Một số thuật ngữ tin học thông dụng

Account: Tài khoản ,là sự kết hợp của hai yếu tố username và password do một dịch vụ nào đó đã cung cấp cho bạn khi bạn đã đăng ký với họ để bảo mật cho bạn

ATM: Là chữ viết tắt của "Asynchronous Transfer Mode". Đây là một kỹ thuật mạng định hướng kết nối mà sử dụng những cell nhỏ có kích thước cố định ở mức thấp nhất. ATM có ưu điểm về khả năng hỗ trợ dữ liệu thoại và video

ACK: Là chữ viết tắt của "Acknowledgement"

ARP: Là chữ viết tắt của "Address Resolution Protocol". Giao thức TCP/IP được sử dụng để liên kết động một địa chỉ IP cấp cao vào một địa chỉ phần cứng cấp thấp

Anonymous: Ẩn danh, nặc danh

Buffer Overflow: Lỗi tràn bộ đệm. Đây là một trong những kỹ thuật Hacking kinh điển nhất

CGI: Là chữ viết tắt của "Common Gateway Interface". Đây là một phương pháp cho phép giao tiếp giữa server và chương trình nhờ các định dạng đặc tả thông tin.
- Lập trình CGI cho phép viết chương trình nhận lệnh khởi đầu từ trang web, trang web dùng định dạng HTML để khởi tạo chương trình
- Chương trình CGI chạy dưới biến môi trường duy nhất. Khi WWW khởi tạo chương trình CGI nó tạo ra một số thông tin đặc biệt cho chương trình và đáp ứng trở lại từ chương trình CGI. Sau đó server xác định loại file chương trình cần thực thi.
- Nói tóm lại lập trình CGI là viết chương trình nhận và truyền dữ liệu qua Internet tới WWW server. Chương trình CGI sử dụng dữ liệu đó và gửi đáp ứng HTML trở lại máy khách

Cookie: Là những phần dữ liệu nhỏ có cấu trú được chia sẻ giữa web site và browser của người dùng đã được mã hoá bởi Website đó. cookies được lưu trữ dưới những file dữ liệu nhỏ dạng text (size dưới 4k). Chúng được các site tạo ra để lưu trữ/truy tìm/nhận biết các thông tin về người dùng đã ghé thăm site và

những vùng mà họ đi qua trong site. Những thông tin này có thể bao gồm tên/định danh người dùng, mật khẩu, sở thích, thói quen...

Crack Password: Bẻ khoá mật khẩu

Compile: Biên dịch (1 chương trình nào đó)

Client: Máy con,khách ,dùng để kết nối với máy chủ (Server)
Covering Tracks: Sau khi đã có những thông tin cần thiết, hacker tìm cách xoá dấu vết, xoá các file log của hệ điều hành làm cho người quản lý không nhận ra hệ thống đã bị xâm nhập hoặc có biết cũng không tìm ra kẻ xâm nhập là ai

Daemon: Daemon (hay còn được gọi là "service") là một chương trình chạy trên một cổng nhất định nào đó. Nó sẽ chịu đáp ứng lại mọi yêu cầu của client khi client này kết nối đến server trên cổng đó. Ví dụ như smtp daemon theo mặc định chạy trên cổng 25. Để có thể check mail, máy của bạn phải kết nối đến server này trên cổng 25, cổng mà smtp daemon đang nắm giữ!

