第十章

阻斷服務

阻斷服務

- 阻斷服務（Denial Of Service，DoS）就是利用攻擊讓某一個系統造成癱瘓無法使用，或者使這個系統因為資源的過度負荷，而明顯的降低了執行速度。

- 攻擊者如果嘗試要入侵某個系統，但是最後無法取得這台主機的存取權限時，很可能會基於報復的心理讓這台機器當機，阻斷服務就是其中一種報復手法。

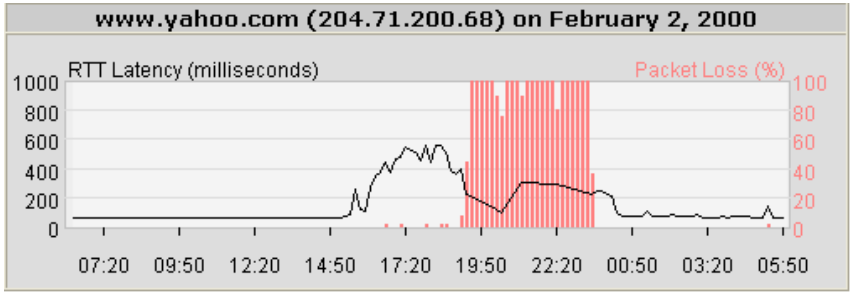
案例

案例 1：1999年IIS漏洞及攻擊，造成網路壅塞。

案例 2：2000年DDoS攻擊，造成Yahoo、eBay、CNN、Amazon等網站癱瘓數小時。

案例 3：2003年SQL Slammer攻擊，造成美洲及亞洲網路嚴重癱瘓。

案例 4：2004年MyDoom病毒攻擊。



阻斷的目標

攻擊者會阻斷的狀況有：

- 可能會嘗試阻止特定的個人。（針對特定個人）
- 可能會嘗試中斷任兩台機器之間的連線。（針對不特定主機）
- 可能會嘗試阻斷一個內部網路。（針對特定使用群）
- 可能會嘗試中斷一個特定系統的服務。（針對特定目的地主機的服務）

