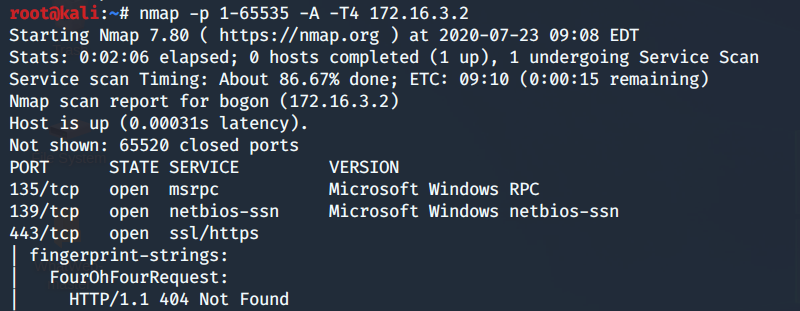
**排查思路：**

**1.查看服务器是否可以弱口令登录。 （暴力破解）**

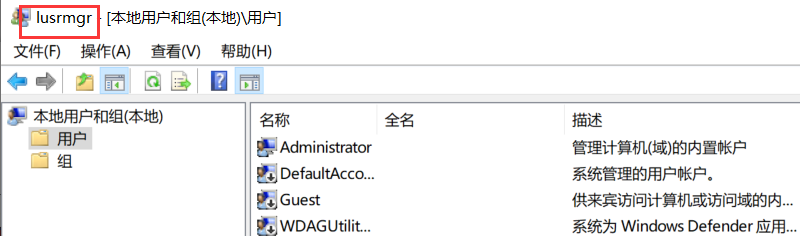
**2.远程管理端口是否对公网开放(3389(远程桌面登录),22(ssh),3306(数据库)，该端口可远程控制)**

**nmap -p 1-65535 -A -T4 172.16.3.2 扫描系统全端口及操作系统类型及tcp端口，**

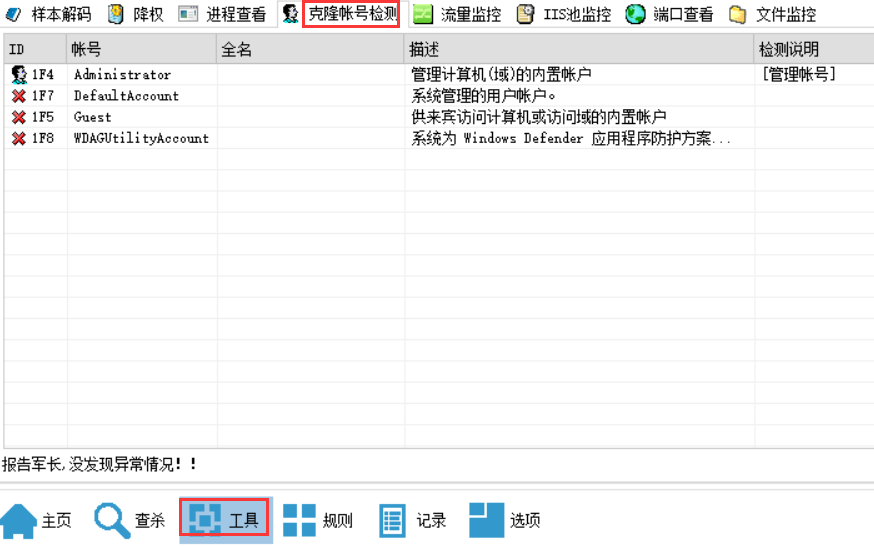


**3.判断是否有可疑账号（hack是否创建新用户和新建组）如有进行禁用或则删除**

**cmd: lusrmgr.msc**



**也可以使用D盾查看是否有隐藏克隆账号**



**4.检查日志**

**cmd: eventvwr.msc**

**重点检测以下事件ID:**

|  |  |
| --- | --- |
| **事件ID** | **说明** |
| **4620** | **创建用户** |
| **4624** | **登录成功** |
| **4625** | **登录失败** |
| **4634** | **注销成功** |
| **4647** | **用户注销** |
| **4672** | **超级用户登录** |

