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 They are full of vague and out of date stuph.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.

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
.
.
.

[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 had a real deadline!) 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

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 hackerworld, 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/~mitz/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

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 informa>

Transfer interrupted!

sts.

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

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

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.

- You have pending charges in another jurisdiction.

What results from all this "bail reform" is that only about 20% of persons arrested make bail. On top of that it takes 1-3 weeks to process your bail papers when property is involved in securing your bond.

Now you're in jail, more specifically you are either in an administrative holding facility or a county jail that has a contract with the Feds to hold their prisoners. Pray that you are in a large enough city to justify its own Federal Detention Center. County jails are typically the last place you would want to be.

H. STATE VS. FEDERAL CHARGES

In some cases you will be facing state charges with the possibility of the Feds "picking them up." You may even be able to nudge the Feds into indicting you. This is a tough decision. With the state you will do considerably less time, but will face a tougher crowd and conditions in prison. Granted Federal Prisons can be violent too, but generally as a non-violent white collar criminal you will eventually be placed into an environment with other low security inmates. More on this later.

Until you are sentenced, you will remain as a "pretrial inmate" in general population with other inmates. Some of the other inmates will be predatorial but the Feds do not tolerate much nonsense. If someone acts up, they'll get thrown in the hole. If they continue to pose a threat to the inmate population, they will be left in segregation (the hole). Occasionally inmates that are at risk or that have been threatened will be placed in segregation. This isn't really to protect the inmate. It is to pr otect the prison from a lawsuit should the inmate get injured.

I. COOPERATING

Naturally when you are first arrested the suits will want to talk to you. First at your residence and, if you appear to be talkative, they will take you back to their offices for an extended chat and a cup of coffee. My advice at this point is tried and true and we've all heard it before: remain silent and ask to speak with an attorney. Regardless of what the situation is, or how you plan to proceed, there is nothing you can say that will help you. Nothing. Even if you know that you are going to cooperate, this is not the time.

This is obviously a controversial subject, but the fact of the matter is roughly 80% of all defendants eventually confess and implicate others. This trend stems from the extremely long sentences the Feds are handing out these days. Not many people want to do 10 to 20 years to save their buddies' hides when they could be doing 3 to 5. This is a decision each individual needs to make. My only advice would be to save your close friends and family. Anyone else is fair game. In the prison system the blacks have a saying "Getting down first." It's no secret that the first defendant in a conspiracy is usually going to get the best deal. I've even seen situations where the big fish turned in all his little fish and eceived 40% off his sentence.

Incidently, being debriefed or interrogated by the Feds can be an ordeal in itself. I would -highly- reccommend reading up on interrogation techniques ahead of time. Once you know their methods it will be all quite transparent to you and the debriefing goes much more smoothly.

When you make a deal with the government you're making a deal with the devil himself. If you make any mistakes they will renege on the deal and you'll get nothing. On some occasions the government will trick you into thinking they want you to cooperate when they are not really interested in anything you have to say. They just want you to plead guilty. When you sign the cooperation agreement there are no set promises as to how much of a sentence reduction you will receive. That is to be decided after your testimony, etc. and at the time of sentencing. It's entirely up to the judge. However, the prosecution makes the recommendation and the judge generally goes along with it. In fact, if the prosecution does not motion the court for your "downward departure" the courts' hands are tied and you get no break.

As you can see, cooperating is a tricky business. Most people, particularly those who have never spent a day in jail, will tell you not to cooperate. "Don't snitch." This is a noble stance to take. However, in some situations it is just plain stupid. Saving someone's ass who would easily do the same to you is a tough call. It's something that needs careful consideration. Like I said, save your friends then do what you have to do to get out of prison and on with your life.

I'm happy to say that I was able to avoid involving my good friends and a former employer in the massive investigation that surrounded my case. It wasn't easy. I had to walk a fine line. Many of you probably know that I (Agent Steal) went to work for the FBI after I was arrested. I was responsible for teaching several agents about hacking and the culture. What many of you don't know is that I had close FBI ties prior to my arrest. I was involved in hacking for over 15 years and had worked as a comp uter security consultant. That is why I was given that opportunity. It is unlikely however, that we will see many more of these types of arrangements in the future. Our relationship ran afoul, mostly due to their passive negligence and lack of experience in dealing with hackers. The government in general now has their own resources, experience, and undercover agents within the community. They no longer need hackers to show them the ropes or the latest security hole.

Nevertheless, if you are in the position to tell the Feds something they don't know and help them build a case against someone, you may qualify for a sentence reduction. The typical range is 20% to 70%. Usually it's around 35% to 50%. Sometimes you may find yourself at the end of the prosecutorial food chain and the government will not let you cooperate. Kevin Mitnick would be a good example of this. Even if he wanted to roll over, I doubt it would get him much. He's just too big of a fish, too much media. My final advice in this matter is get the deal in writing before you start cooperating.

The Feds also like it when you "come clean" and accept responsibility. There is a provision in the Sentencing Guidelines, 3E1.1, that knocks a little bit of time off if you confess to your crime, plead guilty and show remorse. If you go to trial, typically you will not qualify for the "acceptance of responsibility" and your sentence will be longer.

J. STILL THINKING ABOUT TRIAL

Many hackers may remember the Craig Neidorf case over the famous 911 System Operation documents. Craig won his case when it was discovered that the manual in question, that he had published in Phrack magazine, was not proprietary as claimed but available publicly from AT&T. It was an egg in the face day for the Secret Service.

Don't be misled by this. The government learned a lot from this fiasco and even with the laudable support from the EFF, Craig narrowly thwarted off a conviction. Regardless, it was a trying experience (no pun intended) for him and his attorneys. Th e point I'm trying to make is that it's tough to beat the Feds. They play dirty and will do just about anything, including lie, to win their case. If you want to really win you need to know how they build a case in the first place.

K. SEARCH AND SEIZURE

There is a document entitled "Federal Guidelines For Searching And Seizing Computers." It first came to my attention when it was published in the 12-21-94 edition of the Criminal Law Reporter by the Bureau of National Affairs (Cite as 56 CRL 2023) . It's an intriguing collection of tips, cases, mistakes and, in general, how to bust computer hackers. It's recommended reading.

Search and seizure is an ever evolving jurisprudence. What's not permissible today may, through some convoluted Supreme Court logic, be permissible and legal tomorrow. Again, a complete treatment of this subject is beyond the scope of this paper. But suffice it to say if a Federal agent wants to walk right into your bedroom and seize all of your computer equipment without a warrant he could do it by simply saying he had probable cause (PC). PC is anything that gives him an inkling to believe you we re committing a

While I was incarcerated in 95/96, the prison band program was still in operation. I played drums for two different prison bands. It really helped pass the time and when I get out I will continue with my career in music. Now the program has been canceled, all because some senator wanted to be seen as being tough on crime. Bills were passed in Congress. The cable TV is gone, pornography mags are no longer permitted, and the weight piles are being removed. All this means is that prisoners will have m ore spare time on their hands, and so more guards will have to be hired to watch the prisoners. I don't want to get started on this subject. Essentially what I'm saying is make something out of your time. Study, get into a routine and before you know you 'll be going home, and a better person on top of it.

G. DISCIPLINARY ACTIONS

What fun is it if you go to prison and don't get into some mischief? Well, I'm happy to say the only "shots" (violations) I ever received were for having a friend place a call with his three-way calling for me (you can't call everyone collect), and drinking homemade wine. |-) The prison occasionally monitors your phone calls and on the seven or eight hundredth time I made a three-way I got caught. My punishment was ten hours of extra duty (cleaning up). Other punishments for shots include loss of phone use, loss of commissary, loss of visits, and getting thrown in the hole. Shots can also increase your security level and can get you transferred to a higher level institution. If you find yourself having trouble in this area you may want to pick up t he book, "How to win prison disciplinary hearings", by Alan Parmelee, 206-328-2875.