DoS造成的影響

（1）造成網路關閉。
（2）造成組織關閉。
（3）財物的損失。
（4）友好的損失。
（5）造成資源的消耗。
（6）設定資料的破壞或改變。
（7）特定資源的改變。

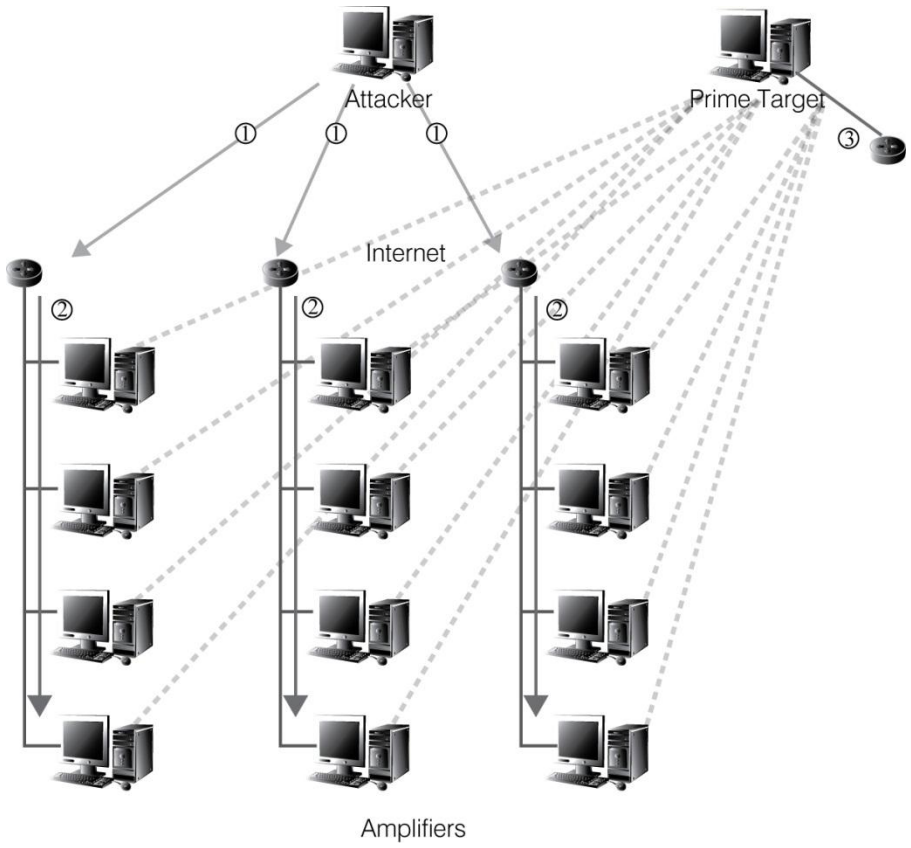
阻斷服務攻擊形態

- DoS攻擊，以單一主機對目標進行阻斷服務攻擊。
- DDos攻擊，以多台機器對目標進行阻斷服務攻擊。

DoS攻擊方法

- **Smurf**

- 這種方法是直接對網路進行廣播，造成網路上很快地充滿垃圾封包，網路因為大量的垃圾封包而中斷。



Smurf

1. Smurf主機以假造的來源IP位址，不斷地將大量偽造的ICMP協定的要求封包送給IP廣播位址。
2. 網路設備會將這些封包廣播送給網路上的所有主機。
3. 然後所有主機在廣播位址上收到要求之後，會傳送ICMP回應封包給目標主機，受害主機若無法處理這麼多封包，將會被阻斷服務。

Smurf

- smurf的攻擊方式因為會在網路上塞滿ICMP的要求封包與回應封包而造成網路中斷，等於是阻斷整個網路的服務，所以常被稱為smurf倍增型攻擊。

- 與smurf攻擊方法類似的是fraggle攻擊，只是其所使用的是UDP echo。

DoS攻擊方法

- **Buffer Overflow**

- 主要原因是因為寫程式的程式設計師的疏忽。
- 當程式設計師的程式中需要一塊記憶體緩衝區，但是這個記憶體緩衝區被規劃的容量太小，當大量的惡意資料進入到這個不足的記憶體緩衝區空間時，就會產生緩衝區溢出的錯誤。
- 這時攻擊者可以蓋掉程式執行路徑上的資料，並且攔截原來程式的控制，轉而去執行攻擊者塞入的程式碼，進行阻斷服務的工作。

DoS攻擊方法

- **Ping of death**

- ping of death是利用ICMP協定的一種攻擊，攻擊者發送一個長度超過65535的Echo需求封包，封包在傳送時雖然會被切成較小的區段（segments），但是在目標主機會重組這些區段，這時候產生的封包會大於65535，造成類似緩衝區溢位的問題，系統通常會重開機或掛掉。

Ping of death

- 以下是Linux上命令的語法：

ping -c 1 -s 65535 192.168.0.1

Error: packet size 65535 is too large. Maximum is 65507

- Linux的ping已經不允許製造過大的封包了，目前新版本的作業系統也已經解決這個缺陷。

DoS攻擊方法

- **TearDrop**

- 使用UDP攻擊，利用IP封包重組的漏洞來進行攻擊。
- 當資料要經由網路傳送時，其IP封包被切割成許多小片段；每個小片段和原來封包的結構除了某些記載位移的資訊不同外，其餘大致都相同，其中這些位移資訊是要使網路主機在收到這些小片段時能夠正確地重組IP封包。

