Misc除第一题外，杂项其实并不怎么套😭1. Music考点：流量分析能力、洞察能力、音频隐写、密码学（？）简介：黑客很喜欢音乐，为此他找了一些音游网站，想要借此下载一些谱面来游玩，但是黑客发现其中一个网站存在命令执行漏洞，于是他下了一些奇怪的东西。流量抓包，分析HTTP流量，得知下载了一张图片（k448.jpg）把图片提取后，分离得到压缩包(Staff.zip）和（music.mp3）（music.mp3）查看频域得到（Staff.zip）压缩包的密码 Diana!aLove8 （Staff.zip）压缩包解压后得到加密的压缩包（whatthisis.zip）和一个需要密码的文档（flag.docx）还有一个（pass.txt）文本文件文本文件（pass.txt）里的内容发现关键信息REVERSE，得知要REVERSE 0A 0A 00 00 00 00 后边的值，也可以把整个文本逆转一下，能看到关键信息93632393439383139313D34696F376E6F637F232F2D6F636E2336313E236963757D6F2F2A33707474786逆转一下得到68747470733A2F2F6D757369632E3136332E636F6D2F232F736F6E673F69643D31393138393439323639然后还原成字符串得到链接https://music.163.com/#/song?id=1918949269密码为评论区里的作者留言T0JRWEc0WjJNWkFHU1kzUElCVkVRWVRQTU5HRzZRQT0=解密为：base64->base32得到pass:f@ico@jHbocLo@文档（whatthisis.zip）密码为：f@ico@jHbocLo@打开文档后，Ctrl+A后Ctrl+D把隐藏文本的勾去掉，这时候会发现屏幕没有任何变化再次Ctrl+A发现一小块文本，放大后得到压缩包（flag.zip）密码0llo00llllO0o0o0lOo0l0IolIlIIolO0llO00ll0lIO0IIo0lIoO0I00OOOlIIO解压压缩包后会得到osu文件，运行OSU谱面后发现假的flag，但仔细查看发现最上面有提示，"Look at your MAP Settings"打开Osu Editor（右键->编辑）后，F4或导航栏查看->地图设置，发现Tag里有东西一串音频加密，复制黏贴下来解密即可‖♬♩‖¶♯‖♬♭‖♬♫‖♫♪♭♯♩‖‖‖‖♩♬‖♬♪‖♩♫♭♭♭‖‖♭‖♩♫♭♭♭♭‖♯‖♬♪‖♩♩‖♩¶‖♫§♭♭♭♭♭♬‖♩¶♭♯♩♭♯♩‖♫§♭♭♭‖¶♬‖‖♭‖♬♫‖♬♬♭‖‖‖♫♫§=也可以直接解压osz文件（osu谱面osz本身就一压缩包），查看\*.osu文件发现Tag信息最后flagflag{N0tes\_1s\_Veruy\_FuNNy\_R1ghT}2. Diana考点：Aztec、基础隐写、编码、无线电简介：小嘉然转啊转啊首先题目给出 Aztec Code 的01数据，写脚本还原成Aztec，中间补上Aztec的定位标扫码得到下载链接/52XMUT密码为52XMUT解压后得到图片binwalk分离得到音频，SSTV慢扫描得到（flag.zip）压缩包密码dMP1c2mZ6nflag解压后，给出一堆SMS PDU数据，排除掉脏（嘉然）数据后，写脚本提取关键数据解开得到Hi, Diana. How are you doing today?挺不错的，今天播了几十分钟，赚了很多钱是嘛，赚了很多钱对吧来让我看看不要啦，听话，让我康康欸你干嘛啦，好好好，给你看哇，Diana！我真的好喜欢你啊！最后提取出来一张图片把图片放到编译器npiet里编译成程序即可回显flagflag{3n8Gyn3\_928cv1ms1X8HibH4aN6B5A1\_19ZceX4nnPq7}3. WOW!!!考点：Ook!、LSB、隐水印简介：对着摄像头跳宅舞就行，人越多越好。这里我推荐幸运星的《拿去吧！水手服》flag{Text in the picture}https://share.weiyun.com/8w7wfyDw6pbgzv识别人头==6后在本地生成一份gift，gift为docx文件，里边藏有mp3隐写文件（header4）和LSB隐写图片（header5）也可以直接py反编译（主要针对打不开的师傅）搞人脸这个是为了增加娱乐性🥰，祝各位师傅玩的开心wav文件（header4）modem数据流解码后，得到一串base64后的Ook!数据波特率为300+++++ ++[-> +++++ ++<]> ..<++ +++[- >++++ +<]>+ +++++ ++++. --.<+ ++++[->+++ ++<]> .<+++ ++++[ ->--- ----< ]>--- ----- -.<++ +++[- >++++ +<]>+.<+++ ++[-> +++++ <]>+. <++++ +++[- >---- ---<] >---. +++++ .<+++ ++[->+++++ <]>++ +++++ +++.< +++++ +[->- ----- <]>-. .<+++ +++[- >++++ ++<]>+++++ +++++ ++.++ ++.<+ +++++ [->-- ----< ]>--- .---- ----- .<Ook!解开得到LSB隐写图片（header5）的密码11TRk1Ke16Y44dhA8LSB解开后得到一堆数据https://github.com/livz/cloacked-pixelROT13转后发现是jpg文件格式得到图片隐水印的图片。。。