

Windows手工入侵排查思路

程序員推薦 今天

以下文章來源於Bypass，作者Bypass



Bypass

致力於分享原創高質量乾貨，包括但不限於：滲透測試、WAF繞過、代碼審計、安全運維。聞道有先後，術業有專攻，如是而已。



來自公眾號：Bypass

Windows系統被入侵後，通常會導致系統資源佔用過高、異常端口和進程、可疑的賬號或文件等，給業務系統帶來不穩定等諸多問題。一些病毒木馬會隨著計算機啟動而啟動並獲取一定的控制權，啟動方式多種多樣，比如註冊表、服務、計劃任務等，這些都是需要重點排查的地方。另外，需要重點關注服務器日誌信息，並從裡面挖掘有價值的信息。

基於以上，我們總結了Windows服務器入侵排查的思路，從Windows入侵現象、啟動方式、安全日誌等方面，對服務器最容易出現安全問題的地方進行入手排查。

01、檢查系統賬號

(1) 檢查遠程管理端口是否對公網開放，服務器是否存在弱口令。

- 檢查方法：

檢查防火牆映射規則，獲取服務器賬號登錄，也可據實際情況諮詢相關管理員。

(2) 查看服務器是否存在可疑賬號、新增賬號。

- 檢查方法：

打開cmd窗口，輸入 `lusrmgr.msc` 命令，查看是否有新增/可疑的賬號，如有管理員群組的（Administrators）裡的新增賬戶，根據實際應用情況，保留或刪除。

(3) 查看服務器是否存在隱藏賬號、克隆賬號。

- 檢查隱藏賬號方法：

CMD命令行使用“`net user`”，看不到“`test$`”這個賬號，但在控制面板和本地用戶和組是可以顯示此用戶的。

- 檢查克隆賬號方法：

打開註冊表，查看管理員對應鍵值。

- 使用D盾_web查殺工具，集成了對克隆賬號檢測的功能。

ID	帳號	全名	描述	D盾_检测说明
3ED	test\$			危险！克隆了[管理帐号]
3EE	test1\$			带\$帐号（一般用于隐藏帐号）
1F4	Administrator		管理计算机(域)的内置...	[管理帐号]
1F5	Guest		供来宾访问计算机或访...	
3E8	IUSR_WIN2008-NE...	Internet 来宾帐户	用于匿名访问 Interne...	

(4) 结合Windows安全日志，查看管理员登录时间、用户名是否存在异常。

- 检查方法：

Win+R打开运行，输入“`eventvwr.msc`”，回车运行，打开“事件查看器”。或者我们可以导出Windows日志—安全，利用Log Parser进行分析。