DNS: Là chữ viết tắt của "Domain Name System". Một máy chủ DNS đợi kết nối ở cổng số 80, có nghĩa là nếu bạn muốn kết nối vào máy chủ đó, bạn phải kết nối đến cổng số 80. Máy chủ chạy DNS chuyển hostname bằng các chữ cái thành các chữ số tương ứng và ngược lại.
Ví dụ : 192.168.2.0 --localhost và localhost--192.168.2.1

DoS: Là chữ viết tắt của "Denial of Service", tức là "Tấn công từ chối dịch vụ". Nghĩa là Hacker sẽ chiếm dụng một lượng lớn tài nguyên trên server, tài nguyên có thể là băng thông, bộ nhớ, cpu, đĩa cứng, ... làm cho server không thể nào đáp ứng các yêu cầu khác từ các clients của những người dùng bình thường và có thể nhanh chónh bị ngừng hoạt động, crash hoặc reboot

Debug: Là chương trình đi kèm với DOS-dĩ nhiên là mọi version của Win đều có chương trình này. Đây là một công cụ tuyệt vời để gỡ rối chương trình,unassembling và cracking,đọc bộ nhớ bị che giấu như boot sector và nhiều hơn nữa... Yêu cầu các bạn phải biết assembly mới dùng được debug

Domain: Là tên miền của 1 Website nào đó
Ví dụ : http://www.langdu.de

Decryption: Giải mã

DES: Là chữ viết tắt của "Data Encrypt Standar". Đây là một trong những chuẩn mã hoá password thông dụng, rất khó bị crack, chỉ có một cách duy nhất và cũng là dễ nhất là dùng tự điển

Exploit: Khai thác (lỗi nào đó)

Encryption: Mã hoá

Ethernet: Là công nghệ nối mạng có năng lực mạnh được sử dụng hầu hết trong các mạng LAN. Đây là mạng dùng CSMA/CD (carrier sense media access/ collision detection)

EGP: Là chữ viết tắt của "Exterior Gateway Protocol". Đây là một thuật ngữ áp dụng cho giao thức nào được sử dụng bởi bộ định tuyến trong một hệ tự quản để thông báo khả năng đi đến mạng cho ho bộ định tuyến trong hệ tự quản khác

Enumeration: Là tìm kiếm những tài nguyên đực bảo vệ kém, hoạch tài khoản người dùng mà có thể sử dụng để xâm nhập. Nó bao gồm các mật khẩu mặc định, các script và dich vụ mặc định. Rất nhiều người quản trị mạng không biết đến hoặc không sửa đổi lại các giá trị này

Escalating Privileges: Là Hacker tìm cách kiểm soát toàn bộ hệ thống. Hacker sẽ tìm cách crack password của admin, hoặc sử dụng lỗ hổng để leo thang đặc quyền trong trường hợp họr xâm nhập được vào mạng với tài khoản guest. John và Riper là hai chương trình crack password rất hay được sử dụng

FTP: Là chữ viết tắt của "File Transfer Protocol". Đây là giao thức truyền file trên mạng. Thường dùng để upload file lên Host, Server. Cổng mặc định là 21

Fake IP: IP giả mạo, IP không có thật

Fragmentation Scanning: Là một bước tiến hoá nữa của các chương trình Scanner. Thay vì gởi các packet như trước để thăm dò , ta sẽ chia nhỏ packet này ra thành nhiều packet nhỏ hơn nhằm tránh sự phát hiện của các chương trình packet filter. Các packet này sau khi lọt qua được các chương trình kiểm tra sẽ được các deamon ráp nối lại .

Firewall: Là bước tường lửa dành cho mạng server hãng xữong hoặc cá nhân.

GNU Debugger: Là chương trình biên dịch gcc và công cụ gỡ rối gdb

GUI: Là chữ viết tắt của "Graphic User Interface". Đây là giao diện đồ hoạ người sử dụng trong hệ điều hành Linux

Get Admin: Là "Leo thang đặc quyền" hay còn gọi là "Leo thang mức ưu tiên". Đây được coi là một trong những bước quan trọng khi Hacker đột nhập vào các hệ thống. Giả sử bạn chiếm được quyền và đăng nhập vào hệ thống Win NT. Nhưng user bạn lấy được không có quyền tương đương như nhóm Administrators mà thuộc nhóm có quyền thấp hơn. Như vậy ta không có quyền làm nhiều thao tác như Admin. Vậy điều ta phải làm là leo thang đặc quyền để có được quyền như Admin. Có rất nhiều cong cụ thể thực hiện điều này : Get

admin, Sechole, ntuser ...

