連線加密的重要性

網路開始之初，各服務都是以分享為目地，隨著科技的發展，人們對網路的依賴越來越重，把許多的資訊放在電腦或網際網路上。網路的快速發展也沿生了很多問題，比方說，越受歡迎的服務表示著人們把更多的資訊放到該伺服器上，當然這也使很多有心人士想要窺視你的密秘一下，一直發展到現在，原本分享資訊的心態就被迫改變，不是所有的東西都是可以分享的，尤其是跟錢有關的資訊。

防止資料外洩的方法有很多，從最基本的防火牆開始，防止一些不速之客防意的闖入；應用程式的漏洞補齊；到現在的連線加密問題。其實連線加密已不是新技術，在很久前就開始應用。

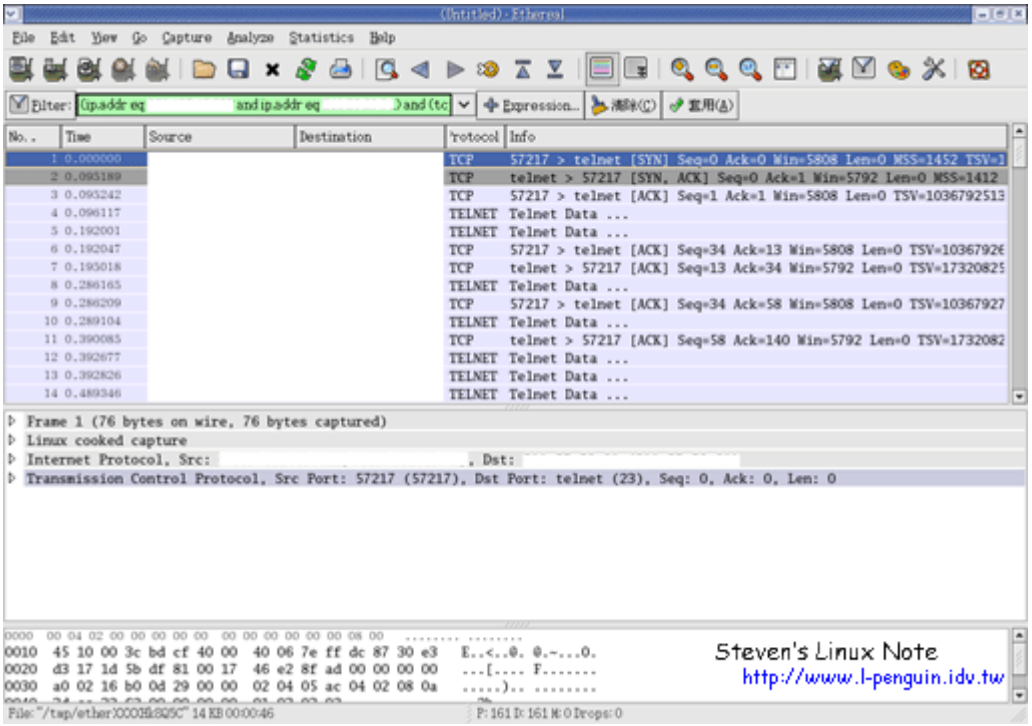
網路連線的加密與不加密差別到底是在那裡呢，我等一下以 Ethereal 來做示範，所以的連線都是跟封包有關，這也就是說，只要能夠截取到封包那麼網路所有連線的資訊都會被一覽無遺。

以遠端連線來說，很久以前 telnet 還在當道的時候，大家不會想說會有封包被“竊聽”，一直到了事實的發生之後，發展出了 SSH 這個新服務，它最重要的地方就是在連線的時候是經過加密的，所以就算你的連線時封包被竊聽，那麼要破解還是需要時間去完成。

