Author: Hieupc
Title: Những thuật ngữ chuyên ngành Security
Publisher: TheGioiEbook.Com

Các bạn có thể tìm thấy trong bài viết này các thuật ngữ thông dụng nhất về lĩnh vực tin học, bao gồm hệ thống, giao thức, bảo mật, lập trình...

FTP

Là từ viết tắt của "File Transfer Protocol". Đây là giao thức truyền file trên mạng dựa theo chuẩn TCP, thường dùng để để upload file lên Host, Server với cổng mặc định là 21

Cú pháp : ftp

Cú Pháp : ping www.tentrangweb.com hoặc ping diachiIP -t (vd: ping 203.162.0.11 -t)

Traceroute

Là chương trình cho phép bạn xác định được đường đi của các gói tin (packet) từ máy bạn đến hệ thống đích trên mạng Internet.

Cú pháp : tracert IPhost

Ví dụ : tracert 203.162.0.11

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 chuyển (Transport Layer).

Telnet

Là một chương trình terminal đầu cuối. Nó thường dùng để đăng nhập vào một máy chủ nào đó trên các daemon khác nhau của máy chủ đó. Bạn có thể thu thập một số thông tin về máy chủ qua telnet. Bạn cũng có thể check mail, gởi mail và đặc biệt là có thể tham gia vào các kênh chat IRC của nước ngoài.

Cú pháp : telnet RFC

Là từ viết tắt của "Request For Comment". Đây 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 một chuẩn, nghi thức cho Internet.

DNS

Là từ viết tắt của "Domain Name System" (Hệ thống tên miền). Một máy chủ DNS đợi kết nối ở cổng số 53, có nghĩa là nếu bạn muốn kết nối vào máy chủ đó, bạn phải kết nối đến cổng số 53. Máy chủ chạy DNS chuyển hostname bằng các chữ cái thành các chữ số tương ứng và ngược lại.

Ví dụ : 127.0.0.1 --> localhost và localhost--->127.0.0.1 (127.0.0.1 là địa chỉ của chính máy bạn đang dùng, hay còn gọi là địa chỉ "loopback")

SMTP

Là từ viết tắt của "Simple Message Transfer Protocol". Giao thức SMTP dùng để gửi thư thông qua một chương trình Sendmail (Sendmail Deamon), tuy phổ biến nhưng kém an toàn.

CGI

Là từ viết tắt của "Common Gateway Interface" (Giao diện cổng chung), cho phép khởi tạo 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 chung, 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

Shell

Là chương trình giữa người dùng với nhân Linux. Mỗi lệnh được đưa 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.

NetBios

Là một giao thức, công nghệ nối mạng của Windows 9.x. Nó được thiết kế trong môi trường mạng LAN để chia sẻ tài nguyên (như dùng chung các File, Folder, máy in và nhiều tài nguyên khác...). Mô hình này rất giống mô hình mạng ngang hàng 2P. Thông thường một mạng dùng giao thức Netbios thường là Netbios Datagram Service (Port 138), Netbios Session Service (Port 139) hoặc cả hai.

SYN

Là từ viết tắt của "The Synchronous Idle Character" (tạm dịch: Ký tự đồng bộ hoá). Quá trình thực hiện SYN sẽ diễn ra như sau:

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 khởi tạo.

Cookies

Là những phần dữ liệu nhỏ có cấu trúc được chia sẻ giữa website và trình duyệt của người dùng đã được mã hoá bởi website đó. Cookies được lưu trữ dưới những file dữ liệu nhỏ dạng text (có dung lượng 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...

LAN

Là từ 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 cục bộ có thể chia sẻ dữ liệu trên đĩa cứng, trong mạng và chia sẻ máy in.

Vulnerability

Là một vùng, điểm dễ bị tổn thương trong hệ thống theo một yêu cầu được phát hiện ra, một đặc điểm hay một tiêu chuẩn, hay một vùng không được bảo vệ trong toàn bộ cấu trúc bảo mật của hệ thống mà để lại cho hệ thống các điểm dễ bị tấn công hoặc chịu ảnh hưởng các vấn đề khác. Các hacker thường khai thác (exploit) vulnerability để tấn công vào hệ thống.

Anonymous

Ẩn danh, nặc danh

IIS

Là chữ viết tắt của "Internet Information Server". Đây là một chương trình WebServer nổi tiếng của Microsoft.

Account

Tài khoản là sự kết hợp của hai yếu tố username (tên người dùng) và password (mật khẩu) do một dịch vụ nào đó đã cung cấp cho bạn khi bạn đã đăng ký với họ để bảo mật cho bạn.

Source Code

Mã nguồn (của của file hay một chương trình nào đó)

Port: Cổng

Compile: Biên dịch

Login: Đăng nhập

Database: Cơ sở dữ liệu

ISP: Là chữ viết tắt của "Internet Service Provider" (Nhà cung cấp dịch vụ Internet).

