而攻擊實例中的木馬程式所使用的 ICMP Echo Reply 封包格式（圖 7），可明顯看出其封包總大小與封包 payload 不同於正常 ping 程式所產生的封包（圖 6）。因此，如果平常有對這些標準沒有定義的欄位特徵進行蒐集，很容易可以偵測到異常狀況的發生。

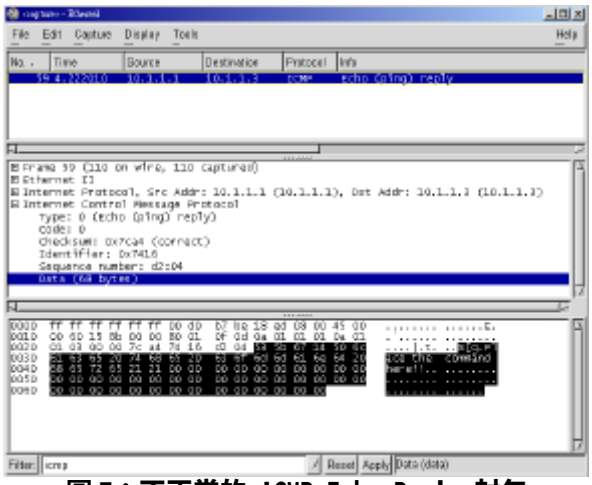

圖 7：不正常的 ICMP Echo Reply 封包

5.4 以 application proxy 進行身份認證並檢查連線封包

所有允許對外的協定，應透過 application proxy 先以身份認證，再檢查為正確的協定格式封包才允許通過，避免以協定作為偽裝的隱密通道。

要防止以上三種以網路協定為基礎的隱密通道，必須對各類協定標準細節相當熟悉，根據標準找出哪裡是正常的。至於標準沒有明確規定的部份，可以依使用系統的種類建立正向列表加以比對，藉此找出看似正常，實為異常的連線。

6. 結論

隱密通道最主要功用就是如何在不被發現的情形下進行資料的交換。隱密通道已被木馬程式用來當作操控端與受控端傳送指令及回應結果訊息的管道。愈來愈隱密的隱密通道實作方式及使用正常協定行為的趨勢，使得偵測隱密通道日益困難。唯有利用更多的方法加以判斷及更強大的設備來找出所有可能的異常狀況，才能偵測及阻擋隱密通道的通訊。雖然無法完全中斷隱密通道所造成的威脅，但是還是可以減少通訊的頻寬，拉長攻擊所需的時間，避免更多的資訊外洩及增加偵測的機率。

7. 參考文獻

[1]黃世昆，防止攻擊跳板主機的安全管理策略，中央警察大學 2000 第二屆網際空間：資訊、法律與社會研討會，中華民國 89 年 12 月。

[2] DoD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria, U.S., 1985.

[3] ISO/IEC 2382-8, Information Technology - Vocabulary: Control, integrity, and security, 1998.

[4] Back Orifice 2000 Web Site, http://bo2k.sourceforge.net.

[5]Back Orifice 2000 Server Enhancement Plugins Web Page, http://bo2k.sourceforge.net/software/bo2k10.html.

[6] Drew Hintz, Covert Channel, DEF CON 10.

[7] Craig H. Rowland, Covert Channel in the TCP/IP Protocol Suite.

[8]揭開木馬的神秘面紗（三），http://www.yesky.com/20010525/181452.shtml。

[9] Ofir Arkin, ICMP Usage in Scanning, http://www.sys-security.com/archive/papers/ICMP_Scanning_v3.0.pdf.

[10] Checkpoint FW-1, Version 4.0 and 4.1 ,Using the INSPECT language to implement stateful ICMP massages, http://www.yassp.org/fw1/icmp.html

[11] Advanced ICMP Basic Rule Base on Snort，http://www.sys-security.com/archive/snort/icmp_rules/ICMP_basic_plus.

[12] ICMP TYPE NUMBERS, http://www.iana.org/assignments/icmp-parameters.