术来进行枚举和操纵）、Windows文件管理机制（NTFS）、Windows注册表管理机制（注册表中的系统自启动挂接点上注册的应用软件可以随系统引导而自动运行，因此也是很多恶意代码及流氓软件普遍的攻击目标）、Windows的网络机制（从OSI网络参考模型的物理层到应用层，各层上对应的Windows网络组件模块包括如下：①各层网卡硬件的设备驱动程序，处于OSI参考模型的物理层②NDIS库及miniport驱动程序，位于OSI链路层③TDI，对应OSI网络层与传输层④网络APIDLL及TDI客户端，对应OSI会话层与表示层⑤网络应用程序与服务进程，对应OSI应用层）。

**Windows操作系统在用户态的代码模块中包含：**

系统支持进程、环境子系统服务进程、服务进程、用户应用软件、核心子系统DLL

环境子系统：

Windows 2000/XP支持三种环境子系统：Win32、POSIX和OS/2，其中最重要的是win32子系统，其他子系统都要通过Win32子系统接收用户的输入和显示输出。环境子系统的作用是将基本的执行体[系统服务](https://baike.baidu.com/item/%E7%B3%BB%E7%BB%9F%E6%9C%8D%E5%8A%A1" \t "_blank)的某些子集提供给应用程序，就是一种借口。

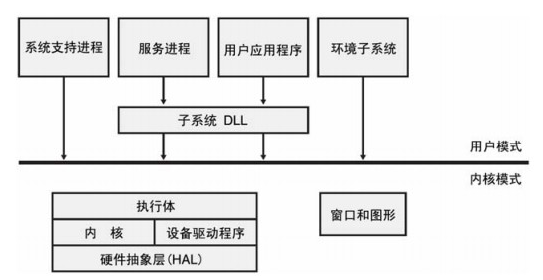
**windows安全机制：**

授权与访问机制UAC

安全审计机制（本地安全策略）

身份认证机制

164. **windows 系统基本构架**



165.软件安装以后不一定快捷方式会对所有的用户可见。

一种可以实现的方法：遍历用户目录，然后在对应的Desktop中创建软件的快捷方式。

1. 有种指定快捷键进行快速关机，输入对象的位置就是shutdown /s
2. 要想对多个文件在某个地方建立快捷键，那么只用对它们进行复制，再在那个目录下进行粘贴快捷键
3. 删除无效快捷键不会进入回收站。有效的会进去。
4. 对于windows 系统的操作不能过快，即便是过了“开机缓慢期”，有一次Shift+Delete，小手一抖，即便眼睛看到的是“是否删除xxx文件等”，但是还是习惯性地按下了回车键。
5. 我在删除WiFi共享精灵时，它的文件直接装在a文件夹中，删除的时候会把a文件夹中的数据都删除，真是哗了狗了。一开始我觉得酷狗没有被删掉，因为软件还是在正常运行的，但是后来一重启又over了。因为装入内存了。
6. 软件打开的windows浏览文件夹那个窗是有记录的，目录的打开情况与之前的一样。打开的窗口还与软件有关，会新开一个。
7. 命令行下按win+Tab可以逐个选择文件。

173. 在操作系统中以控制台打开一个可执行文件或许可以直接输入完整的文件名（有的可以省略后缀），也可以加上相对路径点杠或反斜杠。在windows下，类似与linux统一目录下的文件即.\file，注意不同于linux这里是反斜杆，不过windows亦可以使正斜杆。linux是正斜杠，想到根目录。

在我的ubuntu中不可以直接a.out去运行，必须加上./

1. 双机调试：一个操作系统用于调试，一个操作系统用于跑程序（通常是虚拟机）。