如何编写 Windows 安全检查脚本？（简化为批处理）

之前用 C#写了个一键式的 Windows 服务器日常检查的程序，但是客户还是觉得麻烦。因为有的服务器没有装.NET 环境，非要我写成批处理。

大家应该知道，Windows 系统问题太多，要关注的地方也数不胜数，做日常检查，真的要一个命令一个命令的翻，确实麻烦，而且，重点是注册表，挨个的展开，绝对是一个闹心的活儿。我把一些常用的命令做了个整合，有些检查方法用 C#写起来很方便，用批处理就有点不好写了

这个批处理主要检查的内容是：

1、系统信息检查

2、端口状态检查

3、添加/卸载记录

4、IE 浏览器记录

5、用户检查

6、隐藏用户检查

7、进程检查

8、注册表启动项检查

9、通信检查

10、CMD 使用记录检查

11、C 盘部分文件夹捆绑文件检查等

也就十几项吧。因为是批处理，大家可以自己根据需求添加。一个批处理，没啥技术难度，就不细讲了。

有一个使用重点，如果是涉及到注册表检查的，需要给注册表赋予权限，才能通过 reg query 来读取，大部分注册表是不允许直接读取的。权限问题吧。

这里用到了类似这样的操作

HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names [1 2 19]

注册表相关权限如下：

用 regini，是系统自带的注册表权限工具

1 - Administrators 完全访问

2 - Administrators 只读访问

3 - Administrators 读和写入访问

4 - Administrators 读、写入、删除访问

5 - Creator 完全访问

6 - Creator 读和写入访问

7 - everyone 完全访问

8 - everyone 只读访问

9 - everyone 读和写入访问

10 - everyone 读、写入、删除访问

11 - Power Users 完全访问

12 - Power Users 读和写入访问

13 - Power Users 读、写入、删除访问

14 - System Operators 完全访问

15 - System Operators 读和写入访问

16 - System Operators 读、写入、删除访问

17 - System 完全访问

18 - System 读和写入访问

19 - System 只读访问

20 - Administrators 读、写、执行访问

21 - Interactive User 完全访问

22 - Interactive User 读和写入访问

23 - Interactive User 读、写入、删除访问

命令格式为

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run [2 9 19]

里面部分命令用到了 wmic，这个工具挺好用，就是很多高级的用法，百度没有，能找到的资料真的有限。

因为实在是没太多技术含量的东西，批处理命令，大家都懂得。。

不废话了，贴出脚本命令，供大家娱乐下。

```
@echo off
echo                                    "Windows 系统安全检查脚本"
if exist d:\检查结果\ (
    echo
) else (
md d:\检查结果\
)
if not exist d:\检查结果\ md d:\检查结果\


echo "系统信息检查"
systeminfo >d:\检查结果\系统信息.log
echo "端口信息检查"
netstat -anb >d:\检查结果\端口信息.log
```

echo "进程检查"

tasklist&net start >d:\检查结果\进程检查.log

echo "进程路径检查"

wmic process get name,executablepath,processid >d:\检查结果\进程路径检查.log

echo "默认共享检查"

net share >d:\检查结果\默认共享检查.log

echo "用户信息检查"

net user & net localgroup administrators >d:\检查结果\用户信息检查.log

echo "隐藏用户检查"

echo HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names [1 2 19]>d:\regg.ini&echo HKEY_LOCAL_MACHINE\SAM\SAM\ [1 2 19] >>d:\regg.ini & regini d:\regg.ini&reg query HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names >d:\检查结果\隐藏用户检查.log&del d:\regg.ini

echo "注册表启动项检查"

reg query HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run & reg query HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run >d:\检查结果\注册表启动项检查.log

echo "安全策略检查"

secedit /export /cfg LocalGroupPolicy&type LocalGroupPolicy >d:\检查结果\安全策略检查.log

echo "IE 浏览器记录检查"

reg query HKEY_CURRENT_USER\Software\Microsoft\Internet" "Explorer\TypedURLs >d:\检查结果\IE 浏览器记录检查.log

echo "添加和卸载记录"

reg query HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL /s /v DisPlayname >d:\检查结果\添加和卸载记录.log

echo "异常状态检查"

reg query HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows" "NT\CurrentVersion\SvcHost /s /v netsvcs&reg query