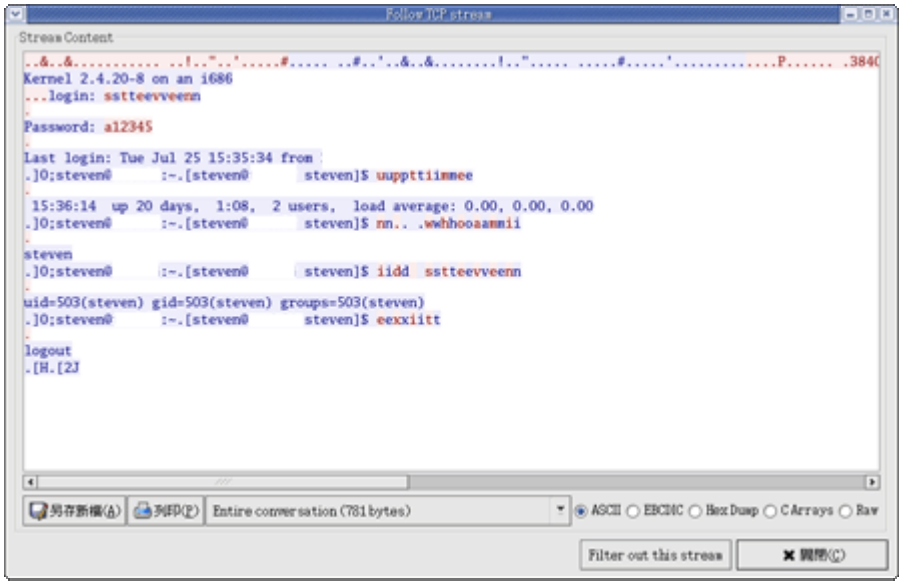
說到了加密，總是要講一下“明文”和“密文”這兩項名詞，就以 telnet 來說，它是屬於明文傳輸的，也就是說你在連線的過程中，所輸入的文字都會一五一十直接傳送而沒有任何的防護；再來是密文，以 SSH 來說，他在連線之前，會先把你輸入的文字加密，然後再傳給遠端伺服器，那麼這樣的話，封包裡的傳輸就不是原始的文字了。