TCP/IP: Là chữ viết tắt của "Transmission Control Protocol and Internet Protocol". Gói tin TCP/IP là một khối dữ liệu đã được nén, sau đó kèm thêm một header và gửi đến một máy tính khác. Phần header trong một gói tin chứa địa chỉ IP của người gửi gói tin.

Whois

Là một chương trình rất hữu ích, giúp bạn tìm ra những thông tin về hosts, networks và administrator của trang web đó là ai (Địa chỉ, Email, IP..)

Security: Bảo mật

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.

UDP: Là chữ viết tắt của "User Datagram Protocol". Có nhiệm vụ giống như TCP, nhưng nó không đảm bảo sự chính xác của thông tin được chuyển tải. UDP chỉ đơn giản là những gói tin có điểm xuất phát và điểm đích xác định

Domain: Là tên miền của một website nào đó
Ví dụ : http://www.microsoft.com

OS: Là chữ viết tắt của "Operation System" - Hệ điều hành

IRC: Là chữ viết tắt của "Internet Relay Chat". Đây là một chương trình độc lập nơi mà bạn có thể tham gia vào các kênh chat.

mIRC: Là chương trình chat client, đựơc Khaled Mardam-Bey viết. Có thể nói mIRC là phần mềm chat đầu tiên rồi sau đó một loạt các sản phẩm khác của Yahoo, AOL (ICQ, AIM) ... mới ra đời.

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 một 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

Encryption: Mã hoá

Decryption: Giải mã

Remote Access: Truy cập từ xa qua mạng

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

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

ActiveX: Là một hệ thống tiêu chuẩn dùng để xây dựng các thành phần (component) trong môi trường Windows. Các thành phần này không những có khả năng vận hành một cách độc lập mà còn có thể được khai thác bởi các thành phần khác. Đây là những thành phần được viết bằng nhiều ngôn ngữ khác nhau và rất đa dạng, có thể là các ActiveX Control (điều khiển độc lập) để nhúng vào chương trình khác từ lúc thiết kế chương trình, có thể là các ActiveX DLL (thư viện liên kết động) mà các chương trình khác tham chiếu đến.

Packet: Gói dữ liệu

Server: Máy chủ

Client: Máy con, dùng để kết nối với máy chủ (Server)

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

Firewall: Là bức tường lửa

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

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

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)

Pwdump: Là chữ viết tắt của "Password Dumper". Đây là một công cụ tuyệt vời không thể thiếu được khi Hack vào hệ thống WinNT

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

OSI: Là chữ viết tắt của "Open System Interconnection", hay còn gọi là mô hình chuẩn OSI. Vậy mô hình OSI là gì?

Thực ra trong quá khứ, việc truyền thông giữa các máy tính từ các nhà cung cấp khác nhau rất khó khăn, bởi lẽ chúng sử dụng các giao thức và định dạng dữ liệu khác nhau. Do vậy Tổ chức tiêu chuẩn hóa quốc tế (ISO) đã phát triển một kiến trúc truyền thông được biết đến như là mô hình Kết nối lẫn nhau qua hệ thống mở - Open System Interconnection (OSI) một mô hình định nghĩa các tiêu chuẩn liên kết các máy tính từ các nhà cung cấp khác nhau.

ACK: Là chữ viết tắt của "Acknowledgement"

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

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 bộ định tuyến trong hệ tự quản khác

DHCP: Là chữ viết tắt của "Dynamic Host Configuration Protocol". Đây là một giao thức mà máy sử dụng để lấy dược tất cả thông tin cấu hình cần thiết, bao gồm cả địa chỉ IP

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

URL: Là chữ viết tắt của "Uniform Resource Locator", dùng để chỉ tài nguyên trên Internet. Sức mạnh của web là khả năng tạo ra những liên kết siêu văn bản đến các thông tin liên quan. Những thông tin này có thì là những trang web khác, những hình ảnh, âm thanh... Những liên kết này thường được biểu diễn bằng những chữ màu xanh có gạch dưới được gọi là anchor. Các URL có thể được truy xuất thông qua một trình duyệt (Browser) như IE hay Netscape

WWW: Là chữ viết tắt của "World Wide Web"

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 (thẻ) 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

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

CPU: Là chữ viết tắt của "Central Processing Unit". Đây là tập hợp nhiều mạch điện dùng để điều khiển mọi hoạt động chính của máy

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

TFTP: Là chữ viết tắt của "Trial File Transfer Protocol". TFTP chạy trên cổng 69 và dùng giao thức UDP nên rất không an toàn

RIP: Là chữ viết tắt của "Routing Information Protocol", chạy trên cổng 512

HyperTerminal: Là chương trình cho phép bạn mở một server trên bất kỳ port nào của máy tính , và cho phép lắng nghe những thông tin đầu vào từ những máy tính xác định.

