

# 電腦網路實驗實驗報告 < Network Security >

姓名：翁佳煌

學號： 409430030

## 1. 實驗名稱

LAB1. 學習使用 Netcat 的 Port scanning。

LAB2. 建立簡易聊天室，建立連線後，此主機與客戶即可進行網路聊天。

LAB3. 傳送檔案，客戶可將 test.doc 傳送到主機。

## 2. 實驗目的

學習利用 Netcat 的使用方法，讓我們理解其許多不同的用途，例如構建簡單的客戶端/服務器應用程序，調試網絡問題，以及進行端口掃描等。

### 3. 實驗設備

Linux 作業系統之電腦。

Netcat 軟體。

#### 4. 實驗步驟

## LAB1:

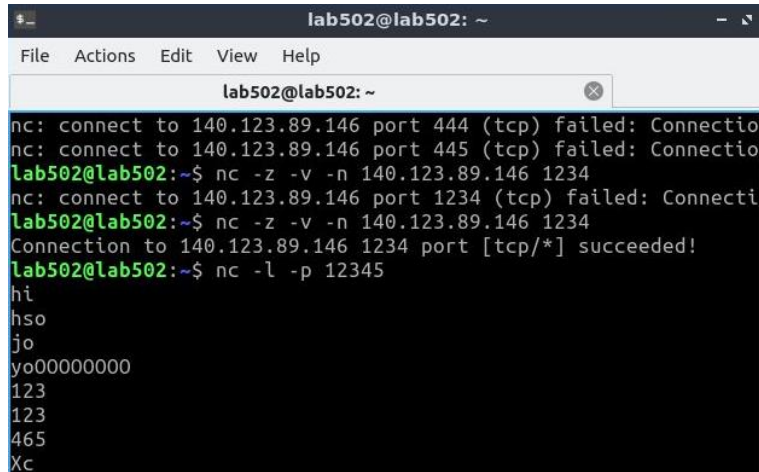
首先開啟一個 terminal，並輸入指令 `- nc -l 1234`，這個命令 `"nc -l 1234"` 是在終端中運行 Netcat 的指令。它的意思是在本地計算機上建立一個 TCP 服務器，並監聽在端口號 1234 上，等待其他計算機的連接。該服務器在連接之後會向連接的對方計算機發送任何接收到的數據。其中 `"-l"` 選項指示 Netcat 要啟動一個監聽模式，等待連接。

接下來，再次開啟一終端機，並輸入 `- nc -z -v -n ip_address port1-port2`，意思是測試對另一台主機的 TCP 端口連接。

[illegible]

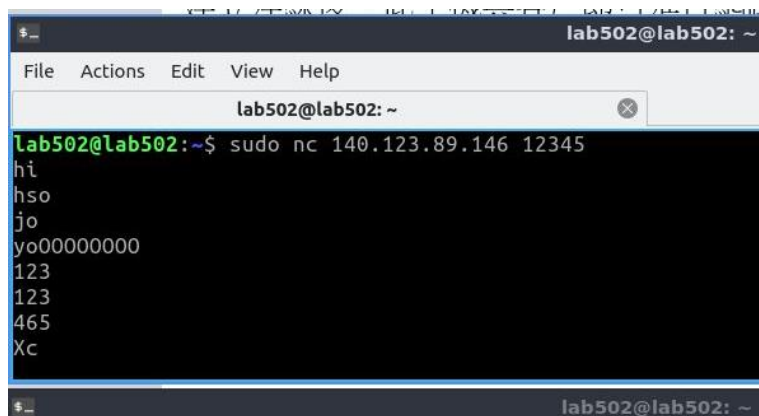
## LAB2:

首先在主機端(ip:140.123.89.146)開啟 terminal，並輸入 `nc -l -p 12345`。這將在本地主機上建立一個 TCP 伺服器，監聽端口號 12345，等待遠程客戶端的連接。



```
lab502@lab502: ~  
File Actions Edit View Help  
lab502@lab502: ~  
nc: connect to 140.123.89.146 port 444 (tcp) failed: Connection refused  
nc: connect to 140.123.89.146 port 445 (tcp) failed: Connection refused  
lab502@lab502:~$ nc -z -v -n 140.123.89.146 1234  
nc: connect to 140.123.89.146 port 1234 (tcp) failed: Connection refused  
lab502@lab502:~$ nc -z -v -n 140.123.89.146 1234  
Connection to 140.123.89.146 1234 port [tcp/*] succeeded!  
lab502@lab502:~$ nc -l -p 12345  
hi  
hso  
jo  
yo00000000  
123  
123  
465  
Xc
```

