应急响应

一、入侵排查篇

当企业发生黑客入侵、系统崩溃或其它影响业务正常运行的安全事件时，急需第一时间进行处理，使企业的网络信息系统在最短时间内恢复正常工作，进一步查找入侵来源，还原入侵事故过程，同时给出解决方案与防范措施，为企业挽回或减少经济损失。

常见的应急响应事件分类：
Web入侵：网页挂马、主页篡改（暗链、云监控）、Webshell
系统入侵：病毒木马、勒索软件、远控后门
网络攻击：DDOS 攻击、DNS 劫持、ARP 欺骗

1.1 Windows入侵排查

使用环境：Windows Server 2008

针对常见的攻击事件，结合工作中应急响应事件分析和解决的方法，常见 Windows 服务器入侵排查的思路如下。

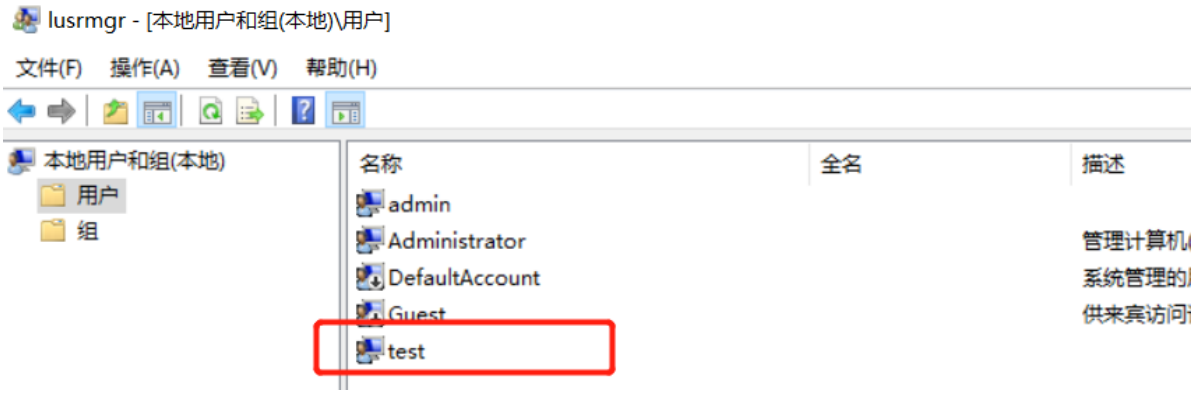
1.1.1 检查系统账号安全

1、查看服务器是否有弱口令，远程管理端口是否对公网开放

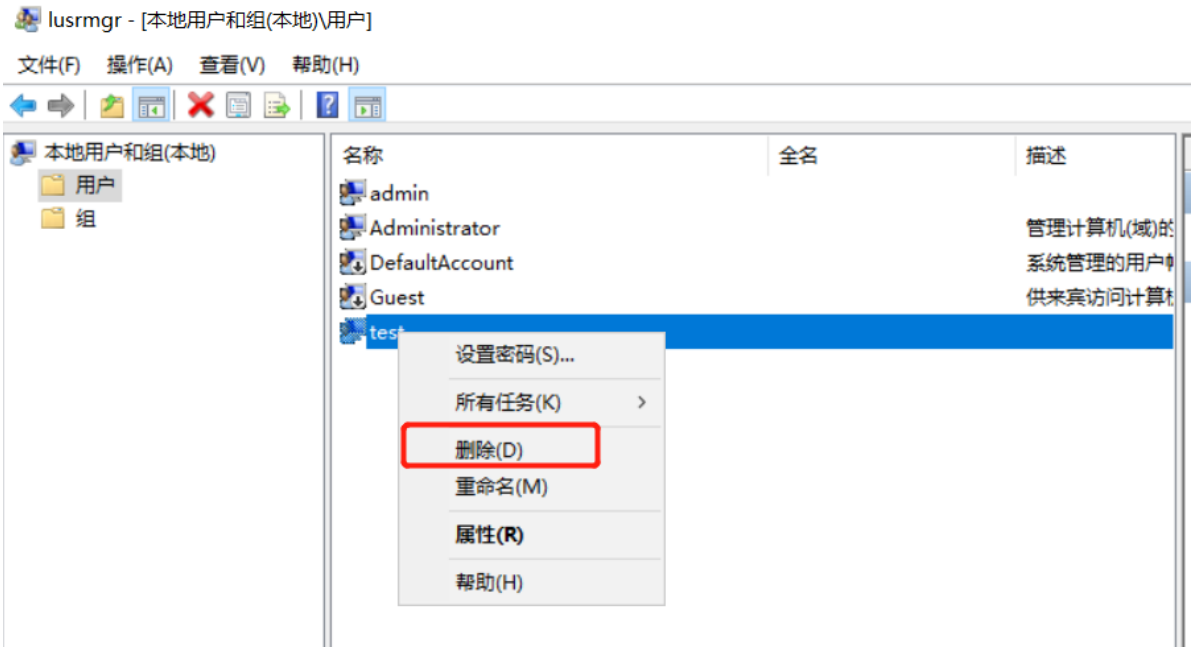
检查方法：根据实际情况咨询相关服务器管理员。

2、查看服务器是否存在可疑账号、新增账号

检查方法：打开 cmd 窗口，输入 `lusrmgr.msc` 命令，查看是否有新增/可疑的账号，如有管理员群组的（Administrators）里的新增账户，请立即禁用或删除。



