Những hiểu biết cơ bản nhất để trở thành Hacker - Phần 1 [10/11/2004 3:02:00 PM]

Nhiều bạn Newbie có hỏi tôi " Hack là như thế nào ? Làm sao để hack ?" Nhưng các bạn đã quên mất một điều là các bạn cần phảI có kiến thức một cách tổng quát , hiểu các thuật ngữ mà những người rành về mạng hay sử dụng . Riêng tôi thì chưa thật giỏi bao nhiêu nhưng qua nghiên cứu tôi cũng đã tổng hợp được một số kiến thức cơ bản , muốn chia sẻ cho tất cả các bạn , nhằm cùng các bạn học hỏi .

Tôi sẽ không chịu trách nhiệm nếu các bạn dùng nó để quậy phá người khác . Các bạn có thể copy hoặc post trong các trang Web khác nhưng hãy điền tiên tác giả ở dưới bài , tôn trọng bài viết này cũng chính là tôn trọng tôi và công sức của tôi , đồng thời cũng tôn trọng chính bản thân các bạn . Trong này tôi cũng có chèn thêm một số cách hack , crack và ví dụ căn bản , các bạn có thể ứng dụng thử và nghiên cứu đọc nó để hiểu thêm , rồi khi bắt gặp một từ mà các bạn không hiểu thì hãy đọc bài này để biết , trong này tôi có sử dụng một số ý của bài viết mà tôi thấy rất hay từ trang Web của HVA , và các trang Web khác mà tôi đã từng ghé thăm . Xin cảm ơn những tác giả đã viết những bài ấy . Bây giờ là vấn đề chính .

1 .) Ta cần những gì để bắt đầu?

Có thể nhiều bạn không đồng ý với tôi nhưng cách tốt nhất để thực tập là các bạn hãy dùng HĐH Window 9X , rồI đến các cái khác mạnh hơn đó là Linux hoặc Unix , dướI đây là những cái bạn cần có :
+ Một cái OS (có thể là DOS , Window 9X , Linux , Unit ….)
+ Một cái trang Web tốt (HVA chẳng hạn hi`hi` greenbiggrin.gif greenbiggrin.gif)
+ Một bộ trình duyệt mạng tốt (là Nescape , IE , nhưng tốt nhất có lẽ là Gozzila)
+ Một công cụ chat tốt (mIRC ,Yahoo Mass …..)
+ Telnet (hoặc những cái tương tự như nmap …)
+ Cái quan trọng nhất mà bất cứ ai muốn trở thành một hacker là đều phảI có một chút kiến thức về lập trình (C , C++ , Visual Basic , Pert …..)

2 .) Thế nào là một địa chỉ IP ?

_ Địa chỉ IP được chia thành 4 số giới hạn từ 0 - 255. Mỗi số được lưu bởi 1 byte - > ! P có kicks thước là 4byte, được chia thành các lớp địa chỉ. Có 3 lớp là A, B, và C. Nếu ở lớp A, ta sẽ có thể có 16 triệu địa chỉ, ở lớp B có 65536 địa chỉ. Ví dụ: Ở lớp B với 132.25,chúng ta có tất cả các địa chỉ từ 132.25.0.0 đến 132.25.255.255. Phần lớn các địa chỉ ở lớp A llà sở hữu của các công ty hay của tổ chức. Một ISP thường sở hữu một vài địa chỉ lớp B hoặc C. Ví dụ: Nếu địa chỉ IP của bạn là 132.25.23.24 thì bạn có thể xác định ISP của bạn là ai. (có IP là 132.25.x.)
_ IP là từ viết tắt của Internet Protocol, trên Internet thì địa chỉ IP của mỗI người là duy nhất và nó sẽ đạI diện cho chính ngườI đó, địa chỉ IP được sử dụng bởi các máy tính khác nhau để nhận biết các máy tính kết nối giữa chúng. Đây là lí do tại sao bạn lại bị IRC cấm, và là cách người ta tìm ra IP của bạn.

Địa chỉ IP có thể dễ dàng phát hiện ra, người ta có thể lấy được qua các cách sau :
+ bạn lướt qua một trang web, IP của bạn bị ghi lại
+ trên IRC, bất kì ai cũng có thể có IP của bạn
+ trên ICQ, mọi người có thể biết IP của bạn, thậm chí bạn chọn ``do not show ip`` người ta vẫn lấy được nó
+ nếu bạn kết nối với một ai đó, họ có thế gõ ``systat –n ``, và biết được ai đang kết nối đên họ
+ nếu ai đó gửi cho bạn một email với một đoạn mã java tóm IP, họ cũng có thể tóm được IP của bạn
(Tài liệu của HVA)

3 .) Làm thế nào để biết được địa chỉ IP của mình ?