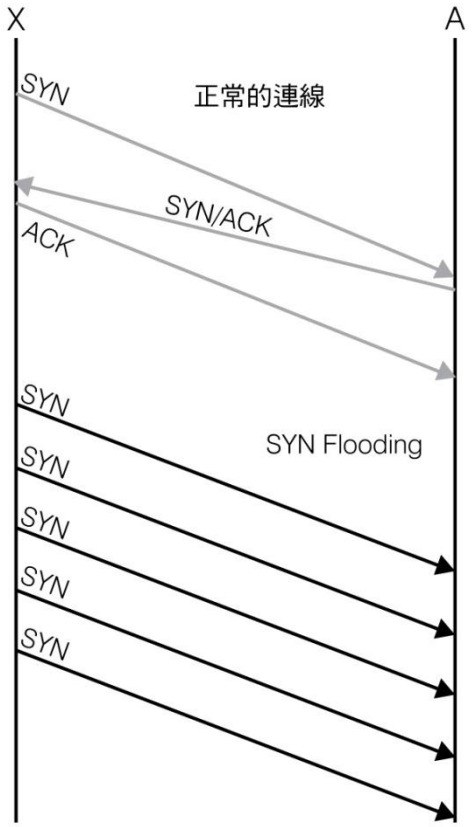
TearDrop

- TearDrop攻擊則憑空創造或修改一些IP片段，但這些片段的位移值卻發生重疊的狀況或故意造成資料片段有間隙（Gaps）。
- 當這些片段被傳送到達目的地主機，作業系統在重組這些IP封包時將會產生疑問，此時可能會造成這部主機的系統當機，也就阻斷服務了。

DoS攻擊方法

- **SYN 攻擊**

- 攻擊者只對目標主機發送一連串的TCP SYN封包給目標主機，每個封包都要求目標主機系統回應一個SYN/ACK封包，然後目標主機系統在回應SYN/ACK封包後，會等待對方送出ACK封包（三方握手）。



SYN 攻擊

- 由於攻擊者並不產生任何ACK封包給目標主機，因此目標主機的系統佇列裏面，會暫存大量的SYN/ACK封包，這些封包必須等待，一直等到接收到ACK封包或是超過時間（Time out）之後才會被移除。
- 如此，目標主機的系統中因為充滿了SYN/ACK封包，將造成無法處理其他使用者的服務與要求，等於阻斷了這部主機的服務。

DDoS攻擊方法

- 網際網路上現在最可怕的是分散式阻斷服務（Distributed Denial Of Service，DDoS），這種攻擊是多台具有危害性的主機去攻擊一台單一的目的地系統，造成目標系統的使用者服務的阻斷。

- 目標系統如同被洪水氾濫，服務通常會被強制關閉，於是合法使用者就無法使用這個系統的服務，因此就形成阻斷服務。

DDoS攻擊方法

- 被攻擊的目的地主機系統稱為主受害者（Primary Victim）。
- 被用來當做發動攻擊的主機稱為次受害者（Secondary Victims），而攻擊者可以輕鬆駕馭許多不知情的電腦做為攻擊平台。