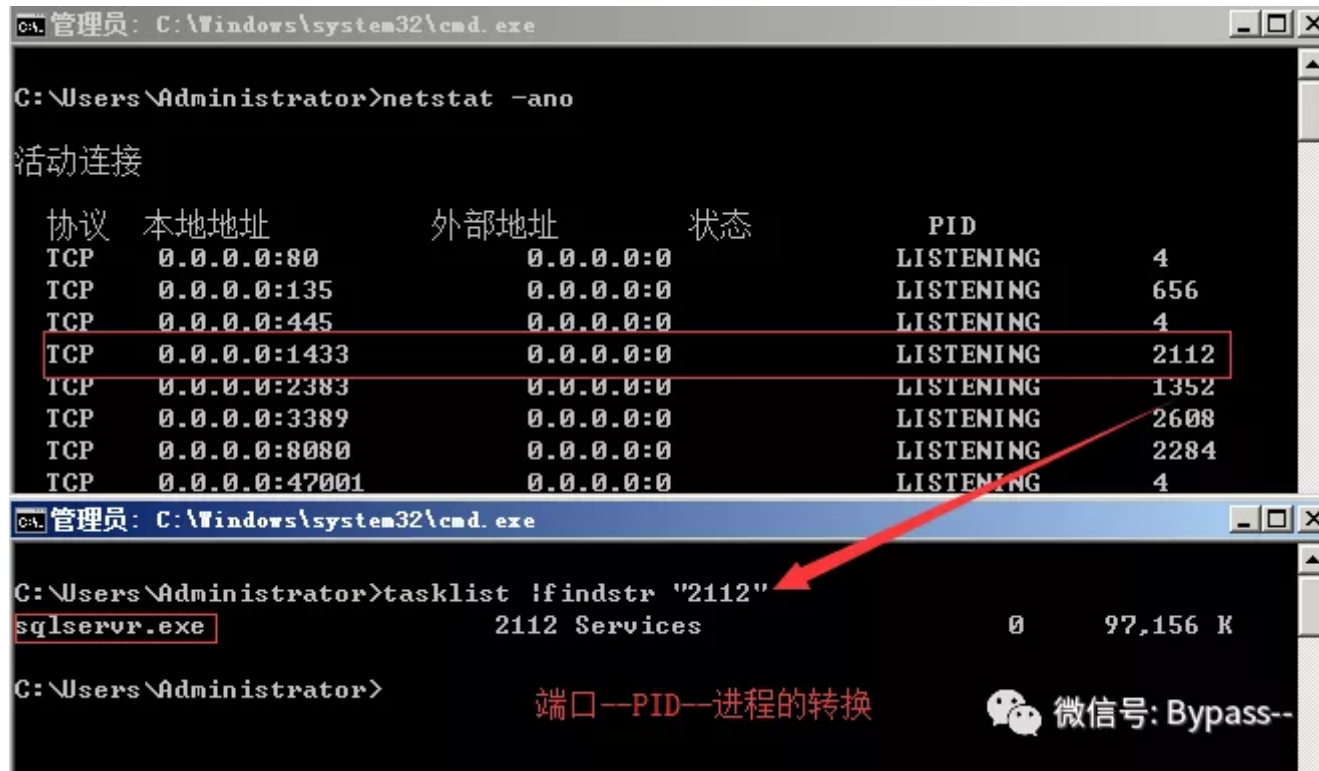
02、检查异常端口

(1) 检查端口连接情况

- 检查方法:

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

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



```
C:\Users\Administrator>netstat -ano

活动连接

协议 本地地址          外部地址          状态          PID
TCP 0.0.0.0:80         0.0.0.0:0         LISTENING      4
TCP 0.0.0.0:135        0.0.0.0:0         LISTENING      656
TCP 0.0.0.0:445        0.0.0.0:0         LISTENING      4
TCP 0.0.0.0:1433      0.0.0.0:0         LISTENING      2112
TCP 0.0.0.0:2383      0.0.0.0:0         LISTENING      1352
TCP 0.0.0.0:3389      0.0.0.0:0         LISTENING      2608
TCP 0.0.0.0:8080      0.0.0.0:0         LISTENING      2284
TCP 0.0.0.0:47001     0.0.0.0:0         LISTENING      4

C:\Users\Administrator>tasklist /f findstr "2112"

sqlservr.exe           2112 Services           0      97,156 K

C:\Users\Administrator>
```

端口—PID—进程的转换

微信号: Bypass--

(2) 检查可疑的网络连接

- 检查方法

检查是否存在可疑的网络连接，如发现异常，可使用Wireshark网络抓包辅助分析。

03、检查异常进程

(1) 检查是否存在可疑的进程

- 检查方法：

- a、开始—运行—输入msinfo32，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、启动时间等。
- b、打开D盾_web查杀工具，进程查看，关注没有签名信息的进程。
- c、通过微软官方提供的 Process Explorer 等工具进行排查。
- d、查看可疑的进程及其子进程。可以通过观察以下内容：

