# 網路安全

```

1.防火牆

1-1防火牆如何運作

1-2防火牆無法防止

1-3SPI狀態封包檢測

1-4周邊網路(Demilitarized zone)

2.網路隔離

2.1VPN

2.2Honeypots.

2.3NAT

3.安全協定

3.1Tunneling Protocol

3.2IPSec

3.3DNNSSec

3.4SET

3.5SSL

4.常見網路攻擊手法

4.1DoS

4.2DDOS

4.3緩衝區溢位

4.4堆疊緩衝區溢位攻擊

4.5DNS Cache Poisoning

4.6網址嫁接

4.7零時差攻擊

4.8跨網站指令碼 XSS攻擊

4.9ARP 偽造攻擊

4.10彊屍網路

4.11風暴彊屍網路

4.12Application Level Floods

4.13網路封鎖

4.14 Spoofing

4.15 Sniffers

4.16 Syn Flood

4.17 LAND Attack

4.18 SQL Injection(資料隱碼)攻撃行為

4.19 攔截式攻擊

```

## 1.防火牆

### 1.1防火牆如何運作

```

Windows防火牆可監視已啟用防火牆之連線中的所有網路流量,防火牆會追蹤所有源自您電腦的通訊,防止來路不明的流量進入您的電腦。

必要時,防火牆會動態開敗連接埠,讓電腦接收您特別要求的流量,例如您已點選位址的網頁等。

如果您沒有要求傳入流量,Windows防火牆會在其到達您電腦前加以封鎖。

針對特殊用途,例如:網路連線、代管線上遊戲或主控自己的網頁伺服器等用途,

您可以選擇要保持開啟的連接埠。這樣做可允許他人和您的電腦建立連線,但同時也會降低安全性。

「連接埠」是一個網路詞彙,意指某個類型的網路流量進入您電腦的點。您 附註:

所開啟的實際連接埠取決於所要傳送和接收的流量類型。

```

### 1.2防火牆無法防止

```

1.電子郵件病毒

防火牆無法判斷電子郵件訊息的內容,因此無法保護您免於這些類型病毒的危害。

開啟電子郵件訊息之前,應該使用防毒程式先掃描和刪除可疑的附件。

2.網路釣魚詐騙

網路釣魚是種用來誘騙電腦使用者透露個人資訊或財務資訊(如銀行帳戶密碼)的技巧。

線上網路釣魚詐騙郵件通常是由很像來自可信賴來源的電子郵件開始,

而實際上其會引導收件者向詐騙網站提供資訊。

```

### 1.3SPI狀態封包檢測

```

SPI狀態封包檢測為目前防火牆較高等級的安全性技術

```

### 1.4周邊網路(Demilitarized zone)

```

第一個防火牆隔開前端伺服器與網際網路，並只允許傳送至該前端伺服器的要求

第二個防火牆隔開前端伺服器與內部網路，存在於兩個防火牆間的系統便稱為周邊網路(DMZ)。

DMZ提供更高的安全性，因為如果前端伺服器被入侵，仍還有一層屏障

供分公司存取的網頁伺服器應該放在周邊網路

```

## 2.網路隔離

### 2.1VPN

```

Virtual Private Network(VPN)可以跨越任何網路，常常需要使用安全功能或某種加密已取得定義中的私有部分

VPN利用已加密的通道協定來達到保密、傳送端認證、資訊準確性等私人訊息安全效果。

若使用得法,這種技術可以用不安全的網路(例如:網際網路)來傳送可靠、安全的訊息。

需要注意的是,加密訊息與否是可以控制的。沒有加密的虛擬私人網路訊息依然有被竊取的危險。

是Windows 及 Linux等所用傳輸協定,不用透過其它網路設備便能達到虛擬私人網路連接。

```

### 2.2Honeypots.

```

1,蜜罐(Honeypots)是一種誘捕系統,目的是以調虎離山的作法引誘攻擊者,讓

攻擊者遠離重要的系統。

2.蜜罐也會收集攻擊者的行為,並且拖延攻擊者在系統所停留的時間,讓管理者能

採取適當的行動。

3,蜜罐内的資訊都是假的、看起來有價值、但合法使用者卻不會存取的資訊。因此,任何存取蜜罐的行為都有可疑之處。

目前最新的作法,是以蜜罐建立完整的網路,以模擬企業完整的網路。

```

### 2.3NAT

```

NAT支援轉換私人的IP位址成公共的IP位址以便和Internet通訊。

這就避免通訊直接進入Internet,同時為小型辦公室或個人使用者節省了取得和維持公共位址的時間和費用。

Network Address Translator,小型的商業網路可以使用私人位址和取得私人位址轉成單一或多個由ISP指派的公共IP位址的NAT對應。

