```
               _ _        _____
              |_\/ |     / _____/
              |_||_|etal/ /hop
              _____/ /
             /_____/
```
                (314)432-0756
           24 Hours A Day, 300/1200 Baud

                 Presents....

                 ==Phrack Inc.==
         Volume One, Issue One, Phile 1 of 8

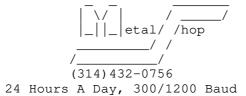   Introduction...

Welcome to the Phrack Inc. Philes. Basically, we are a group of phile writers
who have combined our philes and are distributing them in a group. This
newsletter-type project is home-based at Metal Shop. If you or your group are
interested in writing philes for Phrack Inc. you, your group, your BBS, or any
other credits will be included. These philes may include articles on telcom
(phreaking/hacking), anarchy (guns and death & destruction) or kracking. Other
topics will be allowed also to an certain extent. If you feel you have some
material that's original, please call and we'll include it in the next issue
possible. Also, you are welcomed to put up these philes on your BBS/AE/Catfur/
Etc. The philes will be regularly available on Metal Shop. If you wish to say
in the philes that your BBS will also be sponsering Phrack Inc., please leave
feedback to me, Taran King stating you'd like your BBS in the credits. Later
on.

                 TARAN KING
                 2600 CLUB!
              METAL SHOP SYSOP

This issue is Volume One, Issue One, released on November 17, 1985. Included
are:
1 This Introduction to Phrack Inc. by Taran King
2 SAM Security Article by Spitfire Hacker
3 Boot Tracing on Apple by Cheap Shades
4 The Fone Phreak's Revenge by Iron Soldier
5 MCI International Cards by Knight Lightning
6 How to Pick Master Locks by Gin Fizz and Ninja NYC
7 How to Make an Acetylene Bomb by The Clashmaster
8 School/College Computer Dial-Ups by Phantom Phreaker

Call Metal Shop and leave feedback saying the phile topic and where you got
these philes to get your article in Phrack Inc.

```
                     _ _        _____
                    |‾\/‾|    / ‾‾‾‾‾/
                    |_||_|etal/ /hop
                     _____/ /
                    /_____/
```
                    (314)432-0756
              24 Hours A Day, 300/1200 Baud

                      Presents...

                    ==Phrack Inc.==
            Volume One, Issue One, Phile 2 of 8

     ::>Hacking SAM - A Description Of The Dial-Up Security System<::
                   ::>Written by Spitfire Hacker<::

     SAM is a security system that is being used in many colleges
today as a security feature against intrusion from the outside. This
system utilizes a dial-back routine which is very effective. To
access the computer, you must first dial the port to which SAM is
hooked up. The port for one such college is located at (818) 885-
2082. After you have called, SAM will answer the phone, but will make
no other responses (no carrier signals). At this point, you must
punch in a valid Login Identification Number on a push-button phone.
The number is in this format -- xxyyyy -- where xx is, for the number
mentioned above, 70. 'yyyy' is the last 4 digits of the valid user's
telephone number.
     If a valid LIN is entered, SAM will give one of 3 responses:
1) A 1 second low tone
2) A 1 second alternating high/low tone
3) A tone burst

Responses 1 and 2 indicate that SAM has accepted your passcode and is
waiting for you to hang up. After you hang up, it will dial the valid
users phone number and wait for a second signal.

Response 3 indicates that all of the outgoing lines are busy.

If SAM accepts your passcode, you will have to tap into the valid
users line and intercept SAM when it calls. If you do this, then hit
the '*' key on your phone. SAM will respond with a standard carrier,
and you are in!

That's all that I have hacked out so far, I will write more
information on the subject later.

     -%>Spitfire Hacker<%-
          2600 Club!

