

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
刷ICEMAN固件.bat	2016/12/14 22:24	Windows 批处理...	3 KB
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

pm3_mfuzern.py	2016/11/20 17:52	Python 文件	1 KB
pm3_mfdread.py	2016/11/26 17:52	Python 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	文本文件	99 KB
...

3. 扫描默认密码

```
pm3 --> hf mf chk *1 ? t
No key specified, trying default keys
key[ 0] ffffffff
key[ 1] 000000000000
key[ 2] a0a1a2a3a4a5
key[ 3] b0b1b2b3b4b5
key[ 4] aabbccddeeff
key[ 5] 4d3a99c351dd
key[ 6] 1a982c7e459a
key[ 7] d3f7d3f7d3f7
key[ 8] 714c5c886e97
key[ 9] 587ee5f9350f
key[10] a0478cc39091
key[11] 533cb6c723f6
key[12] 8fd0a4f256e9
.....
Time in checkkeys: 3167 ticks 3 seconds

testing to read key B...
|-----|-----|-----|-----|
|sec|key A          |res|key B          |res|
|-----|-----|-----|-----|
|000| ffffffff         | 1 | ffffffff         | 1 |
|001| ffffffff         | 0 | ffffffff         | 0 |
|002| ffffffff         | 0 | ffffffff         | 0 |
|003| ffffffff         | 1 | ffffffff         | 1 |
|004| ffffffff         | 1 | ffffffff         | 1 |
|005| ffffffff         | 1 | ffffffff         | 1 |
|006| ffffffff         | 1 | ffffffff         | 1 |
|007| ffffffff         | 1 | ffffffff         | 1 |
|008| ffffffff         | 1 | ffffffff         | 1 |
|009| ffffffff         | 1 | ffffffff         | 1 |
|010| ffffffff         | 0 | ffffffff         | 0 |
|011| ffffffff         | 0 | ffffffff         | 0 |
|012| ffffffff         | 0 | ffffffff         | 0 |
|013| ffffffff         | 0 | ffffffff         | 0 |
|014| ffffffff         | 0 | ffffffff         | 0 |
|015| ffffffff         | 0 | ffffffff         | 0 |
|-----|-----|-----|-----|
```

4. 根据步骤 3，使用 `hardnested` 指令破解有密扇区

```
pm3 --> hf mf hardnested 0 A FFFFFFFF 4 A w
--target block no: 4, target key type:A, known target key: 0x000000000000 (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 FFFFFFFF 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

FFFFFFFF: 为 0 块 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

```
0 states...
.....Validating key search space
*
Time for bruteforce 9.2 seconds.
Found key: ffff93831077
Acquired a total of 12880 nonces in 136.9 seconds (5644 nonces/minute)
pm3 --> _
```

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。