Global: Tiện ích dòng lệnh này sẽ hiển thị các thành viên của Global Group trên server hay domain được chỉ định.
Cú pháp : C:>global "Domain Users" domain1

Gaining Access: Là dựa vào những thông tin đã nắm được ở bước Enumeration mà hacker tấn công vào lỗi tràn bộ đệm, lấy và giả mã file password, hay thô thiển nhất là brute force (kiểm tra tất cả các trường hợp) password. Các tool thường được sử dụng ở bước này là NAT, podium, hoặc Lopht

HTTP: Là chữ viết tắt của "Hyper-Text Transfer Protocol". Đây là giao thức được sử dụng trên Internet

HTML: Là chữ viết tắt của "Hyper Text Markup Language", tức là ngôn ngữ siêu văn bản. Đây là một ngôn ngữ dùng để tạo trang web, chứa các trang văn bản và những tag (th&#7867 định dạng báo cho web browser biết làm thế nào thông dịch và thể hiện trang web trên màn hình.

Web page là trang văn bản thô (text only), nhưng về mặt ngữ nghĩa gồm 2 nội dung:
- Đoạn văn bản cụ thể.
- Các tag (trường văn bản được viết theo qui định) miêu tả một hành vi nào đó, thường là một mối liên kết (hyperlink) đến trang web khác

IP: Là chữ viết tắt của "Internet Protocal". Mỗi máy khi kết nối vào Internet đều có 1 địa chỉ duy nhất, đó là địa chỉ IP. Địa chỉ này dùng để phân biệt máy tính đó với các máy khác còn lại trên mạng Internet. Địa chỉ IP chia làm 2 loại : IP động & IP tĩnh. Thường các bạn kết nối bằng PC cá nhân là IP động, còn IP của những server cung cấp Hosting/Domain có IP tĩnh. Địa chỉ IP là một số 32 bit, = 4 byte nên có thể xem một địa chỉ IP được tạo thành từ 4 số có kích thước 1 byte, mỗi số có giá trị từ 0 đến 255. Mỗi địa chỉ IP đều gồm 2 phần là địa chỉ mạng (network) và địa chỉ máy (host). Để xem IP của máy tính mình, bạn vào Start -- > Run rồi gõ : winipcfg
Để xem IP của một trang Web thì bạn dùng lệnh nslookup

ICMP: Là chữ viết tắt của "Internet Control Message Protocol". Đây là giao thức xử lý các thông báo trạng thái cho IP. ICMP được dùng để thông báo các lỗi xảy ra trong quá trình truyền đi của các gói dữ liệu trên mạng. ICMP thuộc tầng vận huyển - Transpoort Layer

IIS: Là chữ viết tắt của "Internet Information Server". Đây là một chương trình WebServer nổi tiếng của Microsoft và đã từng bị một lỗi bảo mật rất lớn

IPC: Là chữ viết tắt của "Inter-Process Communication". Được dùng trong việc chia sẻ dữ liệu giữa các ứng dụng và máy tính trên mạng (NT/2K). Khi một máy

được khởi động và log vào mạng, hdh sẽ tạo 1 chia sẻ ngầm định tên là IPC$. Nó sẽ giúp cho các máy khác có thể nhìn thấy và kết nối đến các chia sẻ trên máy này

Info: Là chữ viết tắt của "Information", tức là thông tin

LAN: Là chữ viết tắt của "Local Area Network". Một hệ thống các máy tính và thiết bị ngoại vi được liên kết với nhau. Người sử dụng mạng nội bộ có thể chia sẻ dữ liệu trên đĩa cứng, trong mạng và chia sẻ máy in

