DNS導論與安全問題

TWCERT/CC 魏銷志

什麼是DNS

- DNS全名
  - Domain Name System
  - 領域名稱解析系統、網域名稱系統
- 領域名稱(Domain Name)與IP位址的轉換
- 將較容易記憶的主機名稱，轉譯成IP位址，可以不用強記IP位址。

台灣電腦網路危機處理中心暨協調中心
Taiwan Computer Emergency Response Team / Coordination Center

DNS的架構

- DNS系統基本是採樹狀階層式(hierarchy)的架構
  - 分散管理
  - 分散儲存
  - 分散查詢

DNS的重要性

- 沒有DNS，Internet沒有辦法將hostname轉換成IP位址
- DNS系統所造成的影響是全面性的
  - 無法存取Web Server，並不會影響SMTP Server但如果DNS有問題??
  - 部份的Firewall或Proxy系統使用hostname的ACL作為限制的依據，DNS有問題則防禦網可能崩潰

DNS運作原理

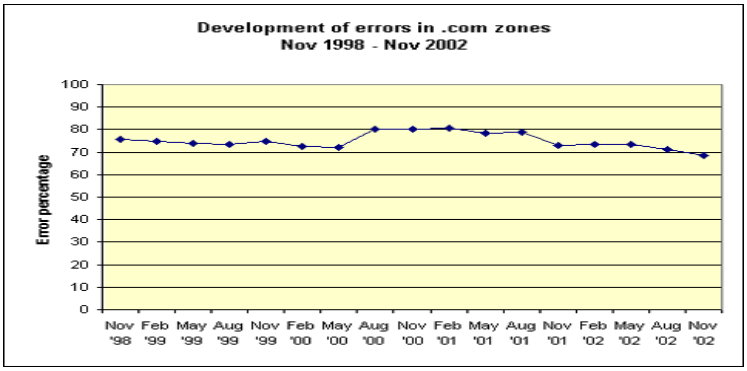
- Recursive(遞迴式)
  - 客戶端只丟出一個詢問給其所屬的DNS伺服器
  - DNS伺服器就會不斷地查詢，直到有結果為止
  - 最後把結果傳回來給客戶端
- Iterative(交談式)
  - 詢問其他DNS伺服器是否知道結果
  - 如果沒有這個記錄，則會傳回一個參考位址，也許這個位址可以查到需要的資料。
- 一般來說Resolver 對 local DNS server 都是 Recursive Query; 而 DNS server 之間的查詢則多是Iterative
- 大部份的 DNS server 都可以接受 Recursive 和 Iterative 兩種查詢方式；但考量負載問題，Root name server 只接受 Iterative查詢

DNS安全考量因素

- 系統設定問題
  - Zone Transfer
- DNS實作問題
  - System Vulnerability
  - DNS Spoofing
  - DNS ID hacking
  - DNS cache poisoning
- DNS規劃與管理問題
  - Split Horizon DNS
  - Split-Service DNS
  - 將DNS安裝在專屬機器上
- Information leak
- DOS & DDOS

.COM Zones Misconfigured

- 68.6% 的 .COM 區域DNS設定有問題



Domain Health Survey 2002.11
http://www.menandmice.com/6000/6150_chart.html

Single Point of Failure

Single Point of Failure	Percentage (N=5000)	Change since Aug '02	Change since *May '01*
All name servers on the same subnet	28.1%	+0.5	+2.6
Only one authoritative name server	6.6%	-0.8	+0.6

Domain Health Survey 2002.11
http://www.menandmice.com/6000/61_recent_survey.html

Zone Transfer問題(1)

- 使用者可透過此種方式，得知整個IP 位址或網域名稱的資料。

Zone Transfer Results	Percentage (N=5000)	Change since Aug '02	Change since Nov '98
No server allowed zone transfer	38.6%	-1.0	-24.96
Some server blocked zone transfer	6.0%	+3.3	-0.36
All name servers allowed zone transfer	55.3%	-1.2	-24.0

Domain Health Survey 2002.11
http://www.menandmice.com/6000/61_recent_survey.html

Zone Transfer問題(2)

- Hacker取得這些資訊的用途
  - 確認目標
  - 獲得相關資訊
    - How many hosts you have
    - What makes and models you have
    - What their names are
- 可經由named.conf 檔案中，設定限制對象或不啟動allow-transfer 選項，以防範這類的問題。

避免SPOF的方法(1)

- 不要把雞蛋放在同一個籃子裏!!!
- 網路方面
  - Don't place all the DNS Servers in the same subnet with the single choke point or router.
  - Don't put all of the DNS servers behind a single leased line
  - Always distribute the DNS Servers in different network in different routing paths.

避免SPOF的方法(2)

- 主機方面
  - At least two different server hosts
  - Running the DNS on different platforms of hardware/OS
    - 管理的複雜度的增加!!!
  - Different versions of DNS Server Software Or Different DNS Servers Software
    - Choose other alternatives
  - Arrange Off-site slave name server

System Vulnerability(1)

- New vulnerabilities are found in DNS Server all the time
- 可能的原因
  - Dsign Phase
  - Implementation Phase
  - Operation Phase
  - Human Nature
- 可能的運用方式
  - Buffer Overflow
  - Format String
  - Etc…

System Vulnerability(2)

- 可能造成的結果
  - Program Error
  - Gain Privilege
  - Denial of Service
  - Information Leak
  - Backdoor/trojan

System Vulnerability(3)

- These vulnerabilities are usually patched quickly
- Stay current with the lastest release or patch update
- Join the mailing list that announces the lastest release or patch update to keep you informed.
- TWCERT/CC Advisory
  - http://www.cert.org.tw/document/advisory

Split Horizon DNS

- 有時DNS提供太多的資訊，可以很明確的得知系統或網路結構
- 有效隱蔽內部DNS結構
- 將DNS Server區分為外部DNS與內部DNS
  - 內部必須以防火牆隔離，嚴防內部結構外洩

Split Service DNS

- Consider creating two kinds of name server, each optimized for a particular function:
  - Advertising name servers:
    - Authoritative for zones to "advertise" to the Internet
    - Listed in parent zones' NS records
    - Queried only by other name servers
    - Non-recursive
  - Resolving name servers:
    - Authoritative for "internal" zones
    - Queried only by known resolvers (or forwarding name servers)
    - Answer recursive queries from trusted sources

將DNS安裝在專屬機器上

- 單獨安裝一套系統於機器上，可以增加系統入侵的困難度
- 可快速的確定入侵的可能方式
- 利用封包過濾掉所有的封包只允許TCP/UDP Port 53的通訊。

Restrict Queries

- If you can't turn off recursion, restrict the queries that your name servers accept to:
  - The addresses they should come from
  - The zones they should ask about
- On most name servers
  - Queries for records in authoritative zones can come from anywhere, because the zones are delegated to the name server
  - Queries for records outside of authoritative zones should only come from internal addresses

Run DNS chroot

- Run with Least Privilege
- To ensure that a vulnerability in BIND doesn't give a hacker access to your host's entire Filesystem
  - You'll need copies of important libraries and system files in that directory
  - For more information, see:
  - http://www.linuxdoc.org/HOWTO/Chroot-BIND-HOWTO.html
  - http://www.etherboy.com/dns/chrootdns.html

DNS與入侵偵測系統

- Firewall can't protect DNS servers
- Harden you DNS server always review your configuration and binaries
  - Tripwire or other similar software to verify the integrity of the DNS binaries&configuration files.
  - Host based IDS
- Install NIDS to prevent DNS attack

問題與指教