发现可疑test账号，删除test账号



3、查看服务器是否存在隐藏账号、克隆账号

检查方法：

a、打开注册表，查看管理员对应键值

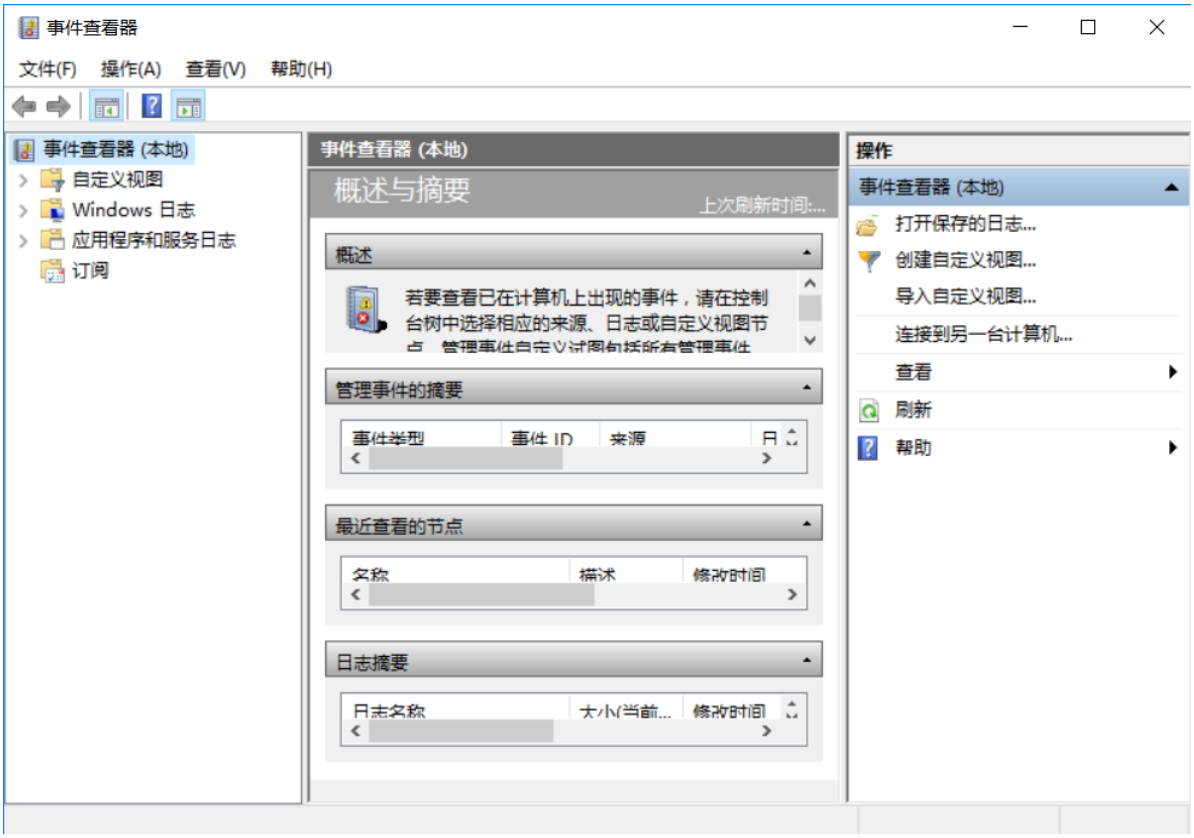
b、使用D盾_web查杀工具，集成了对隐藏、克隆账号检测的功能


```
net user /add test$    # 增加隐藏账号命令
```