H. ADMINISTRATIVE REMEDY

If you have a disagreement with the way staff is handling your case (and you will) or another complaint there is an administrative remedy procedure. First you must try to resolve it informally. Then you can file a form BP-9. The BP-9 goes to the warden. After that you can file a BP-10 which goes to the Region. Finally, a BP-11 goes to the National BOP Headquarters (Central Office). The whole procedure is a joke and takes about six months to complete. Delay and conquer is the BOP motto. Although complete the remedy process to no avail, you may file your action in a civil court. In some extreme cases you may take your case directly to the courts without exhausting the remedy process. Again, the "Prisoners Self-Help Litigation Manual" covers this qu ite well.

My best advice with this remedy nonsense is to keep your request brief, clear, concise and only ask for one specific thing per form. Usually if you request "coming" you will get it. If you don't, or if the BOP can find any reason to deny your request, they will.

For this reason I often took my problems outside the prison from the start. If it was a substantial enough issue I would inform the media, the director of the BOP, all three of my attorneys, my judge and the ACLU. Often this worked. It always pisse d them off. But, alas I'm a man of principle and if you deprive me of my rights I'm going to raise hell. In the past I might have resorted to hacker tactics, like disrupting the BOP's entire communication system bringing it crashing down! But...I'm rehabilitated now. Incidently, most BOP officials and inmates have no concept of the kind of havoc a hacker can wield on an individuals life. So until some hacker shows the BOP which end is up you will have to accept the fact most everyone you meet in prison will have only nominal respect for you. Deal with it, you're not in cyberspace anymore.

I. PRISON OFFICIALS

There are two types, dumb and dumber. I've had respect for several but I've never met one that impressed me as being particularly talented in a way other than following orders. Typically you will find staff that are either just doing their job, or staff that is determined to advance their career. The latter take their jobs and themselves way too seriously. They don't get anywhere by being nice to inmates so they are often quite curt. Ex-military and law enforcement wannabes are commonplace. All in all they're a pain in the ass but easy to deal with. Anyone who has ever been down (incarcerated) for awhile knows it's best to keep a low profile. If they don't know you by name you're in good shape.

Just when you think the fun is all over, after you are released from prison or the CCC, you will be required to report to a Probation Officer. For the next 3 to 5 years you will be on Supervised Release. The government abolished parole, thereby preventing convicts from getting out of prison early. Despite this they still want to keep tabs on you for awhile.

Supervised Release, in my opinion, is nothing more than extended punishment. You are a not a free man able to travel and work as you please. All of your activities will have to be presented to your Probation Officer (P.O.). And probation is essentially what Supervised Release is. Your P.O. can violate you for any technical violations and send you back to prison for several months, or over a year. If you have ANY history of drug use you will be required to submit to random (weekly) urinalyses. If you come up dirty it's back to the joint.

As a hacker you may find that your access to work with, or possession of computer equipment may be restricted. While this may sound pragmatic to the public, in practice it serves no other purpose that to punish and limit a former hacker's ability t o support himself. With computers at libraries, copy shops, schools, and virtually everywhere, it's much like restricting someone who used a car to get to and from a bank robbery to not ever drive again. If a hacker is predisposed to hacking he's going to be able to do it with or without restrictions. In reality many hackers don't even need a computer to achieve their goals. As you probably know a phone and a little social engineering go a long way.

But with any luck you will be assigned a reasonable P.O. and you will stay out of trouble. If you give your P.O. no cause to keep an eye on you, you may find the reins loosening up. You may also be able to have your Supervised Release terminated ea rly by the court. After a year or so, with good cause, and all of your government debts paid, it might be plausible. Hire an attorney, file a motion.

For many convicts Supervised Release is simply too much like being in prison. For those it is best to violate, go back to prison for a few months, and hope the judge terminates their Supervised Release. Although the judge may continue your supervis ion, he/she typically will not.

N. SUMMARY

What a long strange trip it's been. I have a great deal of mixed emotions about my whole ordeal. I can however, say that I HAVE benefitted from my incarceration. However, it certainly was not on the behalf of how I was handled by the government. No, despite their efforts to kick me when I was down, use me, turn their backs after I had assisted them, and in general, just violate my rights, I was still able to emerge better educated than when I went in. But frankly, my release from prison was just in the nick of time. The long term effects of incarceration and stress were creeping up on me, and I could see prison conditions were worsening. It's hard to express the poignancy of the situation but the majority of those incarcerated feel that if drastic changes are not made America is due for some serious turmoil, perhaps even a civil war. Yes, the criminal justice system is that screwed up. The Nation's thirst for vengeance on criminals is leading us into a vicious feedback loop of crime and punishment, and once again crime. Quite simply, the system is not working. My purpose in writing this article was not to send any kind of message. I'm not telling you how not to get caught and I'm not telling you to stop hacking. I wrote this simply because I feel l ike I owe it to whomever might get use of it. For some strange reason I am oddly compelled to tell you what happened to me. Perhaps this is some kind or therapy, perhaps it's just my ego, perhaps I just want to help some poor 18-year-old hacker who really doesn't know what he is getting himself in to. Whatever the reason, I just sat down one day and started writing.

If there is a central theme to this article it would be how ugly your world can become. Once you get grabbed by the law, sucked into their vacuum, and they shine the spotlight on you, there will be little you can do to protect yourself. The vultures and predators will try to pick what they can off of you. It's open season for the U.S. Attorneys, your attorney, other inmates, and prison officials. You become fair game. Defending yourself from all of these forces will require all of your wits, all of your resources, and occasionally your fists.

In fact, soon you will be learning hacks that shed light on how other people (Not you, right? Promise?) may crack into the non-public parts of hosts. And-- these are hacks that anyone can do.

But, there is one thing you really need to get. It will make hacking infinitely easier:

A SHELL ACCOUNT!!!!

A “shell account” is an Internet account in which your computer becomes a terminal of one of your ISP’s host computers. Once you are in the “shell” you can give commands to the Unix operating system just like you were sitting there in front of one of your ISP’s hosts.

Warning: the tech support person at your ISP may tell you that you have a “shell account” when you really don’t. Many ISPs don’t really like shell accounts, either. Guess why? If you don’t have a shell account, you can’t hack!

But you can easily tell if it is a real shell account. First, you should use a “terminal emulation program” to log on. You will need a program that allows you to imitate a VT 100 terminal. If you have Windows 3.1 or Windows 95, a VT 100 terminal program is included as one of your accessory program.

Any good ISP will allow you to try it out for a few days with a guest account. Get one and then try out a few Unix commands to make sure it is really a shell account.

You don’t know Unix? If you are serious about understanding hacking, you’ll need some good reference books. No, I don't mean the kind with breathless titles like “Secrets of Super hacker.” I’ve bought too many of that kind of book. They are full of hot air and thin on how-to. Serious hackers study books on:
a) Unix. I like "The Unix Companion" by Harley Hahn.
b) Shells. I like "Learning the Bash Shell" by Cameron Newham and Bill Rosenblatt. A “shell” is the command interface between you and the Unix operating system.
c) TCP/IP, which is the set of protocols that make the Internet work. I like "TCP/IP for Dummies" by Marshall Wilensky and Candace Leiden.

OK, rant is over. Time to hack!

How would you like to start your hacking career with one of the simplest, yet potentially hairy, hacks of the Internet? Here it comes: telnet to a finger port.

Have you ever used the finger command before? Finger will sometimes tell you a bunch of stuff about other people on the Internet. Normally you would just enter the command:

```
finger Joe_Schmoe@Fubar.com
```

But instead of Joe Schmoe, you put in the email address of someone you would like to check out. For example, my email address is cmeinel@techbroker.com. So to finger me, give the command:

```
finger cmeinel@techbroker.com
```

Now this command may tell you something, or it may fail with a message such as “access denied.”

But there is a more elite way to finger people. You can give the command:

```
telnet llama.swcp.com 79
```

What this command has just done is let you get on a computer with an Internet address of llama.swcp.com through its port 79 -- without giving it a password.

If you have ever done telnet before, you probably just put in the name of the computer you planned to visit, but didn't add in any numbers afterward. But those numbers afterward are what makes the first distinction between the good, boring Internet citizen and someone slaloming down the slippery slope of hackerdom.