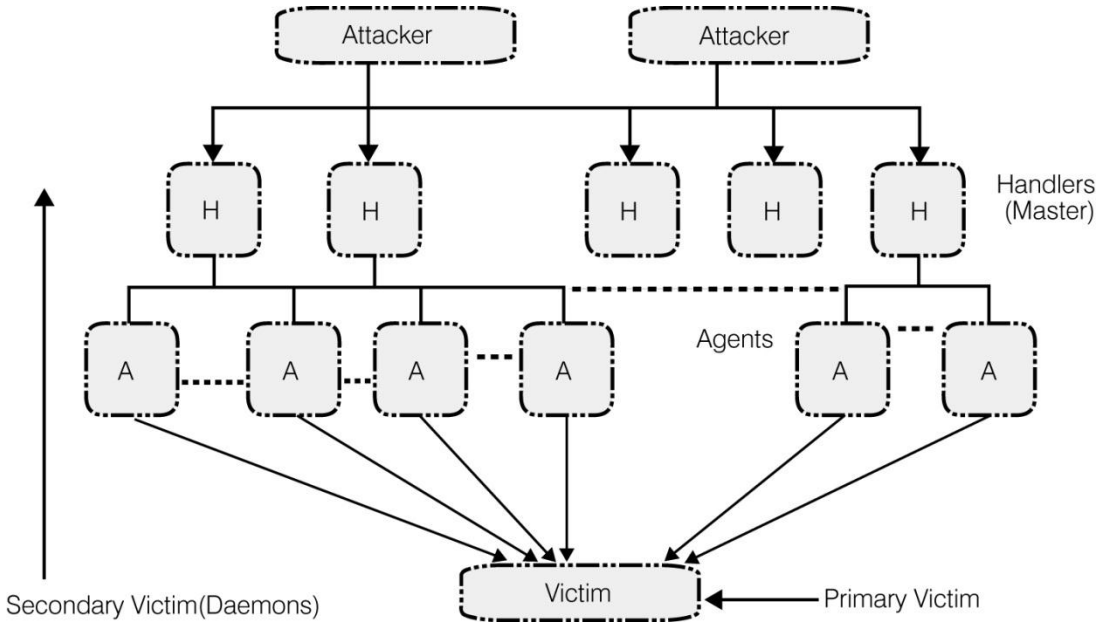
DDoS攻擊方法

- DDoS 難於偵測最原始的攻擊者，且這種攻擊一旦開始，也根本沒有辦法停止或阻止，因為攻擊的原始IP來自於許多不同的主機。

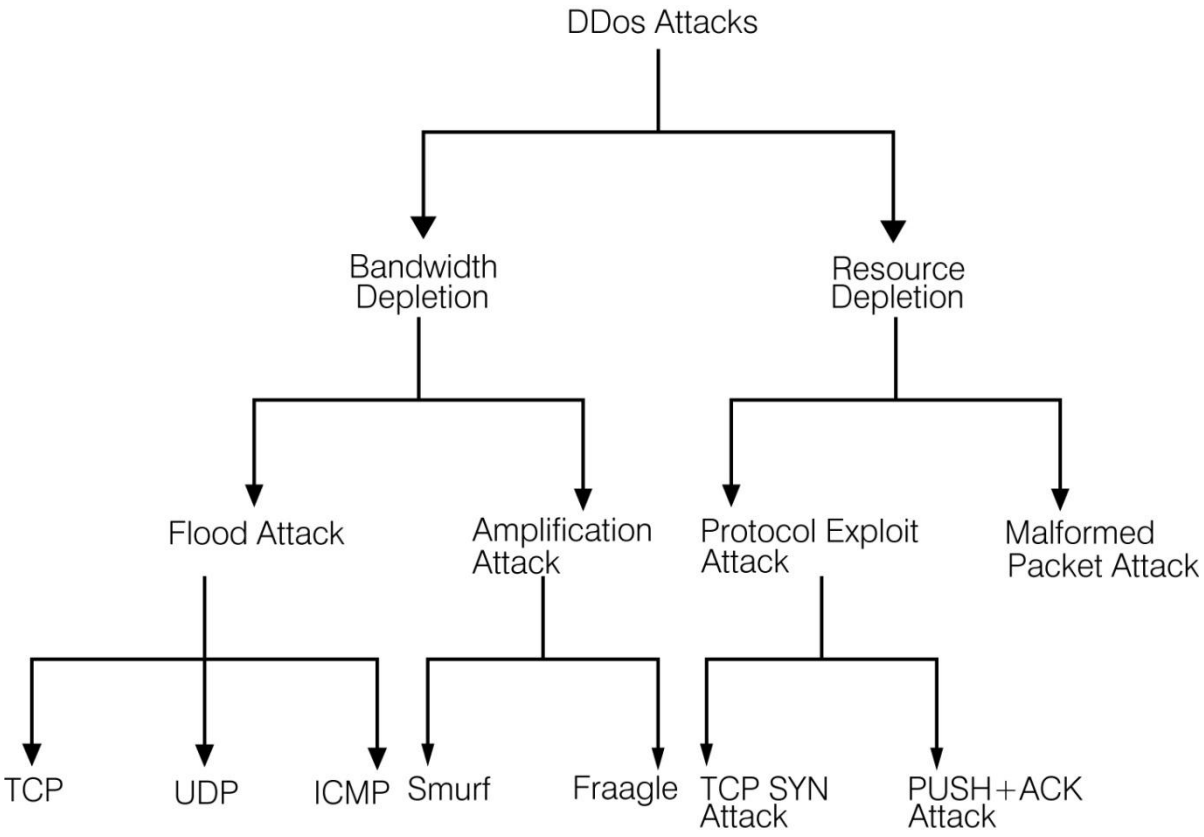
- 假如攻擊的IP位址只有一個，它可以被防火牆阻擋。但是如果是3000個，那麼要阻擋就很困難。

