THE GUIDE

FOR (mostly) HARMLESS

HACKING

#Guides of the Beginner's Series:

-So you want to be a harmless hacker?
-Hacking Windows 95!
-Hacking into Windows 95 (and a little bit of NT lore)!
-Hacking from Windows 3.x, 95 and NT
-How to Get a *Good* Shell Account, Part 1
-How to Get a *Good* Shell Account, Part 2
-How to use the Web to look up information on hacking.
-PGP for Newbies
-The Exploit Files: Basics of Breaking into Computers
-Computer hacking. Where did it begin and how did it grow?

GUIDE TO (mostly) HARMLESS HACKING
Beginners' Series #1
So you want to be a harmless hacker?

"You mean you can hack without breaking the law?"

That was the voice of a high school freshman. He had me on the phone because his father had just taken away his computer. His offense? Cracking into my Internet account. The boy had hoped to impress me with how "kewl" he was.

But before I realized he had gotten in, a sysadmin at my ISP had spotted the kid's harmless explorations and had alerted the parents. Now the boy wanted my help in getting back on line. I told the kid that I sympathized with his father.

What if the sysadmin and I had been major grouches? This kid could have wound up in juvenile detention. Now I don't agree with putting harmless hackers in jail, and I would never have testified against him. But that's what some people do to folks who go snooping in other people's computer accounts -- even when the culprit does no harm.

This boy needs to learn how to keep out of trouble!

Hacking is the most exhilarating game on the planet. But it stops being fun when you end up in a cell with a roommate named "Spike." But hacking doesn't have to mean breaking laws. In this series of Guides we teach safe hacking so that you don't have to keep looking back over your shoulders for narcs and cops.

What we're talking about is hacking as a healthy recreation, and as a free education that can qualify you to get a high paying job. In fact, many network systems administrators, computer scientists and computer security experts first learned their professions, not in some college program, but from the hacker culture. And you may be surprised to discover that ultimately the Internet is safeguarded not by law enforcement agencies, not by giant corporations, but by a worldwide network of, yes, hackers.

You, too, can become one of us.

And -- hacking can be surprisingly easy. Heck, if I can do it, anyone can!

Regardless of why you want to be a hacker, it is definitely a way to have

fun, impress your friends, and get dates. If you are a female hacker you become totally irresistible to men. Take my word for it!;^D

These Guides to (mostly) Harmless Hacking can be your gateway into this world. After reading just a few of these Guides you will be able to pull off stunts that will be legal, phun, and will impress the heck out of your friends.

These Guides can equip you to become one of the vigilantes that keeps the Internet from being destroyed by bad guys. Especially spammers. Heh, heh, heh. You can also learn how to keep the bad guys from messing with your Internet account, email, and personal computer. You'll learn not to be frightened by silly hoaxes that pranksters use to keep the average Internet user in a tizzy.

If you hang in with us through a year or so, you can learn enough and meet the people on our email list and IRC channel who can help you to become truly elite.

However, before you plunge into the hacker subculture, be prepared for that hacker attitude. You have been warned.

So...welcome to the adventure of hacking!

WHAT DO I NEED IN ORDER TO HACK?

You may wonder whether hackers need expensive computer equipment and a shelf full of technical manuals. The answer is NO! Hacking can be surprisingly easy! Better yet, if you know how to search the Web, you can find almost any computer information you need for free.

In fact, hacking is so easy that if you have an on-line service and know how to send and read email, you can start hacking immediately. The GTMHH Beginners' Series #2 will show you where you can download special hacker-friendly programs for Windows that are absolutely free. And we'll

show you some easy hacker tricks you can use them for.
Now suppose you want to become an elite hacker? All you will really need is an inexpensive "shell account" with an Internet Service Provider. In the GTMHH Beginners' Series #3 we will tell you how to get a shell account, log on, and start playing the greatest game on Earth: Unix hacking! Then in Vol.s I, II, and III of the GTMHH you can get into Unix hacking seriously.
You can even make it into the ranks of the Uberhackers without loading up on expensive computer equipment. In Vol. II we introduce Linux, the free hacker-friendly operating system. It will even run on a 386 PC with just 2 Mb RAM! Linux is so good that many Internet Service Providers use it to run their systems.
In Vol. III we will also introduce Perl, the shell programming language beloved of Uberhackers. We will even teach some seriously deadly hacker "exploits" that run on Perl using Linux. OK, you could use most of these exploits to do illegal things. But they are only illegal if you run them against someone else's computer without their permission. You can run any program in this series of Guides on your own computer, or your (consenting) friend's computer -- if you dare! Hey, seriously, nothing in this series of Guides will actually hurt your computer, unless you decide to trash it on purpose.
We will also open the gateway to an amazing underground where you can stay on top of almost every discovery of computer security flaws. You can learn how to either exploit them -- or defend your computer against them!

About the Guides to (mostly) Harmless Hacking

We have noticed that there are lots of books that glamorize

hackers. To read these books you would
think that it takes many years of brilliant work to
become one. Of course we hackers love to perpetuate this myth because it
makes us look so incredibly kewl.
But how many books are out there that tell the beginner step by step how to
actually do this hacking stuph? None! Seriously, have you ever read _Secrets
of a Superhacker_ by The Knightmare (Loomponics, 1994) or _Forbidden Secrets
of the Legion of Doom Hackers_ by Salacious Crumb (St. Mahoun Books, 1994)?
They are full of vague and out of date stuph. Give me a break.
And if you get on one of the hacker news groups on the Internet and ask
people how to do stuph, some of them insult and make fun of you. OK, they
all make fun of you.
We see many hackers making a big deal of themselves and being mysterious and refusing
to help others learn how to hack. Why? Because they don't want you
to know the truth, which is that most of what they are doing is really very
simple!
Well, we thought about this. We, too, could enjoy the pleasure of insulting people who
ask us how to hack. Or we could get big egos by actually teaching
thousands of people how to hack. Muhahaha.

How to Use the Guides to (mostly) Harmless Hacking

If you know how to use a personal computer and are on the Internet, you
already know enough to start learning to be a hacker. You don't even need to
read every single Guide to (mostly) Harmless Hacking in order to become a
hacker.
You can count on anything in Volumes I, II and III being so easy that you
can jump in about anywhere and just follow instructions.
But if your plan is to become "elite," you will do better if you read all
the Guides, check out the many Web sites and newsgroups to which we will

point you, and find a mentor among the many talented hackers who post to our
Hackers forum or chat on our IRC server at
http://www.infowar.com, and on
the Happy Hacker email list (email hacker@techbroker.com with message
"subscribe").
If your goal is to become an Uberhacker, the Guides will end up being only
the first in a mountain of material that you will need to study. However, we
offer a study strategy that can aid you in your quest to reach the pinnacle
of hacking.

How to Not Get Busted

One slight problem with hacking is that if you step over the line, you can
go to jail. We will do our best to warn you when we describe hacks that
could get you into trouble with the law. But we are not attorneys or experts
on cyberlaw. In addition, every state and every country has its own laws.
And these laws keep on changing. So you have to use a little sense.
However, we have a Guide to (mostly) Harmless Hacking Computer Crime Law
Series to help you avoid some pitfalls.
But the best protection against getting busted is the Golden Rule. If you
are about to do something that you would not like to have done to you,
forget it. Do hacks that make the world a better place, or that are at least
fun and harmless, and you should be able to keep out of trouble.
So if you get an idea from the Guides to (mostly) Harmless Hacking that
helps you to do something malicious or destructive, it's your problem if you
end up being the next hacker behind bars. Hey, the law won't care if the
guy whose computer you trash was being a d***. It won't care that the giant
corporation whose database you filched shafted your best buddy once. They

will only care that you broke the law.
To some people it may sound like phun to become a national sensation in the latest
hysteria over Evil Genius hackers. But after the trial, when some reader of these Guides ends up being the reluctant "girlfriend" of a convict
named Spike, how happy will his news clippings make him?

Conventions Used in the Guides

You've probably already noticed that we spell some words funny, like "kewl" and "phun." These are hacker slang terms. Since we often communicate with
each other via email, most of our slang consists of ordinary words with
extraordinary spellings. For example, a hacker might spell "elite" as
"3l1t3," with 3's substituting for e's and 1's for i's. He or she may even
spell "elite" as "31337. The Guides sometimes use these slang spellings to
help you learn how to write email like a hacker.
Of course, the cute spelling stuph we use will go out of date fast. So we do not guarantee that if you use this slang, people will read your email and
think, "Ohhh, you must be an Evil Genius! I'm sooo impressed!"
Take it from us, guys who need to keep on inventing new slang to prove they are "k-rad 3l1t3" are often lusers and lamers. So if you don't want to use
any of the hacker slang of these Guides, that's OK by us. Most Uberhackers
don't use slang, either.

Who are You?

We've made some assumptions about who you are and why you are reading these Guides:

- You own a PC or Macintosh personal computer
- You are on-line with the Internet
- You have a sense of humor and adventure and want to express it by hacking
- Or -- you want to impress your friends and pick up chicks (or guys) by
making them think you are an Evil Genius

So, does this picture fit you? If so, OK, d00dz, start your computers. Are
you ready to hack?

GUIDE TO (mostly) HARMLESS HACKING
Beginners' Series #2, Section One.
Hacking Windows 95!

Important warning: this is a beginners lesson. BEGINNERS. Will all you super k-rad elite haxors out there just skip reading this one, instead reading it and feeling all insulted at how easy it is and then emailing me to bleat "This GTMHH iz 2 ezy your **** up,wee hate u!!!&$%" Go study something that seriously challenges your intellect such as "Unix for Dummies," OK?**

Have you ever seen what happens when someone with an America Online account posts to a hacker news group, email list, or IRC chat session? It gives you a true understanding of what "flame" means, right?

Now you might think that making fun of dumb.newbie@aol.com is just some prejudice. Sort of like how managers in big corporations don't wear dreadlocks and fraternity boys don't drive Yugos.

But the real reason serious hackers would never use AOL is that it doesn't offer Unix shell accounts for its users. AOL fears Unix because it is the most fabulous, exciting, powerful, hacker-friendly operating system in the Solar system... gotta calm down ... anyhow, I'd feel crippled without Unix.

So AOL figures offering Unix shell accounts to its users is begging to get hacked.

Unfortunately, this attitude is spreading. Every day more ISPs are deciding to stop offering shell accounts to their users.

But if you don't have a Unix shell account, you can still hack. All you need is a computer that runs Windows 95 and just some really retarded on-line account like America Online or Compuserve.

In this Beginner's Series #2 we cover several fun things to do with Windows and even the most hacker-hostile Online services.

And, remember, all these things are really easy. You don't need to be a genius. You don't need to be a computer scientist. You don't need to won an expensive computer. These are things anyone with Windows 95 can do.

Section One: Customize your Windows 95 visuals. Set up your startup, background and logoff screens so as to amaze and befuddle your non-hacker friends.

Section Two: Subvert Windows nanny programs such as Surfwatch and the setups many schools use in the hope of keeping kids from using unauthorized programs. Prove to yourself -- and your friends and coworkers -- that Windows 95 passwords are a joke.

Section Three: Explore other computers -- OK, let's be blatant -- hack -- from your Windows home computer using even just AOL for Internet access.

HOW TO CUSTOMIZE WINDOWS 95 VISUALS

OK, let's say you are hosting a wild party in your home. You decide to show your buddies that you are one of those dread hacker d00dz. So you fire up your computer and what should come up on your screen but the logo for "Windows 95." It's kind of lame looking, isn't it? Your computer looks just like everyone else's box. Just like some boring corporate workstation operated by some guy with an IQ in the 80s.

Now if you are a serious hacker you would be booting up Linux or FreeBSD or some other kind of Unix on your personal computer. But your friends don't know that. So you have an opportunity to social engineer them into thinking you are fabulously elite by just by customizing your bootup screen.

Now let's say you want to boot up with a black screen with orange and yellow flames and the slogan " K-Rad Doomsters of the Apocalypse." This turns out to be super easy.

Now Microsoft wants you to advertise their operating system every time you boot up. In fact, they want this so badly that they have gone to court to try to force computer retailers to keep the Micro$oft bootup

screen on the
systems these vendors sell.
So Microsoft certainly doesn't want you messing with their bootup screen,
either. So M$ has tried to hide the bootup screen software. But they didn't
hide it very well. We're going to learn today how to totally thwart their
plans.

****
Evil Genius tip: One of the rewarding things about hacking is to find hidden
files that try to keep you from modifying them -- and then to mess with them
anyhow. That's what we're doing today.
The Win95 bootup graphics is hidden in either a file named c:\logo.sys
and/or ip.sys. To see this file, open File Manager, click "view", then click
"by file type," then check the box for "show hidden/system files." Then,
back on "view," click "all file details." To the right of the file logo.sys
you will see the letters "rhs." These mean this file is "read-only, hidden,
system."
The reason this innocuous graphics file is labeled as a system file -- when it really is just a graphics file with some animation added -- is because
Microsoft is afraid you'll change it to read something like "Welcome to
Windoze 95 -- Breakfast of Lusers!" So by making it a read-only file, and
hiding it, and calling it a system file as if it were something so darn
important it would destroy your computer if you were to mess with it,
Microsoft is trying to trick you into leaving it alone.
****

The easiest way to thwart these Windoze 95 startup and shut down screens is to go to http://www.windows95.com/apps/ and check out their programs. But
we're hackers, so we like to do things ourselves. So here's how to do this
without using a canned program.

We start by finding the MSPaint program. It's probably under the accessories folder. But just in case you're like me and keep on moving things around, here's the fail-safe program finding routine:

1) Click "Start" on the lower left corner of your screen.
2) Click "Windows Explorer"
3) Click "Tools"
4) Click "Find"
5) Click "files or folders"
6) After "named" type in "MSPaint"
7) After "Look in" type in 'C:"
8) Check the box that says "include subfolders"
9) Click "find now"
10) Double click on the icon of a paint bucket that turns up in a window. This loads the paint program.
11) Within the paint program, click "file"
12) Click "open"

OK, now you have MSPaint. Now you have a super easy way to create your new bootup screen:

13) After "file name" type in c:\windows\logos.sys. This brings up the graphic you get when your computer is ready to shut down saying "It's now safe to turn off your computer." This graphic has exactly the right format to be used for your startup graphic. So you can play with it any way you want (so long as you don't do anything on the Attributes screen under the Images menu) and use it for your startup graphic.
14) Now we play with this picture. Just experiment with the controls of MSPaint and try out fun stuff.
15) When you decide you really like your picture (fill it with frightening hacker stuph, right?), save it as c:\logo.sys. This will overwrite the Windows startup logo file. From now on, any time you want to change your startup logo, you will be able to both read and write the file logo.sys.
16) If you want to change the shut down screens, they are easy to find and modify using MSPaint. The beginning shutdown screen is named c:\windows\logow.sys. As we saw above, the final "It's now safe to turn off

your computer" screen graphic is named c:\windows\logos.sys.
17) To make graphics that will be available for your wallpaper, name them
something like c:\windows\evilhaxor.bmp (substituting your filename for
"exilhaxor" -- unless you like to name your wallpaper "evilhaxor.")

****
Evil Genius tip: The Microsoft Windows 95 startup screen has an animated bar
at the bottom. But once you replace it with your own graphic, that animation
is gone. However, you can make your own animated startup screen using the
shareware program BMP Wizard. Some download sites for this goodie include:
http://www.pippin.com/English/ComputersSoftware/Software/Windows95/graphic.html
http://search.windows95.com/apps/editors.html
http://www.windows95.com/apps/editors.html
Or you can download the program LogoMania, which automatically resizes any
bitmap to the correct size for your logon and logoff screens and adds
several types of animation as well. You can find it
at.ftp.zdnet.com/pcmag/1997/0325/logoma.zip
****

Now the trouble with using one of the existing Win95 logo files is that they only allow you to use their original colors. If you really want to go wild,
open MSPaint again. First click "Image," then click "attributes." Set width
320 and height to 400. Make sure under Units that Pels is selected. Now you
are free to use any color combination available in this program. Remember to
save the file as c:\logo.sys for your startup logo, or c:\windows\logow.sys
and or c:\windows\logos.sys for your shutdown screens.
But if you want some really fabulous stuff for your starting screen, you can steal graphics from your favorite hacker page on the Web and import them
into Win95's startup and shutdown screens. Here's how you do it.
1) Wow, kewl graphics! Stop your browsing on that Web page and hit the

"print screen" button.
2) Open MSPaint and set width to 320 and height to 400 with units Pels.
3) Click edit, then click paste. Bam, that image is now in your MSPaint
program.
4) When you save it, make sure attributes are still 320X400 Pels. Name it
c:\logo.sys, c:\windows\logow.sys, c:\windows\logos.sys, or c:\winodws\evilhaxor.bmp depending on which screen or wallpaper you want to
display it on.
Of course you can do the same thing by opening any graphics file you choose in MSPaint or any other graphics program, so long as you save it with the
right file name in the right directory and size it 320X400 Pels.
Oh, no, stuffy Auntie Suzie is coming to visit and she wants to use my
computer to read her email! I'll never hear the end of it if she sees my
K-Rad Doomsters of the Apocalypse startup screen!!!
Here's what you can do to get your boring Micro$oft startup logo back. Just change the name of c:logo.sys to something innocuous that Aunt Suzie won't
see while snooping with file manager. Something like logo.bak. Guess what
happens? Those Microsoft guys figured we'd be doing things like this and hid
a copy of their boring bootup screen in a file named "io.sys." So if you
rename or delete their original logo.sys, and there is no file by that name
left, on bootup your computer displays their same old Windows 95 bootup
screen.
Now suppose your Win95 box is attached to a local area network (LAN)? It
isn't as easy to change your bootup logo, as the network may override your
changes. But there is a way to thwart the network. If you aren't afraid of
your boss seeing your "K-Rad Dommsters of the Apocalypse" spashed over an
x-rated backdrop, here's how to customize your bootup graphics.
0.95 policy editor (comes on the 95 cd) with the default admin.adm will let you change this. Use the policy editor to open the registry, select 'local

computer' select network, select 'logon' and then selet 'logon banner'.
It'll then show you the current banner and let you change it and save it
back to the registry.

****
Evil genius tip: Want to mess with io.sys or logo.sys? Here's how to get
into them. And, guess what, this is a great thing to learn in case you ever
need to break into a Windows computer -- something we'll look at in detail
in the next section.
Click "Start" then "Programs" then "MS-DOS." At the MS_DOS prompt enter the commands:
ATTRIB -R -H -S C:\IO.SYS
ATTRIB -R -H -S C:\LOGO.SYS
Now they are totally at your mercy, muhahaha!
But don't be surprised is MSPaint can't open either of these files. MSPaint only opens graphics files. But io.sys and logo.sys are set up to be used by animation applications.
****

OK, that's it for now. You 31337 hackers who are feeling insulted by
reading this because it was too easy, tough cookies. I warned you. But I'll
bet my box has a happier hacker logon graphic than yours does. K-Rad
Doomsters of the apocalypse, yesss!