```

## 3.安全協定

### 3.1Tunneling Protocol

```

穿隧協定(Tunneling Protocol)用於描述當一個稱作負載協定的網路協定是封裝在另一種不同的傳送協定中。

使用隧道的原因包含在一不相容的傳送網路上攜帶負載,或在不安全網路上提供一個安全路徑。

```

### 3.2IPSec

```

您可以利用Internet Protocol Security (IPSec)對整個系統或部分系統的網路通訊進行加密,

把網路資料加以保密·PSec提供了在兩台電腦之間設定網路連線的身份驗證和加密的功能。

IPSec為 IP傳輸提供完整性保護、驗證和(可選的)私密性以及重新播放保護服務。

IPSec 封包分為兩種類型:

1.「封裝安全有效負載」的P通訊協定50(ESP)格式,它提供私密性、真實性和完整性。

2.「驗證標頭(AH)」P通訊協定51格式,它僅為封包提供完整性和真實性,但不提供私密性。

以兩種模式使用IPSec,「傳輸模式」,它能保護由來源到目的地現有的IP封包安全,以及「通道模式」,

它能將現有的P封包放在一個新的封包中,然后以IPSec格式將新的IP封包傳送至通道端點。

IPSec 傳輸模式能夠用來為兩個通訊系統之間的端對端IP傳輸提供安全,

例如保護TCP 連結安全或保護UDP資料包安全。

IPSec通道模式主要作為網路中點、路由器或閘道器,用來保護PSec通道中其它IP傳輸的安全,

IPSec通道可透過公用網路或不可信任的IP網路(例如Iternet)將一個私人的IP網路與另一個私人的IP網路相連結。

```

### 3.3DNNSSec

```

DNSSEC 是 DNS Security Extensions的縮寫,我們可稱之為 DNS安全擴充或DNS安全協議,目的是增強DNS服務的驗證。

網域名稱系統(DNS)是支援許多日常網際網路活動的基本通訊協定,這些活動包含電子郵件傳遞、網頁瀏覽及即時通訊。

然而,DNS系統是在三十年之前所設計的,没有我們今天面臨的安全題·

DNSSEC 是ETF對確保由DNS中提供的關於戶網路使用特定類型的資訊規格套件。

可以針對DNS主機之間的資料傳遞上加以驗證來源與訊息內容的可信度。

DNSSEC是利用數位簽章的方式來達到驗證的目的:透過公鑰密碼學的機制,

對於互相通訊的 DNS主機之間利用單向雑湊函數(One-way Hash function)檢視訊息内容並產生一組雜湊值,

管理者以私鑰將驗證訊息及雜湊值加密,提供數位簽章。

當DNS接收端收到訊息時,先將數位簽章解密,再利用雜湊值確認訊息内容未受竄改;

DNSSEC 藉數位簽章的簽署與驗章的過程,強化DNS假冒的安全風險,是目前最有效方式。

```

### 3.4SET

```

安全電子交易(Secure Electronic Transactionㆍ SET )

網際網路的盛行 ,消費者團體注意到線上付款安全機制的不足,

於是VISAMasterCard等大型信用卡國際組織在1996年2月・共同以安全電子交易協定(Secure Electronic Transaction Protocol ,SET)

,當作網際網路上,電子交易系統的共通標準。

基本上,一個SET付款機制參與的成員會涵蓋持卡人(Cardholder)、特約商店(Merchant)、

發卡銀行(issuer)、付款中心(Payment Gateway) 及認證中心( Certification Authority,CA) 持卡人、

特約商店及付款中心,均必須事先向認證中心註冊登記,以取得電子證書,方可能進行電子商務相關的交易。

```

### 3.5SSL

```

Secure Sockets Layer(SSI)安全通訊端層,開放標準,目的是建立安全的通訊管

道,以防止重要資訊(如信用卡號碼)遭到攔截。它主要是為了在全球資訊網獲得安全的電子金融交易,但在設計上亦可運用在其他網際網路服務上。

一般而言,在具有S加密機制的網址都是以https://為開頭·而s就代表該網站

具有SL加密機制,同時您會發現在右下方的狀態列上,會出現一個上鎖的圖示

(lcon),如小鎖圖案為鎖上,即表示SL保密機制已啟動,當您在填寫個人資料前,

應先查看該網頁是否已啟動SSL保密機制。

```

## 4.常見網路攻擊手法

### 4.1DoS

```

阻絶服務(Denial of Service, DoS)是以阻止通信設備正常使用為目的的攻擊方式,

這種攻擊方式大多有特定的目標,如阻斷所有指向特定終點的訊息。另一種是讓網路無法正常運作為目的。

不停的發封包給某網站是常見的 DoS例子。