DDoS攻擊方法

- 攻擊者常會先控制主要的Handler主機，然後透過這些控制主機再去操控真正的攻擊主機（Agent）進行攻擊，這裡Handler及Aaent都是次要受害者。



DDoS攻擊分類


DDos Attacks
Bandwidth Depletion
Resource Depletion
Flood Attack
Amplification Attack
Protocol Exploit Attack
Malformed Packet Attack
TCP
UDP
ICMP
Smurf
Fraagle
TCP SYN Attack
PUSH+ACK Attack

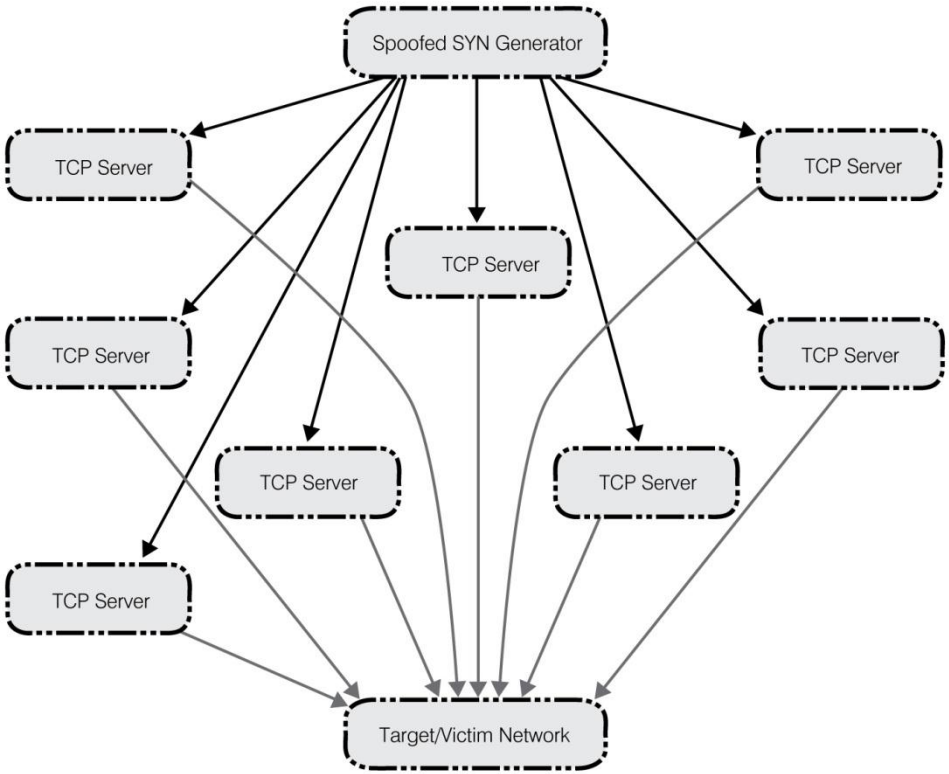
DDoS攻擊分類

（1）頻寬消耗法（Bandwidth Depletion）：又可分為氾濫攻擊（Flood Attack）及擴增型攻擊（Amplification Attack）。氾濫攻擊通常使用TCP、UDP或ICMP進行，擴增型攻擊就是Smurf及Fraggle。