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows"
"NT\CurrentVersion\SvcHost /s /v LocalService >d:\检查结果\异常状态检
查.log

    echo "通信检查"

    netstat -a >d:\检查结果\通信检查.log

    echo "CMD 记录"

    reg query
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ex
plorer\RunMRU >d:\检查结果\CMD 记录.log

    echo "文件记录检查"

    reg query
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ex
plorer\TypedPaths >d:\检查结果\文件记录检查.log

    echo "文件记录检查 2"

    reg query
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ex
plorer\ComDlg32\OpenSaveMRU\* /v * >d:\检查结果\文件记录检查 2.log

    echo "程序记录"
```

reg query HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU >d:\检查结果\程序记录.log

echo "程序记录"

reg query HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU >d:\检查结果\程序记录.log

echo "C 盘捆绑文件检查"

echo "正常可执行文件返回结果为 1，不可执行文件结果为 0，返回结果为 2 的，为存在捆绑内容文件。"

echo "请点击回车继续！"

set /p var=find /c /i "this program" c:* c:\Inetpub* C:\Users\Administrator\Desktop* c:\temp* >d:\检查结果\捆绑文件检查.log

%var%

if %ERRORLEVEL% == 0 goto yes

goto no

:yes

exit

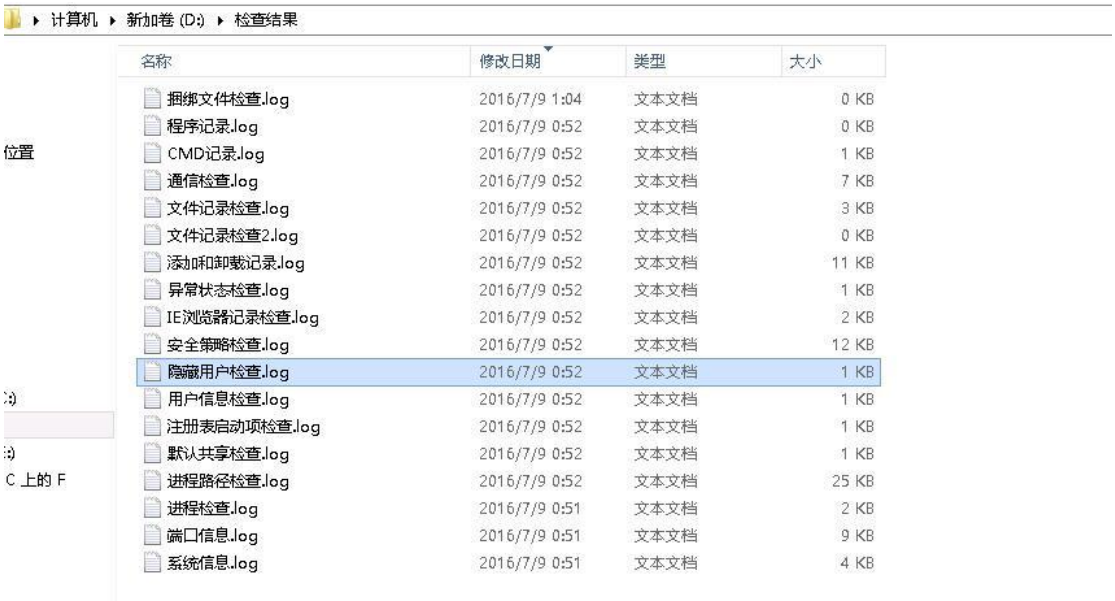
:no

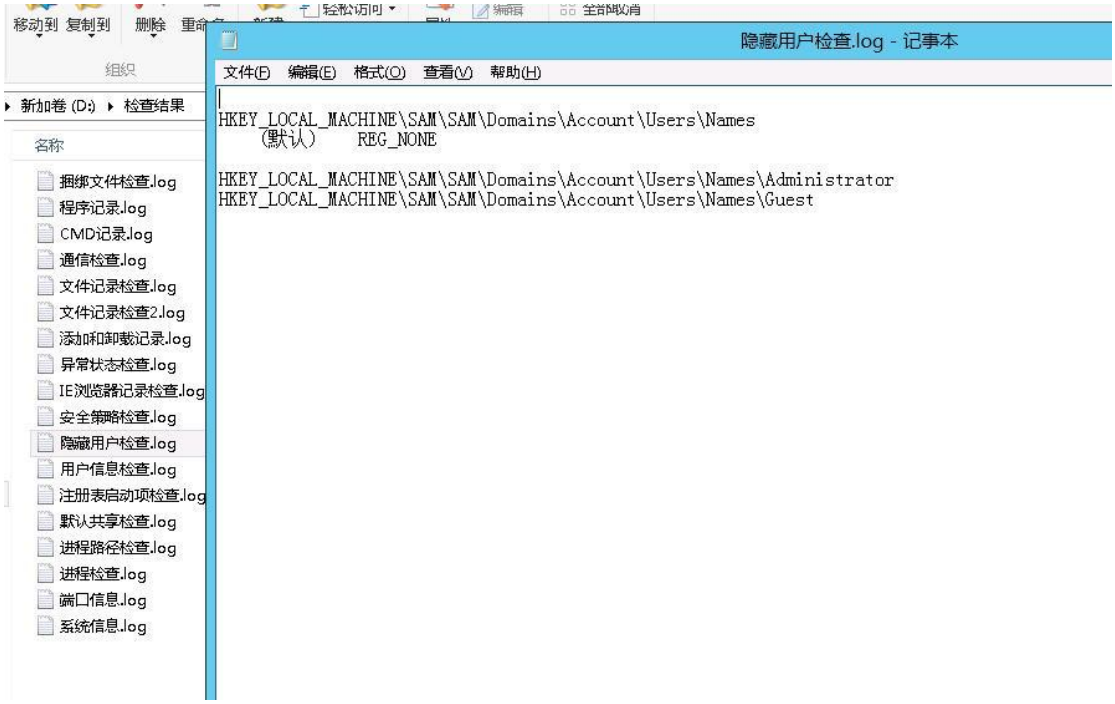
find /c /i "this program" c:* c:\wmpub* c:\Inetpub* C:\Documents and Settings\Administrator\桌面* >d:\检查结果\捆绑文件检查.log

echo "鬼魅羊羔"

执行结果会保存在 D:\检查结果\文件夹下


C:\Windows\System32\cmd.exe
