

msbackdoor

发表于 2021-09-01 分类于 [Challenge](#) , [2021](#) , [工业信息安全技能大赛](#) , [巡回赛-杭州站](#)
Challenge | 2021 | 工业信息安全技能大赛 | 巡回赛-杭州站 | msbackdoor

[点击此处](#)获得更好的阅读体验

WriteUp来源

来自Venom战队

题目描述

分析后门程序，找出其中的c2服务器，并提交其ip。提示：ip地址为中国大陆ip，提交格式：ip。

题目考点

- 样本分析

解题思路

有很多花指令。花指令主要分两种，一个是用call代替jmp，一个是call\$ pop add push ret。处理太麻烦了。

patch掉父进程检测（共三处）

□

patch 掉一个联网验证服务器，包括一处网络连接和一个 strcmp，也可以把硬编码的IP替换成127.0.0.1。

□

□

□

然后直接 strace 即可看到实际 C2 的 IP 和端口。

Flag

```
1 flag{47.100.78.75}
```

- 本文作者：CTFHub
- 本文链接：<https://writeup.ctfhub.com/Challenge/2021/工业信息安全技能大赛/巡回赛-杭州站/iZprw3mmiqhsNuBp1GYcp.html>
- 版权声明：本博客所有文章除特别声明外，均采用 [BY-NC-SA](#) 许可协议。转载请注明出处！

[#Challenge](#) [#2021](#) [#工业信息安全技能大赛](#) [#巡回赛-杭州站](#)

[16](#)

[被黑客修改的程序](#)