Challenge 1

首先通过wireshark的http命令进行过滤，往下翻看到有些请求含有"flag"字段，因此进一步过滤，http contains"flag"，发现类似GET /index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2038,%201))>125 HTTP/1.1 的请求，该请求是尝试SQL注入攻击，使用`subste`和`ascii`函数从结果集中提取一个字符。再进行查看发现`db_flag.tb_flag`，表示从数据库中的`db_flag`数据库的`tb_flag`表中选择一行记录，并使用`limit 0,1`来限制只返回一行结果，以确保只提取一个字符。

经过上述分析，可以进一步加强过滤条件，http contains"db_flag.tb_flag"，得到请求，观察发现使用二分查找来寻找提取的字符，初步读取前四个字符为flag，验证思路是正确的，接下来就读取flag的具体内容了。

> flag:flag{47edb8300ed5f9b28fc54b0d0b009ecdf7}

Challenge 2

首先使用wireshark的命令行工具tshark执行命令 tshark -r dnscap.pcap -T fields -e dns.qry.name > hex 将dns记录提取到hex文本中

然后通过python将得到的hex值进一步简化

```
with open("hex","r") as f:
    content = f.read()
content,repalce("\n","").replace("skullseclab2.org","").replace(".","")
```

然后将其拿到cyberchef里解码，得到一串文本（虽然很多乱码），但是发现其中具有PNG,IHDR等格式，所以知道该题目是在传输过程中传输了png格式的图片，flag极有可能就在那张图片中。根据发现的dnscat以及文档的相关信息，可以得到这是一种通过DNS传递数据的变种协议，可以直接看数据块信息，并在qry.name中去掉其余字段只留下data块从而合并数据，再从hex中提取png，便可得到flag

> AAA{b91011fc}

Challenge 3

首先将题目给的文件解压，发现是个光盘镜像文件，而发现它可以用7-zip继续解压，得到一个crack_zju-01.cap文件和一个.password.txt.swp文件，经查阅可知.swp文件是个需要恢复的文件，因此使用命令`vi -r .password.txt.swp`并保存为flag.txt。

接着结合题目破解wifi协议，使用aircrack-ng的命令 aircrack-ng crack_zju-01.cap -w flag.txt便得到KEY

```
Time left: 0 seconds                                    50.12%

                    KEY FOUND! [ 0YcWPeLMBp ]


Master Key     : 2A 0A 56 2C 6E 44 73 96 60 DB 3B F2 D5 76 9F 1A
                 E4 CD 5B C1 9A 08 62 FA EF 0F 65 E2 34 B4 D1 ED

Transient Key  : ED 4A 32 BA DE 35 3A E4 C3 A2 3A 78 1E F9 CF 65
                 93 30 BA 38 46 8A 08 E9 96 12 DD 41 5D 28 EC DE
                 32 7C 7A 31 EF 22 7B 14 E7 35 D7 3A 78 D0 E1 A6
                 45 FE FA 99 12 C0 55 12 AC 96 E0 CE E6 72 B7 CD

EAPOL HMAC     : 28 A0 12 09 B3 E9 32 1F E7 4A E3 3E 05 5A C9 77
```

因此flag为AAA{0YcWPeLMBp}

Challenge 4

非常抱歉！！这题可能来不及做了/(ＴｏＴ)/~~/(ＴｏＴ)/~~

Bonus Task

在misc的这三节课，我了解了CTF比赛中misc的含义以及基本类型，学习了编解码，古典密码，OSINT的相关内容以及工具使用，图片音频隐写的知识及工具使用，流量取证以及内存取证等知识。总的来说我觉得misc部分还是很有趣的，我个人是比较喜欢OSINT与图片隐写的部分，感觉在做这部分题目时不断尝试，使用各种工具方法，最后得到flag的过程很吸引我。而AI安全这个方向我比较感兴趣，但不知道实际的题目和我想象的会不会一样hhhhh。总而言之，misc这三节课让我学会了很多东西，非常感谢TonyCrane老师！！！