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。

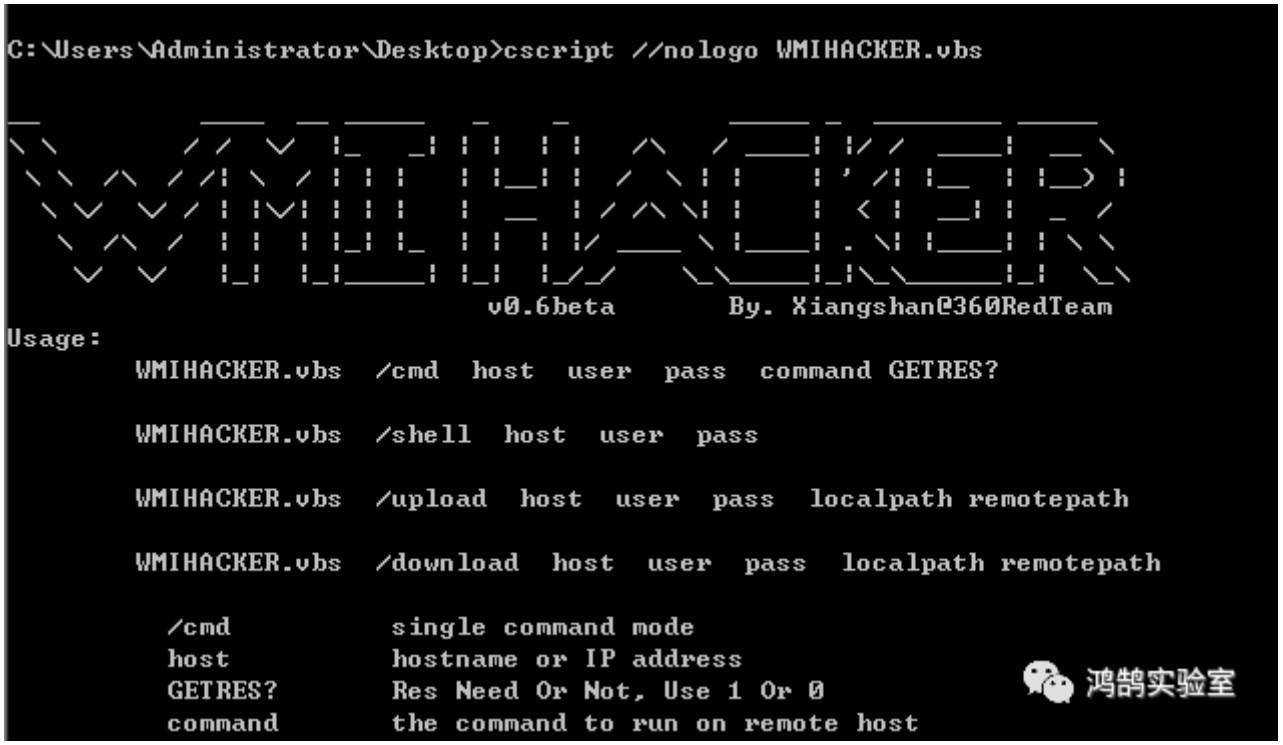
具体的介绍自己去看360的介绍吧，下面演示一下它的基本用法。

测试环境：

攻击机：win2008
受害者：win2008 + 360全家桶


360安全卫士12
我的电脑
木马查杀
电脑清理
系统修复
优化加速
功能大全
横向渗透防护
防止内网渗透攻击 保护本机安全
防御内网中其他中毒电脑对本机的渗透，阻断病毒木马传播扩散
查看详情
已开启
远程服务创建防护
防止内网其他机器在本机中创建恶意服务
远程计划任务创建防护
防止内网其他机器在本机创建恶意计划任务
远程注册表篡改防护
防止内网其他机器恶意篡改本机注册表
远程WMI命令执行防护
防止内网其他机器在本机执行恶意WMI命令
远程com组件调用防护
防止内网其他机器调用本机com组件
远程系统工具进程启动
防止网络恶意启动本机特殊系统进程进行渗透
鸿鹄实验室