                    ==Phrack Inc.==

                        ==Phrack Inc.==
                Volume One, Issue One, Phile 3 of 8

//
/   /
/   Boot Tracing Made Easy   /
/   Written by   /
/   _____   /
/   \Cheap/ \Shades/   /
/   ___/   ____/   /
/   2600 CLUB!   /
/   /
//
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
\   \
\   Be sure to call   \
\   \
\   Kleptic Palice......(314)527-5551 \
\   5 Meg BBS/AE/CF   \
\   Metal Shop.........(314)432-0756   \
\   Elite BBS (Home of 2600 CLUB! \
\   and Phrack Inc.)   \
\   \
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\

About 3 or four years ago, a real good friend of mine was teaching a ML
Programming course for the Apple 2 series. I, being a good friend and
quite bored, asked him about cracking Apple games. He told me that he had
spent the last summer cracking programs. He showed me a method that he came
up with entirely on his own, boot tracing. Little did he know that this was
already quite popular but he developed his own method for doing it which from
reading other files about it, is the simplest I've ever seen. (To give you
an idea, I had SN0GGLE (I've never played the game but a friend had it on
disk.) completely loaded into memory ready to be dumped in about 12 minutes.)
Ok, first of all, ALL programs can be boot traced. The only thing is that some
may not be easily converted into files. The only programs that you should try
if you aren't real good at ML, are ones that load completely into memory. Also
to do this you will need a cassette recorder. (don't worry the program we will
save won't take too long to save, and if all goes well it will only be saved
loaded once.) I hate learning the theory behind anything so I'm not gonna
give any theory behind this. If you want the theory, read some other phile
that does this the hard way.

First make sure your cassette recoder works by BLOADing some program and
typing:
CALL -151
AA60.AA73
You'll see something that looks like this:
AA60-30 02 xx xx xx xx xx xx
AA68-xx xx xx xx xx xx xx xx
AA70-xx xx 00 08
or whatever...The 30 02 is the length ($0230 bytes). The 00 08 is the starting
address ($0800). Oh well, now you need to try and save the program. Type:
800.A2FW   (A2F=$800+$230-1)
1000<800.A2FM
800:00 N 801<800.A2FM
800.A2FR
1000<800.A2FV

Once you are sure that the cassette works, (by the way do be stupid and try
that on a //c!) we can get to the good stuff...
First move the ROM boot-up code into RAM...(all steps will be from the
monitor * prompt.)
8600<C600.C6FFM
86F9:5C FF
(Now load in step 1 of the boot.)
8600G
C0E8 (turn the drive off)
(Now you have successfully loaded in track 0 sector 0) Now since we won't want
to overwrite what we've loaded in this time, Type:

```
8500<800.8FFM
86F9:01 85
8501L
```
Lets see what you've gotten...
First see if they move this part into the keyboard buffer. (A lot of programs
do this and the boot trace files that I've read don't even deal with this.)
```
LDX 00
LDA 800,X
STA 200,X
INX
BNE $803
JMP $211   (or any $2xx)
```
(sometimes done with Y's instead of X's.)
Then the next part will scramble what's in $08xx. but we don't have to worry
about that. Anyways find that JMP $2xx and change it to 4C xx 85 leaving the
xx the same. Usually this will be the next address but just to be safe...
Ok, now scan the code for any other JMP's if you find one that's direct
(indirect ones have the address in parenthesis) change it to 4C 5C FF, but
write down the location that it used to jump to first so you know where to
look. It'll probably be 301 or B700. If it's the B700, you got lucky. If it's
the 301 then you've got some more work ahead. If it was an indirect JMP, most
likely it was JMP ($003E). No if you change that to 4C 5C FF then check 3E
from monitor you'll find that 3E is 00 and 3F is 3E...Monitor uses that
place in zero page for its current memory location. So what you need to do is
```
8400:A5 3F 00 20 DA FD A5 3E 20 DA FD 4C 5C FF
```
then change that indirect jump to
```
85xx:4C 00 84
```
(by the way if the indirect jump is anything other than 3E then most likely
you can can just look at it from monitor if not write a little routine like
the one above to print out the address hidden. (Oh, check the location after
the next run. For now change it to 4C 5C FF.))
Anyways this little game will probably go on no longer than 2 or 3 loads, each
time just move the newly loaded part to another part of memory and change the
jump to jump to monitor (4C 5C FF) and the jump from the part before it to
go to the moved code.
When you find the part that JMP's up to a high area of memory (usually $B700)
you're almost done. The exit routine of the will most likely be the start of
the program. Once you intercept it there, all you have to do now is save it to
cassette and re-load DOS. The starting address for saving should be the
address that the B700 routine exits through. If this is higher than $6000 then
start saving at $2000 to get the Hi-Res pictures. Using WXYZ as your starting
address type:
```
WXYZ.9CFFW   (This will have the main program.)
800.WXYZW    (Save this are in case there is something needed down here we
             don't have to start over from scratch.)
```
Ok now reboot:
```
C600G   (with a DOS disk in the drive!)
CALL -151
WXYZ.9CFFR
```
Bsave PROGRAM,A$WXYZ,L$(Whatever 9CFF-WXYZ+1 is)
If the it gives you an error the file is too big. A quick DOS patch to fix
that is:
```
A964:FF
```
and try again.
Now that the program is saved, try and run it. (It's a good idea to take the
disk out of the drive, there's no telling what the program might try and do
if it sees that DOS is loaded in.)
```
WXYZG
```
(If it works, just to make sure that it's a good crack, power down the system
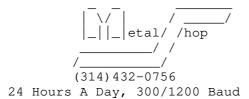and try and BRUN it after a cold boot.)
If your saved the pictures with the program, most likely, it won't run. You
need to add a JMP at 1FFD to JMP to the main program. Then re-BSAVE it with a
starting address of A$1FFD, and add 3 to the length. If the program tries to
go to the drive while its running, I'd suggest giving up unless you really
understand non-DOS disk usage. (but if you did you probably wouldn't be
reading this.) If you get a break at an address less than $2000 then you need
to load in the second program that you saved to cassette. Put a jump in at
$800 to the main program and save the whole damn thing. If it still don't work
you're gonna need to really get fancy.
Now that you've got the thing running, it's time to figure out what is used and