Login: Đăng nhập, liên kết

Log: Là thao tác ghi nhận lại quá trình sử dụng dịch vụ của bạn. Khi xâm nhập 1 máy tính hay server thì việc xoá log là không thể thiếu. Bởi vì, nếu không xoá log thì từ đó người ta có thể tìm ra IP thật của bạn

Local: Giống như Global nhưng nó hiển thị các thành viên của Local Group. Chẳng hạn như bạn muốn truy vấn danh sách Administrator Group.

mIRC: Là chương trình chat (client: dành cho người sử dụng chat) đươc anh chàng Khaled Mardam-Bey khởi đầu, mIRC chỉ chuyên dụng cho Windows thôi, nó được viết bằng VC++ , tuy nhiên vẫn có chương trình chat xài cho Macintosh, linux như: X-Chat ..., có thể nói mIRC là phần mềm chat đầu tiên (hình như vào năm 1989), sau đó là các sản phẩm khác của Yahoo, AOL (ICQ,AIM)

MAC: Là chữ viết tắt của "Media Access Control"

NAV: Là chữ viết tắt của tên chương trình "Norton Anti-Virus" của hãng Symantec. Đây là chương trình quét Virus rất nổi tiếng và phổ biến

Nuke: Là một trong những kỹ thuật khá lợi hại. Nếu như bạn biết được IP của 1 máy tính bất kỳ đang kết nối thì nuke hoàn toàn có thể làm cho máy tính đó disconnect, cho dù đó là của cả 1 mạng LAN

OS: Là chữ viết tắt của "Operation System". Tức là hệ điều hành

OSI: Là chữ viết tắt của "Open System Interconnection".

OWA: Là chữ viết tắt của "Outlock Web Access". Đây là Module của Microsoft Exchanger Server (một Server phục vụ Mail), nó cho phép người dùng truy cập và quản trị Mailbox của họ từ xa thông qua Web Browser

Ping: Là chương trình cho phép bạn xác định một host còn hoạt động (alive) hay không ? rất hữu ích cho việc chẩn đoán mạng

Port: Cổng

Packet: Gói dữ liệu

PPP :Là chữ viết tắt của "Point-to-Point". Đây là 1 giao thức kết nối Internet tin cậy thông qua Modem

POP3: Là chữ viết tắt của "Post Office Protocol Version 3". POP3 daemon thường được chạy ở cổng 110 (đây là cổng chuẩn của nó). Dùng để check mail, bạn phải kết nối đến server đang chạy POP3 daemon ở cổng 110 trong Outlook Express hoặc Outlook

Port surfing: Là kết nối đến các cổng của một máy chủ để thu thập các thông tin, chẳng hạn như thời gian, hệ điều hành, các dịch vụ đang chạy

PKC: Là chữ viết tắt của "Public key cryptos". Có nghĩa là hệ thống mật mã sử dụng từ khóa chung

PHP: Là chữ viết tắt của "PHP Hypertext Preprocessor", tạm dịch là ngôn ngữ tiền xử lý các siêu văn bản. Các mã lệnh PHP được nhúng vào các trang web, các trang này thường có phần mở rộng là .php, .php3, .php4. Khi client gởi yêu cầu "cần tải các trang này về" đến web server, đầu tiên web server sẽ phân tích và thi hành các mã lệnh PHP được nhúng trong, sau đó trả về một trang web kết quả đã được xử lí cho client. PHP là một ngôn ngữ rất dễ dùng, dễ học và cực kì đơn giản hơn nhiều so với các ngôn ngữ khác như C, Perl. PHP hiện nay rất phổ biến tuy nhiên PHP scripts chẳng an toàn chút nào, các Hacker có thể lợi dụng khe hở này để attack các servers

PUB: 1 PUB thông thường có chứa các file để cho mọi người dowload, 1 số PUB có thể cho upload. Tuy nhiên, 1 PUB có thể không chỉ chứa các file dùng cho việc download, mà có thể chứa cả 1 "trang web".