使用方法：



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

```
C:\Users\Administrator\Desktop>cscript //nologo WMIHACKER.vbs /cmd 192.168.0.106
 administrator "abc123!" "ipconfig" 1
```

全程360无反应。

除此之外还有下面的利用方法:

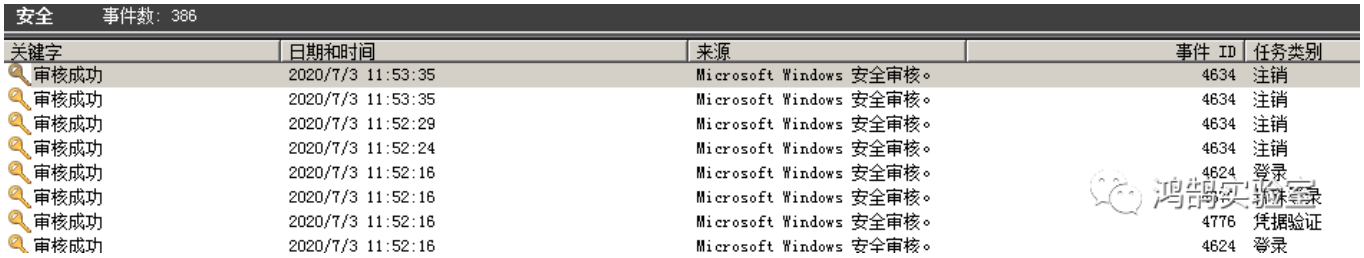
```
cscript wmihacke.vbs /cmd 192.168.0.106 administrator "abc123!" "echo whoami > c:1.txt" 0
```

获得一个交互式shell

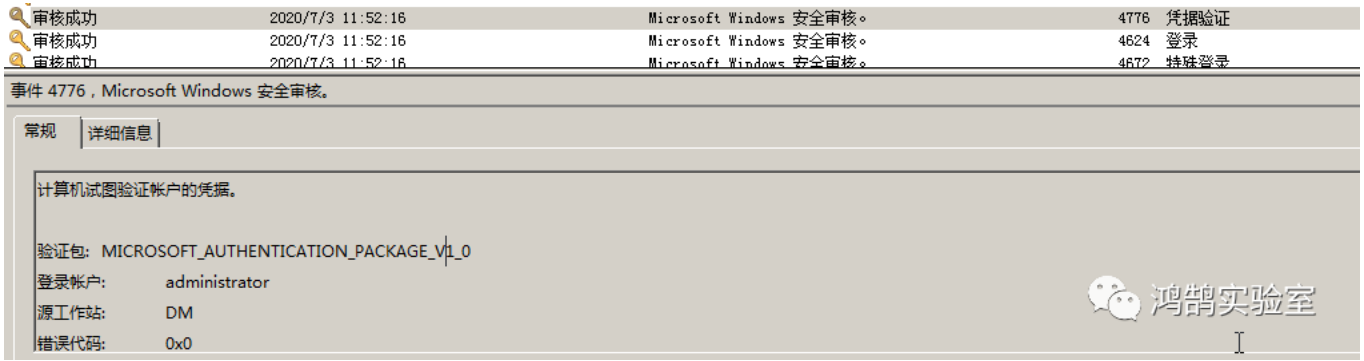
```
C:\Users\Administrator\Desktop>cscript //nologo WMIHACKER.vbs /shell 192.168.0.1
06 administrator "abc123!"
```

当然其还有上传、下载文件的功能。

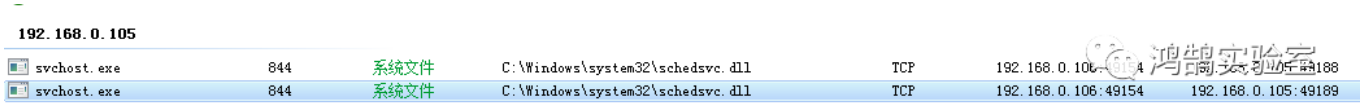
使用该工具时会在目标系统上产生4634、4624、4672、4776的登录日志



且会泄漏源地址：



使用该进程进行通信：



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。