4、结合日志，查看管理员登录时间、用户名是否存在异常

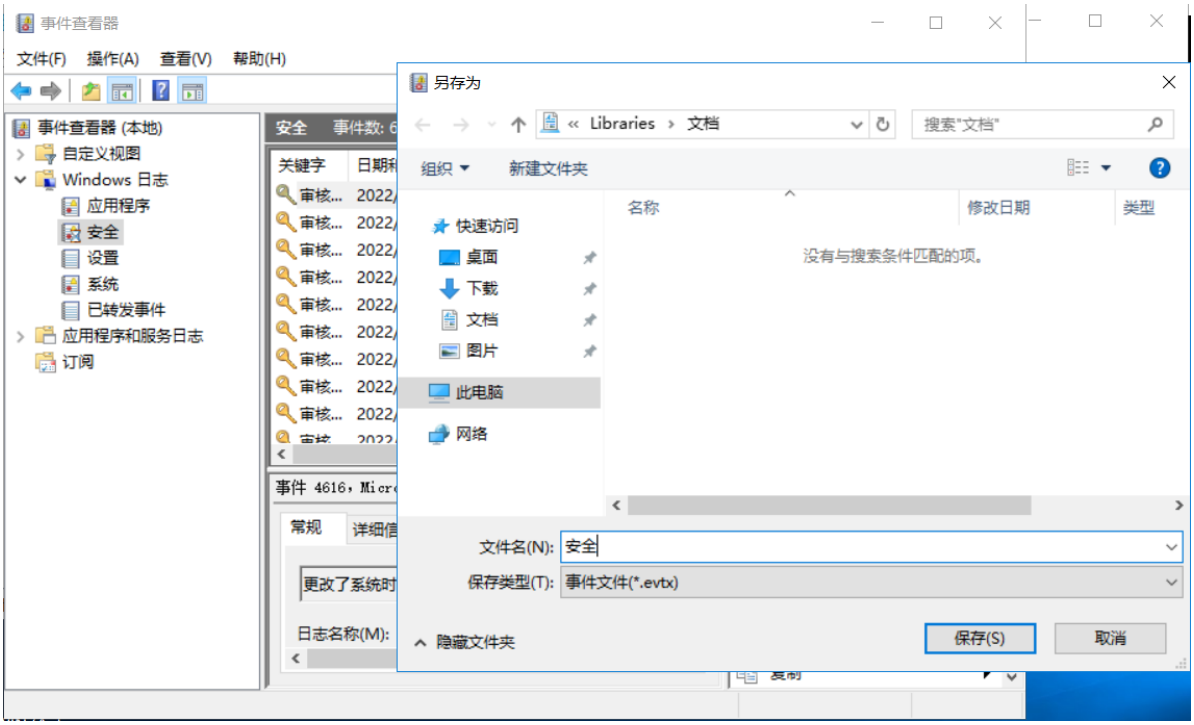
检查方法：

a、Win+R 打开运行，输入"eventvwr.msc"，回车运行，打开“事件查看器”。


事件查看器
文件(F)
操作(A)
查看(V)
帮助(H)
事件查看器 (本地)
自定义视图
Windows 日志
应用程序和服务日志
订阅
事件查看器 (本地)
概述与摘要
上次刷新时间:...
概述
若要查看已在计算机上出现的事件，请在控制台树中选择相应的来源、日志或自定义视图节
管理事件的摘要
事件类型
事件 ID
来源
最近查看的节点
名称
描述
修改时间
日志摘要
日志名称
大小(当前...
修改时间
操作
事件查看器 (本地)
打开保存的日志...
创建自定义视图...
导入自定义视图...
连接到另一台计算机...
查看
刷新
帮助

Windows 事件 ID	Windows Vista 事件 ID	事件类型	描述
512, 513, 514, 515, 516, 518, 519, 520	4608, 4609, 4610, 4611, 4612, 4614, 4615, 4616	系统事件	本地系统进程，例如系统启动，关闭和系统时间的改变。
517	4612	清除的审计日志	所有审计日志清除事件
528, 540	4624	成功用户登录	所有用户登录事件
529, 530, 531, 532, 533, 534, 535, 536, 537 539	4625	登录失败	所有用户登录失败事件
538	4634	成功用户退出	所有用户退出事件
560, 562, 563, 564, 565, 566, 567, 568	4656, 4658, 4659, 4660, 4661, 4662, 4663, 4664	对象访问	当访问一给定的对象（文件，目录等） 访问的类型(例如读，写，删除），访问是否成功或失败，谁实施了这一行为
612	4719	审计政策改变	审计政策的改变
624, 625, 626, 627, 628, 629, 630, 642, 644	4720, 4722, 4723, 4724, 4725, 4726, 4738, 4740	用户帐号改变	用户帐号的改变，像用户帐号创建，删除，改变密码等等
(631 to 641) and (643, 645 to 666)	4727 to 4737, 4739 to 4762	用户组改变	对一个用户组的所有改变，例如添加或移除一个全局组或本地组，从全局组或本地添加或移除成员等等
672, 680	4768, 4776	成功用户帐号验证	当一个域用户帐号在域控制器认证时，生成用户帐号成功登录事件。
675, 681	4771, 4777	失败用户帐号验证	失败用户帐号登录事件，当一个域用户帐号在域控制器认证时 ，生成不成功用户帐号登录事件。
682, 683	4778, 4779	主机会话状态	会话重新连接或断开