GUIDE TO (mostly) HARMLESS HACKING
Beginners' Series #2, Section Two.
Hacking into Windows 95 (and a little bit of NT lore)!

Important warning: this is a beginners lesson. BEGINNERS. Will all you
geniuses who were born already knowing 32-bit Windows just skip reading this
one, OK? We don't need to hear how disgusted you are that not

**everyone
already knows this.**

PARENTAL DISCRETION ADVISED!

**This lesson will lay the foundation for learning how to hack what now is the most commonly installed workstation operating system: Windows NT. In fact,
Windows NT is coming into wide use as a local area network (LAN), Internet,
intranet, and Web server. So if you want to call yourself a serious hacker,
you'd better get a firm grasp on Win NT.
In this lesson you will learn serious hacking techniques useful on both
Windows 95 and Win NT systems while playing in complete safety on your own
computer.**

In this lesson we explore:

- **-Several ways to hack your Windows 95 logon password**
- **-How to hack your Pentium CMOS password**
- **-How to hack a Windows Registry -- which is where access control on
Windows-based LANs, intranets and Internet and Webs servers are hidden!**

**Let's set the stage for this lesson. You have your buddies over to your home to see you hack on your Windows 95 box. You've already put in a really
industrial haxor-looking bootup screen, so they are already trembling at the
thought of what a tremendously elite d00d you are. So what do you do next?
How about clicking on "Start," clicking "settings" then "control panel" then "passwords." Tell your friends your password and get them to enter a secret
new one. Then shut down your computer and tell them you are about to show
them how fast you can break their password and get back into your own box!
This feat is so easy I'm almost embarrassed to tell you how it's done.
That's because you'll say "Sheesh, you call that password protection? Any
idiot can break into a Win 95 box! And of course you're right. But that's**

the Micro$oft way. Remember this next time you expect to keep something on
your Win95 box confidential.
And when it comes time to learn Win NT hacking, remember this Micro$oft
security mindset. The funny thing is that very few hackers mess with NT
today because they're all busy cracking into Unix boxes. But there are
countless amazing Win NT exploits just waiting to be discovered. Once you
see how easy it is to break into your Win 95 box, you'll feel in your bones
that even without us holding your hand, you could discover ways to crack Win
NT boxes, too.
But back to your buddies waiting to see what an elite hacker you are. Maybe you'll want them to turn their backs so all they know is you can break into a Win95 box in less than one minute. Or maybe you'll be a nice guy and show
them exactly how it's done.
But first, here's a warning. The first few techniques we're showing work on most home Win 95 installations. But, especially in corporate local area
networks (LANs), several of these techniques don't work. But never fear, in
this lesson we will cover enough ways to break in that you will be able to
gain control of absolutely *any* Win 95 box to which you have physical
access. But we'll start with the easy ways first.

Easy Win 95 Breakin #1:

Step one: boot up your computer.
Step two: When the "system configuration" screen comes up, press the "F5"
key. If your system doesn't show this screen, just keep on pressing the F5
key.
If your Win 95 has the right settings, this boots you into "safe mode."
Everything looks weird, but you don't have to give your password and you
still can run your programs.
Too easy! OK, if you want to do something that looks a little classier,

here's another way to evade that new password.

Easy Win 95 Breakin #2:

Step one: Boot up.
Step two: when you get to the "system configuration" screen, press the F8
key. This gives you the Microsoft Windows 95 Startup Menu.
Step three: choose number 7. This puts you into MS-DOS. At the prompt, give the command "rename c:\windows*pwl c:\windows*zzz."

****
Newbie note: MS-DOS stands for Microsoft Disk Operating System, an ancient
operating system dating from 1981. It is a command-line operating system,
meaning that you get a prompt (probably c:\>) after which you type in a
command and press the enter key. MS-DOS is often abbreviated DOS. It is a
little bit similar to Unix, and in fact in its first version it incorporated
thousands of lines of Unix code.
****

Step four: reboot. You will get the password dialog screen. You can then
fake out your friends by entering any darn password you want. It will ask
you to reenter it to confirm your new password.
Step five: Your friends are smart enough to suspect you just created a new
password, huh? Well, you can put the old one your friends picked. Use any
tool you like -- File Manager, Explorer or MS-DOS -- to rename *.zzz back to
*.pwl.
Step six: reboot and let your friends use their secret password. It still
works!
Think about it. If someone where to be sneaking around another person's Win 95 computer, using this technique, the only way the victim could determine
there had been an intruder is to check for recently changed files and
discover that the *.pwl files have been messed with

****
Evil genius tip: Unless the msdos.sys file bootkeys=0 option is active, the keys that can do something during the bootup process are F4, F5, F6, F8, Shift+F5, Control+F5 and Shift+F8. Play with them!
****

Now let's suppose you discovered that your Win 95 box doesn't respond to the bootup keys. You can still break in. If your computer does allow use of the boot keys, you may wish to disable them in order to be a teeny bit more secure. Besides, it's phun to show your friends how to use the boot keys and then disable these so when they try to mess with your computer they will discover you've locked them out. The easiest -- but slowest -- way to disable the boot keys is to pick the proper settings while installing Win 95. But we're hackers, so we can pull a fast trick to do the same thing. We are going to learn how to edit the Win 95 msdos.sys file, which controls the boot sequence.

Easy Way to Edit your Msdos.sys File:

Step zero: Back up your computer completely, especially the system files. Make sure you have a Windows 95 boot disk. We are about to play with fire! If you are doing this on someone else's computer, let's just hope either you have permission to destroy the operating system, or else you are so good you couldn't possibly make a serious mistake.

****
Newbie note: You don't have a boot disk? Shame, shame, shame! Everyone ought to have a boot disk for their computer just in case you or your buddies do something really horrible to your system files. If you don't already have a Win 95 boot disk, here's how to make one.

To do this you need an empty floppy disk and your Win 95 installation
disk(s). Click on Start, then Settings, then Control Panel, then Add/Remove
Programs, then Startup Disk. From here just follow instructions.
****

Step one: Find the file msdos.sys. It is in the root directory (usually
C:\). Since this is a hidden system file, the easiest way to find it is to
click on My Computer, right click the icon for your boot drive (usually C:),
left click Explore, then scroll down the right side frame until you find the
file "msdos.sys."
Step two: Make msdos.sys writable. To do this, right click on msdos.sys,
then left click "properties." This brings up a screen on which you uncheck
the "read only" and "hidden" boxes. You have now made this a file that you
can pull into a word processor to edit.
Step three: Bring msdos.sys up in Word Pad. To do this, you go to File
Manager. Find msdos.sys again and click on it. Then click "associate" under
the "file" menu. Then click on "Word Pad." It is very important to use Word
Pad and not Notepad or any other word processing program! Then double click
on msdos.sys.
Step four: We are ready to edit. You will see that Word Pad has come up with msdos.sys loaded. You will see something that looks like this:

```
[Paths]
WinDir=C:\WINDOWS
WinBootDir=C:\WINDOWS
HostWinBootDrv=C
[Options]
BootGUI=1
Network=1
;
;The following lines are required for compatibility with other programs.
;Do not remove them (MSDOS>SYS needs to be >1024 bytes).
;xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

;xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

To disable the function keys during bootup, directly below [Options] you
should insert the command "BootKeys=0."
Or, another way to disable the boot keys is to insert the command BootDelay=0. You can really mess up your snoopy hacker wannabe friends by
putting in both statements and hope they don't know about BootDelay. Then
save msdos.sys.
Step five: since msdos.sys is absolutely essential to your computer, you'd
better write protect it like it was before you edited it. Click on My
Computer, then Explore, then click the icon for your boot drive (usually
C:), then scroll down the right side until you find the file "msdos.sys."
Click on msdos.sys, then left click "properties." This brings back that
screen with the "read only" and "hidden" boxes. Check "read only."
Step six: You *are* running a virus scanner, aren't you? You never know what your phriends might do to your computer while your back is turned. When you
next boot up, your virus scanner will see that msdos.sys has changed. It
will assume the worst and want to make your msdos.sys file look just like it
did before. You have to stop it from doing this. I run Norton Antivirus, so
all I have to do when the virus warning screen comes up it to tell it to
"innoculate."

Hard Way to Edit your (or someone else's) Msdos.sys File.

Step one: This is useful practice for using DOS to run rampant someday in
Win NT LANs, Web and Internet servers. Put a Win 95 boot disk in the a:
drive. Boot up. This gives you a DOS prompt A:\.
Step one: Make msdos.sys writable. Give the command "attrib -h -r -s
c:\msdos.sys" (This assumes the c: drive is the boot disk.)
Step two: give the command "edit msdos.sys" This brings up this

file into
the word processor.
Step three: Use the edit program to alter msdos.sys. Save it.
Exit the edit program.
Step four: At the DOS prompt, give the command "attrib +r +h +s
c:\msdos.sys" to return the msdos.sys file to the status of
hidden,
read-only system file.
OK, now your computer's boot keys are disabled. Does this mean
no one can
break in? Sorry, this isn't good enough.
As you may have guessed from the "Hard Way to Edit your
Msdos.sys"
instruction, your next option for Win 95 breakins is to use a
boot disk that
goes in the a: floppy drive.

How to Break into a Win 95 Box Using a Boot Disk

Step one: shut down your computer.
Step two: put boot disk into A: drive.
Step three: boot up.
Step four: at the A:\ prompt, give the command: rename c:\
windows*.pwl
c:\windows*.zzz.
Step four: boot up again. You can enter anything or nothing at
the password prompt and get in.
Step five: Cover your tracks by renaming the password files back
to what
they were.
Wow, this is just too easy! What do you do if you want to keep
your
prankster friends out of your Win 95 box? Well, there is one more
thing you
can do. This is a common trick on LANs where the network
administrator
doesn't want to have to deal with people monkeying around with
each others'
computers. The answer -- but not a very good answer -- is to use
a CMOS
password.

How to Mess With CMOS #1

The basic settings on your computer such as how many and what
kinds of disk drives and which ones are used for booting are held
in a CMOS chip on the

mother board. A tiny battery keeps this chip always running so that whenever
you turn your computer back on, it remembers what is the first drive to
check in for bootup instructions. On a home computer it will typically be
set to first look in the A: drive. If the A: drive is empty, it next will
look at the C: drive.
On my computer, if I want to change the CMOS settings I press the delete key at the very beginning of the bootup sequence. Then, because I have
instructed the CMOS settings to ask for a password, I have to give it my
password to change anything.
If I don't want someone to boot from the A: drive and mess with my password file, I can set it so it only boots from the C: drive. Or even so that it only boots from a remote drive on a LAN.
So, is there a way to break into a Win 95 box that won't boot from the A:
drive? Absolutely yes! But before trying this one out, be sure to write down
ALL your CMOS settings. And be prepared to make a total wreck of your
computer. Hacking CMOS is even more destructive than hacking system files.
Step one: get a phillips screwdriver, solder sucker and soldering iron.
Step two: open up your victim.
Step three: remove the battery .
Step four: plug the battery back in.
Alternate step three: many motherboards have a 3 pin jumper to reset the
CMOS to its default settings. Look for a jumper close to the battery or look
at your manual if you have one.
For example, you might find a three pin device with pins one and two
jumpered. If you move the jumper to pins two and three and leave it there
for over five seconds, it may reset the CMOS. Warning -- this will not work
on all computers!
Step five: Your victim computer now hopefully has the CMOS default settings.
Put everything back the way they were, with the exception of

setting it to
first check the A: drive when booting up.

****
You can get fired warning: If you do this wrong, and this is a computer you
use at work, and you have to go crying to the systems administrator to get
your computer working again, you had better have a convincing story.
Whatever you do, don't tell the sysadmin or your boss that "The Happy Hacker made me do it"!
****

Step six: proceed with the A: drive boot disk break-in instructions.
Does this sound too hairy? Want an easy way to mess with CMOS? There's a
program you can run that does it without having to play with your mother
board.

How to Mess with CMOS #2

Boy, I sure hope you decided to read to the end of this GTMHH before taking solder gun to your motherboard. There's an easy solution to the CMOS
password problem. It's a program called KillCMOS which you can download from
http://www.koasp.com. (Warning: if I were you, I'd first check out this site
using the Lynx browser, which you can use from Linux or your shell account).
Now suppose you like to surf the Web but your Win 95 box is set up so some
sort of net nanny program restricts access to places you would really like
to visit. Does this mean you are doomed to live in a Brady Family world? No
way.
There are several ways to evade those programs that censor what Web sites
you visit.
Now what I am about to discuss is not with the intention of feeding
pornography to little kids. The sad fact is that these net censorship

programs have no way of evaluating everything on the Web. So what they do is
only allow access to a relatively small number of Web sites. This keeps kids
form discovering many wonderful things on the Web.
As the mother of four, I understand how worried parents can get over what
their kids encounter on the Internet. But these Web censor programs are a
poor substitute for spending time with your kids so that they learn how to
use computers responsibly and become really dynamite hackers! Um, I mean,
become responsible cyberspace citizens. Besides, these programs can all be
hacked way to easily.
The first tactic to use with a Web censor program is hit control-alt-delete. This brings up the task list. If the censorship program is on the list, turn it off.
Second tactic is to edit the autoexec.bat file to delete any mention of the web censor program. This keeps it from getting loaded in the first place.
But what if your parents (or your boss or spouse) is savvy enough to check
where you've been surfing? You've got to get rid of those incriminating
records whowing that you've been surfing Dilbert!
It's easy to fix with Netscape. Open Netscape.ini with either Notepad or
Word Pad. It probably will be in the directory C:\Netscape\ netscape.ini.
Near the bottom you will find your URL history. Delete those lines.
But Internet Explorer is a really tough browser to defeat. Editing the Registry is the only way (that I have found, at least) to defeat the censorship feature on Internet Explorer. And, guess what, it even hides several records of your browsing history in the Registry. Brrrr!

****

Newbie note: Registry! It is the Valhalla of those who wish to crack
Windows. Whoever controls the Registry of a network server controls the
network -- totally. Whoever controls the Registry of a Win 95 or Win NT box
controls that computer -- totally. The ability to edit the

**Registry is
comparable to having root access to a Unix machine.
****

How to edit the Registry:

Step zero: Back up all your files. Have a boot disk handy. If you mess up
the Registry badly enough you may have to reinstall your operating system.

****
You can get fired warning: If you edit the Registry of a computer at work,
if you get caught you had better have a good explanation for the sysadmin
and your boss. Figure out how to edit the Registry of a LAN server at work
and you may be in real trouble.
****

****
You can go to jail warning: Mess with the Registry of someone else's
computer and you may be violating the law. Get permission before you mess
with Registries of computers you don't own.
****

Step one: Find the Registry. This is not simple, because the Microsoft
theory is what you don't know won't hurt you. So the idea is to hide the
Registry from clueless types. But, hey, we don't care if we totally trash
our computers, right? So we click Start, then Programs, then Windows
Explorer, then click on the Windows directory and look for a file named
"Regedit.exe."
Step two: Run Regedit. Click on it. It brings up several folders:
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
HKEY_CURRENT_CONFIG
HKEY_DYN_DATA**

What we are looking at is in some ways like a password file, but it's much
more than this. It holds all sorts of settings -- how your desk top looks,
what short cuts you are using, what files you are allowed to access. If you
are used to Unix, you are going to have to make major revisions in how you
view file permissions and passwords. But, hey, this is a beginners' lesson
so we'll gloss over this part.

****

Evil genius tip: You can run Regedit from DOS from a boot disk. Verrrry
handy in certain situations...

****

Step three: Get into one of these HKEY thingies. Let's check out
CURRENT_USER by clicking the plus sign to the left of it. Play around
awhile. See how the Regedit gives you menu choices to pick new settings.
You'll soon realize that Microsoft is babysitting you. All you see is
pictures with no clue of who these files look in DOS. It's called "security
by obscurity." This isn't how hackers edit the Registry.

Step four: Now we get act like real hackers. We are going to put part of the Registry where we can see -- and change -- anything. First click the
HKEY_CLASSES_ROOT line to highlight it. Then go up to the Registry heading
on the Regedit menu bar. Click it, then choose "Export Registry File." Give
it any name you want, but be sure it ends with ".reg".

Step five: Open that part of the Registry in Word Pad. It is important to
use that program instead of Note Pad or any other word processing program.
One way is to right click on it from Explorer. IMPORTANT WARNING: if you
left click on it, it will automatically import it back into the Registry. If
you were messing with it and accidentally left click, you could trash your
computer big time.

Step six: Read everything you ever wanted to know about Windows

security
that Microsoft was afraid to let you find out. Things that look like:
[HKEY_CLASSES_ROOT\htmlctl.PasswordCtl\CurVer]
@="htmlctl.PasswordCtl.1"
[HKEY_CLASSES_ROOT\htmlctl.PasswordCtl.1]
@="PasswordCtl Object"
[HKEY_CLASSES_ROOT\htmlctl.PasswordCtl.1\CLSID]
@="{EE230860-5A5F-11CF-8B11-00AA00C00903}"
The stuff inside the brackets in this last line is an encrypted password
controlling access to a program or features of a program such as the net
censorship feature of Internet Explorer. What it does in encrypt the
password when you enter it, then compare it with the unencrypted version on
file.
Step seven: It isn't real obvious which password goes to what program. I say delete them all! Of course this means your stored passwords for logging on
to your ISP, for example, may disappear. Also, Internet Explorer will pop up
with a warning that "Content Advisor configuration information is missing.
Someone may have tried to tamper with it." This will look really bad to your parents!
Also, if you trash your operating system in the process, you'd better have a good explanation for your Mom and Dad about why your computer is so sick.
It's a good idea to know how to use your boot disk to reinstall Win 95 it
this doesn't work out.
Step eight: (optional): Want to erase your surfing records? For Internet
Explorer you'll have to edit HKEY_CURRENT_USER,
HKEY_LOCAL_MACHINE and
HKEY_USERS. You can also delete the files c:\windows\cookies\mm2048.dat and
c:\windows\cookies\mm256.dat. These also store URL data.
Step nine: Import your .reg files back into the Registry. Either click on
your .reg files in Explorer or else use the "Import" feature next to the
"Export" you just used in Regedit. This only works if you remembered to name
them with the .reg extension.

Step ten: Oh, no, Internet Explorer makes this loud obnoxious noise the
first time I run it and puts up a bright red "X" with the message that I
tampered with the net nanny feature! My parents will seriously kill me!
Or, worse yet, oh, no, I trashed my computer!
All is not lost. Erase the Registry and its backups. These are in four
files: system.dat, user.dat, and their backups, system.da0 and user.da0.
Your operating system will immediately commit suicide. (This was a really
exciting test, folks, but I luuuv that adrenaline!) If you get cold feet,
the Recycle bin still works after trashing your Registry files, so you can
restore them and your computer will be back to the mess you just made of it.
But if you really have guts, just kill those files and shut it down.
Then use your Win 95 boot disk to bring your computer back to life.
Reinstall Windows 95. If your desk top looks different, proudly tell
everyone you learned a whole big bunch about Win 95 and decided to practice
on how your desk top looks. Hope they don't check Internet Explorer to see
if the censorship program still is enabled.
And if your parents catch you surfing a Nazi explosives instruction site, or if you catch your kids at bianca's Smut Shack, don't blame it on Happy
Hacker. Blame it on Microsoft security -- or on parents being too busy to
teach their kids right from wrong.
So why, instead of having you edit the Registry, didn't I just tell you to
delete those four files and reinstall Win 95? It's because if you are even
halfway serious about hacking, you need to learn how to edit the Registry of
a Win NT computer. You just got a little taste of what it will be like here,
done on the safety of your home computer.
You also may have gotten a taste of how easy it is to make a huge mess when messing with the Registry. Now you don't have to take

my work for it, you
know first hand how disastrous a clumsy hacker can be when messing in
someone else's computer systems.
So what is the bottom line on Windows 95 security? Is there any way to set
up a Win 95 box so no one can break into it? Hey, how about that little key
on your computer? Sorry, that won't do much good, either. It's easy to
disconnect so you can still boot the box. Sorry, Win 95 is totally
vulnerable.
In fact, if you have physical access to *ANY* computer, the only
way to keep you from breaking into it is to encrypt its files with a strong encryption
algorithm. It doesn't matter what kind of computer it is, files on any
computer can one way or another be read by someone with physical access to
it -- unless they are encrypted with a strong algorithm such as RSA.
We haven't gone into all the ways to break into a Win 95 box remotely, but
there are plenty of ways. Any Win 95 box on a network is vulnerable, unless
you encrypt its information.
And the ways to evade Web censor programs are so many, the only
way you can make them work is to either hope your kids stay dumb, or else that they will
voluntarily choose to fill their minds with worthwhile material. Sorry,
there is no technological substitute for bringing up your kids to know right
from wrong.

****
Evil Genius tip: Want to trash most of the policies can be invoked on a
workstation running Windows 95? Paste these into the appropriate locations
in the Registry. Warning: results may vary and you may get into all sorts of
trouble whether you do this successfully or unsuccessfully.
[HKEY_LOCAL_MACHINE\Network\Logon]
[HKEY_LOCAL_MACHINE\Network\Logon]
"MustBeValidated"=dword:00000000

