Proxmark3命令帮助

（重定向自Proxmark3使用手册）

目录

使用技巧

- Proxmark3的命令使用最小匹配模式，每个命令只要输入到可以唯一识别即可，例如 hf mf chk ，在hf mf 下只有一个c开头的命令chk,所以hf mf chk ，hf mf ch， hf mf c都是等价的，所以看到网上资料里的命令不一样不要怀疑，他们是等价的。

- Proxmark3每次运行都会在同目录下产生一个proxmark3.log文本文件，这个文件记录着Proxmark3执行你每条命令的结果。记住，只是命令执行的结果。命令本身存储的同目录.history文件里面。需要看历史记录可以打开proxmark3.log以及.history查看。

- 输入所有存在命令，不加任何参数，会直接显示该命令的帮助信息。

- 所有的命令帮助中，用大括号{}括起来的，并且有省略号的表示有下一级的命令。例如hf命令下的14a、14b、15、legic、iclass、mf的帮助信息都是{ …}形式，表示还存在下一级的命令。

- 当你使用hf mf chk自动化操作的时候，如果全卡为默认Key，请手动创建一个16进制文件名为dumpkeys.bin的文件，并且把已知的所有KeyA/B写入文件内！先写KeyA，在写KeyB，记住不要有空格/回车！然后放在Proxmark3客户端目录下，再执行hf mf dump，你就会得到全卡的dumpdata啦！前提是KeyB为write.

- Em4x的卡直接放卡一直不出ID，可以试试这个技巧：一开始先执行410xwatch，然后再往上放卡，一般就能出Tag ID。

- 高频命令中针对UID卡的所有命令都不需要Key，直接读写UID卡。

help 主帮助命令（基于r830以及以下版本）

help	显示帮助. （使用命令 '<command> help'获取相关命令的详细帮助信息。当然直接输入相关命令，不加help，也能出现该命令的帮助信息。）// 例如 hw help 与 hw 是等价的。
data	图形窗口/缓冲区数据操作等等
exit	退出Proxmark3的终端环境
hf	高频相关命令
hw	硬件检测相关命令
lf	低频相关命令
quit	退出Proxmark3的终端环境等同exit

hw 硬件检测相关命令

help	显示帮助
detectreader	['l'/'h'] --检测外部读卡器频率区域（选项“l”或“h”限制到低频LF或高频HF）
fpgaoff	设置FPGA为关闭
lcd	<16进制命令> <次数> -- 发送命令/数据到LCD
lcdreset	重置LCD
readmem	从芯片中读取10进制地址的存贮器
reset	重置Proxmark3
setlfdivisor	<19 - 255> -- 在12Mhz/(基数+1)驱动LF天线
setmux	<loraw/hiraw/lopkd/hipkd> -- 设置ADC多路复用器为一个特定的值
tune	测量天线的调谐
version	显示Proxmark3的固件版本信息

data 图形窗口/缓冲区数据操作等命令

help	显示帮助
amp	放大峰值
askdemod	<0/1>—尝试调制显示移幅键控的波形
autocorr	<窗口长度> — 自动校正窗口
bitsamples	获得原始样本作为bit
bitstream	[时钟速率] — 转换成比特流的波形
buffclear	清除缓冲样本和图形窗口
dec	抽取样本
detectclock	检测时钟速率
fskdemod	作为HID的FSK显示波形图形窗口
grid	<x> <y> — 在图形上窗口覆盖网格，用0值关闭
hexsamples	<区块> [<偏移>] --作为16进制转储较大缓冲区
hide	隐藏图形窗口
hpf	从轨迹线移除直流偏移
load	<文件名> -- 从文件加载轨迹（给图形窗口）
ltrim	<samples> -- 从左轨迹整理样本
mandemod	[i] [时钟速率] —曼彻斯特解调二进制流（选项“i”颠倒输出）
manmod	[时钟速率] —曼彻斯特解调二进制流
norm	正常大小改变最大/最小至+/-500
plot	显示图形窗口（点击窗口中的'h'显示按键帮助）
samples	[128 - 16000] -- 从图形窗口获取原始样本
save	<文件名> --保存轨迹（从图形窗口）
scale	<数值> -- 设置光标的显示比例
threshold	<阈值> --根据阈值最大化/最小化图形窗口
zerocrossings	计算零交点的时间

lf 低频相关命令

help	显示帮助
cmdread	<off> <'0'> <'1'> <命令> ['h'] -- 在读取之前发送命令来调整LF读卡器周期（以微妙为单位）（'h'选项为134）
em4x	EM4X卡类相关命令...
flexdemod	解调FlexPass样本
hid	HID卡类相关命令...
indalademod	['224'] --解调Indala样本的64位UID（选项'224'是224位）
indalaclone	[UID] ['l']-- 克隆Indala到T55x7卡 （标签必须在天线上)(UID为16进制)(选项'l'表示224位UID)
read	['h'] -- 读取125/134 kHz的低频ID标签(选项'h'是134)
sim	[GAP] -- 从可选GAP的缓冲区模拟低频标签(以微秒为单位)
simbidir	模拟低频标签（在读卡器和标签之间双向传输数据）
simman	<时钟> <比特率> [GAP] 模拟任意曼彻斯特低频标签
ti	TI卡类相关命令...
hitag	Hitag标签与应答相关…
vchdemod	['clone'] - 解调VeriChip公司样本
t55xx	T55xx卡类相关命令...
PCF7931	PCF7931卡类相关命令...

lf em4x (EM4X卡类相关命令...)