b、导出 Windows 日志 -- 安全，利用微软官方工具 Log Parser 进行分析。



工具下载地址：https://www.microsoft.com/en-us/download/details.aspx?id=24659

```
C:\Program Files (x86)\Log Parser 2.2>LogParser.exe

Microsoft (R) Log Parser Version 2.2.10
Copyright (C) 2004 Microsoft Corporation. All rights reserved.

Usage:   LogParser [-i:<input_format>] [-o:<output_format>] <SQL query> |
                   file:<query_filename>[?param1=value1+...]
                   [<input_format_options>] [<output_format_options>]
                   [-q[:ON|OFF]] [-e:<max_errors>] [-iw[:ON|OFF]]
                   [-stats[:ON|OFF]] [-saveDefaults] [-queryInfo]

         LogParser -c -i:<input_format> -o:<output_format> <from_entity>
                   <into_entity> [<where_clause>] [<input_format_options>]
                   [<output_format_options>] [-multiSite[:ON|OFF]]
                   [-q[:ON|OFF]] [-e:<max_errors>] [-iw[:ON|OFF]]
                   [-stats[:ON|OFF]] [-queryInfo]

 -i:<input_format>    :  one of IISW3C, NCSA, IIS, IISODBC, BIN, IISMSID,
                         HTTPERR, URLSCAN, CSV, TSV, W3C, XML, EVT, ETW,
                         NETMON, REG, ADS, TEXTLINE, TEXTWORD, FS, COM (if
                         omitted, will guess from the FROM clause)
 -o:<output_format>   :  one of CSV, TSV, XML, DATAGRID, CHART, SYSLOG,
                         NEUROVIEW, NAT, W3C, IIS, SQL, TPL, NULL (if omitted,
                         will guess from the INTO clause)
 -q[:ON|OFF]          :  quiet mode; default is OFF
 -e:<max_errors>      :  max # of parse errors before aborting; default is -1
```

示例：

```
LogParser.exe -i:evt "select top 100 * from Security.evtx" -o:DATAGRID
LogParser.exe -i:evt "select TimeWritten,Message from Security.evtx" -o:DATAGRID

参数使用
-i:<输入源>
中间部分：SQL语句
-o:<输出格式>
```

1.1.2 检查异常端口、进程

1、检查网络连接情况，是否有远程连接、可疑连接

检查方法：

a、使用`netstat -ano`命令查看目前的网络连接，定位可疑的 ESTABLISHED

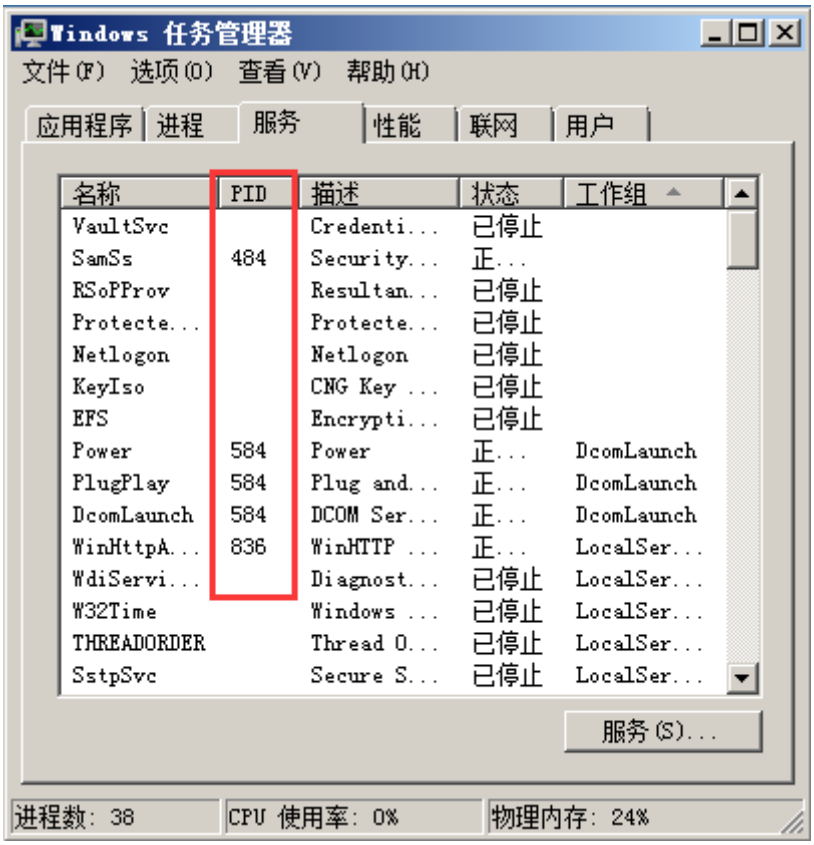
> ESTABLISHED：完成连接并正在进行数据通信的状态。
> LISTENING：表示处于侦听状态，就是说该端口是开放的，等待连接，但还没有被连接。
> CLOSE_WAIT：对方主动关闭连接或者网络异常导致连接中断。
> TIME_WAIT：我方主动调用close()断开连接，收到对方确认后状态变为TIME_WAIT。

b、根据 netstat 命令定位出的 PID 编号，再通过 tasklist 命令进行进程定位 `tasklist | findstr "PID"`

```
C:\Users\Administrator>netstat -ano | find "ESTABLISHED"
  TCP    192.168.85.209:49991   40.90.189.152:443      ESTABLISHED     324
  TCP    192.168.85.209:49992   40.90.189.152:443      ESTABLISHED     8284

C:\Users\Administrator>tasklist  | findstr "8284"
explorer.exe                  8284 Console                    2    111,960 K
```

