資訊處
National Chung Cheng University
Office of Information Technology

資安宣導

網路通訊埠管理的必要性

為什麼需要進行網路通訊埠管理

原由：近日校外對校內網路攻擊日益頻繁，其中以 Telnet 及 DNS 攻擊為甚，每日攻擊數量高達千萬次以上，不但造成系統無法負荷，也容易出現資安問題。

說明：為保障校內網路安全，資訊處擬於108年1月15日起，增加校園網路防火牆資訊安全政策，阻斷外界不明的 Telnet 及 DNS 連線。

為避免各單位正常的 Telnet 及 DNS Service 網路連線被阻斷，各單位可至本處網站，下載 校外對校內網路埠開通申請表，簽核完後以公文傳送回資訊處即可。

備註：

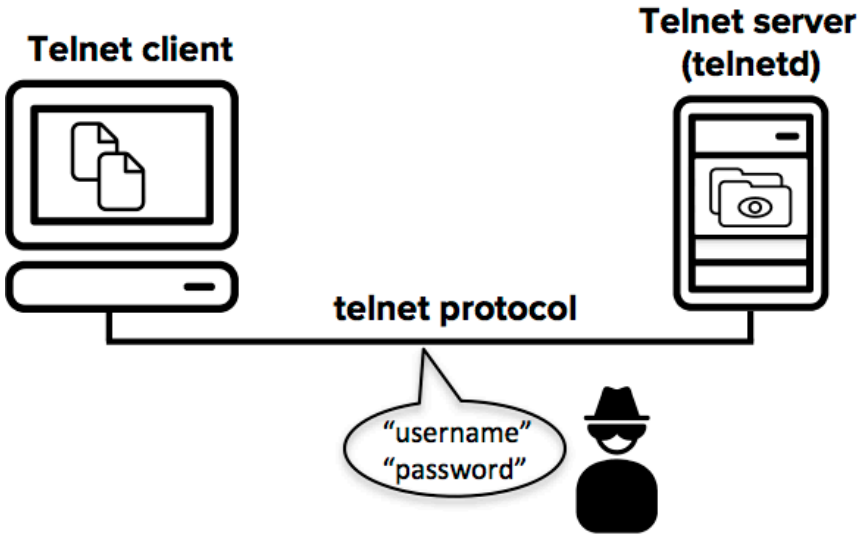
一、Telnet：通常用於同仁或廠商由校外連線回校內，以操作主機及網路設備。如無特別的使用條件，建議改用更安全的 SSH 連線。

二、DNS：只有對系所內提供服務的 DNS server 需要申請開通。

Telnet 攻擊

Telnet 攻擊

- Telnet 是一種網路傳輸協定，讓使用者可以透過網路從遠端連線到主機，並操作被連線的主機。



圖片來源：https://www.ssh.com/ssh/telnet

Telnet 攻擊

- 攻擊方式：暴力攻擊法

  - Telnet是常用的通訊協定，大多數的網路路由器都預設開啟 Telnet 協定，使得駭客有可乘之機。
  - 駭客會以預先設定之字典檔，不斷嘗試進行登入。由於密集的嘗試，大量的封包將造成網路的負荷，甚至癱瘓。
  - 如果使用者設定的密碼不夠安全，駭客可以輕易取得其登入權限，並安裝惡意程式以做為攻擊其它主機的跳板。
  - 防範：加強 Telnet 協定的管理，利用防火牆將其隔離，只開通必要的特定來源，其它連線則予以拒絕。另外，使用者應該要避免使用過短或容易被猜到的密碼。

Telnet 攻擊

- 攻擊方式：側錄法
  - Telnet雖然可以保證資料傳輸的正確性，但並未採取加密協議以保護傳輸資料，因此在操作時，資訊有遭到攔截的可能性。
  - 由於資料是以未經加密的明碼傳輸，駭客可以透過側錄封包軟體，輕易竊取到資訊或取得登入主機的帳號密碼。
  - 防範：改用經過加密的SSH通訊協定。

DNS 攻擊

DNS 攻擊

- DNS攻擊方式：DNS Flooding

  DNS Flooding 攻擊方式是不斷隨機向 DNS Server 送出查詢主機位址的要求，因為多數要查詢的都是不存在的主機，因此伺服器必須不斷遞迴查詢位址，導致效能嚴重耗損，造成系統當機或服務停擺。

- DNS攻擊方式：放大式攻擊

  DNS 要求查詢的字串通常較短，而伺服器回傳的字串則比查詢字串還要長的多，駭客藉由修改來源位址，把回傳字串導向被攻擊者，駭客就可利用少量的流量，放大成數十到數百倍的流量攻擊，造成受害者服務停擺。

DNS 攻擊

- 知名實例：2014 年 6 月美國一家知名遊戲視頻公司，遭到駭客利用大量殭屍主機進行 DNS Flooding 攻擊，巔峰達到每秒 9 億個封包，時間長達 48 小時，期間靠著 ISP 業者的協助，才免於整體系統被駭客癱瘓。

- 防範：目前只能仰賴網路提供者的偵測系統及其資料清洗能力，因此，進行內部DNS的管制是有其必要性的。

資料參考來源

- https://zh.wikipedia.org/wiki/DNS%E6%B4%AA%E6%B0%B4%E6%94%BB%E6%93%8A
- http://newsletter.ascc.sinica.edu.tw/news/read_news.php?nid=2799
- https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=7335
- https://www.ithome.com.tw/tech/87816
- https://www.ithome.com.tw/news/110135
- https://www.datarecovery.com.tw/news/hardware/2010-10-31/792.html
- https://portal.cert.tanet.edu.tw/docs/pdf/20161116101119197688836843562454.pdf
- https://read01.com/zh-tw/zQd0P.html#.XA6y6WgzY2w
- https://zh.wikipedia.org/wiki/Telnet