What that 25 means is that you are commanding telnet to take you to a specific port on your intended victim, er, computer.

****
Newbie note #3: Ports
A computer port is a place where information goes in or out of it. On your home computer, examples of ports are your monitor, which sends information out, your keyboard and mouse, which send information in, and your modem, which sends information both out and in.

But an Internet host computer such as callisto.unm.edu has many more ports than a typical home computer. These ports are identified by numbers. Now these are not all physical ports, like a keyboard or RS232 serial port (for your modem). They are virtual (software) ports.
****

But there is phun in that port 25. Incredible phun. You see, whenever you telnet to a computer's port 25, you will get one of two results: once in awhile, a message saying "access denied" as you hit a firewall. But, more often than not, you get something like this:

```
Trying 129.24.96.10...
Connected to callisto.unm.edu.
Escape character is '^]'.
220 callisto.unm.edu Smail3.1.28.1 #41 ready at Fri, 12 Jul  96 12:17 MDT
```

Hey, get a look at this! It didn't ask us to log in. It just says ...ready.

Notice it is running Smail3.1.28.1, a program used to compose and send email.

Ohmigosh, what do we do now? Well, if you really want to look sophisticated, the next thing you do is ask callisto.unm.edu to tell you what commands you can use. In general, when you get on a strange computer, at least one of three commands will get you information: "help," "?", or "man." In this case I type in:

```
help
```

... and this is what I get

```
250 The following SMTP commands are recognized:
250
250   HELO hostname      startup and give your hostname
250   MAIL FROM:<sender address>  start transaction from sender
250   RCPT TO:<recipient address>    name recipient for message
250   VRFY <address>         verify deliverability of address
250   EXPN <address>            expand mailing list address
250   DATA                    start text of mail message
250   RSET                  reset state, drop transaction
250   NOOP                     do nothing
250   DEBUG [level]          set debugging level,default 1
250   HELP                   produce this help message
250   QUIT                     close SMTP connection
250
250 The normal sequence of events in sending a message is to state the
```

heck, all Internet hosts know that kind of info. I'll just bull ahead and send fake mail anyhow. Again, my input has no numbers in front, while the responses of the computer are prefaced by the number 250:

```
mail from:santa@north.pole.com
250 santa@north.pole.com... Sender is valid.
rcpt to:cmeinel@nmia.com
250 cmeinel@nmia.com... Recipient is valid.
data
354 Enter mail. End with the . character on a line by itself.
It works!
.
250 Ok
quit
221 InterLink.NET: closing the connection.
```

OK, what kind of email did that computer generate? Here's what I saw using Pine:

```
Return Path: <santa@north.pole.org>
Received:
     from InterLink.NET by nmia.com
          with smtp
         (Linux Smail3.1.28.1 #4)
     id m0ueo7t 000LEKC; Fri, 12 Jul 96 13:43 MDT
Received: from plato.nmia.com by InterLink.NET (AIX 3.2/UCB 5.64/4.03)
       id AA23900; Fri, 12 Jul 1996 15:43:20  0400
```

Oops. Here the InterLink.NET computer has revealed the computer I was on when I telnetted to its port 25. However, many people use that Internet host computer.

```
Date: Fri, 12 Jul 1996 15:43:20  040
From: santa@north.pole.org
Message Id: <9607121943.AA23900@InterLink.NET>
Apparently-To: cmeinel@nmia.com

It worked!
```


OK, here it doesn't say "Apparently-From," so now I know the computer ns.Interlink.Net is a pretty good one to send fake mail from. An experienced email aficionado would know from the Received: line that this is fake mail. But its phoniness doesn't just jump out at you.

I'm going to try another computer. Hmmm, the University of California at Berkeley is renowned for its computer sciences research. I wonder what their hosts are like? Having first looked up the numerical Internet address of one of their machines, I give the command:

```
telnet 128.32.152.164 25
```

It responds with:

```
Trying 128.32.152.164...
Connected to 128.32.152.164.
Escape character is '^]'.
220 remarque.berkeley.edu ESMTP Sendmail 8.7.3/1.31 ready at Thu, 11 Jul 1996 12
help
214 This is Sendmail version 8.7.3
```

Trying 203.15.166.46 ...
telnet: connect: Connection refused

This looks a lot like a phony item in the header. If this really was a computer that handles news groups, it should have a nntp port that accepts visitors. It might only accept a visitor for the split second it takes to see that I am not authorized to use it. But in this case it refuses any connection whatever.

There is another explanation: there is a firewall on this computer that filters out packets from anyone but authorized users. But this is not common in an ISP that would be serving a spammer dating service. This kind of firewall is more commonly used to connect an internal company computer network with the Internet.

Next I try to email postmaster@203.15.166.46 with a copy of the spam. But I get back:

Date: Wed, 28 Aug 1996 21:58:13 -0600
From: Mail Delivery Subsystem <MAILER-DAEMON@techbroker.com>
To: cmeinel@techbroker.com
Subject: Returned mail: Host unknown (Name server: 203.15.166.46: host not found)

The original message was received at Wed, 28 Aug 1996 21:58:06 -0600
from cmeinel@localhost

----- The following addresses had delivery problems -----
postmaster@203.15.166.46 (unrecoverable error)

----- Transcript of session follows -----
501 postmaster@203.15.166.46... 550 Host unknown (Name server: 203.15.166.46: host not found)

----- Original message follows -----
Return-Path: cmeinel
Received: (from cmeinel@localhost) by kitsune.sw.com.sg (8.6.9/8.6.9) id

OK, it looks like the nntp server info was forged, too.

Next we check the second from the top item on the header. Because it starts with the word “news,” I figure it must be a computer that hosts news groups, too. So I check out its nntp port:

telnet news.ironhorse.com nntp

And the result is:

Trying 204.145.167.4 ...
Connected to boxcar.ironhorse.com.
Escape character is '^]'.
502 You have no permission to talk. Goodbye.
Connection closed by foreign host

OK, we now know that this part of the header references a real news server. Oh, yes, we have also just learned the name/address of the computer ironhorse.com uses to handle the news groups: “boxcar.”

I try the next item in the path:

telnet news.uoregon.edu nntp

So what's the legal alternative to fighting kiddie porn? Trying to throw Web kiddie porn guys in jail doesn't always work. While there are laws against it in the US, the problem is that the Internet is global. Many countries have no laws against kiddie porn on the Internet. Even if it were illegal everywhere, in lots of countries the police only bust people in exchange for you paying a bigger bribe than the criminal pays.

****
They can go to jail note: In the US and many other countries, kiddie porn is illegal. If the imagery is hosted on a physical storage device within the jurisdiction of a country with laws against it, the person who puts this imagery on the storage device can go to jail. So if you know enough to help the authorities get a search warrant, by all means contact them. In the US, this would be the FBI.
****

But the kind of mass outrage that keeps spammers on the run can also drive kiddie porn off the Web. *We* have the power.

The key is that no one can force an ISP to carry kiddie porn -- or anything else. In fact, most human beings are so disgusted at kiddie porn that they will jump at the chance to shut it down. If the ISP is run by some pervert who wants to make money by offering kiddie porn, then you go to the next level up, to the ISP that provides connectivity for the kiddie porn ISP. There someone will be delighted to cut off the b*****ds.

So, how do you find the people who can put a Web site on the run? We start with the URL.

I am going to use a real URL. But please keep in mind that I am not saying this actually is a web address with kiddie porn. This is being used for purposes of illustration only because this URL is carried by a host with so many hackable features. It also, by at least some standards, carries X-rated material. So visit it at your own risk.

http://www.phreak.org

Now let's say someone just told you this was a kiddie porn site. Do you just launch an attack? No.

This is how hacker wars start. What if phreak.org is actually a nice guy place? Even if they did once display kiddie porn, perhaps they have repented. Not wanting to get caught acting on a stupid rumor, I go to the Web and find the message "no DNS entry." So this Web site doesn't look like it's there just now.

