1. RSA算法之Alice & Bob 难度系数\*\*。

根据给定的Alice&Bob文件，该文件中包含p、q、e，以及base64编码的密文C，求出解密后的明文是什么？提示：首先将base64编码的密文还原，然后根据RSA算法求出d，n再解密c，获得明文。平台有《Alice&Bob》文件。需要在python2下完成。除了参考题解文件外，也可以使用gmpy2，python下的大数库来完成题目。

2. 逆向（静态代码分析） 难度系数\*\*\*\*

给定输入文件src，载入IDA分析伪代码。分析代码流程，编写程序，找出其中的flag。平台有《src》

3. 基于vulhub开源靶场实验（web渗透测试实验）。难度系数 \*\*\*\*（非常推荐，尤其是web常见漏洞）

下载并安装vulhub靶场，并进行相关实验。可参照链接中的系列攻击实验，最好自己尝试。

<https://www.vulnhub.com/>

<https://fuping.site/2017/06/05/Weblogic-Vulnerability-Verification/>

<http://121.42.173.26/archives/877/>

<https://blog.csdn.net/weixin_41038469/article/details/88409725>

<https://zhuanlan.zhihu.com/p/36788686>

4. 口令破解 难度系数\*\*\*

使用口令破解工具尝试破解自己机器的口令，可以参考一下链接，了解口令的处理方式

密码破解全能工具hashcat。可能该工具对于win10的口令不好用？

<http://www.freebuf.com/sectool/164507.html>

http://www.freebuf.com/articles/database/153628.html

<http://www.freebuf.com/news/152641.html>

5. 证书管理及SSL配置 难度系数 \*\*

按照文档《opesnssl证书配置和使用》的要求，选择其中任一实验方法，完成证书服务器CA和SSL配置、并在浏览器进行访问配置好的https站点的验证实验。

6. 利用wireshark进行协议分析。 普通数据包分析难度系数\*\*，无线网络部分难度系数 \*\*\*

上网过程数据包捕获和分析、无线网络中的协议分析、Wifi密码破解等，可参见文档《wireshake数据包嗅探实验》。

7. 缓冲区溢出实验 难度系数\*\*\*

可以编写windows或linux下的缓冲区溢出程序，改变原有程序的执行过程，实现相应的功能。可以参见实验楼的实验，但是需要在自己的虚拟机上来做（实验楼实验成绩为起评分），并适当补充shellcode代码的生成过程，以及gdb的调试过程。也建议在windows下做缓冲区溢出实验，windows下生成shellcode比linux下貌似容易些。

8. 编写基于python的小攻击、破解工具 难度系数\*\*\*

如端口扫描等，可参见BB平台上“实验”下边上传的《phthon绝技》等书籍。

9. MD5碰撞攻击实验。 难度系数 \*\*\*

基于给出的MD5碰撞产生工具，产生两个md5值相同但功能不同的程序。详见文档《md5碰撞攻击实验》

10.信息隐写 难度系数\*\*\*

平台的《misc》压缩文件中包含4个文件，为4个不同类型的隐写方面的题目，请尝试发现其中的flag，提示：“what kind of document is this”一题较难，需用到hashcat。其他题目较简单。做出其中3道题目者得起评分。附件《misc》可在平台下载。

11. Netwox TCP/IP攻击工具的使用 难度系数\*\*\*

Netwox是一款非常强大和易用的开源工具包，可以创造任意的TCP/UDP/IP数据报文。Netwox工具包中包含了超过200个不同功能的网络报文生成工具，每个工具都拥有一个特定的编号。可以在虚拟机下练习使用该工具。尽可能比较完整的完成实验。

<http://www.laurentconstantin.com/en/netw/netwox/>

较完整的实验（TCP/IP攻击实验（ARP，ICMP，SYN，RST，TCP会话劫持）

<https://blog.csdn.net/zengxyuyu/article/details/53434728>

其他不同类别的实验可参加下面的链接

网络层欺骗及传输层协议攻击总结：

<http://www.cnblogs.com/20159217cbs/p/5518320.html>

ICMP路由重定向：

<https://blog.csdn.net/the__apollo/article/details/69963804>

ARP欺骗和ICMP路由重定向：

<https://blog.csdn.net/the__apollo/article/details/69963804>

TCP会话劫持也可以参见Kali下的hunt工具完成类似的攻击效果

<https://blog.csdn.net/the__apollo/article/details/70037511>

提交：包含实验目的、实验内容和实验总结等三个方面的详细实验报告。

实验分数：按照实验难易程度及实验报告内容打分。实验内容较完整，起评分为8分。

实验目的：相关实验旨在提高安全意识，不可以进行蓄意破坏网站及其他恶意行为，如有恶意行为，后果自负。实验中的问题欢迎与老师联系。