

Alice’s Money : 160585991563

My Money: 41293342975

ARP Spoofing:

是一種網路攻擊的技術。藉由偽造ARP Reply，讓網路上的某些機器錯誤地把ARP table裡特定的IP位址對應的MAC address換成攻擊者的MAC address，藉此讓攻擊者能夠截獲某些原本不應該導向它的流量。具體流程如下：

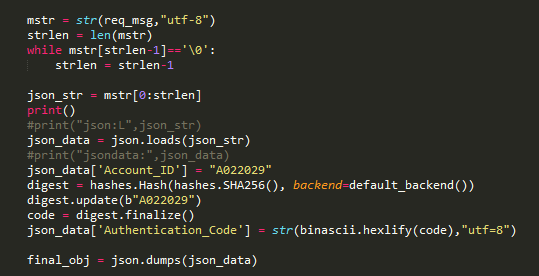
1. 攻擊者首先聆聽區域網路上的ARP Request。當它收到兩台機器A B的Flood過來的ARP Request就可以開始攻擊。
2. 攻擊者傳送一個偽造的ARP Reply給B，裏頭的Sender IP是A，而Sender MAC卻是攻擊者的MAC Address
3. B更新自己的ARP Table
4. B之後要傳送給A的封包在送到交換器的地方時會被轉送給攻擊者

(以上簡單假設三者都在同一個LAN內)

ARP欺騙亦有正當用途。其一是在一個需要登入的網路中，讓未登入的電腦將其瀏覽網頁強制轉向到登入頁面，以便登入後才可使用網路。

The way to generate authentication code:

首先先在不更改authentication code的狀況下直接把request message傳給Bob，得到Response後確認裏頭的Feedback。猜測應該是使用SHA-256。於是使用下面這段CODE來產生我要傳給Bob來要取我的Money資訊的Message



req\_msg是解密後的Alice的request message。首先把後面的padding拿掉，接著轉換成json格式，更改Account\_ID成自己的學號，用python cryptography library裡的hashes.Hash，指定雜湊函式為SHA-256接著產生雜湊值。不過這邊我必須先用binascii.hexlify把產生出來的雜湊值用16進為字串表示再放入json裡的Authentication\_code欄位中，再傳給Bob。

Compile的方法：

在可以執行python的環境下執行 python A022029.py就可以了。(要先確認環境中有python的cryptography函式庫可以import)