what is just wasted memory. This is where I really can't help you but just
make sure that you keep a working copy and before every test power down the
machine to clear anything that might be remaining.

Have phun and good luck.....
```
              _____
              \Cheap/ \Shades/
               \___/   \____/
                 2600 CLUB!
```

Be sure and get a copy of PHRACK INC., available on finer BBS/AE's everywhere.

```
           _ _      _____
          |_\/_|    / _____/
          |_||_|etal/ /hop
          _____/ /
         /_____/
```
         (314)432-0756
       24 Hours A Day, 300/1200 Baud

            Presents...

           ==Phrack Inc.==

       Volume One, Issue One, Phile 4 of 8

THE PHONE PHREAK'S FRY-UM GUIDE

COMPILED BY THE IRON SOLDIER

WITH HELP FROM DR. DOVE

NOTE: THIS GUIDE IS STILL BEING COMPILED, AND AS PHONE PHREAKS LEARN
      MORE IN THE ART OF VENGENCE IT WILL ALWAYS EXPAND.

"Vengence is mine", says the Phreak.

        METHOD 1-PHONE LINE PHUN

Call up the business office. It should be listed at the front of the white
    pages. Say you wanted to diconnect Scott Korman's line. DIAL 800-xxx-xxxx.
    "Hello, this is Mr. Korman, I'm moving to California and would like to have
    my phone service disconnected. I'm at the airport now. I'm calling from a
    payphone, my number is [414] 445 5005. You can send my final bill to
    :(somewhere in California. Thank you."

        METHOD 2-PHONE BOOKS

Call up the business office from a pay phone. Say "Hello, I'd like to order a
    Phone Book for Upper Volta (or any out-of-the way area with Direct
    Dialing). This is Scott Korman, ship to 3119 N. 44th St. Milwaukee, WI
    53216. Yes, I under stand it will cost $xx($25-$75!!). Thank you."

        METHOD 3-PHONE CALLS

Call up a PBX, enter the code and get an outside line. Then dial 0+ the number
    desired to call. You will hear a bonk and then an operator. Say, "I'd
    like to charge this to my home phone at 414-445-5005. Thank you." A friend
    and I did this to a loser, I called him at 1:00 AM and we left the fone off
    the hook all night. I calculated that it cost him $168.