_ Run đánh lệnh “winipcfg” .\ Trong Window : vào Start
_ Trong mIRC : kết nốI đến máy chủ sau đó đánh lệnh “/dns ”
_ Thông qua một số trang Web có hiển thị IP .

4 .) IP Spoofing là gì ?

_ Một số IP có mục đích để xác định một thiết bị duy nhất trên thế giới. Vì vậy trên mạng một máy chủ có thể cho phép một thiết bị khác trao đổi dữ liệu qua lại mà không cần kiểm tra máy chủ.
Tuy nhiên có thể thay đổi IP của bạn, nghĩa là bạn có thể gởi một thông tin giả đến một máy khác mà máy đó sẽ tin rằng thông tin nhận được xuất phát từ một máy nào đó (tất nhiên là không phải máy của bạn). Bạn có thể vượt qua máy chủ mà không cần phải có quyền điều khiển máy chủ đó. Điều trở ngại là ở chỗ những thông tin phản hồi từ máy chủ sẽ được gởi đến thiết bị có IP mà chúng ta đã giả mạo. Vì vậy có thể bạn sẽ không có được sự phản hồi những thông tin mà mình mong muốn. Có lẽ điều duy nhất mà spoof IP có hiệu quả là khi bạn cần vượt qua firewall, trộm account và cần dấu thông tin cá nhân!
(Tài liệu của HVA)

5 .) Trojan / worm / virus / logicbomb là cái gì ?

_ Trojan : Nói cho dễ hiểu thì đây là chương trình điệp viên được cài vào máy của ngườI khác để ăn cắp nhũng tài liệu trên máy đó gửI về cho chủ nhân của nó , Cái mà nó ăn cắp có thể là mật khẩu , accourt , hay cookie ……. tuỳ theo ý muốn của ngườI cài nó .
_ virus : Nói cho dễ hiểu thì đây là chương trình vớI những mã đặc biệt được cài (hoặc lây lan từ máy khác) lên máy của nạn nhân và thực hiện những yêu cầu của mã đó , đa số virut được sử dụng để phá hoạI dữ liệu hoặc phá hoạI máy tính .
_ worm : Đây là chương trình độc lập có thể tự nhân bản bản thân nó và lây lan khắp bên trong mạng .Cũng giống như Virut , nó cũng có thể phá hoạI dữ liệu , hoặc nó có thể phá hoạI bên trong mạng , nhiều khi còn làm down cả mang đó .
_ logicbomb : Là chương trình gửi một lúc nhiều gói dữ liệu cho cùng một địa chỉ , làm ngập lụt hệ thống , tắt nghẽn đường truyền (trên server) hoặc dùng làm công cụ để

“khủng bố” đối phương (bom Mail) ;) .

6 .) PGP là gì ?

_ PGP là viết tắt của từ “Pretty Good Privacy” , đây là công cụ sử dụng sự mã hoá chìa khoá công cộng để bảo vệ những hồ sơ Email và dữ liệu , là dạng mã hoá an toàn cao sử dụng phần mềm cho MS_DOS , Unix , VAX/VMS và cho những dạng khác .

7 .) Proxy là gì ?

_Proxy cung cấp cho người sử dụng truy xuất internet với những host đơn. Những proxy server phục vụ những nghi thức đặt biệt hoặc một tập những nghi thức thực thi trên dual_homed host hoặc basion host. Những chương trình client của người sử dung sẽ qua trung gian proxy server thay thế cho server thật sự mà người sử dụng cần giao tiếp. Proxy server xác định những yêu cầu từ client và quyết định đáp ứng hay không đáp ứng, nếu yêu cầu được đáp ứng, proxy server sẽ kết nối với server thật thay cho client và tiếp tục chuyển tiếp đến những yêu cầu từ clientđến server, cũng như đáp ứng những yêu cầu của server đến client. Vì vậy proxy server giống cầu nối trung gian giữa server và client .
_ Proxy cho user truy xuất dịch vụ trên internet theo nghĩa trực tiếp. Với dual host homed cần phải login vào host trước khi sử dụng dịch vụ nào trên internet. Điều này thường không tiện lợi, và một số người trể nên thất vọng khi họ có cảm giác thông qua firewall, với proxy nó giải quyết được vấn đề này. Tất nhiên nó còn có những giao thức mới nhưng nói chung nó cũng khá tiện lợi cho user. Bởi vì proxy cho phép user truy xuất những dịch vụ trên internet từ hệ thống cá nhân của họ, vì vậy nó không cho phép packet đi trực tiếp giữa hệ thống sử dụng và internet. đường đi là giáng tiếp thông qua dual homed host hoặc thông qua sự kết hợp giữa bastion host và screening rounter.