```

### 4.2DDOS

```

DDOS攻擊,就是透過分散於不同地點、國家的電腦對特定標的物持續發送網路封包,

導致系統與網路無法負載而癱瘓；就好像詐騙集團透過不斷撥電話給你,占用線路,

同時間另外一批人就撥通電話到你家裡,謊稱你被綁架要你交付贖金之類的說詞

但家人卻因為電話線路被占用,怎樣也連絡不上你的状況是一樣的。

```

### 4.3緩衝區溢位

```

緩衝區溢位是駭客社群企圖存取系統所用的一種技術,這種技術相當危險。

駭客們企圖在容器内放入太多資訊,看看他們是不是能夠合理的執行溢位；比方說,

如果被攻擊的程式沒有執行適當的範圍檢查,便會產生溢位,讓駭客趁機執行他想要的功能。

這些溢位常常是在具有完整權限的本機系統帳戶環境下執行的。

```

### 4.4堆疊緩衝區溢位攻擊

```

這類攻擊最常見的是堆疊緩衝區溢位攻擊,這類溢位會覆寫整個堆疊,包括指標在内。

而駭客則調整溢位内的資料量加以控制,然後再傳送電腦專屬的程式碼來執行指令,以及傳回指標的新位址。

最後當系統回到堆疊時,再利用指回堆疊的該位址,執行他們的程式指令。

```

### 4.5DNS Cache Poisoning

```

DNS Cache Poisoning(DNS快取中毒)的攻擊方式便是透過DNS設計上的缺陷,假

冒主要的 DNS主機將錯誤的記錄傳遞給 DNS Cache 主機。

DNS上原本正確合法的記錄遭到非法的竄改時,若再加上「一模一樣」的網頁內容,

瀏覽該網站的使用者根本無從判斷真假。

攻擊手法包括:

1.Man-in-Middle attack(中間人攻撃)

2.DNS Hijacking (DNS綁架)

3.DNS Pharming(DNS嫁接/釣魚假冒)

4.其他

```

### 4.6網址嫁接

```

「網址嫁接」,詐騙者會使用系統,將網際網路訪客導向特定的網站。

網路嫁接者會利用真實網站上的弱點,讓使用者離開原本要造訪的合法網站,並且導向假冒的網站。

```

### 4.7零時差攻擊

```

零時差攻擊(Zero Day Attack)就是當系統或應用程式上被發現具有風險性之弱點

后,但在修正程式發饰之前,或是更新前所進行的惡意攻擊行為。

舉例來說:就像是銀行的金庫保全系統被發現有不周全的地方(譬如攝影機有死角),

但這時候被搶匪發現這個問題,因此趁虛而入輕易得手,銀行卻束手無策一樣。

這也是每當系統或應用程式上被發現新的風險時,所有廠商均致力於完成修正程式,或是採取適當的應變措施原因。

```

### 4.8跨網站指令碼 XSS攻擊

```

跨網站指令碼 XSS(Cross-site scripting)攻擊,是一種針對網站應用程式設計不夠嚴謹所導致的安全弱點攻擊行為。

最原始的弱點是允許攻擊者將惡意程序植入網頁中,導致使用者瀏覧網頁時,受到不同程度的影響,如在背景中下載惡意程序,

後門開啟或是密碼與個人資料之竊取。

新聞事件中常見之XSS攻擊,雖然是針對同樣的弱點進行攻擊,但採用了不同的運作方式。

其原理是讓使用者存取經過特殊設計的網址(該網站本身具有XSS弱點)；使

用者存取時瀏覧器中除了原先正常網站的頁面會出現之外,

也會出現設計惡意網址的作者預計呈現的物件(如影片,圖片,文字)或是希望達成的目標;這樣的運作模式對網站本身並不會造成影響。

```

### 4.9ARP 偽造攻擊

```

當你要連接另外一台電腦時,您的電腦就會先發出ARP封包,詢問網路上有哪台機器對應到這個 MAC位址,才會進行後續的資料傳送。

ARP (Address Resolution Protocol, ARP spoofing) ARP欺騙,

又稱ARP下毒(ARP poisoning) 或ARP攻擊,

是針對乙太網路位址解析協議(ARP)的一種攻擊技術。

此種攻擊可讓攻擊者取得區域網路上的資料封包甚至可蒙改封包,且可讓網路

上特定電腦或所有電腦無法正常連線,