But it could just be the that the machine that runs the disk that holds this Web site is temporarily down. There is a way to tell if the computer that serves a domain name is running: the ping command:

/usr/etc/ping phreak.org

The answer is:

/usr/etc/ping: unknown host phreak.org

Now if this Web site had been up, it would have responded like my Web site does:

/usr/etc/ping techbroker.com

This gives the answer:

techbroker.com is alive

****

ASYLUM.ASYLUM.ORG 205.217.4.17
NS.NEXCHI.NET 204.95.8.2

Next I wait a few hours and ping phreak.org again. I discover it is now alive. So now we have learned that the computer hosting phreak.org is sometimes connected to the Internet and sometimes not. (In fact, later probing shows that it is often down.)

I try telnetting to their login sequence:

```
telnet phreak.org
Trying 204.75.33.33 ...
Connected to phreak.org.
Escape character is '^]'.



_____  _____ __
___  __ \__  / / /__  __ \__  ____/__   |__  //_/_____________________ _
__  /_/ /_  /_/ /__  /_/ /_  __/  __  /| |_  ,<  _  __ \_  ___/_  __ `/
_  ____/_  __ /_  _, _/_  /___  _  ___ | /| |__/ /_/ /  /   _  /_/ /
/_/     /_/ /_/  /_/ |_| /_____/ /_/  |_/_/ |_|(_)____//_/    _\__, /
                                                              /____/



;
Connection closed by foreign host.
```

Aha! Someone has connected the computer hosting phreak.org to the Internet!

The fact that this gives just ASCII art and no login prompt suggests that this host computer does not exactly welcome the casual visitor. It may well have a firewall that rejects attempted logins from anyone who telnets in from a host that is not on its approved list.

Next I finger their technical contact:

```
finger rain@phreak.org
```

Its response is:

```
[phreak.org]
```

It then scrolled out some embarrassing ASCII art. Finger it yourself if you really want to see it. I'd only rate it PG-13, however.

The fact that phreak.org runs a finger service is interesting. Since finger is one of the best ways to crack into a system, we can conclude that either:

1) The phreak.org sysadmin is not very security-conscious, or
2) It is so important to phreak.org to send out insulting messages that the sysadmin doesn't care about the security risk of running finger.

Since we have seen evidence of a fire wall, case 2 is probably true.

With this set up, all your email going out from Eudora will include that line in the headers. You can add as many extra headers to your email as you want by adding new lines that also start with “extra headers=”. For example, in this case I also added “Favorite-color:turquoise.”

****
You can go to jail warning: There still are ways for experts to tell where you sent this email from. So if someone were to use forged email to defraud, threaten or mail bomb people, watch out for that cellmate named Spike.
****

Is it Possible to Mail Bomb Using Eudora?

The obvious way to mail bomb with Eudora doesn’t work. The obvious way is to put the address of your victim into the address list a few thousand times and then attach a really big file. But the result will be only one message going to that address. This is no thanks to Eudora itself. The mail daemons in common use on the Internet such as sendmail, smail and qmail only allow one message to be sent to each address per email.

Of course there are better ways to forge email with Eudora. Also, there is a totally trivial way to use Eudora to send hundreds of gigantic attached files to one recipient, crashing the mail server of the victim’s ISP. But I’m not telling you how because this is, after all, a Guide to (mostly) Harmless Hacking.

But next time those Global kOS dudes try to snooker you into using one of their mail bomber programs (they claim these programs will keep you safely anonymous but in fact you will get caught) just remember all they are doing is packaging up stuff that anyone who knows two simple tricks could do much better with Eudora. (If you are a legitimate computer security professional, and you want to join us at Inf-War in solving the problem, contact me for details and we’ll think about whether to trust you.

****
Evil Genius Tip: This deadly mailbomber thing is a feature, yes, honest-to-gosh intended FEATURE, of sendmail. Get out your manuals and study.
****

The ease with which one may forge perfect mail and commit mail bombings which crash entire ISP mail servers and even shut down Internet backbone providers such as has recently happened to AGIS may well be the greatest threat the Internet faces today. I’m not happy about revealing this much. Unfortunately, the mail forgery problem is a deeply ingrained flaw in the Internet’s basic structure. So it is almost impossible to explain the basics of hacking without revealing the pieces to the puzzle of the perfect forgery and perfect mailbombing.

If you figure it out, be a good guy and don’t abuse it, OK? Become one of us insiders who see the problem -- and want to fix it rather than exploit it for greed or hatred.

Contents of Volume 2:

Internet for Dummies -- skip this if you are a Unix wizard. But if you read on you'll get some more kewl hacking instructions.

The six Guides to (mostly) Harmless Hacking of Vol. 1 jumped immediately into how-to hacking tricks. But if you are like me, all those details of probing ports and playing with hypotheses and pinging down hosts gets a little dizzying.

So how about catching our breath, standing back and reviewing what the heck it is that we are playing with? Once we get the basics under control, we then can move on to serious hacking.

Also, I have been wrestling with my conscience over whether to start giving you step-by-step instructions on how to gain root access to other peoples' computers. The little angel on my right shoulder whispers, "Gaining root without permission on other people's computers is not nice. So don't tell people how to do it." The little devil on my left shoulder says, "Carolyn, all these hackers think you don't know nothin'! PROOVE to them you know how to crack!" The little angel says, "If anyone reading Guide to (mostly) Harmless Hacking tries out this trick, you might get in trouble with the law for conspiracy to damage other peoples' computers." The little devil says, "But, Carolyn, tell people how to crack into root and they will think you are KEWL!"

So here's the deal. In this and the next few issues of Guide to (mostly) Harmless Hacking I'll tell you several ways to get logged on as the superuser in the root account of some Internet host computers. But the instructions will leave a thing or two to the imagination.

My theory is that if you are willing to wade through all this, you probably aren't one of those cheap thrills hacker wannabes who would use this knowledge to do something destructive that would land you in jail.

****

Technical tip: If you wish to become a "serious" hacker, you'll need Linux (a freeware variety of Unix) on your PC. One r>

Transfer interrupted!

o root legally all you want -- on your own computer. It sure beats struggling around on someone else's computer only to discover that what you thought was root was a cleverly set trap and the sysadmin and FBI laugh at you all the way to jail.

Linux can be installed on a PC with as little as a 386 CPU, only 2 Mb RAM and as little as 20 MB of hard disk. You will need to reformat your hard disk. While some people have successfully installed Linux without trashing their DOS/Windows stuff, don't count on getting away with it. Backup, backup, backup!

****

****

You can go to jail warning: Crack into root on someone else's computer and the slammer becomes a definite possibility. Think about this: when you see a news story about some hacker getting busted, how often do you recognize the name? How often is the latest bust being done to someone famous, like Dark Tangent or se7en or Emmanuel Goldstein? How about, like, never! That's because really good hackers figure out how to not do stupid stuff. They learn how to crack into computers for the intellectual challenge and to figure out how to make computers safe from intruders. They don't bull their way into root and make a mess of things, which tends to inspire sysadmins to call the cops.

****

In fact, you can get lots of details on any Unix command with "man."

Have fun with ping -- and be good! But remember, I'm not begging the evil genius wannabes to be good. See if I care when you get busted...

_____

GUIDE TO (mostly) HARMLESS HACKING

Vol. 2 Number 4

More intro to TCP/IP: port surfing! Daemons! How to get on almost any computer without logging in and without breaking the law. Impress your clueless friends and actually discover kewl, legal, safe stuph.

_____

A few days ago I had a lady friend visiting. She's 42 and doesn't own a computer. However, she is taking a class on personal computers at a community college. She wanted to know what all this hacking stuph is about. So I decided to introduce her to port surfing. And while doing it, we stumbled across something kewl.

Port surfing takes advantage of the structure of TCP/IP. This is the protocol (set of rules) used for computers to talk to each other over the Internet. One of the basic principles of Unix (the most popular operating system on the Internet) is to assign a "port" to every function that one computer might command another to perform. Common examp les are to send and receive email, read Usenet newsgroups, telnet, transfer files, and offer Web pages.

****

Newbie note #1: A computer port is a place where information goes in or out of it. On your home computer, examples of ports are your monitor, which sends information out, your keyboard and mouse, which send information in, and your modem, which sends information both out and in.