(Bài viết của Z3RON3 – tài liệu của HVA)

8 .) Unix là gì ?

_ Unix là một hệ điều hành (giống Window) .Nó hiện là hệ điều hành mạnh nhất , và thân thiết với các Hacker nhất . Nếu bạn đã trở thành một hacker thật sự thì HĐH này không thể thiếu đối với bạn . Nó được sử dụng hỗ trợ cho lập trình ngôn ngữ C .

9 .) Telnet là gì ?

_ Telnet là một chương trình cho phép ta kết nối đến máy khác thông qua cổng (port) . Mọi máy tính hoặc máy chủ (server) đều có cổng , sau đây là một số cổng thông dụng :
+ Port 21: FTP
+ Port 23: Telnet
+ Port 25: SMTP (Mail)
+ Port 37: Time

+ Port 43: Whois
_ Ví dụ : bạn có thể gọI Telnet để kết nốI đến mail.virgin.net trên port 25 .

10 .) Làm thế nào để biết mình đã Telnet đến hệ thống Unix ?

_ Ok , tôi sẽ nói cho bạn biết làm sao một hệ thống Unix có thể chào hỏI bạn khi bạn kết nối tới nó . Đầu tiên , khi bạn gọi Unix , thông thường nó sẽ xuất hiện một dấu nhắc : " Log in : " , (tuy nhiên , chỉ với như vậy thì cũng chưa chắc chắn đây là Unix được ngoạI trừ chúng xuất hiện thông báo ở trước chữ " log in :" như ví dụ : Welcome to SHUnix. Please log in ….)
Bây giờ ta đang ở tạI dấu nhắc "log in" , bạn cần phảI nhập vào một account hợp lệ . Một account thông thường gồm có 8 đặc tính hoặc hơn , sau khi bạn nhập account vào , bạn sẽ thấy có một mật khẩu , bạn hãy thử nhập Default Password thử theo bảng sau :

Account----------Default Password

Root---------- Root
Sys---------- Sys / System / Bin
Bin---------- -Sys / Bin
Mountfsy----------M ountfsys
Nuuc---------- Anon
Anon---------- Anon
User---------- -User
Games----------G ames
Install---------- --Install
Demo---------- Demo
Guest---------- Guest

11 .) shell account là cái gì ?

_ Một shell account cho phép bạn sử dụng máy tính ở nhà bạn như thiết bị đầu cuốI (terminal) mà vớI nó bạn có thể đánh lệnh đến một máy tính đang chạy Unix , "Shell" là chương trình có nhiệm vụ dịch những ký tự của bạn gửi đến rồI đưa vào thực hiện lệnh của chương trình Unix . VớI một shell account chính xác bạn có thể sử dụng được một trạm làm việc mạnh hơn nhiều so vớI cái mà bạn có thể tưởng tượng đến được .
Bạn có thể lấy được "shell account" miễn phí tạI trang Web http://www.freeshell.com/ tuy nhiên bạn sẽ không sử dụng được "telnet" cho đến khi bạn trả tiền cho nó .

12 .) Làm cách nào để bạn có thể crack Unix account passwords ?

_ Rất đơn giản , tuy nhiên cách mà tôi nói vớI các bạn ở đây "lạc hậu" rồI , các bạn có thể crack được chúng nếu các bạn may mắn , còn không thì các bạn đọc để tham khảo .