        METHOD 4-MISC SERVICES

Call up the business office once again from a payfone. Say you'd like call
    waiting, forwarding, 3 way, etc. Once again you are the famed loser Scott
    Korman. He pays-you laugh. You don't know how funny it was talking to
    him, and wondering what those clicks he kept hearing were.

        METHOD 5-CHANGED & UNPUB

Do the same as in 4, but say you'd like to change and unlist your (Scott's)
    number. Anyone calling him will get:
    "BEW BEW BEEP. The number you have reached, 445-5005, has been changed to
    a non-published number. No further....."

METHOD 6-FORWRDING

This required an accomplise or two or three. Around Christmas time, go to
Toys 'R' Us. Get everyone at the customer service or manager's desk away
("Hey, could you help me"). then you get on their phone and dial (usually
dial 9 first) and the business office again. This time, say you are from
Toys 'R' Us, and you'd like to add call forwarding to 445-5005. Scott will
get 100-600 calls a day!!!

METHOD 7-RUSSIAN CALLER

Call a payphone at 10:00 PM. Say to the operator that you'd like to book a
call to Russia. Say you are calling from a payphone, and your number is
that of the loser to fry (e.g. 445-5005). She will say that she'll have to
call ya back in 5 hours, and you ok that. Meanwhile the loser (e.g.)
Scott, will get a call at 3:00 AM from an operator saying that the call he
booked to Russia is ready.

IF YOU HAVE ANY QUESTIONS LEAVE E-MAIL FOR ME ON ANY BOARD I'M ON.
        The Iron Soldier
      TSF-The Second Foundation!

```
                    _ _        _____
                   |\/ |      / _____/
                   |_||_|etal/ /hop
                   _____/ /
                  /_____/
                  (314)432-0756
               24 Hours A Day, 300/1200 Baud

                     Presents...

                    ==Phrack Inc.==
            Volume One, Issue One, Phile 5 of 8

                Using MCI Calling Cards
                        by
                   Knight Lightning
                      of the
                     2600 Club!
```

How to dial international calls on MCI:

         "Its easy to use MCI for international calling."

1. Dial your MCI access number and authorization code (code = 14 digit number,
    however the first 10 digits are the card holders NPA+PRE+SUFF).

2. Dial 011

3. Dial the country code
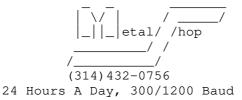
4. Dial the city code and the PRE+SUFF that you want.

Countries served by MCI:

Country	code	Country	code
Algeria	213	New Zealand	64
Argentina	54	Northern Ireland	44
Australia	61	Oman	968
Belgium	32	Papua New Guinea	675
Brazil	55	Qatar	974
Canada	Use Area Codes	Saudi Arabia	966
Cyprus	357	Scotland	44
Denmark	45	Senegal	221
Egypt	20	South Africa	27
England	44	Sri Lanka	94
German Democratic Republic		Sweden	46
(East Germany)	37	Taiwan	886
Greece	30	Tanzania	255
Jordan	962	Tunisa	216
Kenya	254	United Arab Emirates	971
Kuwait	965	Wales	44
Malawi	265		

==
Thats 33 countries in all. To get the extender for these calls dial 950-1022
or 1-800-624-1022.

For local calling:

1. Dial 950-1022 or 1-800-624-1022

2. Wait for tone

3. Dial "0", the area code, the phone number, and the 14 digit authorization
    code. You will hear 2 more tones that let you know you are connected.

   - Knight Lightning --> The 2600 Club!
==

```
      _ _        _____
     |‾\/‾|     / _____/
     |_||_|etal/ /hop
     _____/ /
    /_____/
```

(314)432-0756
24 Hours A Day, 300/1200 Baud

Presents...

==Phrack Inc.==
Volume One, Issue One, Phile 6 of 8

How to Pick Master Locks

By Gin Fizz & Ninja NYC

    Have you ever tried to impress your friends by picking one of those Master combination locks and failed? Well then read on. The Master lock company has made this kind of lock with a protection scheme. If you pull the handle of it hard, the knob won't turn. That was their biggest mistake...... Ok, now on to it.