But an Internet host computer such as callisto.unm.edu has many more ports than a typical home computer. These ports are identified by numbers. Now these are not all physical ports, like a keyboard or RS232 serial port (for your modem). They are virtual (software) ports.

A "service" is a program running on a "port." When you telnet to a port, that program is up and running, just waiting for your input. Happy hacking!

****

So if you want to read a Web page, your browser contacts port number 80 and tells the computer that manages that Web site to let you in. And, sure enough, you get into that Web server computer without a password.

OK, big deal. That's pretty standard for the Internet. Many -- most -- computers on the Internet will let you do some things with them without needing a password,

However, the essence of hacking is doing things that aren't obvious. That don't just jump out at you from the manuals. One way you can move a step up from the run of the mill computer user is to learn how to port surf.

The essence of port surfing is to pick out a target computer and explore it to see what ports are open and what you can do with them.

202.216.224.66 ENSS365.NM.ORG Up,Gateway,H 0 113 se0 1500
192.132.89.3 ENSS365.NM.ORG Up,Gateway,H 0 1100 se0 1500
198.203.196.67 ENSS365.NM.ORG Up,Gateway,H 0 385 se0 1500
160.205.13.3 ENSS365.NM.ORG Up,Gateway,H 0 78 se0 1500
202.247.107.131 ENSS365.NM.ORG Up,Gateway,H 0 19 se0 1500
198.59.167.4 LAWRII.NM.ORG Up,Gateway,H 0 82 se0 1500
128.148.157.6 ENSS365.NM.ORG Up,Gateway,H 0 198 se0 1500
160.45.10.6 ENSS365.NM.ORG Up,Gateway,H 0 3 se0 1500
128.121.50.7 ENSS365.NM.ORG Up,Gateway,H 0 3052 se0 1500
206.170.113.8 ENSS365.NM.ORG Up,Gateway,H 0 1451 se0 1500
128.148.128.9 ENSS365.NM.ORG Up,Gateway,H 0 1122 se0 1500
203.7.132.9 ENSS365.NM.ORG Up,Gateway,H 0 14 se0 1500
204.216.57.10 ENSS365.NM.ORG Up,Gateway,H 0 180 se0 1500
130.74.1.75 ENSS365.NM.ORG Up,Gateway,H 0 10117 se0 1500
206.68.65.15 ENSS365.NM.ORG Up,Gateway,H 0 249 se0 1500
129.219.13.81 ENSS365.NM.ORG Up,Gateway,H 0 547 se0 1500
204.255.246.18 ENSS365.NM.ORG Up,Gateway,H 0 1125 se0 1500
160.45.24.21 ENSS365.NM.ORG Up,Gateway,H 0 97 se0 1500
206.28.168.21 ENSS365.NM.ORG Up,Gateway,H 0 2093 se0 1500
163.179.3.222 ENSS365.NM.ORG Up,Gateway,H 0 315 se0 1500
198.109.130.33 ENSS365.NM.ORG Up,Gateway,H 0 1825 se0 1500
199.224.108.33 ENSS365.NM.ORG Up,Gateway,H 0 11362 se0 1500
203.7.132.98 ENSS365.NM.ORG Up,Gateway,H 0 73 se0 1500
198.111.253.35 ENSS365.NM.ORG Up,Gateway,H 0 1134 se0 1500
206.149.24.100 ENSS365.NM.ORG Up,Gateway,H 0 3397 se0 1500
165.212.105.106 ENSS365.NM.ORG Up,Gateway,H 0 17 se0 1006
205.238.3.241 ENSS365.NM.ORG Up,Gateway,H 0 69 se0 1500
198.49.44.242 ENSS365.NM.ORG Up,Gateway,H 0 25 se0 1500
194.22.188.242 ENSS365.NM.ORG Up,Gateway,H 0 20 se0 1500
164.64.0 LAWRII.NM.ORG Up,Gateway 1 40377 se0 1500
0.0.0 ENSS365.NM.ORG Up,Gateway 2 47284 se0 1500
207.66.1 GLORY.NM.ORG Up,Gateway 0 151 se0 1500
205.166.1 GLORY.NM.ORG Up,Gateway 0 1978 se0 1500
204.134.1 LAWRII.NM.ORG Up,Gateway 0 54 se0 1500
204.134.2 GLORY.NM.ORG Up,Gateway 0 138 se0 1500
192.132.2 129.121.248.1 Up,Gateway 0 6345 se0 1500
204.134.67 GLORY.NM.ORG Up,Gateway 0 2022 se0 1500
206.206.67 GLORY.NM.ORG Up,Gateway 0 7778 se0 1500
206.206.68 LAWRII.NM.ORG Up,Gateway 0 3185 se0 1500
207.66.5 GLORY.NM.ORG Up,Gateway 0 626 se0 1500
204.134.69 GLORY.NM.ORG Up,Gateway 0 7990 se0 1500
207.66.6 GLORY.NM.ORG Up,Gateway 0 53 se0 1500
204.134.70 LAWRII.NM.ORG Up,Gateway 0 18011 se0 1500
192.188.135 GLORY.NM.ORG Up,Gateway 0 5 se0 1500
206.206.71 LAWRII.NM.ORG Up,Gateway 0 2 se0 1500
204.134.7 GLORY.NM.ORG Up,Gateway 0 38 se0 1500
199.89.135 GLORY.NM.ORG Up,Gateway 0 99 se0 1500
198.59.136 LAWRII.NM.ORG Up,Gateway 0 1293 se0 1500
204.134.9 GLORY.NM.ORG Up,Gateway 0 21 se0 1500
204.134.73 GLORY.NM.ORG Up,Gateway 0 59794 se0 1500
129.138.0 GLORY.NM.ORG Up,Gateway 0 5262 se0 1500
192.92.10 LAWRII.NM.ORG Up,Gateway 0 163 se0 1500
206.206.75 LAWRII.NM.ORG Up,Gateway 0 604 se0 1500
207.66.13 GLORY.NM.ORG Up,Gateway 0 1184 se0 1500

11 systat Lots of info on users

13 daytime Time and date at computer's location

15 netstat Tremendous info on networks but rarely used any more

19 chargen Pours out a stream of ASCII characters. Use ^C to stop.

21 ftp Transfers files

22 ssh secure shell login -- encrypted tunnel

23 telnet Where you log in if you don't use ssh:)

25 smpt Forge email from Bill.Gates@Microsoft.org.

37 time Time

39 rlp Resource location

43 whois Info on hosts and networks

53 domain Nameserver

70 gopher Out-of-date info hunter

79 finger Lots of info on users

80 http Web server

110 pop Incoming email

119 nntp Usenet news groups -- forge posts, cancels

443 shttp Another web server

512 biff Mail notification

513 rlogin Remote login
who Remote who and uptime

514 shell Remote command, no password used!
syslog Remote system logging -- how we bust hackers

520 route Routing information protocol

****
Propeller head tip: Note that in most cases an Internet host will use these port number assignments for these services. More than one service may also be assigned simultaneously to the same port. This numbering system is voluntarily offered by the Internet Engineering Task Force (IETF). That means that an Internet host may use other ports for these services. Expect the unexpected!

If you have a copy of Linux, you can get the list of all the IETF assignments of port numbers in the file /etc/services.

Contents of Volume 3:

GUIDE TO (mostly) HARMLESS HACKING

Vol. 3 Number 1

How to protect yourself from email bombs!

Email bombs! People like angry johnny, AKA the "Unamailer," have made the news lately by arranging for 20 MB or more of email -- tens of thousands of messages -- to flood every day into his victims' email accounts.

Email bombing can be bad news for two reasons. One, the victim can't easily find any of their legitimate email in that giant garbage heap of spam. Two, the flood of messages ties up mail servers and chews up communications bandwidth.

Of course, those are the two main reasons that email bombers make their attacks: to mess up people's email and/or harm the ISPs they target. The email bomb is a common weapon of war against Internet hosts controlled by spammers and cyber anarchists. It also is used by users with a grudge.