_ Đầu tiên bạn hãy đăng nhập vào hệ thống có sử dụng Unix như một khách hàng hoặc một ngườI khách ghé thăm , nếu may mắn bạn sẽ lấy được mật khẩu được cất dấu trong những hệ thống chuẩn như :

/etc/passwd

mỗi hàng trong một hồ sơ passwd có một tài khoản khác nhau , nó giống như hàng này :

userid:password:userid#:groupid#:GECOS field:home dir:shell

trong đó :
+ userid = the user id name : tên đăng nhập : có thể là một tên hoặc một số .
+ password : mật mã . Dùng để làm gì hẳn các bạn cũng biết rồI .
+ userid# : là một số duy nhất được thông báo cho ngườI đăng ký khi họ đăng ký mớI ở lần đầu tiên .
+ groupid# : tương tự như userid# , nhưng nó được dùng cho những ngườI đang ở trong nhóm nào đó (như nhóm Hunter Buq của HVA chẳng hạn)
+ GECOS FIELD : đây là nơi chứa thông tin cho ngườI sử dụng , trong đó có họ tên đầy đủ , số điện thoại , địa chỉ v.v…. . Đây cũng là nguồn tốt để ta dễ dàng crack một mật khẩu .
+ home dir : là thư mục ghi lạI hoạt động của người khách khi họ ghé thăm (giống như mục History trong IE vậy)
+ Shell : đây là tên của shell mà nó tự động bắt đầu khi ta login .
_ Hãy lấy file password , lấy file text đã mã hoá về , sau đó bạn dùng chương trình ``CrackerJack`` hoặc ``John the Ripper`` để crack .
_ Các bạn thấy cũng khá dễ phảI không ? Sai bét , không dễ dàng và may mắn để bạn có thể crack được vì hầu hết bây giờ họ cất rất kỹ , hãy đọc tiếp bạn sẽ thấy khó khăn chỗ nào .

13 .) shadowed password là cái gì ?

_ Một shadowed password được biết đến là trong file Unix passwd , khi bạn nhập một mật khẩu , thì ngườI khác chỉ thấy được trình đơn của nó (như ký hiệu " X " hoặc " * ") . Cái này thông báo cho bạn biết là file passwd đã được cất giữ ở nơi khác , nơi mà một ngườI sử dụng bình thường không thể đến được . Không lẽ ta đành bó tay , dĩ nhiên là đốI vớI một hacker thì không rùi , ta không đến được trực tiếp file shadowed password thì ta hãy tìm file sao lưu của nó , đó là file Unshadowed .
Những file này trên hệ thống của Unix không cố định , bạn hãy thử vớI lần lượt những đường dẫn sau :

CODE
AIX 3 /etc/security/passwd !
or /tcb/auth/files/ /
A/UX 3.0s /tcb/files/auth/?/ *
BSD4.3-Reno /etc/master.passwd *

ConvexOS 10 /etc/shadpw *
ConvexOS 11 /etc/shadow *
DG/UX /etc/tcb/aa/user/ *
EP/IX /etc/shadow x
HP-UX /.secure/etc/passwd *
IRIX 5 /etc/shadow x
Linux 1.1 /etc/shadow *
OSF/1 /etc/passwd[.dir|.pag] *
SCO Unix #.2.x /tcb/auth/files/ /
SunOS4.1+c2 /etc/security/passwd.adjunct =##username
SunOS 5.0 /etc/shadow
maps/tables/whatever >
System V Release 4.0 /etc/shadow x
System V Release 4.2 /etc/security/* database
Ultrix 4 /etc/auth[.dir|.pag] *
UNICOS /etc/udb =20

Trước dấu " / "đầu tiên của một hàng là tên của hệ thống tương ứng , hãy căn cứ vào hệ thông thật sự bạn muốn lấy rồI lần theo đường dẫn phía sau dấu "/"đầu tiên .
Và cuốI cùng là những account passwd mà tôi từng crack được , có thể bây giờ nó đã hết hiệu lực rồI :

CODE
arif:x:1569:1000:Nguyen Anh Chau:/udd/arif:/bin/ksh
arigo:x:1570:1000:Ryan Randolph:/udd/arigo:/bin/ksh
aristo:x:1573:1000:To Minh Phuong:/udd/aristo:/bin/ksh
armando:x:1577:1000:Armando Huis:/udd/armando:/bin/ksh
arn:x:1582:1000:Arn mett:/udd/arn:/bin/ksh
arne:x:1583:1000:Pham Quoc Tuan:/udd/arne:/bin/ksh
aroon:x:1585:1000:Aroon Thakral:/udd/aroon:/bin/ksh
arozine:x:1586:1000: Mogielnicki:/udd/arozine:/bin/bash
arranw:x:1588:1000:Arran Whitaker:/udd/arranw:/bin/ksh

Để bảo đảm sự bí mật nên pass của họ tôi xoá đi và để vào đó là ký hiệu " x " , các bạn hãy tìm hiểu thông tin có được từ chúng xem

Hết phần 1