    1st number. Get out any of the Master locks so you know what's going on. 1: The handle part (the part that springs open when you get the combination), pull on it, but not enough so that the knob won't move. 2: While pulling on it turn the knob to the left until it won't move any more. Then add 5 to this number. Congradulations, you now have the 1st number.

    2nd number. (a lot tougher) Ok, spin the dial around a couple of times, then go to the 1st number you got, then turn it to the right, bypassing the 1st number once. WHEN you have bypassed. Start pulling the handle and turning it. It will eventually fall into the groove and lock. While in the groove pull on it and turn the knob. If it is loose go to the next groove; if it's stiff you got the second number.

    3rd number: After getting the 2nd, spin the dial, then enter the 2 numbers, then after the 2nd, go to the right and at all the numbers pull on it. The lock will eventually open if you did it right. If can't do it the first time, be patient, it takes time.

 Have phun...

                    Gin Fizz/2600 Club!/TPM
                     Ninja NYC/TPM

                    ==Phrack Inc.==

```
                          _ _         _____
                         |‾\/‾|     / _____/
                         |_||_|etal/ /hop
                         _____/ /
                        /_____/
                        (314)432-0756
                24 Hours A Day, 300/1200 Baud

                        Presents...

                     ==Phrack Inc.==
                Volume One, Issue One, Phile 7 of 8

.-------------------------------------------------------------.
!               ///////                                       !
!                //                                           !
!               // h e C l a s h m a s t e r ’ s             !
!             .=============================.                 !
!         <            A C E T Y L E N E        >             !
!         <          ->B A L L O O N<-          >             !
!         <          ---->B O M B<----          >             !
!          `=============================’                    !
!               Written exclusively for...                    !
!                   The Phrack Inc.                           !
!                   2600 Club                                 !
!                   Newsletter                     11/01/85!
`-------------------------------------------------------------’
```

        Imagine this. A great, inflated, green garbage bag
slowly wafting down from a tall building. It gains some speed
as it nears the ground. People look up and say, "What the....?"
The garbage bag hits! *BOOM!!!* It explodes in a thundering
fireball of green bits of plastic and flame!
        "What is this?" you may ask. Well, this is the great
"Acetylene Balloon Bomb." And here is how to make it.

Ingredients:
============
(1>   For a small bomb: a plastic bag. Not too big.
           For something big(ger): a green, plastic garbage bag.

(2>   Some "Fun-Snaps". A dozen should be more than enough.

(3>   Some garbage bag twisties. String would also do.

(4>   A few rocks. Not too heavy, but depends on size of
           bomb and desired velocity of balloon/bomb.

(5>   PRIME INGREDIENT: Acetylene. This is what is used in
           acetylene torches. More on this substance later.

(6>   One or more eager Anarchists.

NOTES:
======
Acetylene is a fairly dangerous substance. It is unstable upon
contact with oxygen (air). For this reason, and for your
safety, I recommend you keep all of the acetylene AWAY from any
source of oxygen. This means don’t let it get in touch with
air.

Construction:
=============
(1>   Fill up a bathtub with cold water. Make it VERY full.
(2>   Now get put you garbage bag in the water and fill it
           with water. Make sure ALL air/oxygen is out of the
           bag before proceeding.
(3>   Now take your acetylene source (I used it straight

```
                  from the torch, and I recommend this way also.), and
                  fill the bag up with acetylene.
(4>               Now, being careful with the acetylene, take the bag
                  out of the tub and tie the opening shut with the
                  twisty or string. Let the balloon dry off now. (Put
                  it in a safe place.)
(5>               Okay. Now that it is dry and filled with acetlene,
                  open it up and drop a few rocks in there. Also add
                  some Fun-Snaps. The rocks will carry the balloon
                  down, and the Fun-Snaps will spark upon impact, thus
                  setting off the highly inflammable acetylene.
                  *BABOOM!*
(6>               Now put the twisty or string back on VERY tightly.
                  You now have a delicate but powerful balloon bomb.
```

To use:
=======
Just drop off of a cliff, airplane, building, or whatever. It
will hit the ground a explode in a fireball. Be careful you are
not near the explosion site. And be careful you are not
directly above the blast or the fireball may rise and give you
a few nasty burns.