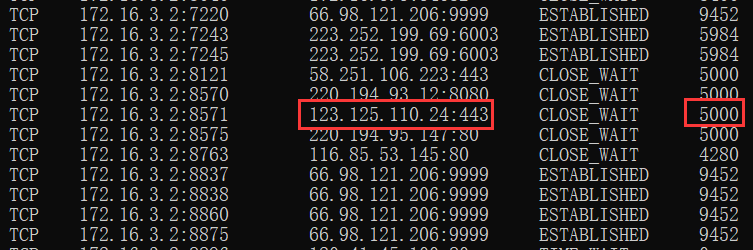
**主要查看是否短时间内有大量的4625时间**



**5.检查服务器端口，并查出其应用**

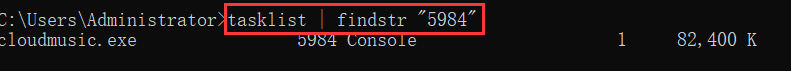
**cmd: netstat -ano**

**查看tcp端口连接的奇怪的ip,找出pid,通过pid找出进程**

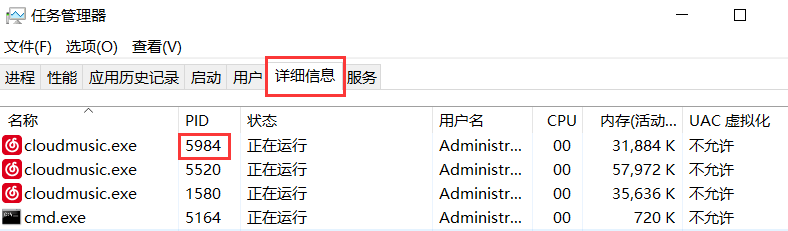


**查看进程所运行的应用：**

**cmd: tasklist | findstr "5984"**



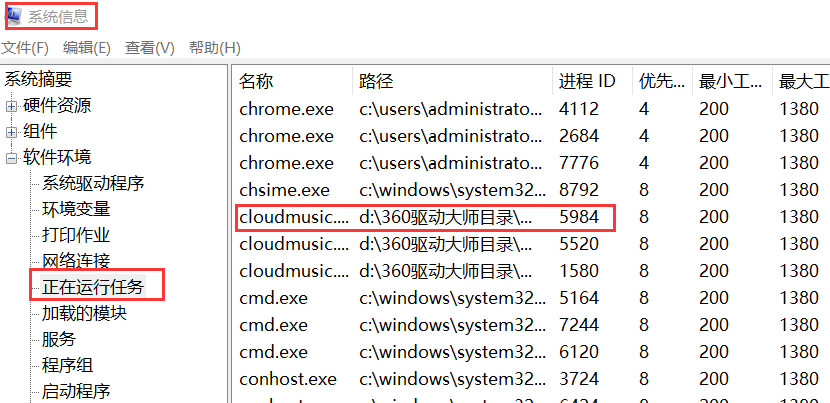
**任务管理器：**



**D盾查看**

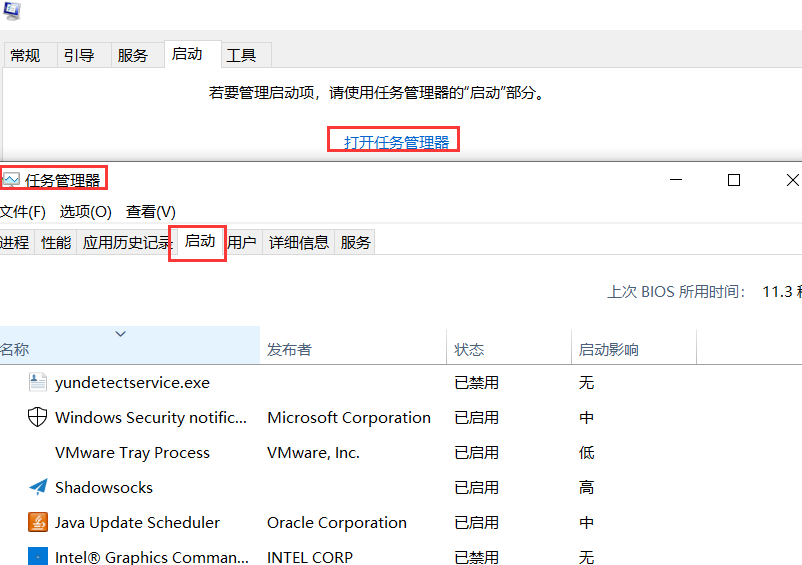


**msinfo32 系统信息**



**6.检查启动项 (系统自启)**

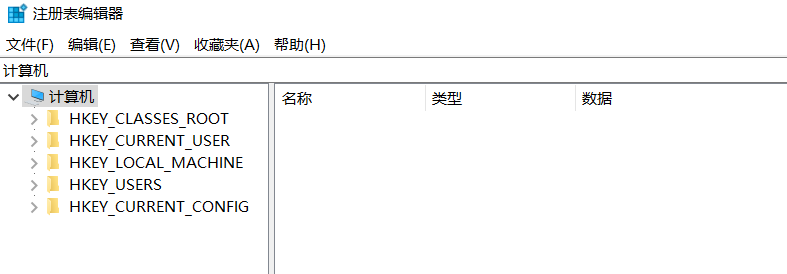
**cmd: msconfig**



**7.检查注册表：**

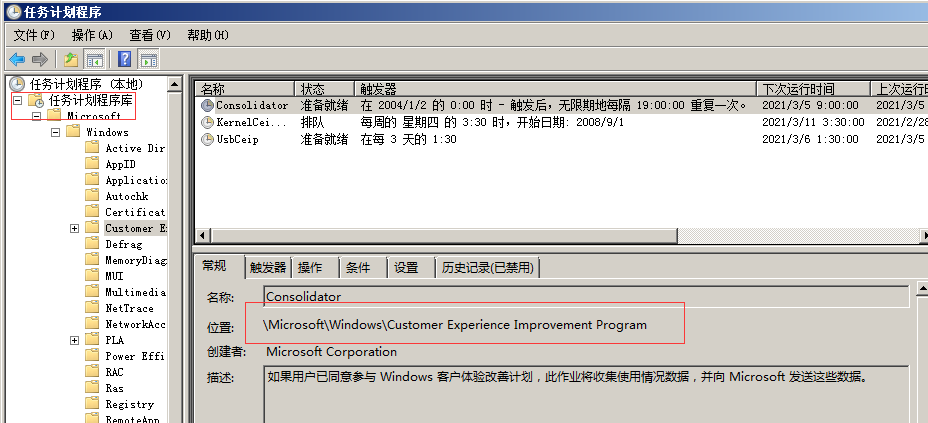
**cmd: regedit 检查是否正常**

**HKEY\_CURRENT\_USER\software\micorsoft\windows\currentversion\run HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce**

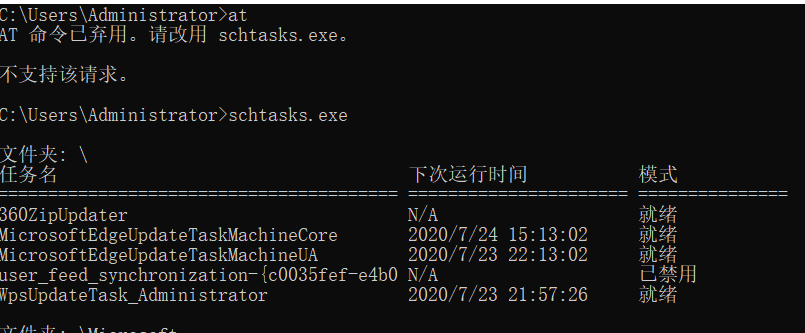