调好参数后显示出文字flag{5Q8qP65U8zqMr}4. Easy Disk考点：数据修复、取证简介：8c26ffa4ca12b34844628f6ab22b780c\_iscc.xmutsec.iloli.moePS：flag{Part1+Joe's Password+Part2}解题步骤：首先 nslookup 查看 xxx.iloli.moe 得TXT数据，得到 base85，解码后得到 pikachupi pi pi pi pi pi pi pi pi pi pika pipi pi pipi pi pi pi pipi pi pi pi pi pi pi pi pipi pi pi pi pi pi pi pi pi pi pi pichu pichu pichu pichu ka chu pipi pipi pipi pipi pi pi pi pi pikachu pi pi pi pi pi pi pi pi pi pi pi pi pikachu pikachu ka ka ka ka pikachu pi pi pi pikachu pichu ka ka ka ka ka ka ka ka ka ka ka ka pikachu ka ka ka ka ka ka ka ka ka ka ka pikachu pikachu pipi pikachu ka ka ka ka ka ka ka ka ka ka ka pikachu ka ka ka ka ka ka ka pikachu pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pikachu ka ka ka ka ka ka ka ka ka ka ka ka ka pikachu pichu ka pikachu pipi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pikachu ka ka ka ka ka ka ka ka ka ka ka ka ka ka ka ka ka ka pikachu pi pi pi pi pikachu pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pikachu ka ka ka ka pikachu ka ka ka ka ka ka ka pikachu pichu pikachu pipi ka ka ka ka ka ka ka ka ka ka ka pikachu pi pi pi pi pi pi pi pi pi pi pi pi pikachu ka ka pikachu pichu pi pikachu pipi ka ka ka ka ka ka ka ka pikachu pichu pi pi pi pi pi pi pi pikachu pi pi pi pi pi pi pi pi pi pi pi pi pi pi pikachu pi pi pi pi pi pi pi pi pi pikachu pipi pi pi pikachu pichu ka ka ka ka ka ka ka ka pikachu pi pi pi pi pikachu ka ka ka ka ka ka ka ka ka ka ka ka ka ka ka ka ka ka ka ka pikachu ka ka ka ka ka ka pikachu pipi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pikachu pichu pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pikachu pipi ka ka ka pikachu pichu pi pi pi pi pi pi pi pikachu pichu pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pi pikachu ka ka ka pikachu 啊 pikachu 解码后得到下载地址密码：xMuT52下载后根据readme.txt信息得知要让我们数据恢复跟取证。readme.txt文件直接挂载硬盘，发现第一个分区被破坏了同时第二个分区存在 BitLockerWinHex打开查看MBR，发现分区地址被删了找到第一个分区地址然后回到MBR并把分区地址补到MBR，再补上类型。。恢复成功。。。。。。重新挂载磁盘，发现有两个分区分区一readme.txt内容小彩蛋：你懂我意思吧ahahahah.png 通过 crc32 爆破发现高度不一样修改高度后得到 BitLocker 的 Key686224-303292-585959-348568-718696-444224-102377-435171分区二解锁后，得到 flag.raw 和 readme1.txt.flag.rawreadme1.txt 文件内容首先查看系统架构（Win7SP1x86\_23418）根据题目得知要获取黑客的密码，直接dump hash或用mimikatz发现存在一个 hacker 用户，将 hash 值解密得到黑客密码为maggie这里改成获取 Joe 得用户密码了，Joe明文解得pass.123同时查看进程，看看关键信息，发现出题人开着 notepad.exe 和 mspaint.exe 把 mspaint.exe 给dump下来，得到打开PS得到然后调整大小，不断移位（4613436,739,1350），得到把图片下载下来后，稍微处理下得到