可以进一步去任务管理器中确认（不一定能找到）



2、进程

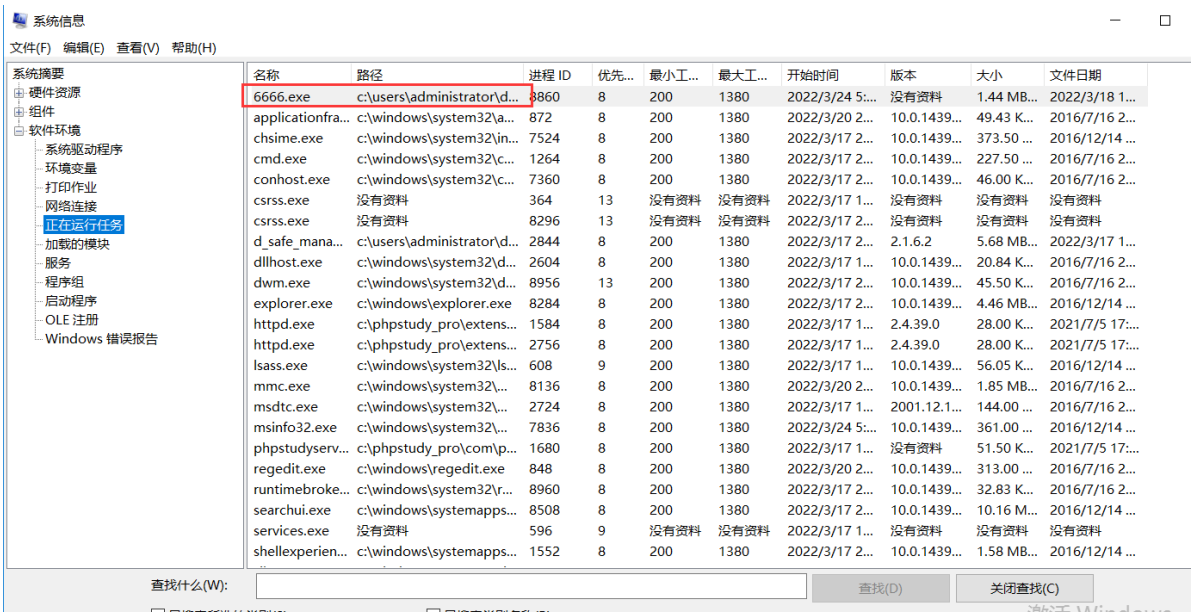
检查方法：依据进程名称查看是否有可疑进程，比如6666.exe可能是木马。

tasklist /svc

```
vm3dservice.exe                1716 VM3DService
svchost.exe                    1728 LanmanServer
dllhost.exe                    2604 COMSysApp
msdtc.exe                      2724 MSDTC
httpd.exe                      2756 暂缺
WmiPrvSE.exe                   2004 暂缺
svchost.exe                    8776 SSDPSRV
csrss.exe                      8296 暂缺
winlogon.exe                   6800 暂缺
dwm.exe                        8956 暂缺
vm3dservice.exe                2668 暂缺
RuntimeBroker.exe              8960 暂缺
svchost.exe                    7772 CDPUserSvc_d9b3e0, OneSyncSvc_d9b3e0
sihost.exe                     7556 暂缺
taskhostw.exe                  9036 暂缺
ChsIME.exe                     7524 暂缺
explorer.exe                   8284 暂缺
ShellExperienceHost.exe        1552 暂缺
SearchUI.exe                   8508 暂缺
vmtoolsd.exe                   8572 暂缺
cmd.exe                        1264 暂缺
conhost.exe                    7360 暂缺
D_Safe_Manage.exe              2844 暂缺
ApplicationFrameHost.exe        872 暂缺
regedit.exe                     848 暂缺
mmc.exe                        8136 暂缺
6666.exe                       8860 暂缺
tasklist.exe                   7472 暂缺

C:\Users\Administrator>
```