Bạn muốn thiết lập nó hãy vào : Start>Programs>Accessories>Communications
Rồi chọn HyperTerminal

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

WU-FTP: Là chữ viết tắt của "Washington University - File Transfer Protocol". Đây là một phần mềm Server phục vụ FTP được dùng khá phổ biến trên các hệt thống Unix & Linux. Chương trình này từng bị một lỗi khá nghiêm trọng, đó là sự thi hành của file globbing trên Server chứa tính dễ tổn thương cho phép các hacker thi hành các code lệnh trên server từ xa (tất nhiên là code có hại rồi). dẫn đến việc ghi đè các file lên servervà cuối cùng dẫn đến crash hệ thống"

NIS: Là chữ viết tắt của "Network Information Server".

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

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

Local: Giống như Global nhưng nó hiển thị các thành viên của Local Group. Chẳng hạn như ta muốn truy vấn danh sách Administrator Group.
Cú pháp : C:>local "administrators" domain1

SOCKS: SOCKS được tạo ra bởi chữ SOCKetS và được phán triển chủ yếu bởI NEC, cũng như được ITEF đưa thành một chuẩn của Internet, được định nghĩ trong RFC (Request for comment). Nhiệm vụ của SOCKS là cầu nối trung gian giữa một đầu của SOCKS server đến đầu kia của SOCKS server:

CLIENT --------> IN - SOCKS SERVER - OUT ----------> SERVER

SOCK được dùng chủ yếu trong công nghệ Proxy server và Firewall. Hiện nay có version

SOCKS4 và SOCKS5. Socks 5 là bản phát triển sau nên có thêm tính năng để authorize, và có thể sử dụng UDP (SOCKS 4 chỉ có TCP).

SQL Injection: Từng là một kiểu tấn công vào trang web phổ biến. Bằng cách chèn các mã SQL query/command vào input trước khi chuyển cho ứng dụng web xử lí, kẻ tấn công có thể đăng nhập 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, có thể dùng Internet Explorer, Netscape, Lynx, ...

DoS: Là chữ viết tắt của "Denial of Service" (Tấn công từ chối dịch vụ). Đây là phương pháp thường được hacker sử dụng để tấn công một trang web khi các phương pháp tấn công khác tỏ ra không có hiệu quả. Đặc điểm của DoS là làm hao tổn một số lượng tài nguyên trên máy chủ, chiếm dụng băng thông, bộ nhớ, CPU, đĩa cứng... làm cho máy chủ không thể đáp ứng được các yêu cầu gửi tới. Kết quả cuối cùng sẽ làm cho máy chủ tê liệt hoặc phải khởi động lại.

Exploit: Khai thác (một lỗi nào đó)

Fake IP: IP giả mạo

Crack Password: Bẻ khoá mật khẩu

Debug: Là chương trình đi kèm với DOS. Đây là một công cụ tuyệt vời để gỡ rối chương trình, crack phần mềm, đọc bộ nhớ bị che giấu như boot sector và nhiều hơn nữa... Để debug được chương trình, bạn cần phải có kiến thức về Assembly.

TCP Port Scanning: Là dạng cơ bản nhất của các chương trình Scanner. Loại chương trình này sẽ thử mở một kết nối TCP đến một Port nào đó để xác định trạng thái của Port này

Web spoofing: Là một dạng tấn công cho phép một người nào đó xem và chỉnh sửa mọi trang web gửi đến máy nạn nhân. Họ có thể theo dõi mọi thông tin do nạn nhân điền vào các form. Điều này đặc biệt nguy hiểm với những thông tin cá nhân như địa chỉ, số thẻ tín dụng, số tài khoản ngân hàng, mật mã truy cập vào tài khoản đó…. Web spoofing hoạt động trên cả IE lẫn Netscape. Nó hoạt động dựa vào việc giao thức SSL được dùng như một dạng giấy chứng nhận cho những Website xác thực. Việc tấn công theo kiểu này có thể được thi hành bằng cách dùng Javascript và Web server plug-ins

Footprinting: Phương thức "In dấu chân" là thu thập tất cả những thông tin quan trọng về mục tiêu của bạn như: Email, IP, Domain... Đây bước cơ bản đầu tiên của hacker trước khi hack vào một hệ thống nào đó.