（2）資源消耗法（Resource Depletion）：又可分為協定弱點攻擊（Protocol Exploit Attack）及變形封包攻擊（Malformed Packet Attack）。協定弱點攻擊包含SYN攻擊及PUSH/ACK攻擊。

反射式DoS攻擊

- 這是一個利用三方握手的弱點所進行的DoS攻擊，攻擊主機先送出大量的SYN封包，但是來源IP是偽造的，假造成受害者主機的IP，任何一個接到SYN封包的機器都會回應四個SYN/ACK的封包，但是這封包卻是送給了受害的目標主機，因此大量的SYN/ACK封包，會讓目標主機與目標所在網路的效能嚴重降低。



對策

- DoS比較容易解決，如果發現DoS攻擊的主機IP，只要將此主機的IP予已封鎖即可。
- 比較難以防範的是DDoS 。
- DDoS的對策主要有五種方法 。

對策

（1）防止次要的受害者

- 次要受害者就是被操縱進行攻擊的主機，這些主機也是受害者。
- 防止次要受害者比較不容易，大部分管理者只能防止自己組織內一般使用者的主機變成次要受害者。
- 防護的方法就是在用戶端的電腦上安裝防毒及防木馬程式，隨時確認有更新病毒碼，並利用這些系統進行檢查及掃描。
- 進階的的方法是在電腦系統的核心硬體及軟體上，直接內建「入侵防禦機制」。

對策

（2）檢測及消滅控制者

- 管理者去學習Handler與Agent之間的通訊協定及流量樣本，以識別網路上Handler，消滅少數的Handler就可以減少許多的Agent運作，相對也就減少很多的DDoS攻擊。

- 但是，這種方法的技術層次相對較高，且主要是針對企業內部的電腦。

對策

（3）檢測潛藏的攻擊

- 在組織的網路出口端進行過濾，掃描離開組織網路的每一個IP封包的表頭。
- DDoS攻擊封包的來源位址有很高的機率是假造的，因此一定不會是一個合法的內部網路IP，這時可以放一個封包嗅探器在網路出口，以過濾出不是正確來源IP位址的主機。

對策

（4）減緩或停止DDoS攻擊

- 負載平衡（Load Balancing）
- 節流閥（Throttling）
  - http://mailman.ipv6.club.tw/pipermail/vowimax/2007-February/000260.html
- 蜂蜜罐（Honey pots）

對策

（5）攻擊鑑識

- 流量樣本分析
- 封包回溯追蹤
- 事件記錄

反射式DoS的對策

- 內部網路在設計時，對於不正確的來源封包能夠過濾（防止有假造SYN產生器），並檢視有哪些是屬於反射伺服器的來源 IP，在路由器上以ACL阻擋（防止目標網路被攻擊）。

- 伺服器本身要能防止不完全的三方握手連線，防止成為反射伺服器或是被攻擊的目標主機。

蠕蟲

- 蠕蟲（Worms）不同於病毒，病毒需要某些人類行為的參與以感染電腦，蠕蟲不需要。

- 蠕蟲因為會經常伴隨著有如DoS或DDoS的行為 。

Slammer Worm

- 2003年1月25日起，全球網際網路開始遭受到SQL Slammer網蟲的威脅。
- 主要以Microsoft SQL Server 2000及Microsoft Desktop Engine（MSDE）2000為目標，有害程式碼能侵入受害主機，再以UDP port 1434高速傳送攻擊封包，溢滿了整個網際網路，形成分散式阻斷服務攻擊（DDoS）。

三色警戒

- 紅色警戒：於機關單位通報資通安全「A」等級事件（將影響政府服務、公共安全、社會秩序、人民生命財產之緊急狀況）。
- 黃色警戒：於平時如元旦、總統就職典禮與十月慶典等重點期間，國家資通安全可能遭受威脅。
- 藍色警戒：平時經收集情報研判電腦網路駭客可能有入侵舉動之異常狀況，以及電腦病毒可能蔓延全國之重大疫情。