接下來在客戶端開啟 terminal，並輸入 `nc 140.123.89.146 12345`，這將使遠程客戶端連接到本地主機上的 TCP 伺服器，開始進行網路聊天。

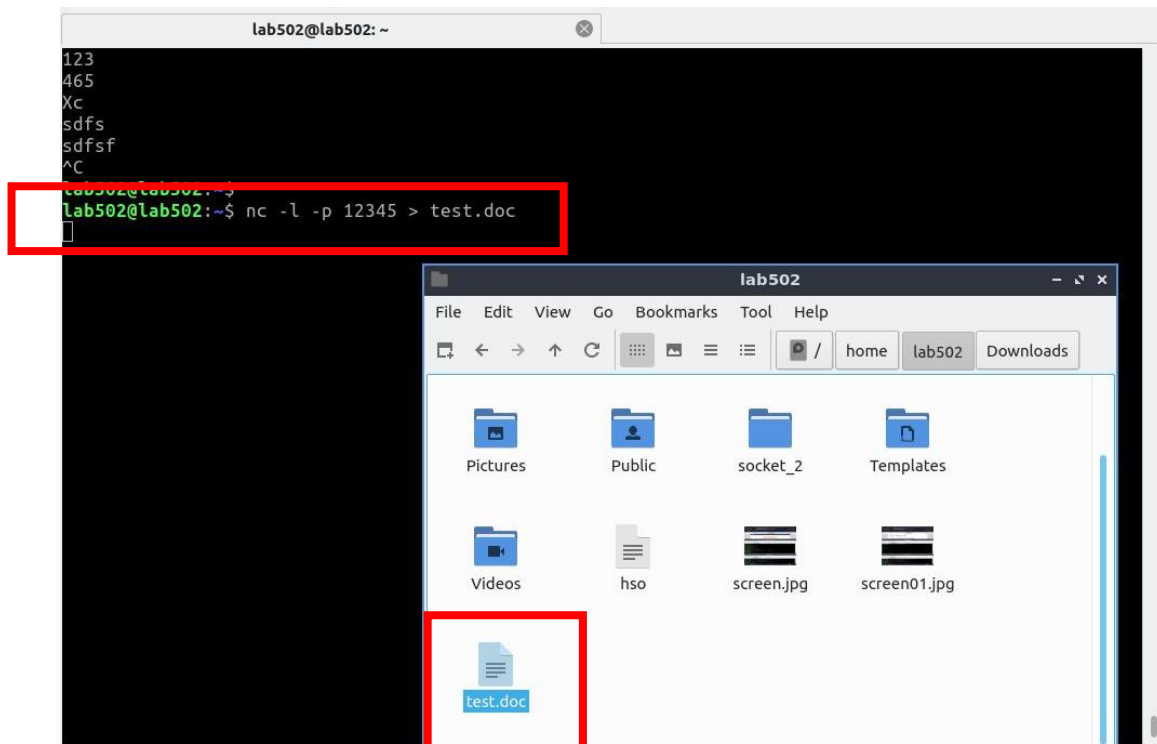


```
lab502@lab502: ~  
File Actions Edit View Help  
lab502@lab502: ~  
lab502@lab502:~$ sudo nc 140.123.89.146 12345  
hi  
hso  
jo  
yo00000000  
123  
123  
465  
Xc  
lab502@lab502: ~
```

