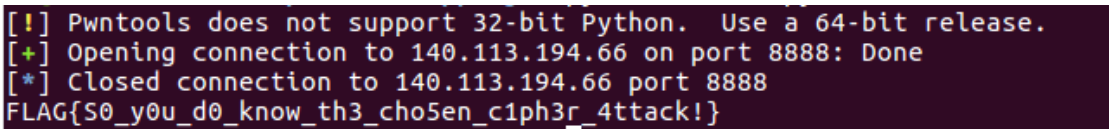
Network Security Lab 1

Chosen Cyphertext Attack 0656511 黃誠發

1. Flag image



2. 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.

3. 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。

4. 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