**8.检查计划任务：**

**查看计划任务属性，便可以发现木马文件的路径。**

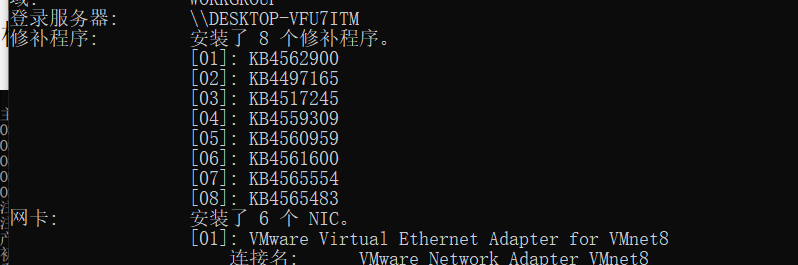


**或则查看at:**



**9.检查系统版本及补丁相关信息**

**systeminfo**



**10.检查可疑目录**

**网上病毒分析：**

**<https://www.virustotal.com/gui/home/upload>**

**微步在线**

**病毒查杀：**

**卡巴斯基：http://devbuilds.kaspersky-labs.com/devbuilds/KVRT/latest/full/KVRT.exe （推荐理由：绿色版、最新病毒库）**

**大蜘蛛：http://free.drweb.ru/download+cureit+free（推荐理由：扫描快、一次下载只能用1周，更新病毒库）**

**火绒安全软件：https://www.huorong.cn**

**360杀毒：<http://sd.360.cn/download_center.html>**

**webshell：**

**D盾\_Web查杀：http://www.d99net.net/index.asp**

**河马webshell查杀：http://www.shellpub.com**

**深信服Webshell网站后门检测工具： http://sec.sangfor.com.cn/download?file=WebShellKillerTool.rar**

**Safe3：http://www.uusec.com/webshell.zip**

**百度webshell查杀: https://scanner.baidu.com/#/pages/intro**

**安全狗:**