**實驗日期：**

June 8, 2023

**實驗名稱：**

1. ITS Exp. 22: NAT
2. ITS Exp. 23: Firewall

**問題與答案：**

**ITS Exp. 22: NAT**

1. 由ITSI送出一個ICMP Echo Request至ITS4,利用ITS3的Message Browser 確定NAT已執行

一張含有 文字, 螢幕擷取畫面, 陳列, 軟體 的圖片

自動產生的描述  
上圖為ITS3的message browser，由紅框可知當ITS1送封包給ITS4時，在ITS3的IP SRC會顯示ITS3的LAN1 IP，回傳的IP DST也是ITS3的LAN1 IP。

1. 試著從任- ITS 發送封包給其它ITS,觀察其現象並討論什麼是「封包偽裝(IP Masquerading)」?對網路來說會有什麼影響?

若從ITS 1、2發送封包給IST 4、5，從IST 3、4、5看來都是從IST 3送出的，而封包偽裝是一種網路攻擊手法，攻擊者會偽造網路封包的來源地址，使其看起來像是從其他地方或主機發送的，這種攻擊可能導致網路阻斷(DoS)，或者欺騙系統或人員以獲得未授權的訪問權限或敏感資料，又或者偽裝成目標主機，向大量的其他主機發送請求，這些主機會將回應封包發送至被偽裝的目標，造成目標主機的資源過載。

**ITS Exp. 23: Firewall**

1. 由ITS1的 Message Browser 確定學生有由ITS1建立TCP連線至ITS4 的 Port 21,結果如 Figure 23.4；由ITS4的Message Browser 確定學生有由ITS4發送ICMP Echo Request至ITSI,結果如Figure 23.5。

一張含有 螢幕擷取畫面, 軟體 的圖片

自動產生的描述  
上圖為ITS 3的訊息，從橘框可以得知內部網路和外部網路已經建立連線，可以互傳ICMP Echo Request。

一張含有 文字, 螢幕擷取畫面, 陳列, 數字 的圖片

自動產生的描述  
上圖為ITS 1的畫面。然而從ITS 建立FTP連線至外網(ITS 4)時，會收到對方送回Reject PORT 21 FTP!!!的訊息。

一張含有 文字, 軟體, 數字, 電腦圖示 的圖片

自動產生的描述  
從ITS 4傳送資訊至ITS 1則是會收到從ITS 3(如黃框所示)的訊息: Reject ICMP。

1. 何謂「IP造假(IP spoofing)」?我們是不是可以用ITS設計一個防火牆解決這個問題?

IP Spoofing是一種網路攻擊手法，攻擊者會修改網路封包的來源IP地址，讓他看起來像是從其他地方或主機發送的，目的通常是隱藏攻擊者的真實身份，或是欺騙目標主機，使其相信來自可信任來源的資料封包。

由於防火牆所採用的封包過濾（Packet Filtering）規則是依據該封包的來源位址而定，所以經由 IP Spoofing 來改變封包的來源位址，佯裝入侵者是來自於被信任的網路，無法阻擋IP Spoofing。

**討論：**

這次的實驗沒有很順利，因為擔任Server的電腦無法送出封包，也無法確認收到的封包，但是我們再三確認所有的設定和接線都沒有問題，經過一學期的歷練，我們果斷換一台電腦當作Server之後果然就沒有問題了。

**補充資料：**

1. [IP位址欺騙 - 維基百科，自由的百科全書 (wikipedia.org)](https://zh.wikipedia.org/zh-tw/IP%E5%9C%B0%E5%9D%80%E6%AC%BA%E9%AA%97)
2. [什麼是 IP 詐騙？ | Cloudflare](https://www.cloudflare.com/zh-tw/learning/ddos/glossary/ip-spoofing/#:~:text=%E5%A6%82%E6%9E%9C%E5%B0%81%E5%8C%85%E8%A2%AB%E5%86%92%E7%94%A8%EF%BC%8C%E4%BE%86%E6%BA%90%E4%BD%8D%E5%9D%80%E5%B0%87%E8%A2%AB%E5%81%BD%E9%80%A0%E3%80%82%20IP,%E8%A9%90%E9%A8%99%E9%A1%9E%E4%BC%BC%E6%96%BC%E6%94%BB%E6%93%8A%E8%80%85%E5%90%91%E6%9F%90%E4%BA%BA%E5%82%B3%E9%80%81%E5%88%97%E5%87%BA%E9%8C%AF%E8%AA%A4%E8%BF%94%E5%9B%9E%E4%BD%8D%E5%9D%80%E7%9A%84%E5%B0%81%E5%8C%85%E3%80%82%20%E5%A6%82%E6%9E%9C%E6%94%B6%E5%88%B0%E5%B0%81%E5%8C%85%E7%9A%84%E4%BA%BA%E6%83%B3%E8%A6%81%E9%98%BB%E6%AD%A2%E5%82%B3%E9%80%81%E8%80%85%E5%82%B3%E9%80%81%E5%B0%81%E5%8C%85%EF%BC%8C%E5%B0%81%E9%8E%96%E6%89%80%E6%9C%89%E4%BE%86%E8%87%AA%E5%81%BD%E9%80%A0%E4%BD%8D%E5%9D%80%E7%9A%84%E5%B0%81%E5%8C%85%E5%B0%87%E6%96%BC%E4%BA%8B%E7%84%A1%E8%A3%9C%EF%BC%8C%E5%9B%A0%E7%82%BA%E8%BF%94%E5%9B%9E%E4%BD%8D%E5%9D%80%E5%BE%88%E5%AE%B9%E6%98%93%E6%9B%B4%E6%94%B9%E3%80%82%20%E8%88%87%E6%AD%A4%E7%9B%B8%E9%97%9C%E7%9A%84%E6%98%AF%EF%BC%8C%E5%A6%82%E6%9E%9C%E6%8E%A5%E6%94%B6%E8%80%85%E6%83%B3%E8%A6%81%E5%9B%9E%E6%87%89%E8%BF%94%E5%9B%9E%E5%9C%B0%E5%9D%80%EF%BC%8C%E4%BB%96%E5%80%91%E7%9A%84%E5%9B%9E%E6%87%89%E5%8C%85%E5%B0%87%E5%89%8D%E5%BE%80%E7%9C%9F%E6%AD%A3%E5%82%B3%E9%80%81%E8%80%85%E4%B9%8B%E5%A4%96%E7%9A%84%E5%85%B6%E4%BB%96%E5%9C%B0%E6%96%B9%E3%80%82)
3. [聯強經銷商專屬網站 (synnex.com.tw)](http://channel.synnex.com.tw/asp/fae_qaDetail.asp?from_prg=&topic=FAE&group=&parent=&classifyid=01534&seqno=17678)