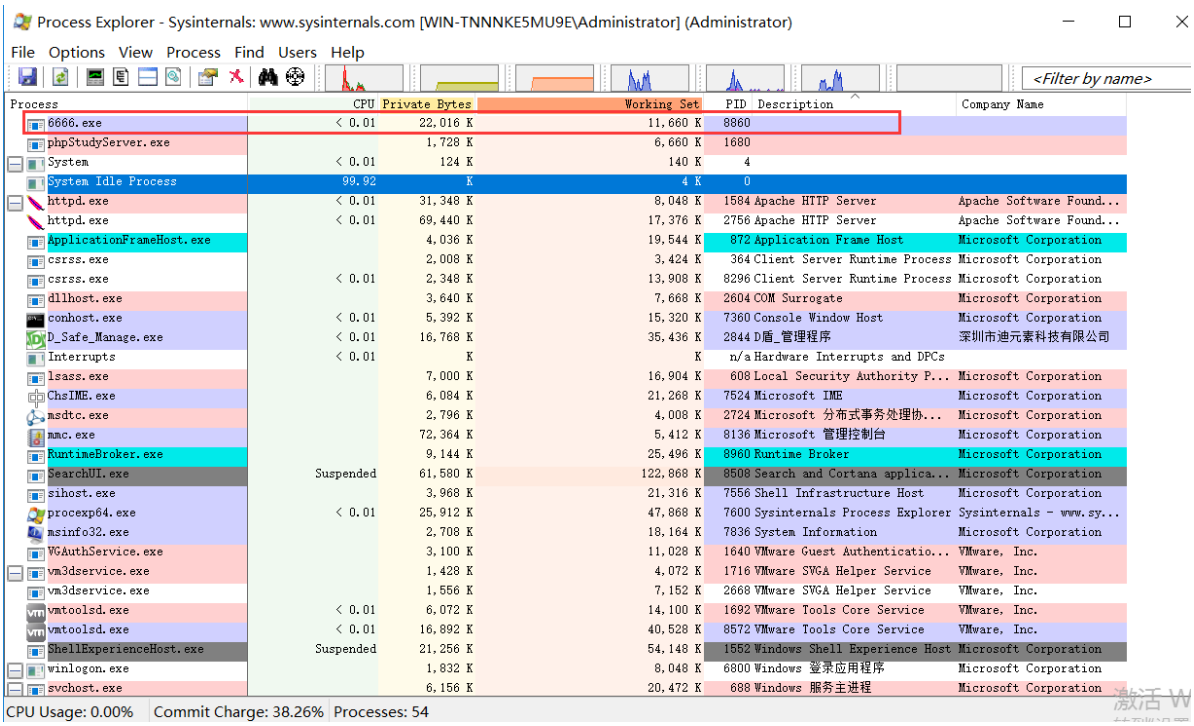
a、开始 -- 运行 -- 输入 `msinfo32` 命令，依次点击 "软件环境 -- 正在运行任务" 就可以查看到进程的详细信息，比如进程路径、进程ID、文件创建日期以及启动时间等。



b、打开D盾_web查杀工具，进程查看，关注没有可疑信息的进程

c、通过微软官方提供的 Process Explorer 等工具进行排查

工具下载地址：https://docs.microsoft.com/zh-cn/sysinternals/downloads/process-explorer



d、查看可疑的进程及其子进程

可以通过观察以下内容

没有签名验证信息的进程
没有描述信息的进程
进程的属主
进程的路径是否合法
CPU或内存资源占用长时间过高的进程（比如挖矿）

常用命令：

```
1）查看端口对应的 PID：netstat -ano | findstr "port"

2）查看进程对应的 PID：任务管理器 -- 查看 -- 选择列 -- PID 或者 tasklist  | findstr "PID"

3）查看进程对应的程序位置：

   任务管理器 -- 选择对应进程 -- 右键打开文件位置
   运行输入wmic，cmd 界面输入 process

4）tasklist /svc   进程 -- PID -- 服务

5）查看Windows服务所对应的端口：

   %systemroot%/system32/drivers/etc/services（一般 %systemroot% 就是 C:\Windows 路径）
```