```
"username"="ByteMe"
"UserProfiles"=dword:00000000
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Policies]
"DisablePwdCaching"=dword:00000000
"HideSharePwds"=dword:00000000
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Policies\Explorer]

"NoDrives"=dword:00000000
"NoClose"=dword:00000000
"NoDesktop"=dword:00000000
"NoFind"=dword:00000000
"NoNetHood"=dword:00000000
"NoRun"=dword:00000000
"NoSaveSettings"=dword:00000000
"NoRun"=dword:00000000
"NoSaveSettings"=dword:00000000
"NoSetFolders"=dword:00000000
"NoSetTaskbar"=dword:00000000
"NoAddPrinter"=dword:00000000
"NoDeletePrinter"=dword:00000000
"NoPrinterTabs"=dword:00000000
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Policies\Network]

"NoNetSetup"=dword:00000000
"NoNetSetupIDPage"=dword:00000000
"NoNetSetupSecurityPage"=dword:00000000
"NoEntireNetwork"=dword:00000000
"NoFileSharingControl"=dword:00000000
"NoPrintSharingControl"=dword:00000000
"NoWorkgroupContents"=dword:00000000
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Policies\System]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Policies\System]

"NoAdminPage"=dword:00000000
"NoConfigPage"=dword:00000000
"NoDevMgrPage"=dword:00000000
"NoDispAppearancePage"=dword:00000000
"NoDispBackgroundPage"=dword:00000000
"NoDispCPL"=dword:00000000
"NoDispScrSavPage"=dword:00000000
"NoDispSettingsPage"=dword:00000000
```

```
"NoFileSysPage"=dword:00000000
"NoProfilePage"=dword:00000000
"NoPwdPage"=dword:00000000
"NoSecCPL"=dword:00000000
"NoVirtMemPage"=dword:00000000
"DisableRegistryTools"=dword:00000000
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Policies\WinOldApp

 [END of message text]
  [Already at end of message]
  PINE 3.91   MESSAGE TEXT   Folder: INBOX  Message 178 of 433
END

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Policies\WinOldApp

]
"Disabled"=dword:00000000
"NoRealMode"=dword:00000000
```

GUIDE TO (mostly) HARMLESS HACKING
Beginners' Series #2, Section 3.
Hacking from Windows 3.x, 95 and NT

This lesson will tell you how, armed with even the lamest of on-line services such as America Online and the Windows 95 operating

system, you can
do some fairly serious Internet hacking -- today!

In this lesson we will learn how to:
· -Use secret Windows 95 DOS commands to track down and port surf computers used by famous on-line service providers.
· -Telnet to computers that will let you use the invaluable hacker tools of whois, nslookup, and dig.
· -Download hacker tools such as port scanners and password crackers designed for use with Windows.
· -Use Internet Explorer to evade restrictions on what programs you can run on your school or work computers.

Yes, I can hear jericho and Rogue Agent and all the other Super Duper
hackers on this list laughing. I'll bet already they have quit reading this
and are furiously emailing me flames and making phun of me in 2600 meetings.
Windows hacking? Pooh!
Tell seasoned hackers that you use Windows and they will laugh at you.
They'll tell you to go away and don't come back until you're armed with a
shell account or some sort of Unix on your PC. Actually, I have long shared
their opinion. Shoot, most of the time hacking from Windoze is like using a
1969 Volkswagon to race against a dragster using one of VP Racing's
high-tech fuels.
But there actually is a good reason to learn to hack from Windows. Some of
your best tools for probing and manipulating Windows networks are found only
on Windows NT. Furthermore, with Win 95 you can practice the Registry
hacking that is central to working your will on Win NT servers and the
networks they administer.
In fact, if you want to become a serious hacker, you eventually will have to learn Windows. This is because Windows NT is fast taking over the Internet
from Unix. An IDC report projects that the Unix-based Web server market
share will fall from the 65% of 1995 to only 25% by the year 2000. The

Windows NT share is projected to grow to 32%. This weak future for Unix Web servers is reinforced by an IDC report reporting that market share of all Unix systems is now falling at a compound annual rate of decline of -17% for the foreseeable future, while Windows NT is growing in market share by 20% per year. (Mark Winther, "The Global Market for Public and Private Internet Server Software," IDC #11202, April 1996, 10, 11.)

So if you want to keep up your hacking skills, you're going to have to get wise to Windows. One of these days we're going to be sniggering at all those Unix-only hackers.

Besides, even poor, pitiful Windows 95 now can take advantage of lots of free hacker tools that give it much of the power of Unix.

Since this is a beginners' lesson, we'll go straight to the Big Question:

"All I got is AOL and a Win 95 box. Can I still learn how to hack?"

Yes, yes, yes!

The secret to hacking from AOL/Win 95 -- or from any on-line service that gives you access to the World Wide Web -- is hidden in Win 95's MS-DOS (DOS 7.0).

DOS 7.0 offers several Internet tools, none of which are documented in either the standard Windows or DOS help features. But you're getting the chance to learn these hidden features today.

So to get going with today's lesson, use AOL or whatever lame on-line service you may have and make the kind of connection you use to get on the Web (this will be a PPP or SLIP connection). Then minimize your Web browser and prepare to hack! Next, bring up your DOS window by clicking Start, then Programs, then MS-DOS.

For best hacking I've found it easier to use DOS in a window with a task bar which allows me to cut and paste commands and easily switch between Windows and DOS programs. If your DOS comes up as a full screen, hold

down the Alt
key while hitting enter, and it will go into a window. Then if you are
missing the task bar, click the system menu on the left side of the DOS
window caption and select Toolbar.
Now you have the option of eight TCP/IP utilities to play with: telnet,
arp, ftp, nbtstat, netstat, ping, route, and tracert.
Telnet is the biggie. You can also access the telnet program directly from
Windows. But while hacking you may need the other utilities that can only be
used from DOS, so I like to call telnet from DOS.
With the DOS telnet you can actually port surf almost as well as from a Unix telnet program. But there are several tricks you need to learn in order to
make this work.
First, we'll try out logging on to a strange computer somewhere. This is a
phun thing to show your friends who don't have a clue because it can scare
the heck out them. Honest, I just tried this out on a neighbor. He got so
worried that when he got home he called my husband and begged him to keep me
from hacking his work computer!
To do this (I mean log on to a strange computer, not scare your neighbors)
go to the DOS prompt C:\WINDOWS> and give the command "telnet." This brings
up a telnet screen. Click on Connect, then click Remote System.
This brings up a box that asks you for "Host Name." Type
"whois.internic.net" into this box. Below that it asks for "Port"
and has the default value of "telnet." Leave in "telnet" for the
port selection. Below that is a box for "TermType." I recommend
picking VT100 because, well, just because I like it best.
The first thing you can do to frighten your neighbors and impress your
friends is a "whois." Click on Connect and you will soon get a prompt that
looks like this:

   [vt100]InterNIC>

Then ask your friend or neighbor his or her email address. Then at this
InterNIC prompt, type in the last two parts of your friend's email address.

For example, if the address is "luser@aol.com," type in "aol.com."
Now I'm picking AOL for this lesson because it is really hard to hack.
Almost any other on-line service will be easier.
For AOL we get the answer:

```
  [vt100] InterNIC > whois aol.com
  Connecting to the rs Database . . . . . .
  Connected to the rs Database
  America Online (AOL-DOM)
         12100 Sunrise Valley Drive
         Reston, Virginia 22091
         USA
         Domain Name: AOL.COM
         Administrative Contact:
         O'Donnell, David B  (DBO3)  PMDAtropos@AOL.COM
         703/453-4255 (FAX) 703/453-4102
         Technical Contact, Zone Contact:
         America Online  (AOL-NOC)  trouble@aol.net
         703-453-5862
         Billing Contact:
         Barrett, Joe  (JB4302)  BarrettJG@AOL.COM
         703-453-4160 (FAX) 703-453-4001
         Record last updated on 13-Mar-97.
         Record created on 22-Jun-95.
         Domain servers in listed order:
         DNS-01.AOL.COM   152.163.199.42
         DNS-02.AOL.COM   152.163.199.56
         DNS-AOL.ANS.NET  198.83.210.28
```

These last three lines give the names of some computers that work for
America Online (AOL). If we want to hack AOL, these are a good place to
start.

****
Newbie note: We just got info on three "domain name servers" for AOL.
"Aol.com" is the domain name for AOL, and the domain servers are the
computers that hold information that tells the rest of the Internet how to
send messages to AOL computers and email addresses.
****

****
Evil genius tip: Using your Win 95 and an Internet connection,

you can run a
whois query from many other computers, as well. Telnet to your target
computer's port 43 and if it lets you get on it, give your query.
Example: telnet to nic.ddn.mil, port 43. Once connected type "whois
DNS-01.AOL.COM," or whatever name you want to check out. However, this only
works on computers that are running the whois service on port 43.
Warning: show this trick to your neighbors and they will really be
terrified. They just saw you accessing a US military computer! But it's OK,
nic.ddn.mil is open to the public on many of its ports. Check out its Web
site www.nic.ddn.mil and its ftp site, too -- they are a mother lode of
information that is good for hacking.
****

Next I tried a little port surfing on DNS-01.AOL.COM but couldn't find any
ports open. So it's a safe bet this computer is behind the AOL firewall.

****
Newbie note: port surfing means to attempt to access a computer through
several different ports. A port is any way you get information into or out
of a computer. For example, port 23 is the one you usually use to log into a
shell account. Port 25 is used to send email. Port 80 is for the Web. There
are thousands of designated ports, but any particular computer may be
running only three or four ports. On your home computer your ports include
the monitor, keyboard, and modem.
****

So what do we do next? We close the telnet program and go back to the DOS
window. At the DOS prompt we give the command "tracert 152.163.199.42." Or
we could give the command "tracert DNS-01.AOL.COM." Either way we'll get the

same result. This command will trace the route that a message takes, hopping
from one computer to another, as it travels from my computer to this AOL
domain server computer. Here's what we get:

```
C:\WINDOWS>tracert 152.163.199.42
Tracing route to dns-01.aol.com [152.163.199.42]
over a maximum of 30 hops:
  1 *** Request timed out.
  2   150 ms   144 ms   138 ms  204.134.78.201
  3   375 ms   299 ms   196 ms  glory-cyberport.nm.westnet.net
[204.134.78.33]
  4   271 ms *  201 ms  enss365.nm.org [129.121.1.3]
  5   229 ms   216 ms   213 ms  h4-
0.cnss116.Albuquerque.t3.ans.net
[192.103.74.45]
  6   223 ms   236 ms   229 ms  f2.t112-0.Albuquerque.t3.ans.net
[140.222.112.221]
  7   248 ms   269 ms   257 ms  h14.t64-0.Houston.t3.ans.net
[140.223.65.9]
  8   178 ms   212 ms   196 ms  h14.t80-1.St-Louis.t3.ans.net
[140.223.65.14]
  9   316 ms *  298 ms  h12.t60-0.Reston.t3.ans.net
[140.223.61.9]
 10   315 ms   333 ms   331 ms  207.25.134.189
 11 *** Request timed out.
 12 *** Request timed out.
 13  207.25.134.189  reports: Destination net unreachable.
```

What the heck is all this stuff? The number to the left is the number of
computers the route has been traced through. The "150 ms" stuff is how long,
in thousandths of a second, it takes to send a message to and from that
computer. Since a message can take a different length of time every time you
send it, tracert times the trip three times. The "*" means the trip was
taking too long so tracert said "forget it." After the timing info comes the
name of the computer the message reached, first in a form that is easy for a
human to remember, then in a form -- numbers -- that a computer prefers.
"Destination net unreachable" probably means tracert hit a firewall.
Let's try the second AOL domain server.

```
C:\WINDOWS>tracert  152.163.199.56
Tracing route to dns-02.aol.com [152.163.199.56]
over a maximum of 30 hops:
  1 *** Request timed out.
  2   142 ms   140 ms   137 ms  204.134.78.201
  3   246 ms   194 ms   241 ms  glory-cyberport.nm.westnet.net
[204.134.78.33]
  4   154 ms   185 ms   247 ms  enss365.nm.org [129.121.1.3]
  5   475 ms   278 ms   325 ms  h4-
0.cnss116.Albuquerque.t3.ans.net [192.103.74.45]
  6   181 ms   187 ms   290 ms  f2.t112-0.Albuquerque.t3.ans.net
[140.222.112.221]
  7   162 ms   217 ms   199 ms  h14.t64-0.Houston.t3.ans.net
[140.223.65.9]
  8   210 ms   212 ms   248 ms  h14.t80-1.St-Louis.t3.ans.net
[140.223.65.14]
  9   207 ms *  208 ms  h12.t60-0.Reston.t3.ans.net
[140.223.61.9]
 10   338 ms   518 ms   381 ms  207.25.134.189
 11 *** Request timed out.
 12 *** Request timed out.
 13  207.25.134.189  reports: Destination net unreachable.
```

Note that both tracerts ended at the same computer named h12.t60-0.Reston.t3.ans.net. Since AOL is headquartered in Reston, Virginia, it's a good bet this is a computer that directly feeds stuff into AOL. But we notice that h12.t60-0.Reston.t3.ans.net , h14.t80-1.St-Louis.t3.ans.net, h14.t64-0.Houston.t3.ans.net and Albuquerque.t3.ans.net all have numerical names beginning with 140, and names that end with "ans.net." So it's a good guess that they all belong to the same company. Also, that "t3" in each name suggests these computers are routers on a T3 communications backbone for the Internet.

Next let's check out that final AOL domain server:

```
C:\WINDOWS>tracert 198.83.210.28
Tracing route to dns-aol.ans.net [198.83.210.28]
over a maximum of 30 hops:
  1 *** Request timed out.
  2   138 ms   145 ms   135 ms  204.134.78.201
  3   212 ms   191 ms   181 ms  glory-cyberport.nm.westnet.net
[204.134.78.33]
  4   166 ms   228 ms   189 ms  enss365.nm.org [129.121.1.3]
  5   148 ms   138 ms   177 ms  h4-
0.cnss116.Albuquerque.t3.ans.net [192.103.74.45]
  6   284 ms   296 ms   178 ms  f2.t112-0.Albuquerque.t3.ans.net
[140.222.112.221]
  7   298 ms   279 ms   277 ms  h14.t64-0.Houston.t3.ans.net
[140.223.65.9]
```

8 238 ms 234 ms 263 ms h14.t104-0.Atlanta.t3.ans.net [140.223.65.18]
9 301 ms 257 ms 250 ms dns-aol.ans.net [198.83.210.28]
Trace complete.
Hey, we finally got all the way through to something we can be pretty certain is an AOL box, and it looks like it's outside the firewall! But look at how the tracert took a different path this time, going through Atlanta instead of St. Louis and Reston. But we are still looking at ans.net addresses with T3s, so this last nameserver is using the same network as the others.
Now what can we do next to get luser@aol.com really wondering if you could actually break into his account? We're going to do some port surfing on this last AOL domain name server! But to do this we need to change our telnet settings a bit.
Click on Terminal, then Preferences. In the preferences box you need to check "Local echo." You must do this, or else you won't be able to see everything that you get while port surfing. For some reason, some of the messages a remote computer sends to you won't show up on your Win 95 telnet screen unless you choose the local echo option. However, be warned, in some situations everything you type in will be doubled. For example, if you type in "hello" the telnet screen may show you "heh lelllo o. This doesn't mean you mistyped, it just means your typing is getting echoed back at various intervals.
Now click on Connect, then Remote System. Then enter the name of that last AOL domain server, dns-aol.ans.net. Below it, for Port choose Daytime. It will send back to you the day of the week, date and time of day in its time zone.
Aha! We now know that dns-aol.ans.net is exposed to the world,

with at least one open port, heh, heh. It is definitely a prospect for further port
surfing. And now your friend is wondering, how did you get something out of
that computer?

****
Clueless newbie alert: If everyone who reads this telnets to the daytime
port of this computer, the sysadmin will say "Whoa, I'm under heavy attack
by hackers!!! There must be some evil exploit for the daytime service! I'm
going to close this port pronto!" Then you'll all email me complaining the
hack doesn't work. Please, try this hack out on different computers and
don't all beat up on AOL.
****

Now let's check out that Reston computer. I select Remote Host again and
enter the name h12.t60-0.Reston.t3.ans.net. I try some port surfing without
success. This is a seriously locked down box! What do we do next?
So first we remove that "local echo" feature, then we telnet back to
whois.internic. We ask about this ans.net outfit that offers links to AOL:

```
[vt100] InterNIC > whois ans.net
Connecting to the rs Database . . . . . .
Connected to the rs Database
ANS CO+RE Systems, Inc. (ANS-DOM)
   100 Clearbrook Road
   Elmsford, NY 10523
   Domain Name: ANS.NET
   Administrative Contact:
  Hershman, Ittai  (IH4)  ittai@ANS.NET
  (914) 789-5337
   Technical Contact:
  ANS Network Operations Center  (ANS-NOC)  noc@ans.net
  1-800-456-6300
   Zone Contact:
  ANS Hostmaster  (AH-ORG)  hostmaster@ANS.NET
  (800)456-6300  fax: (914)789-5310
   Record last updated on 03-Jan-97.
   Record created on 27-Sep-90.
```

Domain servers in listed order:
NS.ANS.NET 192.103.63.100
NIS.ANS.NET 147.225.1.2

Now if you wanted to be a really evil hacker you could call that 800 number and try to social engineer a password out of somebody who works for this network. But that wouldn't be nice and there is nothing legal you can do with ans.net passwords. So I'm not telling you how to social engineer those passwords.

Anyhow, you get the idea of how you can hack around gathering info that leads to the computer that handles anyone's email.

So what else can you do with your on-line connection and Win 95? Well... should I tell you about killer ping? It's a good way to lose your job and end up in jail. You do it from your Windows DOS prompt. Find the gory details in the GTMHH Vol.2 Number 3, which is kept in one of our archives listed at the end of this lesson. Fortunately most systems administrators have patched things nowadays so that killer ping won't work.

But just in case your ISP or LAN at work or school isn't protected, don't test it without your sysadmin's approval!

Then there's ordinary ping, also done from DOS. It's sort of like tracert, but all it does is time how long a message takes from one computer to another, without telling you anything about the computers between yours and the one you ping.

Other TCP/IP commands hidden in DOS include:

· Arp IP-to-physical address translation tables
· Ftp File transfer protocol. This one is really lame. Don't use it. Get a shareware Ftp program from one of the download sites listed below.
· Nbtstat Displays current network info -- super to use on your own ISP
· Netstat Similar to Nbstat
· Route Controls router tables -- router hacking is considered extra elite.

Since these are semi-secret commands, you can't get any details on how to

use them from the DOS help menu. But there are help files hidden away for
these commands:

· For arp, nbtstat, ping and route, to get help just type in the command
and hit enter.
· For netstat you have to give the command "netstat ?" to get help.
· Telnet has a help option on the tool bar.

I haven't been able to figure out a trick to get help for the ftp command.

Now suppose you are at the point where you want to do serious hacking that
requires commands other than these we just covered, but you don't want to
use Unix. Shame on you! But, heck, even though I usually have one or two
Unix shell accounts plus Walnut Creek Slackware on my home computer, I still
like to hack from Windows. This is because I'm ornery. So you can be ornery,
too.

So what is your next option for doing serious hacking from Windows?

How would you like to crack Win NT server passwords? Download the free Win
95 program NTLocksmith, an add-on program to NTRecover that allows for the
changing of passwords on systems where the administrative password has been
lost. It is reputed to work 100% of the time. Get both NTLocksmith and
NTRecover -- and lots more free hacker tools -- from http://www.sysinternals.com.

****

You can go to jail warning: If you use NTRecover to break into someone
else's system, you are just asking to get busted.

****

How would you like to trick your friends into thinking their NT box has
crashed when it really hasn't? This prank program can be downloaded from
http://www.osr.com/insider/insdrcod.htm.

But by far the deadliest hacking tool that runs on Windows can be

downloaded from, guess what?
http://home.microsoft.com
That deadly program is Internet Explorer 3.0. Unfortunately, this program is even better for letting other hackers break into your home computer and do
stuff like make your home banking program (e.g. Quicken) transfer your life
savings to someone in Afghanistan.
But if you're aren't brave enough to run Internet Explorer to surf the Web, you can still use it to hack your own computer, or other computers on your
LAN. You see, Internet Explorer is really an alternate Windows shell which
operates much like the Program Manager and Windows Explorer that come with
the Win 94 and Win NT operating systems.
Yes, from Internet Explorer you can run any program on your own computer. Or any program to which you have access on your LAN.

****
Newbie note: A shell is a program that mediates between you and the
operating system. The big deal about Internet Explorer being a Windows shell
is that Microsoft never told anyone that it was in fact a shell. The
security problems that are plaguing Internet Explorer are mostly a
consequence of it turning out to be a shell. By contrast, the Netscape and
Mosaic Web browsers are not shells. They also are much safer to use.
****

To use Internet Explorer as a Windows shell, bring it up just like you would if you were going to surf the Web.
Kill the program's attempt to establish
an Internet connection -- we don't want to do anything crazy, do we?
Then in the space where you would normally type in the URL you want to surf,
instead type in c:.
Whoa, look at all those file folders that come up on the screen. Look
familiar? It's the same stuff your Windows Explorer would show you. Now for
fun, click "Program Files" then click "Accessories" then click

"MSPaint."
All of a sudden MSPaint is running. Now paint your friends who are watching this hack very surprised.
Next close all that stuff and get back to Internet Explorer. Click on the
Windows folder, then click on Regedit.exe to start it up. Export the
password file (it's in HKEY_CLASSES_ROOT). Open it in Word Pad. Remember,
the ability to control the Registry of a server is the key to controlling
the network it serves. Show this to your next door neighbor and tell her
that you're going to use Internet Explorer to surf her password files. In a
few hours the Secret Service will be fighting with the FBI on your front
lawn over who gets to try to bust you. OK, only kidding here.
So how can you use Internet Explorer as a hacking tool? One way is if you
are using a computer that restricts your ability to run other programs on
your computer or LAN. Next time you get frustrated at your school or library
computer, check to see if it offers Internet Explorer. If it does, run it
and try entering disk drive names. While C: is a common drive on your home
computer, on a LAN you might get results by putting in R: or Z: or any other
letter of the alphabet.
Next cool hack: try automated port surfing from Windows! Since there are
thousands of possible ports that may be open on any computer, it could take
days to fully explore even just one computer by hand. A good answer to this
problem is the NetCop automated port surfer, which can be found at
http://www.netcop.com/.
Now suppose you want to be able to access the NTFS file system that Windows NT uses from
a Win 95 or even DOS platform? This can be useful if you are wanting to use Win 95 as a platform to hack an NT system.
http://www.sysinternals.com/ntfsdos.htm offers a program that allows Win 95
and DOS to recognize and mount NTFS drives for transparent

access.
Hey, we are hardly beginning to explore all the wonderful Windows hacking
tools out there. It would take megabytes to write even one sentence about
each and every one of them. But you're a hacker, so you'll enjoy exploring
dozens more of these nifty programs yourself. Following is a list of sites
where you can download lots of free and more or less harmless programs that
will help you in your hacker career:

ftp://ftp.cdrom.com
ftp://ftp.coast.net
http://hertz.njit.edu/%7ebxg3442/temp.html
http://www.alpworld.com/infinity/void-neo.html
http://www.danworld.com/nettools.html
http://www.eskimo.com/~nwps/index.html
http://www.geocities.com/siliconvalley/park/2613/links.html
http://www.ilf.net/Toast/
http://www.islandnet.com/~cliffmcc
http://www.simtel.net/simtel.net
http://www.supernet.net/cwsapps/cwsa.html
http://www.trytel.com/hack/
http://www.tucows.com
http://www.windows95.com/apps/
http://www2.southwind.net/%7emiker/hack.html

GUIDE TO (mostly) HARMLESS HACKING
Beginners' Series #3 Part 1
How to Get a *Good* Shell Account

In this Guide you will learn how to:
· -tell whether you may already have a Unix shell account
· -get a shell account
· -log on to your shell account

You've fixed up your Windows box to boot up with a lurid hacker logo. You've renamed "Recycle Bin" "Hidden Haxor Secrets." When you run Netscape or Internet Explorer, instead of that boring corporate logo, you have a full-color animated Mozilla destroying New York City. Now your friends and neighbors are terrified and impressed. But in your heart of hearts you know Windows is scorned by elite hackers. You keep on seeing their hairy exploit programs and almost every one of them requires the Unix operating system. You realize that when it comes to messing with computer networks, Unix is the most powerful operating system on the planet. You have developed a burning desire to become one of those Unix wizards yourself. Yes, you're ready for the next step. You're ready for a shell account. SHELL ACCOUNT!!!!

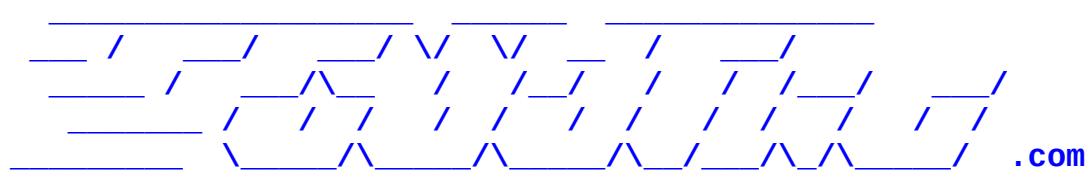
****
Newbie note: A shell account allows you to use your home computer as a terminal on which you can give commands to a computer running Unix. The "shell" is the program that translates your keystrokes into Unix commands. With the right shell account you can enjoy the use of a far more powerful workstation than you could ever dream of affording to own yourself. It also is a great stepping stone to the day when you will be running some form of Unix on your home computer.
****

Once upon a time the most common way to get on the Internet was through a Unix shell account. But nowadays everybody and his brother are on

the
Internet. Almost all these swarms of surfers want just two things: the Web,
and email. To get the pretty pictures of today's Web, the average Internet
consumer wants a mere PPP (point to point) connection account. They wouldn't
know a Unix command if it hit them in the snoot. So nowadays almost the only
people who want shell accounts are us wannabe hackers.
The problem is that you used to be able to simply phone an ISP, say "I'd
like a shell account," and they would give it to you just like that. But
nowadays, especially if you sound like a teenage male, you'll run into
something like this:
ISP guy: "You want a shell account? What for?"
Hacker dude: "Um, well, I like Unix."
"Like Unix, huh? You're a hacker, aren't you!" Slam, ISP guy hangs up on
you.
So how do you get a shell account? Actually, it's possible you may already
have one and not know it. So first we will answer the question, how do you
tell whether you may already have a shell account? Then, if you are certain
you don't have one, we'll explore the many ways you can get one, no matter
what, from anywhere in the world.
How Do I Know Whether I Already Have a Shell Account?
First you need to get a program running that will connect you to a shell
account. There are two programs with Windows 95 that will do this, as well
as many other programs, some of which are excellent and free.
First we will show you how to use the Win 95 Telnet program because you
already have it and it will always work. But it's a really limited program,
so I suggest that you use it only if you can't get the Hyperterminal
program to work.
1) Find your Telnet program and make a shortcut to it on your desktop.
One way is to click Start, then Programs, then Windows Explorer.

When Explorer is running, first resize it so it doesn't cover the entire
desktop.
Then click Tools, then Find, then "Files or Folders."
Ask it to search for "Telnet."
It will show a file labeled C:\windows\telnet (instead of C:\ it may have
another drive). Right click on this file.
This will bring up a menu that includes the option "create shortcut."
Click on "create shortcut" and then drag the shortcut to the desktop and
drop it.
Close Windows Explorer.
2) Depending on how your system is configured, there are two ways to connect
to the Internet. The easy way is to skip to step three. But if it fails, go
back to this step. Start up whatever program you use to access the Internet.
Once you are connected, minimize the program. Now try step three.
3) Bring up your Telnet program by double clicking on the shortcut you just made.
First you need to configure Telnet so it actually is usable. On the
toolbar click "terminal," then "preferences," then "fonts." Choose "Courier
New," "regular" and 8 point size. You do this because if you have too big a
font, the Telnet program is shown on the screen so big that the cursor from
your shell program can end up being hidden off the screen. OK, OK, you can
pick other fonts, but make sure that when you close the dialog box that the
Telnet program window is entirely visible on the screen. Now why would there
be options that make Telnet impossible to use? Ask Microsoft.
Now go back to the task bar to click Connect, then under it click "Remote
system." This brings up another dialog box.
Under "host name" in this box type in the last two parts of your email
address. For example, if your email address is jane_doe@boring.ISP.com, type
"ISP.com" for host name.
Under "port" in this box, leave it the way it is, reading

"telnet."
Under "terminal type," in this box, choose "VT100."
Then click the Connect button and wait to see what happens.
If the connection fails, try entering the last three parts of your email
address as the host, in this case "boring.ISP.com."
Now if you have a shell account you should next get a message asking you to login. It may
look something like this:
Welcome to Boring Internet Services, Ltd.
Boring.com S9 - login: cmeinel
Password:
Linux 2.0.0.
Last login: Thu Apr 10 14:02:00 on ttyp5 from pm20.kitty.net.
sleepy:~$
If you get something like this you are in definite luck. The important thing here, however,
is that the computer used the word "login" to get you
started. If is asked for anything else, for example "logon," this is not a
shell account.
As soon as you login, in the case of Boring Internet Services you have a
Unix shell prompt on your screen. But instead of something this simple you
may get something like:
BSDI BSD/OS 2.1 (escape.com) (ttyrf)
login: galfina
Password:
Last login: Thu Apr 10 16:11:37 from fubar.net
Copyright 1992, 1993, 1994, 1995 Berkeley Software Design, Inc.
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
The Regents of the University of California. All rights reserved.



PLEASE NOTE:
Multiple Logins and Simultaneous Dialups From Different Locations Are

NOT Permitted at Escape Internet Access.

_
Enter your terminal type, RETURN for vt100, ? for list:
Setting terminal type to vt100.
Erase is backspace.

  MAIN
Escape Main Menu

[05:45PM]--
 ==> H) HELP   Help & Tips for the Escape Interface. (M)
 I) INTERNET   Internet Access & Resources (M)
 U) USENETMUsenet Conferences (Internet Distribution) (M)
 L) LTALK Escape Local Communications Center (M)
 B) BULLETINS Information on Escape, Upgrades, coming events.
(M)
 M) MAIL   Escape World Wide and Local Post Office (M)
 F) HOME   Your Home Directory (Where all your files end up)
 C) CONFIG Config your user and system options (M)
 S) SHELL The Shell (Unix Environment) [TCSH]
 X) LOGOUT Leave System
 BACK MAIN HOME MBOX ITALK LOGOUT
----[Mesg: Y]-----------[TAB key toggles menus]-------
[Connected:
0:00]---
CMD>
In this case you aren't in a shell yet, but you can see an option
on the
menu to get to a shell. So hooray, you are in luck, you have a
shell
account. Just enter "S" and you're in.
Now depending on the ISP you try out, there may be all sorts of
different
menus, all designed to keep the user from having to ever stumble
across the
shell itself. But if you have a shell account, you will probably
find the
word "shell" somewhere on the menu.

If you don't get something obvious like this, you may have to do
the single most humiliating
thing a wannabe hacker will ever do. Call tech support and ask
whether you have a shell account
and, if so, how to login. It may be
that they just want to make it really, really hard for you to
find your

shell account.
Now personally I don't care for the Win 95 Telnet program. Fortunately there are many other
ways to check whether you have a shell account. Here's how to use the Hyperterminal program,
which, like Telnet, comes free with the
Windows 95 operating system. This requires a different kind of connection.
Instead of a PPP connection we will do a simple phone dialup, the same sort
of connection you use to get on most computer bulletin board systems (BBS).
1) First, find the program Hyperteminal and make a shortcut to your desktop.
This one is easy to find. Just click Start, then Programs, then Accessories.You'll find
Hyperterminal on the accessories menu. Clicking on it will bring up a window with a bunch
of icons. Click on the one labeled
"hyperterminal.exe."
2) This brings up a dialog box called "New Connection." Enter the name of
your local dialup, then in the next dialog box enter the phone dialup number
of your ISP.
3) Make a shortcut to your desktop.
4) Use Hyperterminal to dial your ISP. Note that in this case you are making a direct
phone call to your shell account rather than trying to reach it through a PPP connection.
Now when you dial your ISP from Hyperterminal you might get a bunch of
really weird garbage scrolling down your screen. But don't give up. What is
happening is your ISP is trying to set up a PPP connection with Hyperterminal. That is
the kind of connection you need in order to get pretty pictures on the Web. But Hyperterminal
doesn't understand PPP.
Unfortunately I've have not been able to figure out why this happens
sometimes or how to stop it. But the good side of this picture is that the
problem may go away the next time you use Hyperterminal to connect to your
ISP. So if you dial again you may get a login sequence. I've found it often

helps to wait a few days and try again. Of course you can complain to tech
support at your ISP. But it is likely that they won't have a clue on what
causes their end of things to try to set up a PPP session with your
Hyperterminal connection. Sigh.
But if all goes well, you will be able to log in. In fact, except for the
PPP attempt problem, I like the Hyperterminal program much better than Win
95 Telnet. So if you can get this one to work, try it out for awhile. See if
you like it, too.
There are a number of other terminal programs that are really good for
connecting to your shell account. They include Qmodem, Quarterdeck Internet
Suite, and Bitcom. Jericho recommends Ewan, a telnet program which also runs on Windows 95.
Ewan is free, and has many more features than either Hyperterminal or Win 95 Telnet. You may
download it from jericho's ftp site
at sekurity.org in the /utils directory.
OK, let's say you have logged into your ISP with your favorite program. But perhaps it still
isn't clear whether you have a shell account. Here's your
next test. At what you hope is your shell prompt, give the command "ls
-alF." If you have a real, honest-to-goodness shell account, you should get
something like this:

```
> ls -alF
total 87
drwx--x--x5 galfina  user1024 Apr 22 21:45 ./
drwxr-xr-x  380 root wheel   6656 Apr 22 18:15 ../
-rw-r--r--1 galfina  user2793 Apr 22 17:36 .README
-rw-r--r--1 galfina  user 635 Apr 22 17:36 .Xmodmap
-rw-r--r--1 galfina  user 624 Apr 22 17:36 .Xmodmap.USKBD
-rw-r--r--1 galfina  user 808 Apr 22 17:36 .Xresources
drwx--x--x2 galfina  user 512 Apr 22 17:36 www/
```

etc.
This is the listing of the files and directories of your home directory.
Your shell account may give you a different set of directories and files
than this (which is only a partial listing). In any case, if you

see
anything that looks even a little bit like this, congratulations, you
already have a shell account!

****
Newbie note: The first item in that bunch of dashes and letters in front of
the file name tells you what kind of file it is. "d" means it is a
directory, and "-" means it is a file. The rest are the permissions your
files have. "r" = read permission, "w" = write permission, and "x" = execute
permission (no, "execute" has nothing to do with murdering files, it means
you have permission to run the program that is in this file). If there is a
dash, it means there is no permission there.
The symbols in the second, third and fourth place from the left are the
permissions that you have as a user, the following three are the permissions
everyone in your designated group has, and the final three are the
permissions anyone and everyone may have. For example, in galfina's
directory the subdirectory "www/" is something you may read, write and
execute, while everyone else may only execute. This is the directory where
you can put your Web page. The entire world may browse ("execute") your Web
page. But only you can read and write to it.
If you were to someday discover your permissions looking like:
 drwx--xrwx newbie user 512 Apr 22 17:36 www/
Whoa, that "w" in the third place from last would mean anyone with an
account from outside your ISP can hack your Web page!
****

Another command that will tell you whether you have a shell account is
"man." This gives you an online Unix manual. Usually you have to give the
man command in the form of "man <command>" where <command> is the name of

the Unix command you want to study. For example, if you want to know all
the different ways to use the "ls" command, type "man ls" at the prompt.
On the other hand, here is an example of something that, even though it is
on a Unix system, is not a shell account:
BSDI BSD/386 1.1 (dub-gw-2.compuserve.com) (ttyp7)
Connected to CompuServe
Host Name: cis
Enter choice (LOGON, HELP, OFF):
The immediate tip-off that this is not a shell account is that it asks you
to "logon" instead of "login:"

How to Get a Shell Account

What if you are certain that you don't already have a shell account? How do you find an ISP
that will give you one?
The obvious place to start is your phone book. Unless you live in a really
rural area or in a country where there are few ISPs, there should be a
number of companies to choose from.
So here's your problem. You phone Boring ISP, Inc. and say, "I'd like a
shell account." But Joe Dummy on the other end of the phone says, "Shell?
What's a shell account?" You say "I want a shell account. SHELL ACCOUNT!!!"
He says, "Duh?" You say "Shell account. SHELL ACCOUNT!!!" He says, "Um, er,
let me talk to my supervisor." Mr. Uptight Supervisor gets on the phone. "We
don't give out shell accounts, you dirty &%$*# hacker."
Or, worse yet, they claim the Internet access account they are giving you a shell account
but you discover it isn't one.
To avoid this embarrassing scene, avoid calling big name ISPs. I can
guarantee you, America Online, Compuserve and Microsoft Network don't give
out shell accounts.
What you want to find is the seediest, tiniest ISP in town. The one that
specializes in pasty-faced customers who stay up all night

playing MOOs and
MUDs. Guys who impersonate grrrls on IRC. Now that is not to say that MUD
and IRC people are typically hackers. But these definitely are your serious
Internet addicts. An ISP that caters to people like that probably also
understands the kind of person who wants to learn Unix inside and out.
So you phone or email one of these ISPs on the back roads of the Net and
say, "Greetings, d00d! I am an evil haxor and demand a shell account
pronto!"
No, no, no! Chances are you got the owner of this tiny ISP on the other end of the line.
He's probably a hacker himself. Guess what? He loves to hack
but he doesn't want hackers (or wannabe hackers) for customers. He doesn't
want a customer who's going to be attracting email bombers and waging hacker
war and drawing complaints from the sysadmins on whom this deadly dude has
been testing exploit code.
So what you do is say something like "Say, do you offer shell accounts? I
really, really like to browse the Web with lynx. I hate waiting five hours
for all those pretty pictures and Java applets to load. And I like to do
email with Pine. For newsgroups, I luuuv tin!"
Start out like this and the owner of this tiny ISP may say something like,
"Wow, dude, I know what you mean. IE and Netscape really s***! Lynx uber
alles! What user name would you like?"
At this point, ask the owner for a guest account. As you will learn below,
some shell accounts are so restricted that they are almost worthless.
But let's say you can't find any ISP within reach of a local phone call that
will give you a shell account. Or the only shell account you can get is
worthless. Or you are well known as a malicious hacker and you've been
kicked off every ISP in town. What can you do?

Your best option is to get an account on some distant ISP, perhaps even in another country. Also, the few medium size ISPs that offer shell accounts (for example, Netcom) may even have a local dialup number for you. But if they don't have local dialups, you can still access a shell account located *anywhere* in the world by setting up a PPP connection with your local dialup ISP, and then accessing your shell account using a telnet program on your home computer.

****

Evil Genius Tip: Sure, you can telnet into your shell account from another ISP account. But unless you have software that allows you to send your password in an encrypted form, someone may sniff your password and break into your account. If you get to be well known in the hacker world, lots of other hackers will constantly be making fun of you by sniffing your password. Unfortunately, almost all shell accounts are set up so you must expose your password to anyone who has hidden a sniffer anywhere between the ISP that provides your PPP connection and your shell account ISP. One solution is to insist on a shell account provider that runs ssh (secure shell).

****

So where can you find these ISPs that will give you shell accounts? One good source is http://www.celestin.com/pocia/. It provides links to Internet Service Providers categorized by geographic region. They even have links to allow you to sign up with ISPs serving the Lesser Antilles!

****

Evil Genius tip: Computer criminals and malicious hackers will often get a guest account on a distant ISP and do their dirty work during the few hours

this guest account is available to them. Since this practice provides the
opportunity to cause so much harm, eventually it may become really hard to
get a test run on a guest account.
****

But if you want to find a good shell account the hacker way, here's what you do. Start with a
list of your favorite hacker Web sites. For example, let's try http://ra.nilenet.com/~mjl/hacks/codez.htm.
You take the beginning part of the URL (Uniform Resource Locator) as your
starting point. In this case it is "http://ra.nilenet.com." Try surfing to
that URL. In many cases it will be the home page for that ISP. It should
have instructions for how to sign up for a shell account. In the case of
Nile Net we strike hacker gold:
 Dial-up Accounts and Pricing
NEXUS Accounts
NEXUS Accounts include: Access to a UNIX Shell, full
Internet access, Usenet newsgroups, 5mb of FTP and/or
WWW storage space, and unlimited time.
One Time Activation Fee: $20.00
Monthly Service Fee: $19.95 or
Yearly Service Fee: $199.95
Plus which they make a big deal over freedom of online speech. And they host a great hacker
page full of these Guides to (mostly) Harmless Hacking!

How to Login to Your Shell Account

Now we assume you finally have a guest shell account and are ready to test
drive it. So now we need to figure out how to login. Now all you hacker
geniuses reading this, why don't you just forget to flame me for telling
people how to do something as simple as how to login. Please remember that
everyone has a first login. If you have never used Unix, this first time can
be intimidating. In any case, if you are a Unix genius you have no business
reading this Beginners' Guide. So if you are snooping around here

looking
for flamebait, send your flames to /dev/null.

****
Newbie note: "Flames" are insulting, obnoxious rantings and ravings done by
people who are severely lacking in social skills and are a bunch of &$%@#!!
but who think they are brilliant computer savants. For example, this newbie
note is my flame against &$%@#!! flamers.
 "/dev/null" stands for "device null." It is a file name in a Unix operating
system. Any data that is sent to /dev/null is discarded. So when someone
says they will put something in "/dev/null" that means they are sending it
into permanent oblivion.
****

The first thing you need to know in order to get into your shell account is your user name
and password. You need to get that information from the ISP that has just signed you up. The second thing you need to remember is that
Unix is "case sensitive." That means if your login name is "JoeSchmoe" the
shell will think "joeschmoe" is a different person than "JoeSchmoe" or
"JOESCHMOE."
OK, so you have just connected to your shell account for the first time. You may see all
sorts of different stuff on that first screen. But the one thing you will always see is the prompt:
 login:
Here you will type in your user name.
In response you will always be asked :
 Password:
Here you type in your password.
After this you will get some sort of a prompt. It may be a simple as:
 %
or
 $
or
 >
Or as complicated as:

sleepy:~$
Or it may even be some sort of complicated menu where you have to choose a
"shell" option before you get to the shell prompt.
Or it may be a simple as:
#

****

Newbie note: The prompt "#" usually means you have the superuser powers of
a "root" account. The Unix superuser has the power to do *anything* to the
computer. But you won't see this prompt unless either the systems
administrator has been really careless -- or someone is playing a joke on
you. Sometimes a hacker thinks he or she has broken into the superuser
account because of seeing the "#" prompt. But sometimes this is just a trick
the sysadmin is playing. So the hacker goes playing around in what he or she
thinks is the root account while the sysadmin and his friends and the police
are all laughing at the hacker.

****

Ready to start hacking from your shell account? Watch out, it may be so
crippled that it is worthless for hacking. Or, it may be pretty good, but
you might inadvertently do something to get you kicked off. To avoid these
fates, be sure to read Beginners' Series #3 Part 2 of How to Get a *Good*
Shell Account, coming out tomorrow.

In case you were wondering about all the input from jericho in this Guide,
yes, he was quite helpful in reviewing it and making suggestions. Jericho is
a security consultant runs his own Internet host, obscure.sekurity.org.

Thank you, jericho@dimensional.com, and happy hacking!

GUIDE TO (mostly) HARMLESS HACKING

Beginners' Series #3 Part 2
How to Get a *Good* Shell Account

In this section you will learn:
· -how to explore your shell account
· -Ten Meinel Hall of Fame Shell Account Exploration Tools
· -how to decide whether your shell account is any good for hacking
· -Ten Meinel Hall of Fame LAN and Internet Exploration Tools
· -Meinel Hall of Infamy Top Five Ways to Get Kicked out of Your Shell Account

How to Explore Your Shell Account

So you're in your shell account. You've tried the "ls -alF" command and are pretty sure this really, truly is a shell account. What do you do next?
A good place to start is to find out what kind of shell you have. There are many shells, each of which has slightly different ways of working. To do this, at your prompt give the command "echo $SHELL." Be sure to type in the same lower case and upper case letters. If you were to give the command "ECHO $shell," for example, this command won't work.
If you get the response:
/bin/sh
That means you have the Bourne shell.
If you get:
/bin/bash
Then you are in the Bourne Again (bash) shell.
If you get:
/bin/ksh
You have the Korn shell.
If the "echo $SHELL" command doesn't work, try the command "echo $shell," remembering to use lower case for "shell." This will likely get you the answer:
/bin/csh
This means you have the C shell.
Why is it important to know which shell you have? For right now,

you'll want a shell that is
easy to use. For example, when you make a mistake in typing, it's nice to hit the backspace
key and not see ^H^H^H on your screen. Later, though, for running those super hacker exploits,
the C shell may be better for you.
Fortunately, you may not be stuck with whatever shell you have when you log in. If your shell
account is any good, you will have a choice of shells.
Trust me, if you are a beginner, you will find bash to be the easiest shell to use. You may be
able to get the bash shell by simply typing the word
"bash" at the prompt. If this doesn't work, ask tech support at your ISP for
a shell account set up to use bash. A great book on using the bash shell is
Learning the Bash Shell, by Cameron Newham and Bill Rosenblatt, published
by O'Reilly.
If you want to find out what other shells you have the right to use, try
"csh" to get the C shell; "ksh" to get the Korn shell, "sh" for Bourne
shell, "tcsh" for the Tcsh shell, and "zsh" for the Zsh shell. If you don't
have one of them, when you give the command to get into that shell you will
get back the answer "command not found."
Now that you have chosen your shell, the next thing is to explore. See what riches your ISP
has allowed you to use. For that you will want to learn, and I mean *really learn* your most
important Unix commands and auxiliary
programs. Because I am supreme arbiter of what goes into these Guides, I get
to decide what the most important commands are. Hmm, "ten" sounds like a
famous number. So you're going to get the:
Ten Meinel Hall of Fame Shell Account Exploration Tools
1) man <command name>
This magic command brings up the online Unix manual. Use it on each of the commands below,
today! Wonder what all the man command options are? Try the
"man -k" option.
2) ls
Lists files. Jericho suggests "Get people in the habit of using
"ls -alF".

This will come into play down the road for security-conscious users." You'll see a huge list
of files that you can't see with the "ls" command alone, and lots of details. If you see such
a long list of files that they scroll off the terminal screen, one way to solve the problem is
to use "ls -alF|more."
3) pwd
Shows what directory you are in.
4) cd <directory>
Changes directories. Kewl directories to check out include /usr, /bin and
/etc. For laughs, jericho suggests exploring in /tmp.
5) more <filename>
This shows the contents of text files. Also you might be able to find "less" and "cat" which
are similar commands.
6) whereis <program name>
Think there might be a nifty program hidden somewhere? Maybe a game you
love? This will find it for you. Similar commands are "find" and "locate."
Try them all for extra fun.
7) vi
An editing program. You'll need it to make your own files and when you start programming
while in your shell account. You can use it to write a really lurid file for people to read when they finger you. Or try "emacs." It's
another editing program and IMHO more fun than vi. Other editing programs
you may find include "ed" (an ancient editing program which I have used to
write thousands of lines of Fortran 77 code), "ex," "fmt," "gmacs,"
"gnuemacs," and "pico."
8) grep
Extracts information from files, especially useful for seeing what's in
syslog and shell log files. Similar commands are "egrep," "fgrep," and
"look."
9) chmod <filename>
Change file permissions.
10) rm <filename>
Delete file. If you have this command you should also find "cp" for copy

file, and "mv" for move file.

How to Tell Whether Your Shell Account Is any Good for Hacking

Alas, not all shell accounts are created equal. Your ISP may have decided to cripple your budding hacker career by forbidding your access to important tools. But you absolutely must have access to the top ten tools listed above. In addition, you will need tools to explore both your ISP's local area network (LAN) and the Internet. So in the spirit of being Supreme Arbiter of Haxor Kewl, here are my:

Ten Meinel Hall of Fame LAN and Internet Exploration Tools

1) telnet <hostname> <port number or name>

If your shell account won't let you telnet into any port you want either on its LAN or the Internet, you are totally crippled as a hacker. Dump your ISP now!

2) who

Shows you who else is currently logged in on your ISP's LAN. Other good commands to explore the other users on your LAN are "w," "rwho, " "users."

3) netstat

All sorts of statistics on your LAN, including all Internet connections. For real fun, try "netstat -r" to see the kernel routing table. However, jericho warns "Be careful. I was teaching a friend the basics of summing up a Unix system and I told her to do that and 'ifconfig'. She was booted off the system the next day for 'hacker suspicion' even though both are legitimate commands for users."

4) whois <hostname>

Get lots of information on Internet hosts outside you LAN.

5) nslookup

Get a whole bunch more information on other Internet hosts.

6) dig

Even more info on other Internet hosts. Nslookup and dig are not redundant. Try to get a shell account that lets you use both.

7) finger

Not only can you use finger inside your LAN. It will sometimes

get you
valuable information about users on other Internet hosts.
8) ping
Find out if a distant computer is alive and run diagnostic tests -- or just plain be a
meanie and clobber people with pings. (I strongly advise *against* using ping to annoy or harm others.)
9) traceroute
Kind of like ping with attitude. Maps Internet connections, reveals routers and boxes
running firewalls.
10) ftp
Use it to upload and download files to and from other computers.
If you have all these tools, you're in great shape to begin your hacking
career. Stay with your ISP. Treat it well.
Once you get your shell account, you will probably want to supplement the
"man" command with a good Unix book . Jericho recommends _Unix in a Nutshell_ published
by O'Reilly. "It is the ultimate Unix command reference, and only costs 10 bucks.
O'Reilly r00lz."

How to Keep from Losing Your Shell Account

So now you have a hacker's dream, an account on a powerful computer running Unix. How do
you keep this dream account? If you are a hacker, that is not so easy. The problem is that
you have no right to keep that account. You can
be kicked off for suspicion of being a bad guy, or even if you become
inconvenient, at the whim of the owners.
Meinel Hall 'O Infamy

Top Five Ways to Get Kicked out of Your Shell Account

1) Abusing Your ISP
Let's say you are reading Bugtraq and you see some code for a new way to
break into a computer. Panting with excitement, you run emacs and paste in
the code. You fix up the purposely crippled stuff someone put in to keep
total idiots from running it. You tweak it until it runs under your flavor

of Unix. You compile and run the program against your own ISP. It works! You
are looking at that "#" prompt and jumping up and down yelling "I got root!
I got root!" You have lost your hacker virginity, you brilliant dude, you!
Only, next time you go to log in, your password doesn't work. You have been
booted off your ISP. NEVER, NEVER ABUSE YOUR ISP!

****
You can go to jail warning: Of course, if you want to break into another
computer, you must have the permission of the owner. Otherwise you are
breaking the law.
****

2) Ping Abuse.
Another temptation is to use the powerful Internet connection of your shell account
(usually a T1 or T3) to ping the crap out of the people you don't like. This is especially common on Internet Relay Chat. Thinking of ICBMing
or nuking that dork? Resist the temptation to abuse ping or any other
Internet Control Message Protocol attacks. Use ping only as a diagnostic
tool, OK? Please? Or else!
3) Excessive Port Surfing
Port surfing is telnetting to a specific port on another computer. Usually
you are OK if you just briefly visit another computer via telnet, and don't
go any further than what that port offers to the casual visitor. But if you
keep on probing and playing with another computer, the sysadmin at the
target computer will probably email your sysadmin records of your little
visits. (These records of port visits are stored in "messages," and
sometimes in "syslog" depending on the configuration of your target computer
-- and assuming it is a Unix system.)
Even if no one complains about you, some sysadmins habitually check the

shell log files that keep a record of everything you or any other user on
the system has been doing in their shells. If your sysadmin sees a pattern
of excessive attention to one or a few computers, he or she may assume you
are plotting a break-in. Boom, your password is dead.
4) Running Suspicious Programs
If you run a program whose primary use is as a tool to commit computer
crime, you are likely to get kicked off your ISP. For example, many ISPs
have a monitoring system that detects the use of the program SATAN. Run
SATAN from your shell account and you are history.

****
Newbie note: SATAN stands for Security Administration Tool for Analyzing
Networks. It basically works by telnetting to one port after another of the
victim computer. It determines what program (daemon) is running on each
port, and figures out whether that daemon has a vulnerability that can be
used to break into that computer. SATAN can be used by a sysadmin to figure
out how to make his or her computer safe. Or it may be just as easily used
by a computer criminal to break into someone else's computer.
****

5) Storing Suspicious Programs
It's nice to think that the owners of your ISP mind their own business. But they don't.
They snoop in the directories of their users. They laugh at your email. OK, maybe they are really high-minded and resist the temptation to
snoop in your email. But chances are high that they will snoop in your shell
log files that record every keystroke you make while in your shell account.
If they don't like what they see, next they will be prowling your program
files.
One solution to this problem is to give your evil hacker tools innocuous

names. For example, you could rename SATAN to ANGEL. But your sysdamin may
try running your programs to see what they do. If any of your programs turn
out to be commonly used to commit computer crimes, you are history.
Wait, wait, you are saying. Why get a shell account if I can get kicked out even for legal,
innocuous hacking? After all, SATAN is legal to use. In
fact, you can learn lots of neat stuff with SATAN. Most hacker tools, even
if they are primarily used to commit crimes, are also educational. Certainly
if you want to become a sysadmin someday you will need to learn how these
programs work.
Sigh, you may as well learn the truth. Shell accounts are kind of like
hacker training wheels. They are OK for beginner stuff. But to become a
serious hacker, you either need to find an ISP run by hackers who will
accept you and let you do all sorts of suspicious things right under their
nose. Yeah, sure. Or you can install some form of Unix on your home
computer. But that's another Guide to (mostly) Harmless Hacking (Vol. 2
Number 2: Linux!).
If you have Unix on your home computer and use a PPP connection to get into the Internet,
your ISP is much less likely to snoop on you. Or try making
friends with your sysadmin and explaining what you are doing. Who knows, you
may end up working for your ISP!
In the meantime, you can use your shell account to practice just about
anything Unixy that won't make your sysadmin go ballistic.

****
Would you like a shell account that runs industrial strength Linux -- with
no commands censored? Want to be able to look at the router tables, port
surf all.net, and keep SATAN in your home directory without getting kicked
out for suspicion of hacking? Do you want to be able to telnet in

on ssh
(secure shell)so no one can sniff your password? Are you willing to pay $30
per month for unlimited access to this hacker playground? How about a seven
day free trial account? Email haxorshell@techbroker.com for details.
****

In case you were wondering about all the input from jericho in this Guide, yes,
he was quite helpful in reviewing this and making suggestions. Jericho is a security
consultant and also runs his own Internet host,
obscure.sekurity.org. Thank you,
jericho@dimensional.com, and happy hacking!

GUIDE TO (mostly) HARMLESS HACKING
Beginners' Series Number 4
How to use the Web to look up information on hacking.
This GTMHH may be useful even to Uberhackers (oh, no, flame alert!)

Want to become really, really unpopular? Try asking your hacker friends too many questions of the wrong sort. But, but, how do we know what are the wrong questions to ask? OK, I sympathize with your problems because I get flamed a lot, too. That's partly because I sincerely believe in asking dumb questions. I make my living asking dumb questions. People pay me lots of money to go to conferences, call people on the phone and hang out on Usenet news groups asking dumb questions so I can find out stuff for them. And, guess what, sometimes the dumbest questions get you the best answers. So that's why you don't see me flaming people who ask dumb questions.

****
Newbie note: Have you been too afraid to ask the dumb question, "What is a flame?" Now you get to find out! It is a bunch of obnoxious rantings and ravings made in email or a Usenet post by some idiot who thinks he or she is proving his or her mental superiority through use of foul and/or impolite language such as "you suffer from rectocranial inversion," f* y***, d****, b****, and of course @#$%^&*! This newbie note is my flame against those**

flamers to whom I am soooo superior.
****

But even though dumb questions can be good to ask, you may not like the
flames they bring down on you. So, if you want to avoid flames, how do you
find out answers for yourself?
This Guide covers one way to find out hacking information without having to ask people
questions: by surfing the Web. The other way is to buy lots and lots of computer manuals, but that costs a lot of money. Also, in some parts
of the world it is difficult to get manuals. Fortunately, however, almost
anything you want to learn about computers and communications is available
for free somewhere on the Web.
First, let's consider the Web search engines. Some just help you search the Web itself.
But others enable you to search Usenet newsgroups that have been archived for many years back. Also, the best hacker email lists are archived
on the Web, as well.
There are two major considerations in using Web search engines. One is what search
engine to use, and the other is the search tactics themselves.
I have used many Web search engines. But eventually I came to the conclusion
that for serious research, you only need two: Alavista (http://altavista.digital.com)
and Dejanews (http://www.dejanews.com).
Altavista is the best for the Web, while Dejanews is the best one for
searching Usenet news groups. But, if you don't want to take me at my word,
you may surf over to a site with links to almost all the Web and Newsgroup
search engines at http://sgk.tiac.net/search/.
But just how do you efficiently use these search engines? If you ask them to find
"hacker" or even "how to hack," you will get bazillions of Web sites
and news group posts to read. OK, so you painfully surf through one hacker
Web site after another. You get portentous-sounding organ music, skulls with

red rolling eyes, animated fires burning, and each site has links to other
sites with pretentious music and ungrammatical boastings about "I am 31337,
d00dz!!! I am so *&&^%$ good at hacking you should bow down and kiss my
$%^&&*!" But somehow they don't seem to have any actual information. Hey,
welcome to the wannabe hacker world!
You need to figure out some words that help the search engine of your choice get
more useful results. For example, let's say you want to find out whether I, the
Supreme R00ler of the Happy Hacker world, am an elite hacker chick or merely some poser.
Now the luser approach would to simply go to
http://www.dejanews.com and do a search of Usenet news groups for "Carolyn
Meinel," being sure to click the "old" button to bring up stuff from years
back. But if you do that, you get this huge long list of posts, most of
which have nothing to do with hacking:
CDMA vs GSM - carolyn meinel <cmeinel@unm.edu> 1995/11/17
Re: October El Nino-Southern Oscillation info gonthier@usgs.gov (Gerard J.
Gonthier) 1995/11/20
Re: Internic Wars MrGlucroft@psu.edu (The Reaver) 1995/11/30
shirkahn@earthlink.net (Christopher Proctor) 1995/12/16
Re: Lyndon LaRouche - who is he? lness@ucs.indiana.edu (lester john ness)
1996/01/06
U-B Color Index observation data - cmeinel@nmia.com (Carolyn P. Meinel)
1996/05/13
Re: Mars Fraud? History of one scientist involved gksmiley@aol.com (GK
Smiley) 1996/08/11
Re: Mars Life Announcement: NO Fraud Issue twitch@hub.ofthe.net 1996/08/12
Hackers Helper E-Zine wanted - rcortes@tuna.hooked.net (Raul Cortes)
1996/12/06
Carolyn Meinel, Soooooooper Genius - nobody@cypherpunks.ca (John Anonymous
MacDonald, a remailer node) 1996/12/12
Anyhow, this list goes on and on and on.

But if you specify "Carolyn Meinel hacker" and click "all" instead of "any" on the
"Boolean" button, you get a list that starts with:
Media: "Unamailer delivers Christmas grief" - Mannella@ipifidpt.difi.unipi.it
(Riccardo Mannella) 1996/12/30 Cu Digest, #8.93, Tue 31 Dec 96 - Cu Digest
(tk0jut2@mvs.cso.niu.edu)
<TK0JUT2@MVS.CSO.NIU.EDU> 1996/12/31
RealAudio interview with Happy Hacker - bmcw@redbud.mv.com (Brian S.
McWilliams) 1997/01/08
Etc.
This way all those posts about my boring life in the world of science don't
show up, just the juicy hacker stuff.
Now suppose all you want to see is flames about what a terrible hacker I am.
You could bring those to the top of the list by adding (with the "all"
button still on) "flame" or "f***" or "b****" being careful to spell out
those bad words instead fubarring them with ****s. For example, a search on
