B-1 网络爬虫渗透测试：

1. 找到kali攻击机的/root目录下的request.py文件，编辑该Python程序文件，使该程序实现网络爬虫渗透测试批量获取目标靶机关键文件的功能，填写该文件当中空缺的F1字符串，将该字符串作为Flag值提交；

2. 继续编辑命名为request.py的Python程序文件，使该程序实现网络爬虫渗透测试，批量获取Flag文件的功能，填写该文件当中空缺的F2字符串，将该字符串作为Flag值提交；

3. 继续编辑命名为request.py的Python程序文件，使该程序实现网络爬虫渗透测试批量获取目标靶机关键文件的功能，填写该文件当中空缺的F3字符串，将该字符串作为Flag值提交；

4. 继续编辑命名为request.py的Python程序文件，使该程序实现网络爬虫渗透测试批量获取目标靶机关键文件的功能，填写该文件当中空缺的F4字符串，将该字符串作为Flag值提交；

5. 继续编辑命名为request.py的Python程序文件，使该程序实现网络爬虫渗透测试批量获取目标靶机关键文件的功能，填写该文件当中空缺的F5字符串，将该字符串作为Flag值提交；

6. 继续编辑命名为request.py的Python程序文件，使该程序实现网络爬虫渗透测试批量获取目标靶机关键文件的功能，填写该文件当中空缺的F6字符串，将该字符串作为Flag值提交；

7. 继续编辑命名为request.py的Python程序文件，使该程序实现网络爬虫渗透测试批量获取目标靶机关键文件的功能，填写该文件当中空缺的F7字符串，将该字符串作为Flag值提交。

B-2 Python 程序渗透：

1. 从靶机服务器的 FTP 上下载 password.py，编辑 Python 程序，使该程序实现弱口令爆破，填写该文件当中空缺的 F1 字符串，生成密码列表

2. 编辑 Python 程序 password.py，使该程序实现弱口令爆破，填写该文件当中空缺的 F2 字符串，填写连接的 host；

3. 编辑 Python 程序 password.py，使该程序实现弱口令爆破，填写该文件当中空缺的 F3 字符串，填写连接的密码；

4. 编辑 Python 程序 password.py，使该程序实现弱口令爆破，填写该文件当中空缺的 F4 字符串，写出连接失败的处理逻辑；

5. 编辑 Python 程序 password.py，使该程序实现弱口令爆破，填写该文件当中空缺的 F5 字符串，写出连接成功的处理逻辑；

6. 编辑 Python 程序 password.py，使该程序实现弱口令爆破，填写该文件当中空缺的 F6 字符串，写出判断 result 的值即可知道是否爆破成功；

B-3 Redis 未授权访问：

1.从靶机服务器的 FTP 上下载 0011.py，编辑 Python 程序，使该程序实现基于 socket 的 redis 未授权识别，填写该文件当中空缺的 F1 字符串，生成 socket 对象

2. 编辑 Python 程序 0011.py,使该程序实现基于 socket 的 redis 未授权识别，填写该文件当中空缺的 F2 字符串，连接目标机；

3. 编辑 Python 程序 0011.py,使该程序实现基于 socket 的 redis 未授权识别，

填写该文件当中空缺的F3字符串，发送数据；

4. 编辑Python程序0011.py,使该程序实现基于socket的redis未授权识别，填写该文件当中空缺的F4字符串，接收数据

5. 编辑Python程序0011.py,使该程序实现基于socket的redis未授权识别，填写该文件当中空缺的F5字符串，关闭连接对象；

6. 编辑Python程序0011.py,使该程序实现基于socket的redis未授权识别，填写该文件当中空缺的F6字符串，写出if成立的执行语句；