News stories make it sound like email bombing victims are, ahem, s*** out of luck. But we aren't. We know, because angry – the Christmas email bomber – told the press that he had targeted the Happy Hacker list's Supreme Commanderess, Carolyn Meinel. (Someone simultaneously attempted to email bomb the Happy Hacker list itself but no one has stepped forward to take credit for the attempt).

But as you know from the fact that we got the Happy Hacker Digest out after the attack, and by the fact that I kept answering my email, there are ways to beat the email bombers.

Now most of these are techniques for use by experts only. But if you are, like most of us on this list, a newbie, you may be able to win points with your ISP by emailing its technical help people with some of the information within this guide. Maybe then they'll forgive you if your shell log file gets to looking a little too exciting!

My first line of defense is to use several on-line services. That way, whenever one account is getting hacked, bombed, etc., I can just email all my correspondents and tell them where to reach me. Now I've never gotten bombed into submission, but I have gotten hacked badly and often enough that I once had to dump an ISP in disgust. Or, an ISP may get a little too anxious over your hacking experiments. So it's a good idea to be prepared to jump accounts.

But that's a pretty chicken way to handle email bombing. Besides, a member of the Happy Hacker list says that the reason angry johnny didn't email bomb all the accounts I most commo nly use is because he

What happened was an inconvenience--equivalent, in my estimation, to the same kind of inconvenience people experienced when young people blocked the streets of major cities in protest against the war in Vietnam. People were
inconvenienced --- but the protesters were making a point about an illegal and unnecessary war that even the prosecutors of the war, like Robert McNamara knew from the beginning was a lost venture. Hundreds of thousands
of people lost their lives in that war -- and if some people found themselves inconvenienced by people protesting against it – I say, too d*** bad.

Thank you for forwarding my remarks to your list

Ahem. I'm flattered, I guess. Is Koch suggesting the Happy Hacker list -- with its habit of ***ing out naughty words -- and evangelist Billy Graham -- whose faith I share -- are of an Earth-shaking level of political bad newsness comparable to the Vietnam War?

So let's say you don't feel that it is OK for any two-bit hacker wannabe to keep you from receiving email. what are some more ways to fight email bombs?

For bombings using email lists, one approach is to run a program that sorts through the initial flood of the email bomb for those "Welcome to the Tomato Twaddler List!" messages which tell how to unsubscribe. These programs then automatically compose unsubscribe messages and send them out.

Another way your ISP can help you is to provide a program called Procmail (which runs on the Unix operating system. For details, Zach Babayco (zachb@netcom.com) has provided the following article. Thank you, Zach!

****
Defending Against Email-Bombing and Unwanted Mail

Copyright (C) Zach Babayco 1996

[Before I start this article, I would like to thank Nancy McGough for letting me quote liberally from her Filtering Mail FAQ, available at http://www.cis.ohio-state.edu/hypertext/faq/usenet/mail/filtering-faq/faq.html. This is one of the best filtering-mail FAQs out there, and if you have any problems with my directions or want to learn more about filtering mail, this is where you should look.]

Lately, there are more and more people out there sending you email that you just don't want, like "Make Money Fast!" garbage or lame ezines that you never requested or wanted in the first place. Worse, there is the email bomb.

There are two types of email bombs, the Massmail and the Mailing List bomb:

1) Massmail-bombing. This is when an attacker sends you hundreds, or perhaps even thousands of pieces of email, usually by means of a script and fakemail. Of the two types, this is the easier to defend against, since the messages will be coming from just a few addresses at the most.

2) Mailing List bombs. In this case, the attacker will subscribe you to as many mailing lists as he or she can. This is much worse than a massmail because you will be getting email from many different mailing lists, and will have to save some of it so that you can figure out how to unsubscribe from each list.

This is where Procmail comes in. Procmail (pronounced prok-mail) is a email filtering program that can do some very neat things with your mail, like for example, if you subscribe to several high-volume mailing lists,

"|exec /usr/local/bin/procmail USER=nancym"
In another world:
"|IFS=' ';exec /usr/local/bin/procmail #nancym"
In a different world:
"|IFS=' ';exec /usr/local/bin/procmail USER=nancym"
In a smrsh world:
"|/usr/local/bin/procmail #nancym"

Now that you have all the necessary files made, it's time to test this filter. Go into your mailreader and create a new folder called Ebombtest. This procedure differs from program to program, so you may have to experiment a little. Then open up the rc.noebomb file and change /dev/null to Ebombtest. (You should have already changed Conditions 2 and 3 to what you want; if not, go do it now!) Finally, open up .procmailrc and remove the # from the last line.

You will need to leave this on for a bit to test it. Ask some of the people in Condition 2 to send you some test messages. If the messages make it through to your Inbox, then that condition is working fine. Send yourself some fake email under a different name and check to see if it
ends up in the Ebombtest folder. Also, send yourself some fakemail from root@wherever.com to make sure that Condition 1 works. If you're on any mailing lists, those messages should be ending up in your Inbox as well.

If all of these test out fine, then congratulations! You now have a working defense against email bombs. For the moment, change the Ebombtest line in the rc.noebomb file back to /dev/null, and put the # in front of the INCLUDERC line in the .procmailrc file. If someone ever decides to emailbomb you, you only need to remove the #, and you will have greatly cut down on the amount of messages coming into your Inbox, giving you a little bit of breathing room to start unsubscribing to all those lists, or start tracking down those idiots who did it and get their
asses kicked off their ISP's.

If you have any comments or questions about this, email me at zasha@netcom.com. Emailbombs WILL go to /dev/null, so don't bother!

Disclaimer: When you activate this program, it is inevitable that a small amount of wanted mail MAY get put into /dev/null, due to the fact that it is nearly impossible to know the names of all the people that may write to you. Therefore, I assume no responsibility for any email which
may get lost, and any damages which may come from those lost messages.

****
Don't have procmail? If you have a Unix box, you can download procmail from ftp://ftp.informatik.rwth-aachen.de/pub/packages/procmail/
****

A note of thanks goes to Damien Sorder (jericho@dimensional.com) for his assistance in reviewing this guide.

And now, just to make certain you can get this invaluable Perl script to automatically unsubscribe email lists, here is the listing:

```
#!/usr/local/bin/perl

#  unsubscribe
#
# A perl script by Kim Holburn, University of Canberra 1996.
# kim@canberra.edu.au
```

```
foreach $file (@ARGV) {
  %addresses=();
  if (!$usersupplied) { $user=$file; }
  $user =~ s@^.*/@@;
  if ($file =~ /^\./) { print "skipping wrong type of file \"$file\"\n"; next; }
  if ($file =~ /\.lock/)
    { print "skipping lock file\"$file\"\n"; next; }
  if ($file =~ /\./) { print "skipping wrong type of file\"$file\"\n"; next; }
  $user =~ s/^\.//;
  $user =~ s/\..*$//;
  if (!open (MYFILE, "<$file" ))
    { print "Couldn't open file \"$file\"\n"; next; }
  print "-------------------------opening file\"$file\"\n";
  while (<MYFILE>) {
#    if (/(\bnews-[-\w.]+@)|([-\w.]+-news@)/i)
#    if (/(\brequest-[-\w.]+@)|([-\w.]+-request@)/i)
    if (/(\bowner-[-\w.]+@)|([-\w.]+-owner@)/i) {
      chop;
      tr/A-Z/a-z/;
      if (/\bowner-[-\w.]+@/) { s/^.*\bowner-([-\w.]+@[\w.]+)\b.*$/\1/; }
      else { s/(^|^.*[^-\w.])([-\w.]+)-owner(@[\w.]+)\b.*$/\2\3/; }
      if (/[^a-z0-9@.-]/) { next; }
      if (!defined ($addresses{$_})) { $addresses{$_}=""; }
    }
    if (/(\bl-[-\w.]+@)|([-\w.]+-l@)/i) {
      chop;
      tr/A-Z/a-z/;
      if (/\bl-[-\w.]+@/) { s/^.*\bl-([-\w.]+@[\w.]+)\b.*$/\1/; }
      else { s/(^|^.*[^-\w.])([-\w.]+)-l(@[\w.]+)\b.*$/\2\3/; }
      if (/[^a-z0-9@.-]/) { next; }
      if (!defined ($addresses{$_})) { $addresses{$_}=""; }
    }
  }
  close MYFILE;
  while (($key,$value)=each %addresses) { print "$key\n"; }
  if (! keys %addresses ) { print "no listservers\n";  next; }
  if (! open (MYFILE, "<$file" ))
   { print "Couldn't open file \"$file\"\n"; next; }
  print "looking for listserver addresses\n";
  while (<MYFILE>) {
    foreach $address (keys %addresses) {
      $host=$address;
      $host =~ s/^.*@//;
      if (/(listserv|listproc|majordomo)@$host/i) {
        $addresses{$address}=$1;
#       print "found 1 = \"$1\"\n";
      }
    }
  }
  close MYFILE;
  while (($key,$value)=each %addresses) {
    $host=$key;
    $host=~s/^.*@//;
    $list=$key;
```

