注意: Hardnested 指令针对的是扫描出默认密码,而解不出有密扇区的卡。对电脑配置要求较高,建议太老电脑就不要使用了。

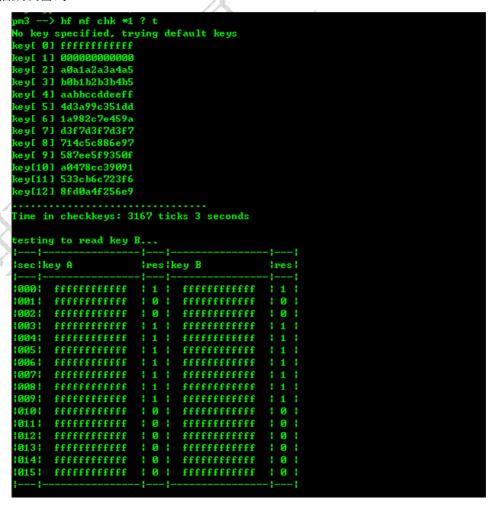
1. 刷 iceman 固件

名称	修改日期	类型	大小
🖟 firmware_win	2016/12/14 22:18	文件夹	
🔟 flasher.exe	2016/11/19 18:10	应用程序	135 KB
⊗ libgcc_s_dw2-1.dll	2016/11/19 18:10	应用程序扩展	116 KB
剧ICEMAN固件.bat	2016/12/14 22:24	Windows 批处理	3 KB
③ 刷出厂固件.bat	2016/11/28 22:37	Windows 批处理	3 KB
🔍 刷离线嗅探固件.bat	2016/11/28 22:37	Windows 批处理	3 KB

2. 进入 PM3 发布资料_DEC\官方软件固件\pm3-bin-iceman\client 打开

		All	
ртпо_тпаzетп.ру	2010/11/20 17:32	FT X1+	1 VD
pm3_mfdread.py	2016/11/26 17:52	PY 文件	9 KB
PM3指令台.bat	2016/11/28 22:46	Windows 批处理	2 KB
proxmark3.exe	2016/11/26 18:37	应用程序	2,703 KB
proxmark3.log	2016/12/14 22:30	文本文档	99 KB
A OLEC III	2016/10/21 0 01	ト目も中さま	E 220 KD

3. 扫描默认密码



4. 根据步骤 3,使用 hardnested 指令破解有密扇区

```
pm3 --> hf mf hardnested 0 A FFFFFFFFFFF 4 A w
--target block no: 4, target key type:A, known target key: 0x00000000000 (not
set), file action: write, Slow: No, Tests: 0
Allocating memory for partial statelists...
Generating partial statelists...
Generating bitflip statelist...
```

解释: hf mf hardnested 0 A FFFFFFFFFF 4 A w

0: 为默认密码的扇区块号,比如根据步骤 3,得知道 0扇区是默认密码,那么 0扇区 0块肯定是这个密码,

A: 代表 0 块的 A 密码

4: 代表第四块区,即第 1 扇区,从步骤 3 的图可以看到第 1 扇区不是默认密码。如果要破解其他扇区的话,数字应该为设扇区号*4

A: 代表破解的是第四块区的 A 密码

5. 破解出密码

这个过程会根据卡的破解难易程度,耗费的时间不等,对计算机占用不较高,建议关闭 其他的操作。

6. 记录每次破解的密码。有了密码就可以读出扇区内容。