telnet 的封包：

我使用了 Ethereal 軟體來截取 telnet 封包，所有有關 telnet 連線的資訊都會被錄下來。



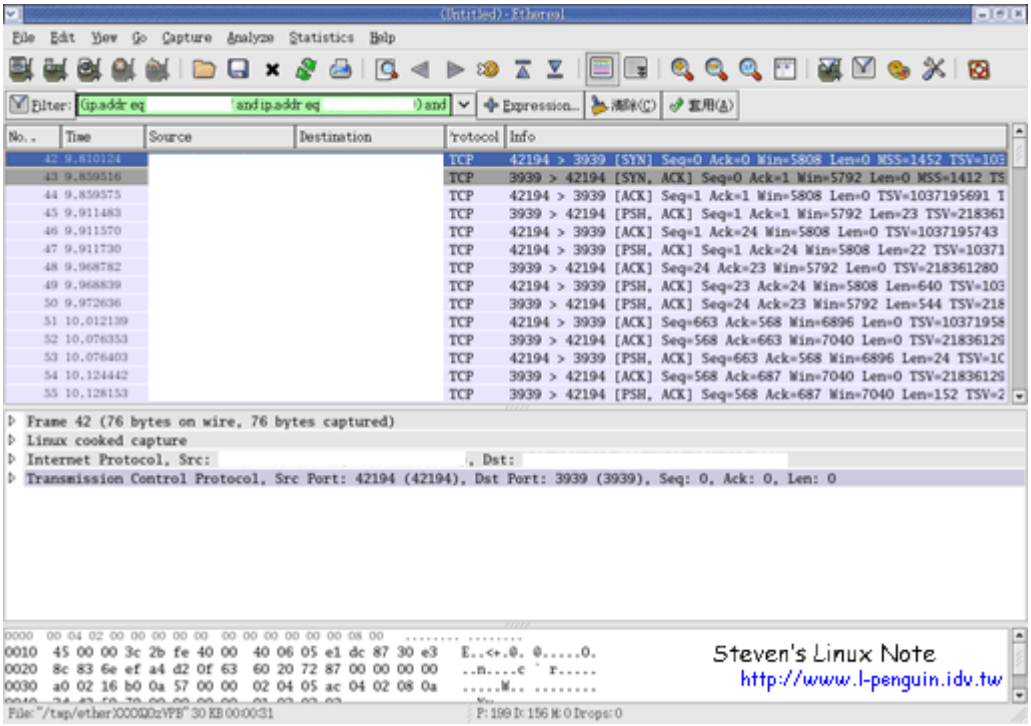
現在來嘗試“重新組合”當初連線的過程。



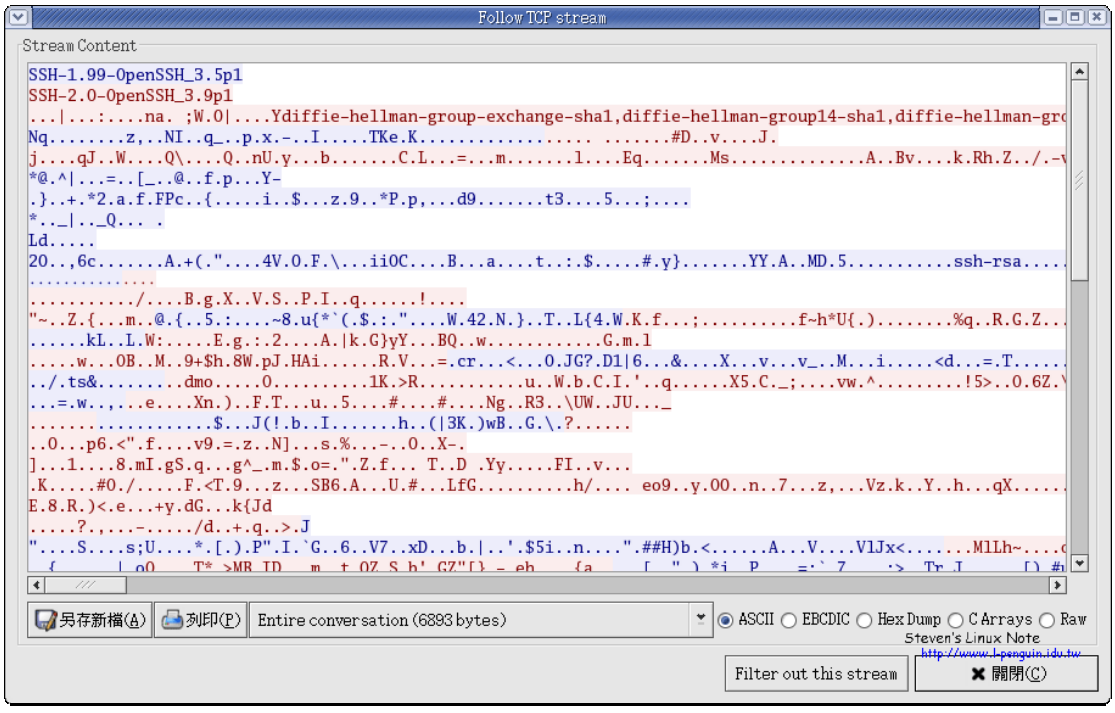
你可以很輕楚的看到，經過 telnet 連線的資訊不用解碼就可以直接“讀”，如果你仔細看圖片內容的話，你還能發現連登入帳號和密碼都能輕易的看到。

SSH 的封包

看完了 telnet 的“明文”封包，現在來看看 SSH 的封包，它們兩個到底是差別在那裡。



跟之前一樣，來嘗試重新組合原始的連線資訊。



你可以發現一經重組之後，所有的文字的資訊都是被加密過的，所以就算得到了封包，還是要花時間去解密才行。

什麼服務需要加密？

需要加密的服務，端看資料的重要性，如果你常常傳輸客戶或銀行帳款的資料，那麼我還是建議你快把你的連線加密吧，但是加密這東西可不是單方面做就可以了，而是要 Server / Client 都配合才可以，一般都是 Server 先做，再由

Client 配合。

最常看到的服務加密對應如下。

- HTTP -> HTTP over SSL (https)
- SSH
- FTP -> FTP over SSL (sftp)
- LDAP, mail over SSL -> Using Transport Layer Security (TLS) protocol.

封包軟體的取得

如果你要嘗試著挑戰了解封包內容，那麼你可以使用 Ethereal 軟體來試，它是免費的套件，發行了 Widows、Mac 和 Linux 的版本，使用方法都一樣。當然如果你了解了封包內容之後，相信對於網路的連線傳輸一定有更深的認知。不過你在跟朋友討論時一定不會想和他討論封包 :)

市面上也有很強的封包截取軟體

- siffer
- sniffit
- tcpdump (這個其實只有截取封包表頭而已): http://www.tcpdump.org/
- Ethereal: http://www.ethereal.com/
- Any others ...

封包分析套件

- ntop: http://www.ntop.org/
- Any others ...

了解封包的參考書

- RFC 1180: http://www.ietf.org/rfc/rfc1180.txt?number=1180
- TCP/IP 網路管理 第三版 (O'Reilly, ISBN：986-7794-16-8): http://www.oreilly.com.tw/product_network.php?id=a127

For more articles, please visit http://www.l-penguin.idv.tw/

作者：廖子儀 (Tzu-Yi Liao)
Certified：LPIC Level I、LPIC Level II、RHCE
E-mail：steven@l-penguin.idv.tw
Web site：http://www.l-penguin.idv.tw/