you are a beginner, you will find bash (for Bourne again shell) to be easiest to use. Ask tech support at your ISP for a shell account set up to use bash. Or, you may be able to get the bash shell by simply typing the word “bash” at the prompt. If your ISP doesn’t offer shell accounts, get a new ISP that does offer it. A great book on using the bash shell is _Learning the Bash Shell_, by Cameron Newham and Bill Rosenblatt, published by O’Reilly.
****

So for our mapping expedition, let’s start by visiting the Internet in Botswana! Wow, is Botswana even on the Internet? It’s a lovely landlocked nation in the southern region of Africa, famous for cattle ranching, diamonds and abundant wildlife. The language of commerce in Botswana is English, so there’s a good chance that we could understand messages from their computers.

Our first step in learning about Botswana’s Internet hosts is to use the Unix program nslookup.

****
Evil genius tip: Nslookup is one of the most powerful Internet mapping tools in existence. We can hardly do it justice here. If you want to learn how to explore to the max, get the book _DNS and BIND_ by Paul Albitz and Cricket Liu, published by O’Reilly, 1997 edition.
****

The first step may be to find where your ISP has hidden the program by using the command “whereis nslookup.” (Or your computer may use the “find” command.) Aha -- there it is! I give the command:

->/usr/etc/nslookup
Default Server: swcp.com
Address: 198.59.115.2
>

These two lines and the slightly different prompt (it isn’t an arrow any more) tell me that my local ISP is running this program for me. (It is possible to run nslookup on another computer from yours.) Now we are in the program, so I have to remember that my bash commands don’t work any more. Our next step is to tell the program that we would like to know what computers handle any given domain name.

> set type=ns

Next we need to know the domain name for Botswana. To do that I look up the list of top level domain names on page 379 of the 1997 edition of _DNS and BIND_. For Botswana it’s bw. So I enter it at the prompt, remembering -- this is VERY important -- to put a period after the domain name:

> bw.
Server: swcp.com
Address: 198.59.115.2

Non-authoritative answer:

This “non-authoritative answer” stuff tells me that this information has been stored for awhile, so it is possible, but unlikely, that the information below has changed.

bw nameserver = DAISY.EE.UND.AC.ZA
bw nameserver = RAIN.PSG.COM
bw nameserver = NS.UU.NET
bw nameserver = HIPPO.RU.AC.ZA
Authoritative answers can be found from:
DAISY.EE.UND.AC.ZA inet address = 146.230.192.18

script. Don't use it. If you do, I'll give another interview to PC World magazine (http://www.pcworld.com/news/newsradio/meinel/index.html) about how a three-year-old could run the attack. And if you get caught we'll all laugh at you as you get hustled off in chains while your journalist friend gets a $250K advance on his or her book deal about you.
****

I give the command:

->whereis traceroute
traceroute: /usr/local/bin/traceroute

OK, now we're ready to map in earnest. I give the command:

->/usr/local/bin/traceroute DAISY.EE.UND.AC.ZA

And the answer is:

traceroute to DAISY.EE.UND.AC.ZA (146.230.192.18), 30 hops max, 40 byte packets
1 sisko (198.59.115.1) 3 ms 4 ms 4 ms
2 glory-cyberport.nm.westnet.net (204.134.78.33) 47 ms 8 ms 4 ms
3 ENSS365.NM.ORG (129.121.1.3) 5 ms 10 ms 7 ms
4 h4-0.cnss116.Albuquerque.t3.ans.net (192.103.74.45) 17 ms 41 ms 28 ms
5 f2.t112-0.Albuquerque.t3.ans.net (140.222.112.221) 7 ms 6 ms 5 ms
6 h14.t16-0.Los-Angeles.t3.ans.net (140.223.17.9) 31 ms 39 ms 84 ms
7 h14.t8-0.San-Francisco.t3.ans.net (140.223.9.13) 67 ms 43 ms 68 ms
8 enss220.t3.ans.net (140.223.9.22) 73 ms 58 ms 54 ms
9 sl-mae-w-F0/0.sprintlink.net (198.32.136.11) 97 ms 319 ms 110 ms
10 sl-stk-1-H11/0-T3.sprintlink.net (144.228.10.109) 313 ms 479 ms 473 ms
11 sl-stk-2-F/T.sprintlink.net (198.67.6.2) 179 ms * *
12 sl-dc-7-H4/0-T3.sprintlink.net (144.228.10.106) 164 ms * 176 ms
13 sl-dc-7-F/T.sprintlink.net (198.67.10.1) 143 ms 129 ms 3[illegible] ms
14 gsl-dc-3-Fddi0/0.sprint.net (204.59.144.197) 135 ms 152 ms 130 ms
15 204.59.225.66 (204.59.225.66) 582 ms 545 ms 565 ms
16 * * *
17 e0.csir00.uni.net.za (155.232.249.1) 516 ms 436 ms 400 ms
18 s1.und00.uni.net.za (155.232.70.1) 424 ms 485 ms 492 ms
19 e0.und01.uni.net.za (155.232.190.2) 509 ms 530 ms 459 ms
20 s0.und02.uni.net.za (155.232.82.2) 650 ms * 548 ms
21 Gw-Uninet1.CC.und.ac.za (146.230.196.1) 881 ms 517 ms 478 ms
22 cisco-unp.und.ac.za (146.230.128.8) 498 ms 545 ms *
23 IN.ee.und.ac.za (146.230.192.18) 573 ms 585 ms 493 ms

So what does all this stuff mean?

The number in front of each line is the number of hops since leaving the computer that has the shell account I am using.

The second entry is the name of the computer through which this route passes, first in text, and then in parentheses its numerical representation.

The numbers after that are the time in milliseconds it takes for each of three probe packets in a row to make that hop. When an * appears, the time for the hop timed out. In the case of this traceroute command, any time greater than 3 seconds causes an * to be printed out.

[ ] enable-incoming-folders
[ ] enable-jump-shortcut
[ ] enable-mail-check-cue
[ ] enable-suspend
[ ] enable-tab-completion
[ ] enable-unix-pipe-cmd
[ ] expanded-view-of-addressbooks
[ ] expanded-view-of-folders
[ ] expunge-without-confirm
[ ] include-attachments-in-reply

? Help E Exit Config P Prev - PrevPage
X [Set/Unset] N Next Spc NextPage W WhereIs

You first highlight the line that says “enable-full-header-command” and then press the “x” key. The give “e” to exit saving the change. Once you have done this, when you are reading your email you will be able to see full headers by giving the “h” command.

Elm is another Unix email reading program. It actually gives slightly more detailed headers than Pine, and automatically shows full headers.

WHAT DOES ALL THAT STUFF IN YOUR HEADERS MEAN?

We’ll start by taking a look at a mildly interesting full header. Then we’ll examine two headers that reveal some interesting shenanigans. Finally we will look at a forged header.