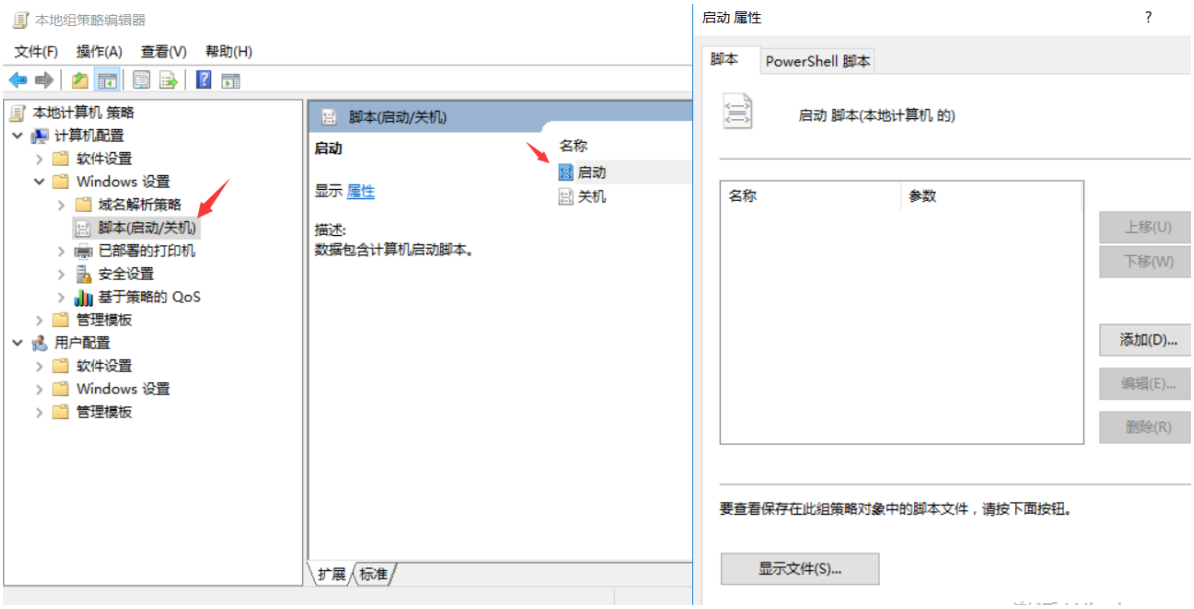
1.1.3 检查启动项、计划任务、服务

1. 检查服务器是否有异常的启动项

检查方法：
a、登录服务器，单击【开始】>【所有程序】>【启动】，默认情况下此目录在是一个空目录，确认是否有非业务程序在该目录下。
b、单击开始菜单 >【运行】，输入 `msconfig`，查看是否存在命名异常的启动项目，是则取消勾选命名异常的启动项目，并到命令中显示的路径删除文件。
c、单击【开始】>【运行】，输入 regedit，打开注册表，查看开机启动项是否正常，特别注意如下三个注册表项：