XSS: Là chữ viết tắt của "Cross site scripting". Đây là thuật ngữ nói đến việc website sử dụng cách nào đó để ăn cắp thông tin của người dùng (ví dụ như cookie chẳng hạn). Hacker sẽ dụ nạn nhân đến trang web của mình bằng cách đưa một siêu liên kết (hyperlink) hấp dẫn. Dĩ nhiên những hacker giỏi thường mã hóa cả hyperlink của mình để giảm thiểu sự nghi ngờ. Sau khi dữ liệu của nạn nhân bị đánh cắp, nó sẽ gửi đến cho hacker và đưa ra một trang web có nội dung phù hợp với hyperlink giả

Race Conditions: Race Conditions (tình trạng tranh đua) 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

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

Nuke: Là một trong những kỹ thuật khá lợi hại. Nếu như bạn biết được IP của một 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 một mạng LAN

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, ...

Log: Là thao tác ghi nhận lại quá trình sử dụng dịch vụ của bạn. Khi xâm nhập một 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

Trojan: Là một chương trình bất hợp pháp được chứa bên trong một chương trình hợp pháp. Chương trình không hợp pháp này thực hiện những hàm bí mật mà người dùng không biết hay không cần đến. Trojan có nhiều loại nhưng vẫn chủ yếu là 2 loại chính :

+ Trojan lấy password rồi gửi password lấy được qua email (vd : Kuang2, Hooker, barok...)

+ Trojan dùng để điều khiển từ xa (vd : Sub Seven 7, Back Orifice 2000...)

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,...

Finger: Là một chương trình rất hữu ích, giúp bạn thu thập rất nhiều thông tin về users (thường bị disable)

Nmap: Là chữ viết tắt của "Network exploration tool and security scanner" . Đây là chương trình quét hàng đầu với tốc độ cực nhanh và cực mạnh. Nó có thể quét trên mạng diện rộng và đặc biệt tốt đối với mạng đơn lẻ. NMAP giúp bạn xem những dịch vụ nào đang chạy trên server (services/ports:webserver,ftpserver,pop3,...), server đang dùng hệ điều hành gì, loại tường lửa mà server sử dụng, ... và rất nhiều tính năng khác. Nói chung NMAP hỗ trợ hầu hết các kỹ thuật quét như : ICMP (ping aweep), IP protocol, Null scan, TCP SYN (half open), ... NMAP được đánh giá là công cụ hàng đầu của các Hacker cũng như các nhà quản trị mạng trên thế giới.

Netcat: Là một công cụ không thể thiếu đối với hacker khi muốn tấn công vào các website, server. Chương trình này đọc và ghi dữ liệu qua mạng thông qua giao thức TCP hoặc UDP. Kẻ tấn công có thể dùng Netcat một cách trực tiếp hoặc sử dụng chương trình, script khác để điều khiển Netcat. Netcat được coi như một exploitation tool do nó có thể tạo được liên kết giữa kẻ tấn công và server cho việc đọc và ghi dữ liệu.

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 hacker chiếm được quyền và đăng nhập vào hệ thống Win NT. Nhưng user hacker lấy được không có quyền tương đương như nhóm Administrators mà thuộc nhóm có quyền thấp hơn. Như vậy hacker không có quyền làm nhiều thao tác như Admin. Do vậy, hacker phải thực hiện biện pháp "Get Admin" để đoạt quyền cao hơn nhằm kiểm soát hệ thống.

Netwatch: Là công cụ hiển thị các tài nguyên dùng chung trên hệ thống mạng mà bạn muốn hack

Usestat: Tiện ích dòng lệnh này có thể hiển thị User, Full name, ngày tháng và thời gian đăng nhập cho mỗi người dùng trên mỗi doamin đã chỉ định.

FootPrinting: Là cách mà hacker làm khi muốn lấy một lượng thông tin tối đa về máy chủ/doanh nghiệp/người dùng. Nó bao gồm chi tiết về địa chỉ IP, Whois, DNS ..v.v đại khái là những thông tin chính thức có liên quan đến mục tiêu. Nhiều khi đơn giản hacker chỉ cần sử dụng các công cụ

tìm kiếm trên mạng để tìm những thông tin đó

Enumeration: Là tìm kiếm những tài nguyên được 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. Rât nhiều người quản trị mạng không biết đến hoặc không sửa đổi lại các giá trị này

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

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 họ xâm nhập được vào mạng với tài khoản Guest. "The John and Riper" là hai chương trình crack password rất hay được sử dụng

Pilfering: Là hacker sử dụng các máy tìm kiếm lại được sử dụng để tìm các phương pháp truy cập vào mạng. Những file text chứa password hay các cơ chế không an toàn khác có thể là mồi ngon cho hacker.

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

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 lí 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: Một PUB thông thường có chứa các file để cho mọi người dowload, một số PUB có thể cho upload. Tuy nhiên, một PUB có thể không chỉ chứa các file dùng cho việc download, mà có thể chứa cả một "TRANG WEB".

Local Exploit: Là khai thác cục bộ. Đây là một trong những phương pháp tấn công cao cấp của hacker (ST)