"Carolyn Meinel hacker flame" with Boolean "all" turns up only one post.
This important tome says the Happy Hacker list is a dire example of what
happens when us prudish moderator types censor naughty words and inane
diatribes.

****

Newbie note: "Boolean" is math term. On the Dejanews search engine they
figure the user doesn't have a clue of what "Boolean" means so they give you
a choice of "any" or "all" and then label it "Boolean" so you feel stupid if
you don't understand it. But in real Boolean algebra we can use the
operators "and" "or" and "not" on word searches (or any searches of sets).
"And" means you would have a search that turns up only items that have "all"
the terms you specify; "or" means you would have a search that turns up

"any" of the terms. The "not" operator would exclude items that included the
"not" term even if they have any or all of the other search terms. Altavista
has real Boolean algebra under its "advanced"" search option.
****

But let's forget all those Web search engines for a minute. In my humble yet old-fashioned
opinion, the best way to search the Web is to use it exactly the way its inventor, Tim Berners-Lee, intended. You start at a good spot
and then follow the links to related sites. Imagine that!
Here's another of my old fogie tips. If you want to really whiz around the
Web, and if you have a shell account, you can do it with the program lynx.
At the prompt, just type "lynx followed by the URL you want to visit.
Because lynx only shows text, you don't have to waste time waiting for the
organ music, animated skulls and pornographic JPEGs to load.
So where are good places to start? Simply surf over to the Web sites listed at
the end of this Guide. Not only do they carry archives of these Guides, they carry a
lot of other valuable information for the newbie hacker, as well as links to other
quality sites. My favorites are:
http://www.cs.utexas.edu/users/matt/hh.html and
http://www.silitoad.org
Warning: parental discretion advised. You'll see some other great starting
points elsewhere in this Guide, too.
Next, consider one of the most common questions I get: "How do I break into a
computer????? :(:("
Ask this of someone who isn't a super nice elderly lady like me and you will get a
truly rude reaction. Here's why. The world is full of many kinds of
computers running many kinds of software on many kinds of networks. How you
break into a computer depends on all these things. So you need to thoroughly
study a computer system before you an even think about planning a strategy

to break into it. That's one reason breaking into computers is widely
regarded as the pinnacle of hacking. So if you don't realize even this much,
you need to do lots and lots of homework before you can even dream of
breaking into computers.
But, OK, I'll stop hiding the secrets of universal computer breaking and
entry. Check out:
Bugtraq archives: http://geek-girl.com/bugtraq
NT Bugtraq archives: http://ntbugtraq.rc.on.ca/index.html

****
You can go to jail warning: If you want to take up the sport of breaking
into computers, you should either do it with your own computer, or else get
the permission of the owner if you want to break into someone else's
computer. Otherwise you are violating the law. In the US, if you break into
a computer that is across a state line from where you launch your attack,
you are committing a Federal felony. If you cross national boundaries to
hack, remember that most nations have treaties that allow them to extradite
criminals from each others' countries.
****

Wait just a minute, if you surf over to those site you won't instantly
become an Ubercracker. Unless you already are an excellent programmer and
knowledgeable in Unix or Windows NT, you will discover the information at
these two sites will *NOT* instantly grant you access to any victim computer
you may choose. It's not that easy. You are going to have to learn how to
program. Learn at least one operating system inside and out.
Of course some people take the shortcut into hacking. They get their
phriends to give them a bunch of canned break-in programs. Then they try
them on one computer after another until they stumble into root

and
accidentally delete system files. The they get busted and run to the
Electronic Freedom Foundation and whine about how the Feds are persecuting
them.
So are you serious? Do you *really* want to be a hacker badly enough to
learn an operating system inside and out? Do you *really* want to populate
your dreaming hours with arcane communications protocol topics? The
old-fashioned, and super expensive way is to buy and study lots of manuals.
<Geek mode on> Look, I'm a real believer in manuals. I spend about $200 per
month on them. I read them in the bathroom, while sitting in traffic jams,
and while waiting for doctor's appointments. But if I'm at my desk, I prefer
to read manuals and other technical documents from the Web. Besides, the Web
stuff is free! <Geek mode off>
The most fantastic Web resource for the aspiring geek, er, hacker, is the
RFCs. RFC stands for "Request for Comment." Now this sounds like nothing
more than a discussion group. But actually RFCs are the definitive documents
that tell you how the Internet works. The funny name "RFC" comes from
ancient history when lots of people were discussing how the heck to make
that ARPAnet thingy work. But nowadays RFC means "Gospel Truth about How the
Internet Works" instead of "Hey Guys, Let's Talk this Stuff Over."

****
Newbie note: ARPAnet was the US Advanced Research Projects Agency experiment
launched in 1969 that evolved into the Internet. When you read RFCs you will
often find references to ARPAnet and ARPA -- or sometimes DARPA. That "D"
stands for "defense." DARPA/ARPA keeps on getting its name changed between

these two. For example, when Bill Clinton became US President in 1993, he
changed DARPA back to ARPA because "defense" is a Bad Thing. Then in 1996
the US Congress passed a law changing it back to DARPA because "defense" is
a Good Thing.
****

Now ideally you should simply read and memorize all the RFCs. But there are zillions of
RFCs and some of us need to take time out to eat and sleep. So those of us without photographic memories and gobs of free time need to be
selective about what we read. So how do we find an RFC that will answer
whatever is our latest dumb question?
One good starting place is a complete list of all RFCs and their titles at
ftp://ftp.tstt.net.tt/pub/inet/rfc/rfc-index. Although this is an ftp (file
transfer protocol) site, you can access it with your Web browser.
Or, how about the RFC on RFCs! That's right, RFC 825 is "intended to clarify
the status of RFCs and to provide some guidance for the authors of RFCs in the future.
It is in a sense a specification for RFCs." To find this RFC,
or in fact any RFC for which you have its number, just go to Altavista and
search for "RFC 825" or whatever the number is. Be sure to put it in quotes
just like this example in order to get the best results.
Whoa, these RFCs can be pretty hard to understand! Heck, how do we even know
which RFC to read to get an answer to our questions? Guess what, there is
solution, a fascinating group of RFCs called "FYIs" Rather than specifying
anything, FYIs simply help explain the other RFCs. How do you get FYIs?
Easy! I just surfed over to the RFC on FYIs (1150) and learned that:
FYIs can be obtained via FTP from NIC.DDN.MIL, with the pathname FYI:mm.TXT,
or RFC:RFCnnnn.TXT (where "mm" refers to the number of the FYI and "nnnn" refers to the
number of the RFC). Login with FTP, username ANONYMOUS and

password GUEST. The NIC also
provides an automatic mail service for those sites which cannot use FTP. Address the
request to SERVICE@NIC.DDN.MIL and in the subject field of the message indicate the FYI or
RFC number, as in "Subject: FYI mm" or "Subject: RFC nnnn".
But even better than this is an organized set of RFCs hyperlinked together
on the Web at http://www.FreeSoft.org/Connected/. I can't even begin to
explain to you how wonderful this site is. You just have to try it yourself.
Admittedly it doesn't contain all the RFCs. But it has a tutorial and a
newbie-friendly set of links through the most important RFCs.
Last but not least, you can check out two sites that offer a wealth of
technical information on computer security:
http://csrc.nist.gov/secpubs/rainbow/
http://GANDALF.ISU.EDU/security/security.html security library
I hope this is enough information to keep you busy studying for the next
five or ten years. But please keep this in mind. Sometimes it's not easy to
figure something out just by reading huge amounts of technical information.
Sometimes it can save you a lot of grief just to ask a question. Even a dumb question.
Hey, how would you like to check out the Web site for those of us who make our living asking people dumb questions? Surf over to http://www.scip.org.
That's the home page of the Society of Competitive
Information Professionals, the home organization for folks like me. So, go
ahead, make someone's day. Have phun asking those dumb questions. Just
remember to fireproof your phone and computer first!

GUIDE TO (mostly) HARMLESS HACKING
Beginners' Series Number 5
PGP for Newbies

Do you cringe at the idea of people snooping on your email and through the files on your computer? Encryption is the only way to be absolutely certain you can keep your private stuff really private. Even if you are a newbie, encryption can be surprisingly easy -- if you use the free PGP program, the encryption technique so powerful that it is illegal to use in some countries! The following GTMHH was written by Keydet89 <keydet89@yahoo.com>, so if you want to ask questions, email him and not me! (Carolyn Meinel).

This Guide will tell you about:
- -Creating your own keys
- -Importing keys
- -Creating a group of keys
- -Making your public key public
- -Encrypting Files
- -Encrypting your email

PGP is a personal encryption program that you can use to encrypt files or email.
PGP is 'Pretty Good Privacy', originally created by Phil Zimmerman. The long and short of the story is that Phil released his encryption program to the public and was investigated by the federal government. As soon as the investigation was closed, Phil started a company based on his product, which was later purchased by Network Associates.
You can get the freeware version of PGP from:
http://www.nai.com/products/security/pgpfreeware.asp
**Be prepared for a wait, as this is approximately a 5.5Mb file.
Note: All of the examples used in this Guide are performed using PGPfreeware 6.0. The link above is for this version.

****

Newbie Note: How to use PGP will be described, but if you want to make it a little easier to use, download the Eudora email client and install PGP's Eudora plug-in. The tools from PGP appear as icons on the toolbar in Eudora, and

encrypting or decrypting an email is as easy as selecting an icon.
To get Eudora freeware to use with PGP, go to:
http://www.eudora.com/products/
****

Once you have the PGP freeware program, double-click on the icon to install it. Just follow the instructions, they are very straight-forward, and there are no tricks or surprises along the way. You will have to reboot your computer, though, but when you do, PGP Tray should be in your Startup group, and there will be a little lock icon on the TaskBar.
NOTE: For the purposes of this Guide, PGP 6.0 was installed on NT 4.0/SP 3. However, there should be no great difference with 95/98.
Okay, once you have PGP installed, you need to create your own keys. But before we get started on that, let's briefly describe how all of this works...
Briefly, the idea is this...PGP generates strong cryptographic keys, a public and a private key. You keep the private key, and distribute your public key...attach it to your email by using a signature file, post it on a web page, whatever. You get your friends public keys and import them into PGP Tools. When you want
to send an encrypted email, you encrypt the email using the public
key of whomever you are sending it to...and only that person will be able to decrypt it using their private key. You can also sign the files and emails so that whomever has your public key in their
key ring will know that the file is from you, and not someone pretending to be you.

Creating your own keys

Now, let's generate a key pair. Click Start -> Programs -> PGP -> PGP Keys. Note: This assumes that you installed PGP using the default options. You will see lots of keys already in the PGP Keys
tool...these are the keys of the folks at PGP, Inc, which is now part of Network Associates. Scroll down until you find Phil Zimmerman's key...he is the creator of PGP.
To create your own pair, choose Keys -> New Key... and follow the instructions. The second screen of the Key Generation Wizard asks
for your full name and an email address. If you have one of the

free email accounts from Yahoo or HotMail, you may choose to use that email address. The third screen asks you to pick how large of a key pair you wish to generate...since the Happy Hacker herself
uses 3072 bits, we'll choose the same strength.

****
Newbie Note: The size of the key determines its strength... the larger the key, the harder it is to crack.
****

On the fourth screen, choose 'Key pair never expires'. The fifth screen asks for a
passphrase to protect your private key. Choose something that is not at all easy to guess...and
then mix in numbers, capital letters, and punctuation. After you confirm your passphrase and
click 'Next', there will be a way cool graphic while PGP generates your key pair.
Next, since we're just setting this up on our own system, and not connecting to a root server (a server that is used by companies to
manage lots of keys), do not check the 'Send my key to the root server now' box.
You now have your own key pair!!

Importing keys

Okay, now what? Hhhmmm....let's look at an example of how to import keys. Go to:
http://koan.happyhacker.org/~satori/satori.asc
There are two key blocks on this page...looks like two different versions of PGP. Great. Look at the larger one...now highlight it, including the lines that contain 'BEGIN (END) PGP PUBLIC KEY BLOCK'.
NOTE: We are only going to import the lower key block. Do not include the upper key block...the smaller one that says 'Version 2.6.2'.
Highlight the entire 'Version: PGPfreeware 5.0i' block, and press 'ctrl-c' (ie, hold down the control key, and press the 'c' key) or choose Edit -> Copy from your browser.
Minimize the browser and open PGP Keys.
Choose Edit -> Paste, and you'll see Satori's key in the dialog window. The email address used is 'satori@rt66.com'.
Click 'Import'. Now you have Satori's public key, and you can encrypt messages to him...and only him.
PGP ships with two public key servers built in. To see them,

open PGPKeys, and choose Server -> Search. The drop-down box at the top of the Search Window will list an LDAP server at PGP.COM and an HTTP connection to MIT.EDU. You can search for keys by typing in the name of the user you are looking for...I found the Happy Hacker's public key in a matter of seconds! I just clicked on her key, and dragged it to my PGPKeys window... Hint: For the search, use the UserID of 'Carolyn Meinel'.

Creating a group of keys

Now let's create a group of keys. What this does is keep several keys together, so if you have several keys from friends and you want to encrypt a file for all of them, you don't have to go about
encrypting the file for each person.
In PGPKeys, choose Groups -> New Group..., and enter the information asked for.
Choose Groups -> Show Groups, and a lower dialog window will open in PGPKeys, with the name of the group you just created.
To add keys to the group, highlight the key you want to add and click 'ctrl-c' to copy the keys to the clipboard.
Highlight the group, right-click on it to open the popup menu, and choose Paste. The keys will be pasted into the group.

Making your public key public

There are a couple of ways to make your public key available. We'll describe two methods...using a public key server, or saving the key to a text file
so that someone else can import it.
First, as stated above, PGP ships with two public servers...one at PGP.COM, the other at MIT. When you are connected to the Internet, open PGPKeys, select your key pair, and click Server -> Send to, and choose the server you want to send your public key to.
The other method is to save your public key to a file. This file can be sent to your friends, or pasted into your signature file on your email. To save your public key to a file:
Open PGPKeys, and select your key pair.
Click Keys -> Export, and a file dialog will open.
Choose a filename.
To save your public key into a document that already exists, such as a signature file for your email:
Select your key pair.
Click Edit -> Copy (or hit ctrl-c).
Move to the document where you want the key saved, and choose Edit -> Paste from the menubar for the document (or hit ctrl-v).

Encrypting Files

Warning: The next example shows you how to encrypt and decrypt your files. Choose a file to try the example on but do NOT try it on a system file or other important file!!

Want to encrypt a file on your machine? Great, let's try it. Open up any folder, and choose any file. Right-click on the file, and go to PGP in the popup menu. Choose 'Encrypt', and choose your key pair from the dialog window. Now, click on the pair, and drag it into the lower window. PGP will encrypt the file and you'll see another icon pop up...an armor plate with a lock on it. Very appropriate, if you think about it.

Now to decrypt the file, make sure that you've moved or deleted the original file (make sure that you aren't using a system or other important file for this example!!) and double-click on the encrypted file. Enter your passphrase in the lower dialog window, and BANG!, your file is decrypted.

This is a great way to protect your files. And it's free!

To encrypt a file for the group, just follow the same steps as above, but choose the group name instead of a single key.

Encrypting your email

Now, encrypting your email...if you are using Eudora or (god forbid!!) Outlook, then you could have opted to use the PGP plug-ins for either of them.

However, if you don't use either of the two mail clients, then in order to encrypt your email, can choose a couple of options.

First, using an email client such as Netscape, you can easily encrypt the file as described above, and attach it to the email.

Another option is to type what you want into the message area of the email, and then highlight it and click 'ctrl-c' to copy the text to the clipboard. Then right-click on the PGP Tray icon on the TaskBar (the little lock) and choose 'Encrypt & Sign Clipboard'.

The PGPKeys window will open, and you need to choose to whom you wish to encrypt the message.

You'll be prompted for your passphrase, as the message will be signed, so that your friend (who has your public key) will know that it's from you.

Once the text on the clipboard is encrypted, go back to the email (or file) and highlight the text again, and click 'ctrl-v' (hold down the control key and hit 'v') and the encrypted

message will be pasted into the email over the original message.

****
Newbie Note: If the PGP Tray icon isn't on your TaskBar,
check your Startup folder. If it's not in the Startup folder,
add a shortcut to PGPTray.exe to the folder.
If at any time you are having difficulty trying to do anything
with your keys, simply open the Help in PGP. The help documents
are very good...they are clear, descriptive, and concise.
****

Here's my (Keydet89) public key:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.0 for non-commercial use
<http://www.pgp.com>

mQGiBDYMk4YRBAD3QaP+/6SFBzkdZLc+iVlfRJ1q7F3axQOK3uAgEMQ41kyJVQju
Ynn+ZnVG8qgPRnvD3DkapzmWpl/lgc+ezmA9Af6pezrFKEBP9NWZN8u53qXNKPxo
CaIIikhoOcd+5YnrsezKvDN6ab8vWcYgrui3ecMu6AmAxnFAj+rCiQizvQCg/6V8
sYmhkBIqTbu8eMwZ/G7OXq8D/13LtUsoLB/Z9Wtza661GtZ/O9NLiA0qlJbDOkvf
cv9k76KvzHCshvTwM/s9sqmc5EuB4cvNNILelW0wMcQrM+NBNNxtgGf/Q4+nh0kB
11GSOOijIEDFLSb2MIu3I1wDeFLiSD30F88MjpK517bhLIPY+xt5EtIBzFx6Xh27
23EFA/9IZkLzO7fwAtjljWCyw72e4sxXDPO5v1GFBG+TZF9DM+Zzbfext9Wkw5MW
DMStICIaCYAsq5ywaQUrzPe2WJfeQqNbSOi9QULnri7dg0jBOxHHPkMDy4wxKqmu
dS4txrCedXKWALKVnFfDy2bfrLZ9WYP2YIqta3QoYvg5Qkpy+LQdS2V5ZGV0ODkg
PGtleWRldDg5QHlhaG9vLmNvbT6JAEsEEBECAAsFAjYMk4YECwMCAQAKCRA5IB4E
SkfiCzxJAJ9I8COJS34TOJftyPXFLHz1qpAFiwCg8c9G3jZRv4ki5MjufpPDtnOQ
5zG5Aw0ENgyThhAMAMwdd1ckOErixPDojhNnl06SE2H22+slDhf99pj3yHx5sHId
OHX79sFzxIMRJitDYMPj6NYK/aEoJguuqa6zZQ+iAFMBoHzWq6MSHvoPKs4fdIRP
yvMX86RA6dfSd7ZCLQI2wSbLaF6dfJgJCo1+Le3kXXn11JJPmxiO/CqnS3wy9kJX
twh/CBdyorrWqULzBej5UxE5T7bxbrlLOCDaAadWoxTpj0BV89AHxstDqZSt90xk
hkn4DIO9ZekX1KHTUPj1WV/cdlJPPT2N286Z4VeSWc39uK50T8X8dryDxUcwYc58
yWb/Ffm7/ZFexwGq01uejaClcjrUGvC/RgBYK+X0iP1YTknbzSC0neSRBzZrM2w4
DUUdD3yIsxx8Wy2O9vPJI8BD8KVbGI2Ou1WMuF040zT9fBdXQ6MdGGzeMyEstSr/
POGxKUAYEY18hKcKctaGxAMZyAcpesqVDNmWn6vQClCbAkbTCD1mpF1Bn5x8vYlL
IhkmuquiXsNV6UwybwACAgv+PxYBW2jJR/SP7xiaZ0TZ8E1QsgyZfN0EBHb8oogw
hpNmJzqjmTLWrPpTMRlHVkPxikunEnUIL1tBzrPGaz+CuUOhCFAVqXr/JwCF2ocQ
Zus/rtucN7PPqvkC5IMYW04MvBGE4n/7pbNFelXZb790nkyOamVh0zqMokraQtfW
mi4qQrlg0yEqiLt1JUvf/mdaSR2UdYiLMLg43oIPXmp608DjtUWXBU8nZuYLq60v
dQde2dX82cOvlswR3/z43KGrhsklQwKZoPq1IkcP3pA9Jjqq3ltLXf5A74vFCetl
JBoLUW0pCIuN1GcG4qAIeUusTuyX6QtO6pfvfYyNhyEF+ylJGyt93VSUssNF1wR/
UodXQ3NdtQAWYrNXTWwrXDN9Sm4rG/rHU/BPbd0VLC8PH8wraVluk/NzMrMdPGhj
mnxeHcBRb0WtIA6hZt+rIJBsel7In6ayl0UbnZWFkp0AZshmh0DKBy46Tr4V2UYM
NdjL9AemPh4kd64VmvJ2GHleiQBGBBgRAgAGBQI2DJOGAAoJEDkgHgRKR+IL3BwA
oIkAAwmgpFp9CLq1SX4sPj871eekAKCag3rN+zsu1dh3lBJQ4lYw7TmtAg==
=0E/c
-----END PGP PUBLIC KEY BLOCK-----

GUIDE TO (mostly) HARMLESS HACKING
Beginners' Series Number 6
The Exploit Files

How many times have you read hacker newsgroups or email lists and seen posts that begged "teach me to hack," or asked "how do I hack this"? It often looks as though the person asking the question just doesn't understand the basics of vulnerabilities and their exploits. The purpose of this Guide is to explain what vulnerabilities and exploits are, and how they relate to computer security.
Let's start with an example. Suppose that you are trying to sell something by phone. So you start by calling phone numbers, and you keep calling until you get someone to answer, not an answering machine, but a real live person.
Then if the person who answers the phone speaks the same language as you and can understand you, you try to sell your product. Lots of people will hang up on you, but eventually, someone will buy something...bang! You've scored!

In this Guide you will learn:
- What is a vulnerability
- What is an exploit
- How to look for vulnerabilities

So what does this have to do with 'hacking'? Look at your dialing of phone numbers as port scanning IP (Internet protocol) addresses on the Internet.
Some Internet host computers won't answer. Maybe a firewall is blocking the ports that you're scanning. Some hosts will answer, and at that point maybe, just maybe, you've found a vulnerable computer.

****
Newbie note: What are these 'ports' we are talking about? This kind of

'port' is a number used to identify a service on an Internet host. For this reason they are often called 'TCP/IP' (transfer control protocol/Internet protocol) ports, to distinguish them from other kinds of computer ports such as modems, ports to printers, etc. Each host computer connected to the Internet is identified by an IP address such as 'victim.fooisp.com.' Since each host may have many services running, each service uses a different port. To contact any of these ports across the Internet, you use the host's IP address and port number -- it's kind of like dialing a phone number.

****

Now maybe you have connected to telnet, port 23. You get a login prompt, but you don't know any valid username/password combinations. So the host "hangs up" on you. After many hours of trying, you connect to a host on the right port, and Shazam!! You're greeted with a login prompt, and you quickly guess a valid username and password combination. The next thing you know, you have a command prompt. You have discovered a vulnerability -- an easily guessed password! So being the 'white hat hacker' that you are, you send an email to the sysadmin of the site and leave quietly.

****

Newbie note: A 'host' is a computer connected to the Internet. A 'service' is a program that is running on a port of an Internet host. Each service is a program that will respond to certain commands. If you give it the right command, you will get it to do something for you.
The simplest example of a service is 'chargen', or character generator (port 19). If you make a telnet connection on the chargen port to a server running the chargen service, this program will react to this connection by sending a string of characters which

you will see being repeated
across your telnet screen. All you need to do is connect to the service.
Another example of a service is finger (port 79). If you run a finger
program to request information on a particular user from a specific host,
and the finger service (or 'fingerd') is running, and if the user has not
instructed the finger service to ignore requests about him or her, you will
get back information on that user.
****

What services are run from these ports, and how can we learn more about
them? Ports numbered from 1 to 1024 are called the 'well-known' ports.
These are listed in RFC 1700 (see
http://www.internetnorth.com.au/keith/networking/rfc.html). Many of the
well-known ports are also listed in a file on your computer
called 'services'. On Win95, it's c:\windows\services; on NT,
it's c:\winnt\system32\drivers\etc\services; on many Unix type computers (your
shell account) it's /etc/services.
These ports are called 'well-known' because they are commonly used by
certain services. For example, the well-known port for sending email is the
SMTP port, or port 25. Because it is 'well-known', anyone can send email to
anyone else. Because port 110 is the well-known port for checking email,
all email clients know that they have to connect to a POP server on port 110
in order to retrieve email.
An excellent FAQ (frequently asked questions) on TCP/IP ports can be found
at http://www.technotronic.com/tcpudp.html

****
You can get punched in the nose warning: There are many port scanning
tools, and wannabe hackers use them ... a lot. But for what purpose? In
most cases all that happens is that a sysadmin or firewall

administrator
goes through the logs that computer keeps of who has tried to hack that
site. He or she then decides whether to ignore your scan or call the
sysadmin of the site that your scan came from. Even though (in the US at
least) port scanning is legal, it makes systems administrators really mad at
you! To avoid getting kicked off your Internet provider, get permission to
scan first!
****

What Is a Vulnerability?

A 'vulnerability' is anything about a computer system that will allow
someone to either keep it from operating correctly, or that will let
unauthorized people take it over. There are many types of vulnerabilities.
They may be a misconfiguration in the setup of a service, or a flaw in the
programming of the service.
An example of a setup misconfiguration is leaving the 'wiz' or 'debug'
commands operational in older versions of sendmail, or incorrectly setting
directory permissions on your FTP server so people can download the password
file. In these cases, the vulnerability is not how the program was written,
but with how the program is configured. Allowing file sharing on your
Windows 95 or 98 computer when it is not necessary, or failing to put a
password on file sharing, is another example.
Examples of errors in the programming of services are the large number of
buffer overflow vulnerabilities in the programs that run services on port of
Internet host computers. Many of these buffer overflow problems allow
people to use the Internet to break into and take control of host computers
(check out "Smashing the Stack", by Aleph One, at:

http://www.happyhacker.org/docs/smash.txt).

What Is an Exploit?

An 'exploit' is a program or technique that takes advantage of a vulnerability. For example, the FTP-Bounce vulnerability occurs when an FTP server (used to allow people to upload and download files) is configured to redirect FTP connections to other computers. There really is no good reason to allow this feature. It has become a vulnerability because this 'bounce' feature allows someone to use it to port scan other computers on the same local area network (LAN) as that FTP server. So even though a firewall may be keeping port scanners form directly scanning other computers on this LAN, the FTP server would bounce a scan past the firewall.
So really an exploit is any technique that takes advantage of a vulnerability to enable you to carry out your own schemes, despite the wishes of the sysadmin of your target. Exploits depend on operating systems and their configurations, the configurations of programs running on computer systems, and of the LAN they are on.
Operating systems such as NT, VMS and Unix are very different, and the various versions of Unix have their differences, as well. (Examples of Unix operating systems include BSD, AIX, SCO, Irix, Sun OS, Solaris, and Linux).
Even the various versions of the Linux form of Unix are different.
This means exploits that will work against NT systems will probably not work against Unix systems, and exploits for Unix systems will probably not work against NT. NT services are run by different programs from what you may find on Unix type computers. Further, different versions of the same service running on any particular operating system will probably not be vulnerable to the same exploit, because each version of a service is run by a

different program. Sometimes this different program may have the same name
but only have a different version number. For example sendmail 8.9.1a is
different from 8.8.2. Many of the differences are that 8.9.1a has been
fixed so that none of the old sendmail exploit programs will work on it.
For example, the "Leshka" exploit explained in the GTMHH on advanced shell
programming clearly explains that it only works on versions 8.7-8.8.2 of the
SMTP service program called 'sendmail.' We observed a number of people who
were playing the hacker wargame trying to run the Leshka exploit against a
later, fixed version of sendmail.
So remember, an exploit for one operating system or service is unlikely to
work against another operating system. This isn't to say that it definitely
won't...it's just not likely. However, you are pretty much guaranteed that
any Win95 or NT exploit will not work against any kind of Unix.

How to Look for Vulnerabilities

Now let's start someplace where you are unlikely to get punched in the nose by looking at
some ports on your own computer. You can do this by typing 'netstat -a' at the command prompt.
You should see something such as:

```
Active Connections
Proto  Local AddressForeign Address  State
TCPlocalhost:1027   0.0.0.0:0LISTENING
TCPlocalhost:1350.0.0.0:0LISTENING
TCPlocalhost:1350.0.0.0:0LISTENING
TCPlocalhost:1026   0.0.0.0:0LISTENING
TCPlocalhost:1026   localhost:1027   ESTABLISHED
TCPlocalhost:1027   localhost:1026   ESTABLISHED
TCPlocalhost:1370.0.0.0:0LISTENING
TCPlocalhost:1380.0.0.0:0LISTENING
TCPlocalhost:nbsession  0.0.0.0:0LISTENING
UDPlocalhost:135*:*
UDPlocalhost:nbname *:*
UDPlocalhost:nbdatagram *:*
```

Hhhmm...nothing much going on here. The 'Local Address' (ie, my

local
machine) seem to be listening on ports 135, 137, 138, and 'nbsession' (which
translates to port 139...type 'netstat -an' to see just the port numbers,
not the names of the ports). This is okay...those ports are part of
Microsoft networking, and need to be active on the LAN my machine is
connected to.
Now we connect our Web browser to http://www.happyhacker.org and at the same
time run Windows telnet and connect to a shell account at example.com.
Let's see what happens. Here's the output of the 'netstat -a' command,
slightly abbreviated:

```
Active Connections
Proto  Local Address  Foreign Address  State
TCPlocalhost:1027 0.0.0.0:0LISTENING
TCPlocalhost:135  0.0.0.0:0LISTENING
TCPlocalhost:135  0.0.0.0:0LISTENING
TCPlocalhost:2508 0.0.0.0:0LISTENING
TCPlocalhost:2509 0.0.0.0:0LISTENING
TCPlocalhost:2510 0.0.0.0:0LISTENING
TCPlocalhost:2511 0.0.0.0:0LISTENING
TCPlocalhost:2514 0.0.0.0:0LISTENING
TCPlocalhost:1026 0.0.0.0:0LISTENING
TCPlocalhost:1026 localhost:1027   ESTABLISHED
TCPlocalhost:1027 localhost:1026   ESTABLISHED
TCPlocalhost:137  0.0.0.0:0LISTENING
TCPlocalhost:138  0.0.0.0:0LISTENING
TCPlocalhost:139   0.0.0.0:0LISTENING
TCPlocalhost:2508 zlliks.505.ORG:80ESTABLISHED
TCPlocalhost:2509 zlliks.505.ORG:80ESTABLISHED
TCPlocalhost:2510 zlliks.505.ORG:80ESTABLISHED
TCPlocalhost:2511 zlliks.505.ORG:80ESTABLISHED
TCPlocalhost:2514 example.com:telnet   ESTABLISHED
```

So what do we see now? Well, there are the ports listening for Microsoft
networking, just like in the first example. And there also are some new
ports listed. Four are connected to 'zlliks.505.org' on port 80, and one to
'example.com' on the telnet port. These correspond to the client connections
that I set up. See, this way you know the name of the computer

that was running the
happy Hacker Web site at this time.
But what is with the really high port numbers? Well, remember the
'well-known' ports that we talked about above? Client applications, such as
browsers and telnet clients (clients are programs that connect to servers)
need to use a port to receive data on, so they randomly select ports from
outside the 'well-known' port range...above 1024. In this case, my browser
has opened up four ports...2508 through 2511.
Now suppose you want to scan your friend's ports. This is the best way to
scan, as you won't have to worry about your friend getting you kicked off
your ISP for suspicion of trying to break into computers. How do you know
what your friend's IP address is? Ask him or her to run the command (from
the DOS prompt) 'netstat -r'. This shows something like this:
C:\WINDOWS>netstat -r
Route Table
Active Routes:
Network Address NetmaskGateway Address Interface   Metric
0.0.0.0 0.0.0.0 198.59.999.200   198.59.999.200   1
127.0.0.0   255.0.0.0   127.0.0.1127.0.0.11
198.59.999.0255.255.255.0   198.59.999.200   198.59.999.200   1
198.59.999.200 255.255.255.255 127.0.0.1127.0.0.11
198.59.999.255 255.255.255.255 198.59.999.200   198.59.999.200
1
224.0.0.0   224.0.0.0   198.59.999.200   198.59.999.200   1
255.255.255.255 255.255.255.255 198.59.999.200   0.0.0.0 1
Active Connections
  Proto Local Address Foreign AddressState
  TCPlovely-lady:1093   mack.foo66.com:smtp ESTABLISHED
That 'gateway address' and 'interface' both give the current IP address of
your computer. If you are on a LAN, the gateway should be different from
your own computer's IP address. If you or your friend are on a LAN,
however, you should think twice before port scanning each other, or the
LAN's sysadmin may notice your activity. Warning, sysadmins have quite an

arsenal of larts to use on suspicious-acting users.

****
Newbie note: Lart? What the heck is a lart? It is a "luser attitude
readjustment tool." This is a generic class of techniques used by sysadmins
to punish lusers. What is a luser? A wayward user. To get a sampling of
popular larts, see http://mrjolly.cc.waikato.ac.nz. You want your sysadmins
to be your FRIENDS, right? Never forget this!
****

What are some of the vulnerabilities to win95 and NT, you ask? Check
previous GTMHHs for this information. Perhaps the most important thing to
remember about Windows is equal to root in Unix), can run a program that
uses any port it wants, even a well-known port. This vulnerability is
demonstrated by a program from Weld Pond of L0pht fame called 'netcat'. The
program can be obtained from:
http://www.l0pht.com/~weld/netcat
Read the documentation that ships with the program, or the Guides on (a)
win95 and telnet from:
http://www.happyhacker.org/gtmhh.shtml
or (b) NT security from:
http://www.infowar.com/hacker/hacker.html-ssi
for information on uses of netcat.
Of course, various Windows applications, such as Internet Explorer, have
their own vulnerabilities.
By now, you're probably wondering where you can learn more about various
vulnerabilities and exploits for just about any computer you might find on
the Internet.
Here is a list of sites:
ISS X-Force
http://www.iss.net/xforce
RootShell
http://www.rootshell.com
TechnoTronic

http://www.technotronic.com
Packet Storm Security Site
http://www.Genocide2600.com/~tattooman/index.shtml
Bugtraq archives:
http://www.netspace.org/lsv-archive/bugtraq.html
NTBugTraq
http://www.ntbugtraq.com
Aelita Software
http://www.ntsecurity.com
This site has the RedButton program, which demonstrates the capability to
connect to an NT machine via a null session and retrieve registry information. This is a relatively simple problem to fix...see the NT
security Guides at: http://www.infowar.com/hacker/hacker.html-ssi
NTSecurity
http://www.ntsecurity.net
Active Matrix's HideAway
http://www.hideaway.net/exploits.html
CERT
http://www.cert.org

GUIDE TO (mostly) HARMLESS HACKING
Beginners' Series Number 7
Computer hacking. Where did it begin and how did it grow?

If you wonder what it was like in days of yore, ten, twenty, thirty years
ago, how about letting and old lady tell you the way it used to be.
Where shall we start? Seventeen years ago and the World Science Fiction
Convention in Boston, Massachusetts? Back then the World Cons were the
closest thing we had to hacker conventions.
Picture 1980. Ted Nelson is running around with his Xanadu guys: Roger
Gregory, H. Keith Henson (now waging war against the Scientologists) and K.
Eric Drexler, later to build the Foresight Institute. They dream of creating

what is to become the World Wide Web. Nowadays guys at hacker cons might
dress like vampires. In 1980 they wear identical black baseball caps with
silver wings and the slogan: "Xanadu: wings of the mind." Others at World
Con are a bit more underground: doing dope, selling massages, blue boxing
the phone lines. The hotel staff has to close the swimming pool in order to
halt the sex orgies.
Oh, but this is hardly the dawn of hacking. Let's look at the Boston area
yet another seventeen years further back, the early 60s. MIT students are
warring for control of the school's mainframe computers. They use machine
language programs that each strive to delete all other programs and seize
control of the central processing unit. Back then there were no personal
computers.
In 1965, Ted Nelson, later to become leader of the silver wing-headed
Xanadu gang at the 1980 Worldcon, first coins the word "hypertext" to
describe what will someday become the World Wide Web. Nelson later spreads
the gospel in his book Literacy Online. The back cover shows a Superman-type
figure flying and the slogan "You can and must learn to use computers now."
But in 1965 the computer is widely feared as a source of Orwellian powers.
Yes, as in George Orwell's ominous novel , "1984," that predicted a future
in which technology would squash all human freedom. Few are listening to
Nelson. Few see the wave of free-spirited anarchy the hacker culture is
already unleashing. But LSD guru Timothy Leary's daughter Susan begins to
study computer programming.
Around 1966, Robert Morris Sr., the future NSA chief scientist, decides to
mutate these early hacker wars into the first "safe hacking" environment. He

and the two friends who code it call their game "Darwin." Later "Darwin"
becomes "Core War," a free-form computer game played to this day by some of
the uberest of uberhackers.
Let's jump to 1968 and the scent of tear gas. Wow, look at those rocks
hurling through the windows of the computer science building at the
University of Illinois at Urbana-Champaign! Outside are 60s antiwar
protesters. Their enemy, they believe, are the campus' ARPA-funded
computers. Inside are nerdz high on caffeine and nitrous oxide. Under the
direction of the young Roger Johnson, they gang together four CDC 6400s and
link them to 1024 dumb vector graphics terminals. This becomes the first
realization of cyberspace: Plato.
1969 turns out to be the most portent-filled year yet for hacking.
In that year the Defense Department's Advanced Research Projects Agency
funds a second project to hook up four mainframe computers so researchers
can share their resources. This system doesn't boast the vector graphics of
the Plato system. Its terminals just show ASCII characters: letters and
numbers. Boring, huh?
But this ARPAnet is eminently hackable. Within a year, its users hack
together a new way to ship text files around. They call their unauthorized,
unplanned invention "email." ARPAnet has developed a life independent of its
creators. It's a story that will later repeat itself in many forms. No one
can control cyberspace. They can't even control it when it is just four
computers big.
Also in 1969 John Goltz teams up with a money man to found Compuserve using the new packet
switched
technology being pioneered by ARPAnet. Also in 1969 we see a remarkable birth at Bell Labs

as Ken Thompson invents a new operating system: Unix. It is to become the gold standard of hacking and the Internet, the operating system with the power to form miracles of computer legerdemain.

In 1971, Abbie Hoffman and the Yippies found the first hacker/phreaker magazine, YIPL/TAP (Youth International Party -- Technical Assistance Program). YIPL/TAP essentially invents phreaking -- the sport of playing with phone systems in ways the owners never intended. They are motivated by the Bell Telephone monopoly with its high long distance rates, and a hefty tax that Hoffman and many others refuse to pay as their protest against the Vietnam War. What better way to pay no phone taxes than to pay no phone bill at all?

Blue boxes burst onto the scene. Their oscillators automate the whistling sounds that had already enabled people like Captain Crunch (John Draper) to become the pirate captains of the Bell Telephone megamonopoly. Suddenly phreakers are able to actually make money at their hobby. Hans and Gribble peddle blue boxes on the Stanford campus.

In June 1972, the radical left magazine Ramparts, in the article "Regulating the Phone Company In Your Home" publishes the schematics for a variant on the blue box known as the "mute box." This article violates Californian State Penal Code section 502.7, which outlaws the selling of "plans or instructions for any instrument, apparatus, or device intended to avoid telephone toll charges." California police, aided by Pacific Bell officials, seize copies of the magazine from newsstands and the magazine's offices. The financial stress leads quickly to bankruptcy.

As the Vietnam War winds down, the first flight simulator programs in history unfold on the Plato network. Computer graphics, almost

unheard of in
that day, are displayed by touch-sensitive vector graphics terminals.
Cyberpilots all over the US pick out their crafts: Phantoms, MIGs, F-104s,
the X-15, Sopwith Camels. Virtual pilots fly out of digital airports and try
to shoot each other down and bomb each others' airports. While flying a
Phantom, I see a chat message on the bottom of my screen. "I'm about to
shoot you down." Oh, no, a MIG on my tail. I dive and turn hoping to get my
tormentor into my sights. The screen goes black. My terminal displays the
message "You just pulled 37 Gs. You now look more like a pizza than a human
being as you slowly flutter to Earth."
One day the Starship Enterprise barges in on our simulator, shoots everyone down and vanishes back
into cyberspace. Plato has been hacked! Even in 1973 multiuser game players have to worry about
getting "smurfed"! (When a hacker breaks into a multiuser game on the Internet and kills players
with
techniques that are not rules of the game, this is called "smurfing.")
1975. Oh blessed year! Under a Air Force contract, in the city of Albuquerque, New Mexico, the Altair is born. Altair. The first microcomputer. Bill Gates writes
the operating system. Then Bill's mom persuades him to move to Redmond, CA where she
has some money men who want to see what this operating system business is all about.
Remember Hans and Gribble? They join the Home Brew Computer club and choose Motorola
microprocessors to build their own. They begin selling their computers, which they brand name the Apple, under their real names of Steve
Wozniak and Steve Jobs. A computer religion is born.
The great Apple/Microsoft battle is joined. Us hackers suddenly have boxes
that beat the heck out of Tektronix terminals.
In 1978, Ward Christenson and Randy Suess create the first personal
computer bulletin board system. Soon, linked by nothing more than the long

distance telephone network and these bulletin board nodes, hackers create a
new, private cyberspace. Phreaking becomes more important than ever to
connect to distant BBSs.
Also in 1978, The Source and Compuserve computer networks both begin to
cater to individual users. "Naked Lady" runs rampant on Compuserve. The
first cybercafe, Planet Earth, opens in Washington, DC. X.25 networks reign
supreme.
Then there is the great ARPAnet mutation of 1980. In a giant leap it moves
from Network Control Protocol to Transmission Control Protocol/Internet
Protocol (TCP/IP). Now ARPAnet is no longer limited to 256 computers -- it
can span tens of millions of hosts! Thus the Internet is conceived within
the womb of the DoD's ARPAnet. The framework that would someday unite
hackers around the world was now, ever so quietly, growing. Plato fades,
forever limited to 1024 terminals.
Famed science fiction author Jerry Pournelle discovers ARPAnet. Soon his
fans are swarming to find excuses -- or whatever -- to get onto ARPAnet.
ARPAnet's administrators are surprisingly easygoing about granting accounts,
especially to people in the academic world.
ARPAnet is a pain in the rear to use, and doesn't transmit visuals of
fighter planes mixing it up. But unlike the glitzy Plato, ARPAnet is really
hackable and now has what it takes to grow. Unlike the network of hacker
bulletin boards, people don't need to choose between expensive long distance
phone calls or phreaking to make their connections. It's all local and it's
all free.
That same year, 1980, the "414 Gang" is raided. Phreaking is more
hazardous than ever.
In the early 80s hackers love to pull pranks. Joe College sits

down at his
dumb terminal to the University DEC 10 and decides to poke around the campus
network. Here's Star Trek! Here's Adventure! Zork! Hmm, what's this program
called Sex? He runs it. A message pops up: "Warning: playing with sex is
hazardous. Are you sure you want to play? Y/N" Who can resist? With that "Y"
the screen bursts into a display of ASCII characters, then up comes the
message: "Proceeding to delete all files in this account." Joe is weeping,
cursing, jumping up and down. He gives the list files command. Nothing!
Zilch! Nada! He runs to the sysadmin. They log back into his account but his
files are all still there. A prank.
In 1983 hackers are almost all harmless pranksters, folks who keep their
distance from the guys who break the law. MITs "Jargon file" defines hacker
as merely "a person who enjoys learning about computer systems and how to
stretch their capabilities; a person who programs enthusiastically and
enjoys dedicating a great deal of time with computers."
1983 the IBM Personal Computer enters the stage powered by Bill Gates'
MS-DOS operating system. The empire of the CP/M operating system falls.
Within the next two years essentially all microcomputer operating systems
except MS-DOS and those offered by Apple will be dead, and a thousand
Silicon Valley fortunes shipwrecked. The Amiga hangs on by a thread. Prices
plunge, and soon all self-respecting hackers own their own computers.
Sneaking around college labs at night fades from the scene.
In 1984 Emmanuel Goldstein launches 2600: The Hacker Quarterly and the
Legion of Doom hacker gang forms. Congress passes the Comprehensive Crime
Control Act giving the US Secret Service jurisdiction over computer fraud.
Fred Cohen, at Carnegie Melon University writes his PhD thesis on

the brand
new, never heard of thing called computer viruses.
1984. It was to be the year, thought millions of Orwell fans, that the
government would finally get its hands on enough high technology to become
Big Brother. Instead, science fiction author William Gibson, writing
Neuromancer on a manual typewriter, coins the term and paints the picture of
"cyberspace." "Case was the best... who ever ran in Earth's computer matrix.
Then he doublecrossed the wrong people..."
In 1984 the first US police "sting" bulletin board systems appear.
Since 1985, Phrack has been providing the hacker community with information on
operating systems, networking technologies, and telephony, as well as relaying other
topics of interest to the international computer underground.
The 80s are the war dialer era. Despite ARPAnet and the X.25 networks, the
vast majority of computers can only be accessed by discovering their
individual phone lines. Thus one of the most treasured prizes of the 80s
hacker is a phone number to some mystery computer.
Computers of this era might be running any of dozens of arcane operating
systems and using many communications protocols. Manuals for these systems
are often secret. The hacker scene operates on the mentor principle. Unless
you can find someone who will induct you into the inner circle of a hacker
gang that has accumulated documents salvaged from dumpsters or stolen in
burglaries, you are way behind the pack. Kevin Poulson makes a name for
himself through many daring burglaries of Pacific Bell.
Despite these barriers, by 1988 hacking has entered the big time. According to a list of
hacker groups compiled by the editors of Phrack on August 8, 1988, the US hosts hundreds
of them.
The Secret Service covertly videotapes the 1988 SummerCon convention.

In 1988 Robert Tappan Morris, son of NSA chief scientist Robert Morris Sr., writes an exploit that will forever be known as the Morris Worm. It uses a combination of finger and sendmail exploits to break into a computer, copy itself and then send copy after copy on to other computers. Morris, with little comprehension of the power of this exponential replication, releases it onto the Internet. Soon vulnerable computers are filled to their digital gills with worms and clogging communications links as they send copies of the worms out to hunt other computers. The young Internet, then only a few thousand computers strong, crashes. Morris is arrested, but gets off with probation.

1990 is the next pivotal year for the Internet, as significant as 1980 and the launch of TCP/IP. Inspired by Nelson's Xanadu, Tim Berners-Lee of the European Laboratory for Particle Physics (CERN) conceives of a new way to implement hypertext. He calls it the World Wide Web. In 1991 he quietly unleashes it on the world. Cyberspace will never be the same. Nelson's Xanadu, like Plato, like CP/M, fades.

1990 is also a year of unprecedented numbers of hacker raids and arrests.

The US Secret Service and New York State Police raid Phiber Optik, Acid Phreak, and Scorpion in New York City, and arrest Terminus, Prophet, Leftist, and Urvile.

The Chicago Task Force arrests Knight Lightning and raids Robert Izenberg, Mentor, and Erik Bloodaxe. It raids both Richard Andrews' home and business.

The US Secret Service and Arizona Organized Crime and Racketeering Bureau conduct Operation Sundevil raids in Cincinnatti, Detroit, Los Angeles, Miami, Newark, Phoenix, Pittsburgh, Richmond, Tucson, San Diego, San Jose, and San Francisco. A famous unreasonable raid that year was the

Chicago Task
Force invasion of Steve Jackson Games, Inc.
June 1990 Mitch Kapor and John Perry Barlow react to the excesses of all
these raids to found the Electronic Frontier Foundation. Its initial purpose
is to protect hackers. They succeed in getting law enforcement to back off
the hacker community.
In 1993, Marc Andreesson and Eric Bina of the National Center for Supercomputing Applications release Mosaic, the first WWW browser that can
show graphics. Finally, after the fade out of the Plato of twenty years
past, we have decent graphics! This time, however, these graphics are here
to stay. Soon the Web becomes the number one way that hackers boast and
spread the codes for their exploits. Bulletin boards, with their tightly
held secrets, fade from the scene.
In 1993, the first Def Con invades Las Vegas. The era of hacker cons moves
into full swing with the Beyond Hope series, HoHocon and more.
1996 Aleph One takes over the Bugtaq email list and turns it into the first public
"full disclosure" computer security list. For the first time in history, security flaws that can be used to break into computers are being
discussed openly and with the complete exploit codes. Bugtraq archives are
placed on the Web.
In August 1996 I start mailing out Guides to (mostly) Harmless Hacking.
They are full of simple instructions designed to help novices understand
hacking. A number of hackers come forward to help run what becomes the Happy
Hacker Digest.
1996 is also the year when documentation for routers, operating systems,
TCP/IP protocols and much, much more begins to proliferate on the Web. The
era of daring burglaries of technical manuals fades.
In early 1997 the readers of Bugtraq begin to tear the Windows NT operating system to shreds.
A new mail list, NT Bugtraq, is launched just to handle the high

volume of NT security flaws
discovered by its readers.
Self-proclaimed hackers Mudge and Weld of The L0pht, in a tour de force of
research, write and release a password cracker for WinNT that rocks the
Internet. Many in the computer security community have come far enough along
by now to realize that Mudge and Weld are doing the owners of NT networks a
great service.
Thanks to the willingness of hackers to share their knowledge on the Web,
and mail lists such as Bugtraq, NT Bugtraq and Happy Hacker, the days of
people having to beg to be inducted into hacker gangs in order to learn
hacking secrets are now fading.
Where next will the hacker world evolve? You hold the answer to that in
your hands.

Where are those back issues of GTMHHs and Happy Hacker Digests? Check out
the official Happy Hacker Web page at http://www.happyhacker.org.
We are against computer crime. We support good, old-fashioned hacking of the kind that led to
the creation of the Internet and a new era of freedom of information. But we hate computer crime. So don't email us about any crimes
you may have committed!
To subscribe to Happy Hacker and receive the Guides to (mostly) Harmless
Hacking, please email hacker@techbroker.com with message "subscribe
happy-hacker" in the body of your message.

"Saïmo"
1/1