TiWorker.exe 12000 Services 0 7,504 K
tasklist.exe 5588 RDP-Tcp#0 2 5,972 K
"进程路径检查"
"默认共享检查"
"用户信息检查"
\\WIN-83PG3NM6QEM 的用户帐户
Administrator Guest
命令成功完成。
"隐藏用户检查"
"注册表启动项检查"
"安全策略检查"
任务成功结束。
有关详细信息，请参阅日志 %windir%\security\logs\scesrv.log。
"IE浏览器记录检查"
"添加和卸载记录"
"异常状态检查"


计算机 ▸ 新加卷 (D:) ▸ 检查结果
名称 修改日期 类型 大小
捆绑文件检查.log 2016/7/9 1:04 文本文档 0 KB
程序记录.log 2016/7/9 0:52 文本文档 0 KB
CMD记录.log 2016/7/9 0:52 文本文档 1 KB
通信检查.log 2016/7/9 0:52 文本文档 7 KB
文件记录检查.log 2016/7/9 0:52 文本文档 3 KB
文件记录检查2.log 2016/7/9 0:52 文本文档 0 KB
添加和卸载记录.log 2016/7/9 0:52 文本文档 11 KB
异常状态检查.log 2016/7/9 0:52 文本文档 1 KB
IE浏览器记录检查.log 2016/7/9 0:52 文本文档 2 KB
安全策略检查.log 2016/7/9 0:52 文本文档 12 KB
隐藏用户检查.log 2016/7/9 0:52 文本文档 1 KB
用户信息检查.log 2016/7/9 0:52 文本文档 1 KB
注册表启动项检查.log 2016/7/9 0:52 文本文档 1 KB
默认共享检查.log 2016/7/9 0:52 文本文档 1 KB
进程路径检查.log 2016/7/9 0:52 文本文档 25 KB
进程检查.log 2016/7/9 0:51 文本文档 2 KB
端口信息.log 2016/7/9 0:51 文本文档 9 KB
系统信息.log 2016/7/9 0:51 文本文档 4 KB
位置



注：

1、C 盘捆绑文件检查有时候会有些问题，如果检查的目录不存在，这个命令就会被丢弃。。大家根据需要自己改吧。

2、默认输出的文件夹是在 D:\检查结果\中 ,这个也可以根据需要自己改下。

也许有的人看完会说，这么简单的批处理也拿出来发。确实这东西没什么技术含量，但是，因为我是个菜鸟，也是为了造福跟我一样的菜鸟们而已，就这么简单。

超级文件监控程序 V2.0 改进版（网站防挂马好手），这个是根据 shack2 的文件监控程序改的，除了监控以外，增加了对触发创建、修改、更名等文件的内容判断功能，如果内容中含有 webshell 特征，则会自动进行处理。被检测到的网马存活不会超过 20 秒。监控网站目录是个利器哟，只不过还是 C#的。。。

增加了大概 170 多个特征和关键函数的识别，还是有一定的识别能力的。