LCTF-学习-Crypt450/RE100-200

原创

Kn1ght_Gin 于 2016-11-06 10:08:01 发布 547 收藏
分类专栏： CTF 文章标签： CTF学习 信息安全竞赛

本文链接：https://blog.csdn.net/Kn1ght_Gin/article/details/53053138

0x0 Crypt450：

类型：

首先是个流量包分析，找其http请求，发现其一共3个http请求，为去http://192.168.138.136/Somethingneeded.z

知识点：

1.CRC：循环冗余校验(Cyclic Redundancy Check, CRC)是一种根据网络数据包或电脑文件等数据产生简短固定位数校验码的一种散列函数，

2.Wiener Attack：可利用Wiener Attack进行RSA低解密指数攻击（加密指数过长），攻击密文和公钥获得私钥。

3.Elgamal签名算法：https://my.oschina.net/u/1382972/blog/330630。

讲解还是比较麻烦啊，根据课上学的来说吧。

（1）原理：选一个素数p，以及两个小于p的随机数g和x，计算y=g^x mod p,以(y,g,p)作为公开秘钥，x作为私密

（2）加密：设欲加密消息为M，随机选择一个与p-1互素的整数k，计算C1=g^k mod p,C2=(y^k)*M mod p,密文为

（3）解密：M=C2/C1^x mod p.

4.hash已知部分明文的python爆破脚本。

0x1 RE100：

类型：

Qt编写的...比较难分析

知识点：

留坑，，根据writeup还未分析出来...

0x2 RE200:

类型：

linux程序的逆向

知识点：

留坑，，