```

### 4.10彊屍網路

```

Waledac對全世界的影響有多大?Waledac彊屍網路是全美十大殭屍網路之一,

影響全球最少數十萬台個人電腦,而此彊屍網路具備每天傳送15億封垃圾郵件的驚人實力,

足以嚴重影響全球網路活動:根據微軟的調查,光是2009年12月3日到21日,

僅統計傳送到hotmail的惡意垃圾郵件就高達6.51億封。

```

### 4.11風暴彊屍網路

```

風暴彊屍網路或稱為風暴蠕蟲疆屍網路,

是一種受遠端控制的彊屍電腦(或直譯機器人網路)組成的網路。

該網路是由暴風蠕蟲(一種透過垃圾電子郵件散播的木馬)連起來的。

```

### 4.12Application Level Floods

```

Application level loods主要是針對應用軟體層的,也就是高於OSI的。它同樣是以大量消耗系統賈源為目的,

透過向還樣的網路服務程式提出無節制的資源申請來迫害正常的網路服務

```

### 4.13網路封鎖

```

網路封鎖是指政府或者機構處於政治或者經濟的原因,透過技術手段限制對某些網站或者服務的存取。

為了防止員工在上班時間存取網站或使用如FaceBook Windows Live Messenger 等軟體進行聊天而算致效率大幅度下降,

網路管理員通常會使用防火檔封閉來自伺服器的80埠服務或僅封鎖部分網路協定(如UDP),

這樣幾乎所有的Web服務都曾權瘓或部分網路聊天工具不能被正常連線,

員工就不能在上班時間存取WB真面或僅可以存取WEB 但不能使用聊天軟體。

```

### 4.14 Spoofing

```

Spoofing(詐騙),入侵者所使用的一種技術,可透過偽造已知網路憑證,

取得對電腦系統或網路的未授權網路存取。

iP詐編是入侵者取得對霍腦系統或網路的未授權路存取的一種常見方法。

```

### 4.15 Sniffers

```

偵測(Sniffers)是一種夥客的竊聽手段,一般是指使用價測器對數據流的數據截獲。

1.分析網蹈信息流通量

2.探測企圖入侵網路的攻擊

3.探測由内邵和外邵的用戶濫用網路資源

4.探測網路入侵後的影機

5.監測連結網際網路宽頻流星

6.監測網路使用流量(包括内部用戶,外部用戶和系統)

7.監測網際網路和用戶電腦的安全状態

8.獲取帳號一般為管理員帳號與密碼等機密信息

9.滲透與欺霸

```

### 4.16 Syn Flood

```

SYN flood 或稱 SYN洪水、SYN洪水是一種阻断服務攻擊,

起因於攻擊者傳送一系列的 SYN 請求到目標系統.當用戶端試著與伺服器問建立TCP連線時,

正常情況下用戶端與伺服器端交換一系列的信息如下:

1.用戶端透過傳送SYN同步(synchronize) 信息到伺服器要求建立連總。

2,伺服器透過響應用戶就SYN-ACK 以抄收(acknowledge) 請求。

3.用戶端答應ACK,連線隨之建立。

```

### 4.17 LAND Attack

```

這種攻撃方式與 SYN floods 類似,不過在LANDattack攻擊包中的原位址和標的位址都是攻擊物件的iP。

這種攻馨會導致被攻擊的機器無窮迴圈,最終耗盡資源而當機。

```

### 4.18 SQL Injection(資料隱碼)攻撃行為

```

駭客運用搜尋引弊尋找網頁上的漏洞,並運用自動化工具攻響網路服務器。

一個<script ...>字串附加到在後端運行的SQL伺服器中所有的文本或可變長字中

列中。

```

### 4.19 攔截式攻擊

```

1,數位簽章通常是用來防止攔截式攻擊的。

2,攔截式攻擊在信號鍵結中需要有個插入點,當處理訊息的實體硬體裝置遇受破壊時,就可能發生還個情況。

例如,在線路被更換過或重設路徑過的情況下,還有電信伺服器遭到破壞並可能發生電路重設時。

3,比較可能的技巧是將用於維護網路的軟體重新設定。

例如,通訊埠發生重新指派或重設路徑,還有在通訊應用程式中建立軟體插入點。

當檔案是以撰寫模式開改時,其鎖定工作針對其他應用程式的使用。

同樣地,當管道用戶端連結到管道伺服器時,會鎖定該管道供該用戶端所專用,一直到該用戶端中斷連接前,都會維持鎖定狀態。

4,成功的攔截式攻擊取決於某個微妙的小地方,例如時間安排探索攔截式改擊需要耗費許多時間、耐心和非常達慎的態度。

一個200毫秒的等候,就足以讓整個銷售部門的機空外洩。

```