06 Wireshark解SMTP的帳號和密碼解base64的編碼

工具

UBS-5008具有Port Mirror功能的Switch Hub



一台Windows有安裝Wireshark的Notebook

或是直接把wireshark安裝在Exchnage Server上面,不過此方法比較不建議

因為搞不好那台Server有問題 XD

架構如下



UBS-5008設定如下



安裝Wireshark的Notebook裝在Port 8

Mirror Port 1的Firewall和Port 2的Mail Server

Wireshark抓一段tcp port 25的





抓完之後

搜尋 String 是 AUTH LOGIN

AUTH LOGIN是Base64的Login方法

直接找寄信最多的那一組



把他Copy到記事本



這一串解碼是username

在這解碼

<http://www.ublink.org/index.php/new/base64-.html>





這一串才是 janus

Response: 334 VXNlcm5hbWU6\r\n 解出Username:

Command: ZXJpYw==\r\n 解出eric

Response: 334 UGFzc3dvcmQ6\r\n 解出Password:

Command: MTIzNDU2\r\n 解出123456

這樣就可以很快找到被Relay的帳號跟密碼了