MSBlast

- 又名疾風病毒，至2003/8/13，已知的全球受害電腦超過一百萬台，而國內有二百家大型企業和二千家小型企業的通報，初步估計全台約有五萬台電腦受害。
- 病毒會自行複製，然後再透過網路搜尋其他可攻擊的電腦大量散播，並造成電腦系統不穩定，有的案例甚至造成當機（例如重新開機）。
- RPC是Windows所使用的通訊協定，但是RPC在TCP/IP上處理訊息交換的部分有一個弱點，攻擊者能夠利用此弱點在受影響的系統上使用本機系統權限執行程式碼，並進行任何動作。

MyDoom.B

- Mydoom是一種大量傳送郵件的蠕蟲，通常以.bat、.cmd、.exe、.pif、.scr或.zip的副檔名格式夾帶在信件中，透過Kazza軟體的點對點檔案網路分享功能於網路上散播。
- 它會對www.sco.com及www.microsoft.com執行DoS攻擊，受影響之系統：Windows 2000、Windows 95、Windows 98、Windows Me、Windows NT、Windows Server 2003、Windows XP。如果中毒電腦的系統日期是2004年2月1日以後的日期（包括2月1日當天），病毒便會攻擊該網站。

DDoS攻擊步驟

步驟1：寫一隻病毒程式，會送出Ping或SYN封包到目的地網路或網站。

步驟2：用這個病毒感染至少30,000台電腦，並且讓這些電腦變成可以控制的殭屍電腦（zombies）。

步驟3：藉由覺醒信號（wake-up signals）或特定資料觸發殭屍電腦發起攻擊。

步驟4：殭屍電腦將持續攻擊目標伺服器，直到殭屍電腦被解毒為止。

工具程式

- **Jolt2 （Unix） -TearDrop**

- jolt2.c是一個無限循環的程式，其不停發送一個ICMP/UDP的IP碎片，可以使Windows系統的機器鎖死。

工具程式

- **Land and LaTierra（Unix）-SYN**

- 運用IP假造（Spoofing）技術送出一連串TCP的SYN封包給目標主機，並讓目標主機系統誤以為這些封包是由自己發送的（來源位址與目的位址相同）。
- 由於目標主機在處理這些封包的時候，它自己並無法回應給自己SYN-ACK封包，因而造成系統當機。

工具程式

- **Targa（Unix）**

- Targa可以用來執行八種不同的DoS攻擊，它是一堆工具的集合，攻擊者可以選擇性的使用部份或全部的工具進行攻擊。

工具程式

- **Trin00**

- 是第一個被散佈及廣泛使用的DDoS攻擊工具，可以用來對許多來源進行協同式的UDP洪水（Flood）阻斷攻擊。
- 攻擊者只要指揮Trinoo Master對一個或多個IP去進行發起阻斷服務攻擊，並可指定攻擊的起訖時間。
- 通常trin00Agent會被安裝在具有Remote Buffer Overrun弱點的系統中。

工具程式

- **Tribe Flow Network（TFN）**

- tribe.c及td.c提供攻擊者消耗目標頻寬及資源的攻擊能力。TFN工具提供UDP及ICMP氾濫、TCP SYN及Smurf攻擊。
- Agents及Handlers間的通訊使用ICMP_ECHO_REPLY封包，這種封包比UDP流量更難於偵測，而且有能力穿透防火牆。

工具程式

- **TFN2K**

- 基於TFN架構，但是TFN2K流量難於辨識與過濾，可遠端執行命令但隱藏假造攻擊來源的真實IP，可透過多個傳輸層協定來傳輸TFN2K流量，包括UDP、TCP及ICMP。

- UNIX、Solaris、Windows NT平台都會受其攻擊影響。

工具程式

- **Stacheldraht**

- 它是基於較早版本的TFN改良的DDoS攻擊工具，如同TFN包含了ICMP flood、UDP flood、TCP SYN攻擊選項。

- 在攻擊者與handler系統間也提供了安全的telnet對稱加密，以防止系統管理者監聽流量及識別。