- 1 没有签名验证信息的进程
- 2 没有描述信息的进程
- 3 进程的属主
- 4 进程的路径是否合法
- 5 CPU或内存资源占用长时间过高的进程

(2) 如何找到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

04、检查启动项

(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：

```
1 HKEY_CURRENT_USER\software\micorsoft\windows\currentversion\run
2 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
3 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。

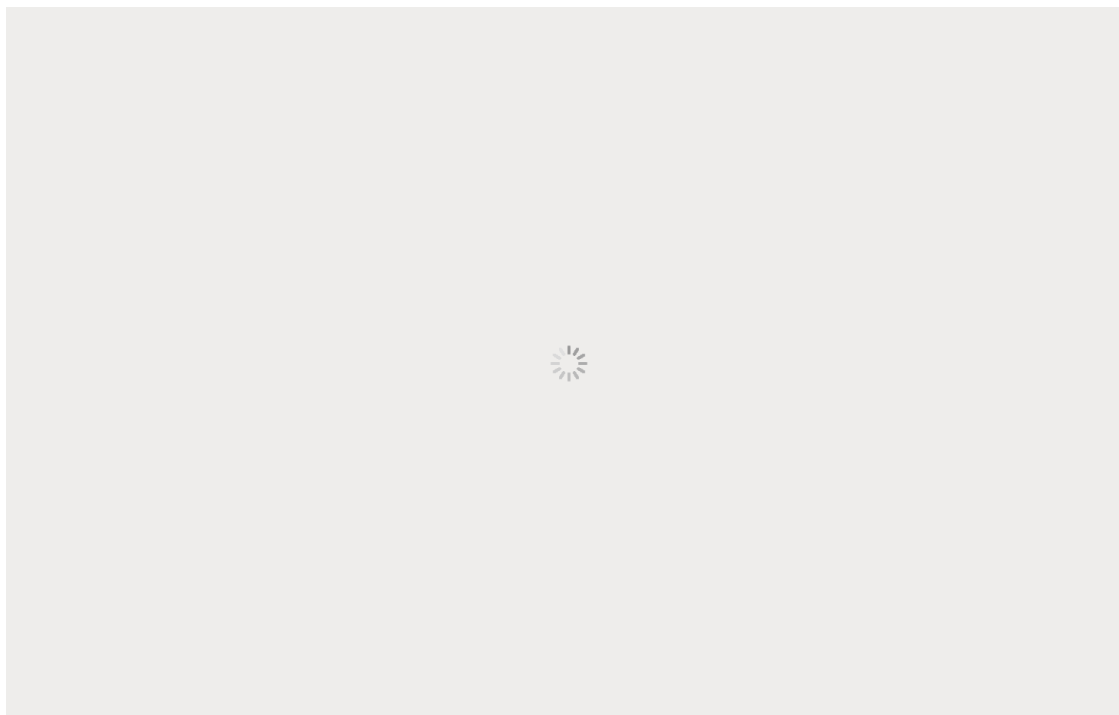
05、检查计划任务

(1) 检查计划任务里是否有可疑的脚本执行

- 检查方法：

a、单击【开始】>【设置】>【控制面板】>【任务计划】，查看计划任务属性，便可以发现木马文件的路径。

b、单击【开始】>【运行】；输入cmd，然后输入at，检查计算机与网络上的其它计算机之间的会话或计划任务，如有，则确认是否为正常连接。

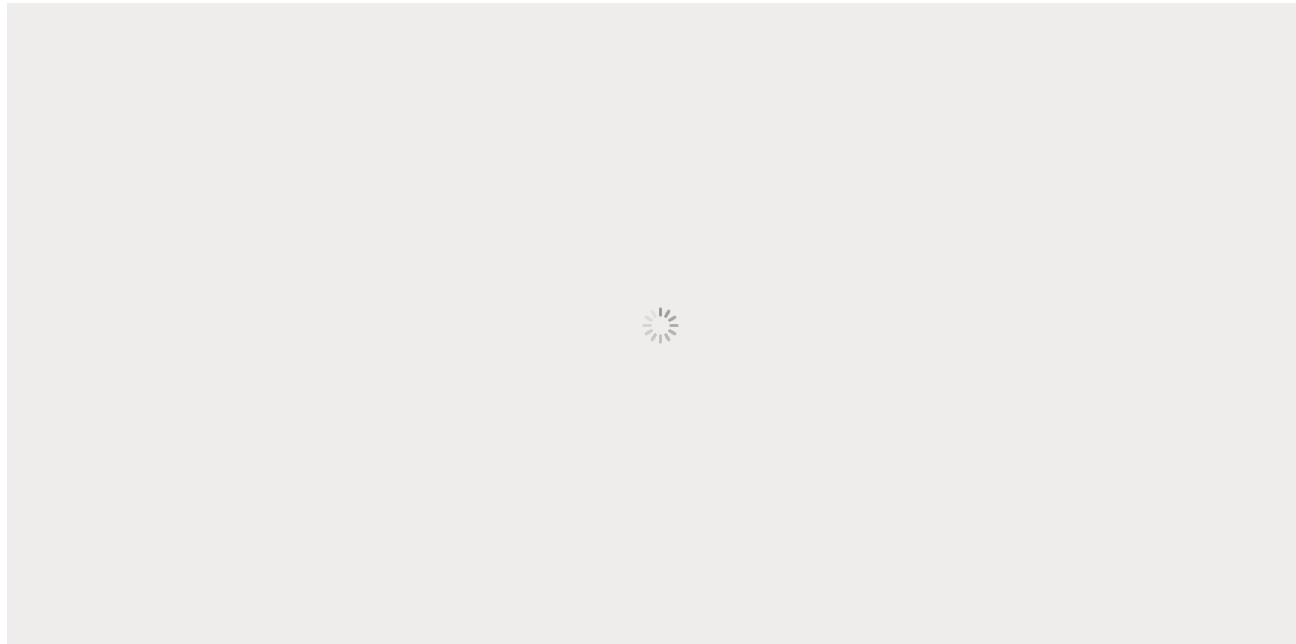


06、检查服务

(1) 检查系统服务名称、描述和路径，确认是否异常

- 检查方法：

单击【开始】>【运行】，输入services.msc，注意服务状态和启动类型，检查是否有异常服务。



07、检查可疑文件

(1) 检查新建文件、最近访问文件和相关下载目录等

- 检查方法：

- a、查看用户目录，新建账号会在这个目录生成一个用户目录，查看是否有新建用户目录。

Window 2003 C:\Documents and Settings

Window 2008R2 C:\Users\

- b、单击【开始】>【运行】，输入%UserProfile%\Recent，分析最近打开分析可疑文件。