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce
```

检查右侧是否有启动异常的项目，如有请删除，并建议安装杀毒软件进行病毒查杀，清除残留病毒或木马。
d、利用安全软件查看启动项、开机时间管理等。
e、组策略，运行 `gpedit.msc`

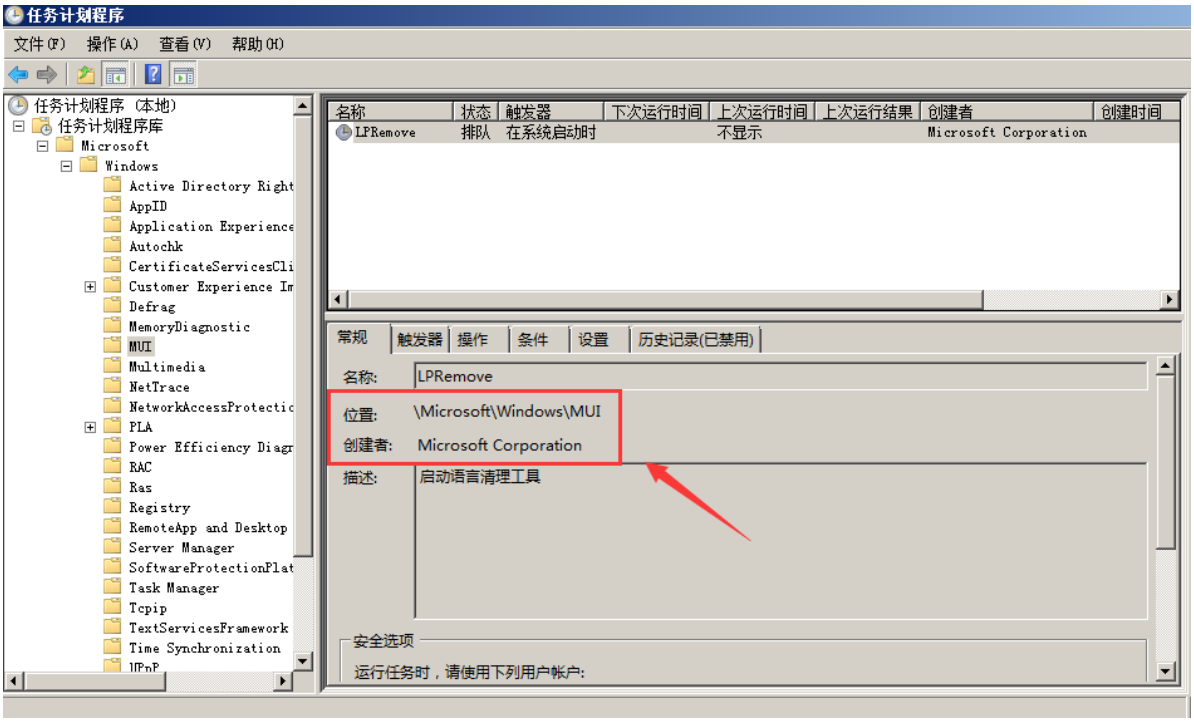


2. 检查服务器是否有异常的计划任务

检查方法：

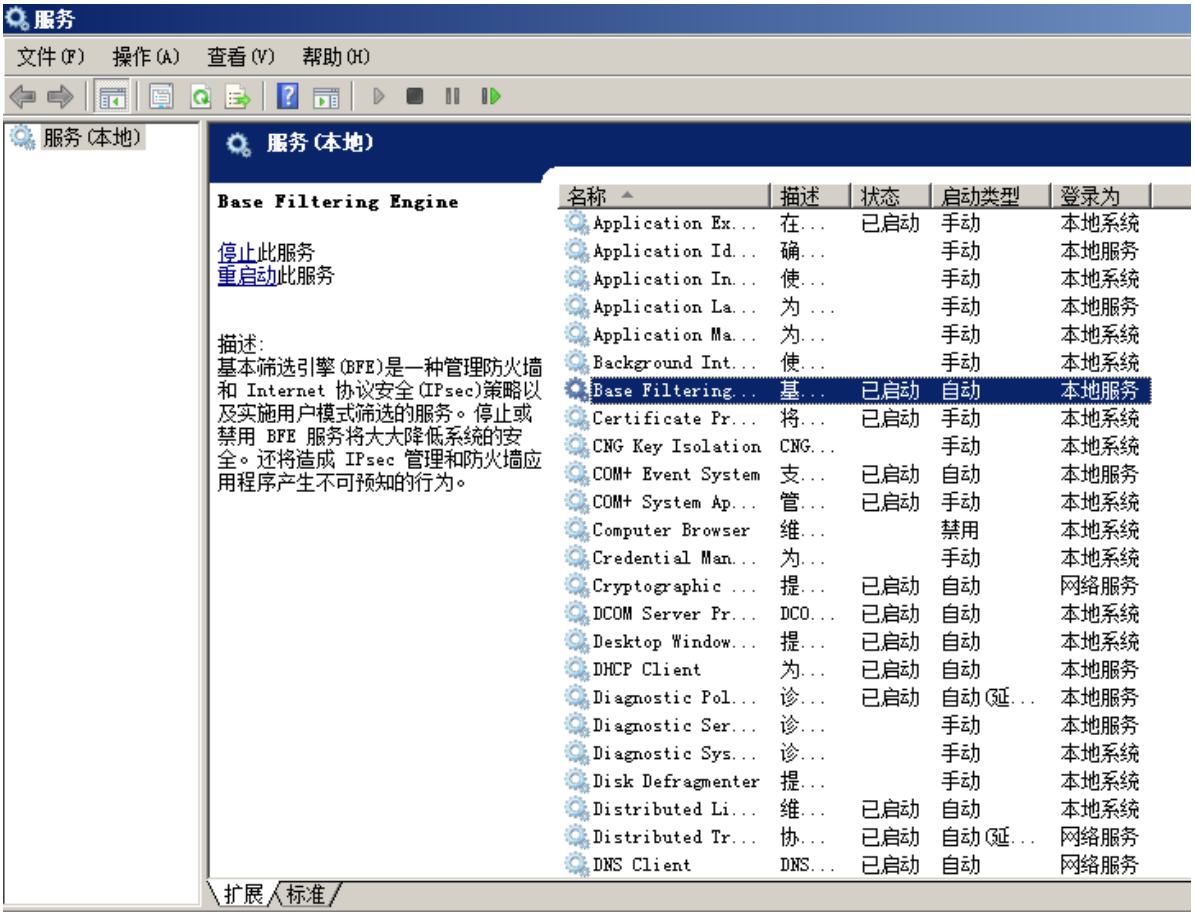
a、在桌面打开【运行】，输入 control 打开控制面板，然后在"系统与安全"中查看计划任务，便可以看到具体的计划任务及相关属性。

b、利用安全软件查看计划任务。



3. 检查服务器是否有异常的服务

检查方法：在桌面打开【运行】，输入 services.msc，查看服务状态和启动类型，检查是否有异常服务。


服务
文件(F) 操作(A) 查看(V) 帮助(H)
服务(本地)
服务(本地)
Base Filtering Engine
停止此服务
重启动此服务
描述:
基本筛选引擎(BFE)是一种管理防火墙和 Internet 协议安全(IPsec)策略以及实施用户模式筛选的服务。停止或禁用 BFE 服务将大大降低系统的安全。还将造成 IPsec 管理和防火墙应用程序产生不可预知的行为。
名称 描述 状态 启动类型 登录为
Application Ex... 在... 已启动 手动 本地系统
Application Id... 确... 手动 本地服务
Application In... 使... 手动 本地系统
Application La... 为 ... 手动 本地服务
Application Ma... 为... 手动 本地系统
Background Int... 使... 手动 本地系统
Base Filtering... 基... 已启动 自动 本地服务
Certificate Pr... 将... 已启动 手动 本地系统
CNG Key Isolation CNG... 手动 本地系统
COM+ Event System 支... 已启动 自动 本地服务
COM+ System Ap... 管... 已启动 手动 本地系统
Computer Browser 维... 禁用 本地系统
Credential Man... 为... 手动 本地系统
Cryptographic ... 提... 已启动 自动 网络服务
DCOM Server Pr... DCO... 已启动 自动 本地系统
Desktop Window... 提... 已启动 自动 本地系统
DHCP Client 为... 已启动 自动 本地服务
Diagnostic Pol... 诊... 已启动 自动(延... 本地服务
Diagnostic Ser... 诊... 手动 本地服务
Diagnostic Sys... 诊... 手动 本地系统
Disk Defragmenter 提... 手动 本地系统
Distributed Li... 维... 已启动 自动 本地系统
Distributed Tr... 协... 已启动 自动(延... 网络服务
DNS Client DNS... 已启动 自动 网络服务
扩展 标准