help	显示帮助
em410xread	[时钟速率] -- 提取EM410x标签的ID
em410xsim	<UID> — 模拟EM410x标签
em410xwatch	读取EM410x标签，2000次取样获取ID
em410xwrite	<UID> <'0' T5555> <'1' T55x7> --把EM410x UID写入T5555(Q5)或T55x7标签
em4x50read	从EM4x50标签中读取数据
readword	<Word>—读取EM4xxx字符数据
readwordPWD	<Word><Password>--在密码模式下读取EM4xxx字符数据
writeword	<Word>—写入EM4xxx字符数据
writewordPWD	<Data><Word><Password>—在密码模式下写入EM4xxx字符数据

lf hid (HID卡类相关命令...)

help	显示帮助
demod	解调HID Prox卡II（不是最佳）
fskdemod	实时的HID FSK解调器
sim	<ID> — 模拟HID标签
clone	<ID> — 克隆HID到T55x7卡（标签必须是在天线上）

lf ti (TI卡类相关命令...)

help	显示帮助
demod	TI型LF标签解调原始位
read	读取和解码TI类134kHz的标签
write	新的数据写入一个能读/写的TI类134kHz标签

lf hitag (Hitag标签与应答相关…)

help	显示帮助
list	列出Hitag嗅探的数据
reader	作为读卡器读取Hitag标签的数据
sim	模拟Hitag应答
snoop	窃听Hitag通信

hf 高频相关命令

help	显示帮助
14a	ISO14443A卡的相关命令...
14b	ISO14443B卡的相关命令...
15	ISO15693卡的相关命令...
epa	德国身份证的相关命令...
legic	LEGIC卡的相关命令...
iclass	ICLASS卡的相关命令...
mf	MIFARE卡的相关命令...
tune	连续测量高频天线的调谐

hf 14a （ISO14443A卡的相关命令...）

help	显示帮助
list	列出窃听到的ISO14443A类卡与读卡器的通信历史记录
reader	读取ISO14443A类卡的UID等数据
cuids	收集指定数目的随机UID，显示开始和结束时间。
sim	<UID> -- 模拟ISO14443A类标签
snoop	窃听ISO14443A类卡与读卡器的通信数据
raw	使用RAW格式命令发送指令到标签

hf 14b （ISO14443B卡的相关命令...）

help	显示帮助
demod	调制ISO14443B协议的标签
list	列出窃听到的ISO14443B类卡与读卡器通信历史记录
read	读取ISO14443B类卡的信息
sim	模拟ISO14443B类标签
simlisten	从高频样本中模拟ISO14443B类标签
snoop	监听ISO14443B类卡与读卡器之间的通信数据
sri512read	<int> -- 读取SRI512标签的内容
srix4kread	<int> -- 读取SRIX4K标签的内容
raw	使用RAW格式命令发送指令到标签

hf 15 （ISO15693卡的相关命令...）

help	显示帮助
demod	调制ISO15693协议的标签
read	读取ISO15693类卡的信息
record	记录ISO15693标签样本
reader	作为ISO15693卡类的读卡器，读取UID等信息
sim	模拟ISO15693协议的标签
cmd	向ISO15693协议的标签直接发送命令
findafi	暴力一个ISO15693标签的AFI
dumpmemory	读取ISO15693标签的所有页内存数据

hf epa （德国身份证相关命令...）

help	显示帮助
cnonces	<m> <n> <d>——在d秒内收集n个字节长度为m的加密值。

hf legic （LEGIC卡的相关命令...）

help	显示帮助
decode	显示非混淆的解码后的LEGIC的射频标签数据（在使用hf legic reader之后）
save	<filename> [<length>] —存储样本数据
load	<filename> -- 恢复样本数据
sim	[phase drift [frame drift [req/resp drift]]] 开始模拟标签 (在使用load或者read之后)
write	<offset> <length> -- 向缓冲区写数据(在使用load或者read之后)
fill	<offset> <length> <value> — 填写/写标签恒定值

hf iclass （ICLASS卡的相关命令...）

help	显示帮助
list	列出窃听到的iClass类卡与读卡器的通信历史记录
snoop	窃听iClass类卡与读卡器的通信数据
sim	模拟iClass标签
reader	读取iClass标签

hf mf （MIFARE卡的相关命令...）

help	显示帮助
dbg	设置默认调试模式
rdbl	读取MIFARE classic卡的区块数据
rdsc	读取MIFARE classic卡的扇区数据
dump	导出MIFARE classic卡的数据到二进制文件
restore	从二进制文件恢复数据到空白的MIFARE classic卡
wrbl	改写MIFARE classic卡的区块数据
chk	测试MIFARE classic卡的各个区块KEY A/B
mifare	基于PRNG漏洞，执行mifare “DarkSide”攻击操作
nested	测试嵌套认证漏洞，基于一个已知Key，获取都有扇区Keys
sniff	嗅卡片与读写器之间的通讯(等同于hf 14a snoop)
sim	模拟一个MIFARE卡片
eclr	清除仿真内存的各区块数据
eget	获取仿真内存的各区块数据
eset	设置仿真内存的各区块数据
eload	从导出的文件加载仿真数据
esave	导出保存仿真数据到文件
ecfill	利用仿真器的keys来填补仿真内存
ekeyprn	打印输出仿真内存中的keys
csetuid	直接设置可改UID卡的UID
csetblk	把对应区块数据写入UID卡
cgetblk	读取UID卡对应区块数据
cgetsc	读取UID卡对应扇区数据
cload	写入dump数据到UID卡。注意 (http://wiki.radiowar.org/%E9%97%AE%E9%A2%98%E6%B1%87%E9%9B%86#.E4.B8.BA.E4.BB.80.E4.B9.88.E4.BD.BF.E7.94.A8cload.E5.AF.BC.E5.
csave	保存UID卡数据到文件或者仿真内存

取自“http://wiki.radiowar.org/index.php?title=Proxmark3命令帮助&oldid=1024”
分类： Proxmark3
