HACKING INTO COMPUTER SYSTEMS

A Beginners Guide

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.
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.htm
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).
;xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
;xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
.
.
.

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 zero. 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? W ant 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.
'em

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 nine: 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