

CTFHub

Writeup



WiFi

📅 2021-09-01 | 📁 Challenge , 2021 , 工业信息安全技能大赛 , 巡回赛-上海站

Challenge | 2021 | 工业信息安全技能大赛 | 巡回赛-上海站 | WiFi

[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

在无线WIFI通信中，黑客截获了数据包，想破解里面的密码，请找出里面的flag。

题目考点

- 力控软件使用

解题思路

将 may目录下的文件内容去掉 [] 之后组成字典，使用 **aircrack-ng** 直接跑包，找到的密码即为 flag

```
→ 桌面 aircrack-ng -w ./dict.txt ./-01.cap  
Opening ./-01.capplease wait...  
Read 3473 packets.
```

#	BSSID	ESSID	Encryption
1	EE:52:37:27:75:EB	target	WPA (1 handshake)

```
Choosing first network as target.
```

```
Opening ./-01.capplease wait...  
Read 3473 packets.
```

```
1 potential targets
```



Flag



```
1 flag{0TUMVxz0JrUSDxHG}
```

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-上海站/sTf9se8XNHRV7dep7CgE9P.html>

版权声明：本博客所有文章除特别声明外，均采用 [CC 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-上海站](#)

< Modbus

baby_hash >

© 2019 – 2022 ❤ CTFHub

由 [Hexo](#) & [NexT.Gemini](#) 强力驱动