Have fun!
But be careful...

NOTE: I, The Clashmaster, am in NO WAY responsible for the use
===== of this information in any way. This is for purely
      informational purposes only!

This has been a 2600 Club production.

```
                  -=*Clash*=-
                   2600 Club
```

```
          _ _         _____
         |_\/ |      / _____/
         |_||_|etal/ /hop
          _____/ /
         /_____/
          (314)432-0756
      24 Hours A Day, 300/1200 Baud

          Presents...

         ==Phrack Inc.==
  Volume One, Issue One, Phile 8 of 8


     Schools and University Numbers
     ``````````````````````````````
Harvard University   617-732-1251
Yale   203-436-2111
District 214   312-398-8170
Chicago Board of Education 312-254-1919
Spence Schools   212-369-5114
University of Texas   214-688-1400
University of Missouri   314-341-2776
                           314-341-2910
                    (1200) 314-341-2141
Cal-Tech   213-687-4662
University of Nevada   402-472-5065
Princeton University   609-452-6736
Stony Brook University   516-246-9000
Depaul   312-939-8388
University of San Diego   619-452-6792
RPI School   518-220-6603
William State University   313-577-0260
Harvard   617-732-1802
Stockton   209-944-4523
Northwestern   312-492-3094
Circle Campus   312-996-5100
                           312-996-6320
University of Mexico   505-588-3351
University of Florida   904-644-2261
Queens College   212-520-7719
University of Denver   303-753-2737
                           303-753-2733
University of Syracuse   315-423-1313
University of Illinois   312-996-5100
University of Virginia   703-328-8086
MIT Research   1-800-545-0085
St.Louis Community College 314-645-1289
SIUE   618-692-2400
                           618-692-2401
                           618-692-2402
                           618-692-2403
                           618-692-2404
                           618-692-2405
                           618-692-2406
                           618-692-2407
                           618-692-2408
Universiti-------   215-787-1011
Willaim --------   313-577-0260
University of Florida   904-392-5533
Col & Union College   301-279-0632
Georgia State   404-568-2131
University of Mass.   413-545-1600
Purdue   317-494-1900
Northwestern   312-492-7110
University of New Mexico   505-227-3351
University of Texas   214-688-1400
Temple University   215-787-1010
Melville High School   516-751-6806
UCSD   619-452-6900
```

```
Oakland Schools   313-857-9500
University of Maryland   301-454-6111
California St. Fulerton   714-773-3111
N.Y.U.   212-777-7600
University of San Diego   619-293-4510
University of Colorado   303-447-2540
University of Colorado   303-447-2538
MIT Research   617-258-6001
Dartmouth College   603-643-63q0
Spence School   212-369-5114
University of Washington   206-543-9713
University of Washington   206-543-9714
University of Washington   206-543-9715
University of Washington   206-543-9716
University of Washington   206-543-9717
University of NC   919-549-0881
Harvard-Law,Busi,Med Sch.   617-732-1251
Virginia University   703-328-8086
WVU   304-293-2921 thru 304-293-2939
WVU   304-293-4300 thru 304-293-4309
WVU(1200)304-293-4701 thru 304-293-4708
WVU(1200)304-293-5591 thru 304-293-5594
WVU(134.5 bps)   304-293-3601
WVU(134.5 bps)   304-293-3602
Lake Wash. School   206-828-3499
University of San Diego   619-452-6792
RPL School   518-220-6603
Another School   212-369-5114
Harvard   617-732-1251
Harvard   617-732-1802
William State University   313-577-0260
Florida University   904-644-2261
Wayne State   313-577-0260
U of F   904-644-2261
High School   513-644-3840
`````````````````````````````````````````
        File provided by the Alliance
           6 1 8 - 6 6 7 - 3 8 2 5
              7 p m  -  7 a m
```

Uploaded by Phantom Phreaker