- c、在服务器各个目录，可根据文件夹内文件列表时间进行排序，查找可疑文件。

d、回收站、浏览器下载目录、浏览器历史记录

e、修改时间在创建时间之前的为可疑文件

(2) 发现一个WEBSHELL或远控木马的创建时间，如何找出同一时间范围内创建的文件？

- 检查方法：

a、利用 Registry Workshop 注册表编辑器的搜索功能，可以找到最后写入时间区间的文件。

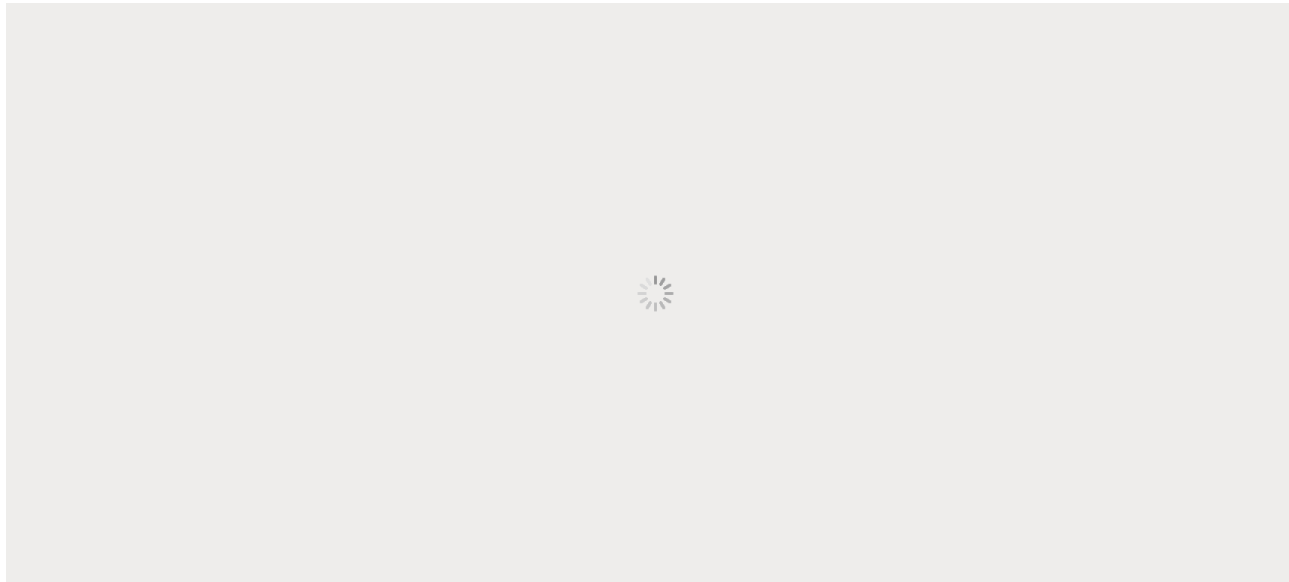
b、利用计算机自带文件搜索功能，指定修改时间进行搜索。

08、检查系统日志

(1) 检查系统安全日志

一般来说，可以通过检查Windows安全日志来获悉账号登录情况，比如成功/失败的次数。

```
1 LogParser.exe -i:EVT -o:DATAGRID "SELECT EXTRACT_TOKEN(Strings,10,'|') as EventType, EXTRACT_TOKEN(Strings,5,'
```

(2) 历史命令记录

高版本Powershell会记录PowerShell的命令，所有的PowerShell命令将会保存在固定位置：

```
1 %appdata%\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt
```

查看PowerShell历史记录：

```
1 Get-Content (Get-PSReadlineOption).HistorySavePath
```

默认Powershell v5支持,Powershell v3和Powershell v4，需要安装Get-PSReadlineOption後才可以使用。

關注我們，查看更多乾貨！ ▼ ▼ ▼



程序員推薦

推薦各種程序員乾貨，包括但不限於程序員書籍資料、軟件開發工具、編程項目實戰及程序員熱點資訊。

5篇原創內容



公眾號

喜歡此內容的人還喜歡

樂觀鎖與悲觀鎖各自適用場景是什麼？

後端Q



快速弄懂陌生領域是一項“賺錢”的能力

跨界架構師



Chrome正在獲得新的漸進式Web應用程序功能

OSC開源社區