RFC: Là chữ viết tắt của "Request For Comment", là tập hợp những tài liệu về kiến nghị, đề xuất và những lời bình luận liên quan trực tiếp hoặc gián tiếp đến công nghệ, nghi thức mạng INTERNET. Các tài liệu RFC được chỉnh sửa, thay đổi đến khi tất cả các kỹ sư thành viên của IETF (Internet Engineering Task Force) đồng ý và duyệt, sau đó những tài liệu này được xuất bản và được công nhận là 1 chuẩn, nghi thức cho Internet. Tài liệu RFC nổi tiếng và làm tạo được tiếng vang lớn nhất là tài liệu RFC số 822 về Internet Email bởi Dave Crocker.

Race Conditions: là một trong những cuộc tấn công phổ biến trên các hệ thống Unix/Linux

Race Conditions xảy ra khi một chương trình hoặc quy trình xử lý nào đó thực hiện một sự kiểm tra. Giữa thời gian mà một sự kiểm tra được làm và hoạt động được thực hiện, kết quả của cuộc kiểm tra đó có thể sẽ phản chiếu trạng thái của hệ thống. Hacker sẽ lợi dụng chương trình hoặc quy trình này trong lúc nó

thực hiện đặc quyền

Remote Access: Truy cập từ xa qua mạng

Shell: Là chương trình giữa bạn và Linux (hay nói chính xác hơn là giữa bạn với nhân Linux). Mỗi lệnh bạn gõ ra sẽ được Shell diễn dịch rồi chuyển tới nhân Linux. Nói một cách dễ hiểu Shell là bộ diễn dịch ngôn ngữ lệnh, ngoài ra nó còn tận dụng triệt để các trình tiện ích và chương trình ứng dụng có trên hệ thống…

SYN: Là chữ viết tắt của "The Synchronous Idle Character" nghĩa là ký tự đồng bộ hoá. Đầu tiên, A sẽ gửi cho B yêu cầu kết nối và chờ cho B trả lời. Sau khi B nhận được yêu cầu này sẽ trả lời lại A là "đã nhận được yêu cầu từ A" (ACK) và "đề nghị trả lời lại để hoàn thành kết nối" (SYN). Đến lúc này, nếu A trả lời lại "đồng ý" (SYN) thì kết nối sẽ được tạo

SQL Injection: Là một trong những kiểu hack web đang dần trở nên phổ biến hiện nay. Bằng cách inject các mã SQL query/command vào input trước khi chuyển cho ứng dụng web xử lí, bạn có thể login mà không cần username và password, remote execution, dump data và lấy root của SQL server. Công cụ dùng để tấn công là một trình duyệt web bất kì, chẳng hạn như Internet Explorer, Netscape, Lynx

Source Code: Mã nguồn (của 1 file hay 1 chương trình nào đó)

SUID: Là chữ viết tắt của "Set User ID on execution".

SGID: Là chữ viết tắt của "Set Group ID on execution", tức là đặt thuộc tính thừa kế groupid cho một thư mục nào đó

Sniffer: Là chương trình cho phép bạn chộp tất cả các gói dữ liệu đang chuyển card mạng của máy bạn. Các dữ liệu đó có thể là tên người dùng, mật khẩu, một số thông tin quan trọng khác

SSI: Là chữ viết tắt của "Server Side Includes". Đây là các chỉ dẫn được đặt trong các file html. Server sẽ chịu trách nhiệm phân tích các chỉ dẫn này và sẽ chuyển kết quả cho client

Server: Máy chủ chứa tài liệu

Serial Direct Cable Connection: Là công nghệ kết nối máy tính bằng Cable truyền nhận dữ liệu

SMB: Là chữ viết tắt của "Server Message Block". Đây là một trong những protocols phổ biến cho PC, cho phép bạn dùng những share files, disks, directory, printers và trong vài hướng cả cổng COM