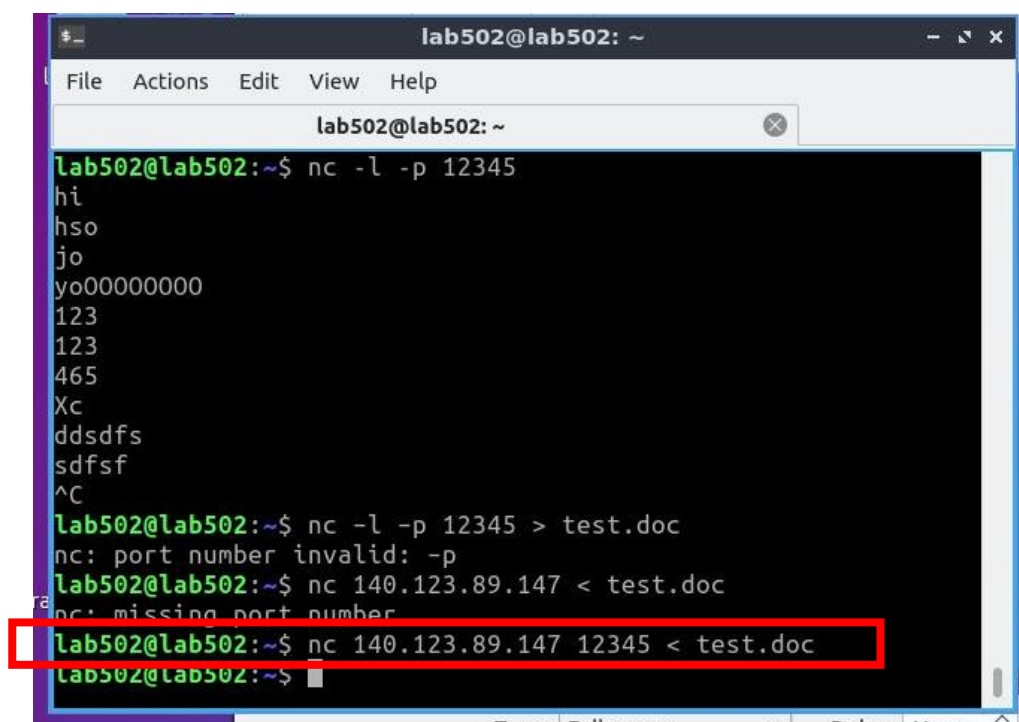
### LAB3:

LAB3 為 Homework，目標為客戶端可將 test.doc 傳送到主機。

首先開啟 terminal 並輸入 `nc -l -p 12345 > test.doc`，這將在主機端上建立一個 TCP 伺服器，監聽端口號為 12345，等待客戶端的連接，當接收到來自客戶端的檔案時，將檔案內容保存為 "test.doc"。



接著，在客戶端上，輸入 `nc 192.168.1.1 12345 < test.doc`，這將在客戶端上建立一個 TCP 連接到主機端的 TCP 伺服器，並將 "test.doc" 檔案內容傳送到主機端。



## 5. 問題與討論

使用 Netcat 進行檔案傳輸可能會存在一些安全風險，因為 Netcat 並沒有提供任何加密功能，傳輸的內容都是明文傳輸，容易被截聽和竊取。此外，也容易受到中間人攻擊的威脅。攻擊者可以在客戶端和主機端之間插入自己的電腦來竊取敏感信息，而使用加密通信可以防止這種攻擊。

為了確保安全，建議使用加密的傳輸方式，例如使用 SSH 或 SSL/TLS，或使用其他安全傳輸協議，以保護信息不被竊取或操縱。

## 6. 心得與感想

透過實驗學習使用 Netcat 進行網路操作，可以幫助我們更深入地了解網路通訊的原理，從而提升我們的技能和知識。在實驗中，我學習了如何使用 Netcat 的 port scanning，以及如何使用 Netcat 進行網路聊天和檔案傳輸。這些技能在實際工作中都非常實用，尤其是在網路安全和系統管理方面。

此外，在實驗過程中，我也了解到了 Netcat 的一些安全風險，例如明文傳輸和中間人攻擊等。因此，在實際應用中，我們需要注意選擇合適的傳輸方式，以保護敏感信息的安全。

總之，通過實驗學習 Netcat，我獲得了寶貴的網路操作經驗，這些經驗將對我未來的工作和學習產生極大的幫助。

## 7. 參考文獻

<https://blog.gtwang.org/linux/linux-utility-netcat-examples/>

<https://ithelp.ithome.com.tw/articles/10136033>

<https://zh.wikipedia.org/zh-tw/Netcat>

<https://amingosec.blog/netcat-nc-commands/>