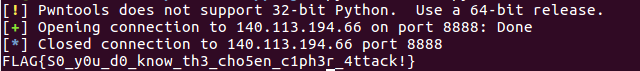
Network Security Lab 1

Chosen Cyphertext Attack 0656511黃誠發

1. Flag image



1. How to decrypt

我們不能直接餵原本的flag.enc進到server，所以我們必須透過運算製造一個新的且假的flag.enc餵到server讓他吐出真正的值，然而作業簡介中的P值即為新flag的算法。

概念就是把舊的值和一個與n互質的數generate出一個新的值而這個值可以透過數學運算解出真正的plaintext.

1. Way to decrypt
   * 一開始先對sever運用pwntools建連線。
   * 因為沒有private key所以要連到server才可以順利找到真正的解。透過觀察server端的code發現可以用python的套件找到 RSA public key而可以得到其中的n和e.
   * 透過介紹我們可以需要找一個與n互質的數，我發現n 為…60859，所以我選擇10肯定會跟他互質的數做處理。
   * C要先做前處理，因為他是透過base64編碼及RSA加密，所以我必須找到C的int型態才可以做數學運算。
   * 首先先將讀進來的flag做base64解密轉成byte string編成16 進位的int做計算，算出Y，轉成hex去掉前面的0x，再用binascii.unhexlify將hex轉回byte string，並做base64加密，達成破解的秘文。
   * 最後再送回server解密，再將得到的明文經過base64 decode 和byte string to int再投入公式取得想要的真正明文。
2. Something learned
   * 運用pwntools取代socket做連線
   * 了解RSA結構
   * 了解chosen cyphertext attack原理
   * 數值型態轉換