OK, let us return to that fairly ordinary full header we looked at above. We will decipher it piece by piece. First we look at the simple version:

From: Vegbar Fubar <fooha@ifi.fo[illegible]
Date: Fri, 11 Apr 1997 18:00:[illegible] GMT
To: hacker@techbr[illegible].com

The information within any header consists of a series of fields separated from each other by a “newline” character. Each field consists of two parts: a field name, which includes no spaces and is terminated by a colon; and the contents of the field. In this case the only fields that show are “From:,” “Date:,” and “To:”.

In every header there are two classes of fields: the “envelope,” which contains only the sender and recipient fields; and everything else, which is information specific to the handling of the message. In this case the only field that shows which gives information on the handling of the message is the Date field.

When we expand to a full header, we are able to see all the fields of the header. We will now go through this information line by line.

Received: by o200.fooway.net (950413.SGI.8.6.12/951211.SGI)for techbr@fooway.net id OAA07210; Fri, 11 Apr 1997 14:10:06 -0400

This line tells us that I downloaded this email from the POP server at a computer named o200.fooway.net. This was done on behalf of my account with email address of techbr@fooway.net. The (950413.SGI.8.6.12/951211.SGI) part identifies the software name and version running that POP server.

****

Received: by o200.fooway.net (950413.SGI.8.6.12/951211.SGI)for techbr@fooway.net id MAA07059; Mon, 14 Apr 1997 12:05:25 -0400
Date: Mon, 14 Apr 1997 12:05:22 -0400

We already looked at this computer o200.fooway.net above. But, heck, let's probe a little more deeply. Since I suspect this is a POP server, I'm going to telnet to port 110, which is normally the POP server port.

> telnet o200.fooway.net 110
Trying 207.xxx.192.57...
Connected to o200.fooway.net.
Escape character is '^]'.
+OK QUALCOMM Pop server derived from UCB (version 2.1.4-R3) at mail starting.

Now we know more about Fooway Technology's POP server. If you have ever run one of those hacker "strobe" type programs that tell you what programs are running on each port of a computer, there is really no big deal to it. They just automate the process that we are doing here by hand. But in my humble opinion you will learn much more by strobing ports by hand the same way I am doing here.

Now we could do lots more strobing, but I'm getting bored. So we check out the second field in this header:

Date: Mon, 14 Apr 1997 12:05:22 -0400

That -0400 is a time correction. But to what is it correcting? Let's see the next field in the header:

Received: from mocha.icefubarnet.com by o200.fooway.net via ESMTP (950413.SGI.8.6.12/951211.SGI) for <hacker@techbroker.com> id MAA06380; Mon, 14 Apr 1997 12:05:20 -0400

Hmmm, why is mocha.icefubarnet.com in the header? If this header isn't forged, it means this mail server was handling the Happy Hacker Digest mailing. So where is mocha.icefubarnet.com located? A quick use of the whois command tells us:

> whois icefubarnet.com
ICEFUBARNET INTERNET, INC (ICEFUBARNET-DOM)
  2178 Fooway
  North Bar, Oregon 97xxx
  USA

Now this is located four time zones earlier than the computer o200.fooway.net. So this explains the time correction notation of -0400.

Next field on the header tells us:

Received: from cmeinel (hd14-211.foo.compuserve.com [206.xxx.205.211]) by mocha.icefubarnet.com (Netscape Mail Server v2.01) with SMTP id AAP3428; Mon, 14 Apr 1997 08:51:02 -0700

This tells us that the Happy Hacker Digest was delivered to the mail server (SMTP stands for simple mail transport protocol) at mocha.icefubarnet.com by Compuserve. But, and this is very important to observe, once again I did not use the Compuserve mail system. This merely represents a PPP session I set up with Compuserve. How can you tell? Playing with nslookup shows that the numerical representation of my Compuserve connection isn't an Internet host. But you can't learn much more easily because Compuserve has great security -- one reason I use it. But take my word for it, this is another way to see a Compuserve PPP session in a header.

Now we get to the biggie, the message ID:

Message-Id: <2.2.16.19970414100122.4387d20a@mail.fooway.net>

Whoa, how come that ID is at the computer mail.fooway.net? It's pretty simple. In Eudora I specified my POP server as mail.fooway.net. But if you were to do a little stobing, you would discover that while fooway.net has a POP server, it doesn't have an SMTP or ESMTP server. You can get mail from Fooway, but you can't mail stuff out from Fooway. But the marvelous workings of the Internet combined with the naivete of the Eudora Pro 2.2 program sent my message ID off to mail.fooway.net anyhow.

On the message ID, the "2.2.16" was inserted by Eudora. That signifies it is the 2.2 version for a 16 bit operating system.

The remaining fields of the header were all inserted by Eudora:

X-Sender: techbr@mail.fooway.net (Unverified)
X-Mailer: Windows Eudora Pro Version 2.2 (16)
Mime-Version: 1.0
Content-Type: text/plain; charset="iso-8859-1"
To: (Recipient list suppressed)
From: "Carolyn P. Meinel" <cmeinel@techbroker.com>
Subject: Happy Hacker Digest April 12, 1997

Notice Eudora does let us know that techbr@mail.fooway.net is unverified as sender. And in fact, it definitely is not the sender. This is a very important fact. The message ID of an email is not necessarily stored with the computer that sent it out.

So how was I able to use Icefubarnet Internet's mail server to send out the Happy Hacker Digest? Fortunately Eudora's naivete makes it easy for me to use any mail server that has an open SMTP or ESMTP port. You may be surprised to discover that there are uncountable Internet mail servers that you may easily commandeer to send out your email -- if you have the right program or if you know how to telnet to port 25 (which runs using the SMTP or ESMTP protocols) and give the commands to send email yourself.

Why did I use Icefubarnet? Because at the time it was hosting an ftp site that was being used to download email bomber programs (http://www.icefubarnet.com/~astorm/uy4beta1.zip). Last time I checked the owner of the account from which he was offering this ugly stuff was unhappy because Icefubarnet Internet had made him take it down.

But -- back to how to commandeer mail servers while sending your message Ids elsewhere. In Eudora, just specify your victim mail server under the hosts section of the options menu (under tools). Then specify the computer to which you want to send your message ID under "POP Server."

But if you try any of this monkey business with Pegasus, it gives a nasty error message accusing you of trying to forge email.

Of course you can always commandeer mail servers by writing your own program to commander mail servers. But that will be covered in the upcoming GTMHH on shell programming.

****
Newbie note: Shell programming? What the heck izzat? It means writing a program that uses a sequence of commands available to you in your Unix shell. If you want to be a real hacker, you *must* learn Unix! If you are serious about continuing to study these GTMHHs, you *must* either get a shell account or install some form of Unix on your home computer. You may find places where you can sign up for shell accounts through http://www.celestin.com/pocia/. Or email haxorshell@techbroker.com for information on how to

Zabu451: nonono its working now

NewfPyr: They’re still coming, just in case.

Zabu451: STOP THEM NOW

NewfPyr: I can't break AOL Policy.

Zabu451: POEPLE ARE COMING TO MY HOUSE?!?!?!?!??

NewfPyr: No! To your server. You know, where you're calling AOL from.

Zabu451: im calling from my house

NewfPyr: But you said you where calling from the server!

Zabu451: i lied im not reely a server guy

NewfPyr: But you said you were!

Zabu451: i lied i trying to get passwords please make them stop
NewfPyr: Okay. The repair team isn't coming anymore.

Zabu451: good

NewfPyr: But a team of FBI agents is.

Zabu451: NONONONO
Zabu451: im sorry
Zabu451: ill never do it again please make them not come
Zabu451: PLEASE IL STOP ASKING FOR PASSWORDS FOREVER PLEASE MAKE THEM STOP!!

NewfPyr: I’m sorry, I can't do that. They should be at your house in 5 minutes.

Zabu451: IM SORRY IL DO ANYTHING PLEASE I DONT WANT THEM TO HURT ME
Zabu451: PLEASE
Zabu451: PLEEEEEEEEEEEEEEAAAAAAAAASSSSSSSSE

NewfPyr: They won't hurt you! You'll probably only spend a year of prison.

Zabu451: no IM ONLY A KID

NewfPyr: You are? That makes it different. You won’t go to prison for a year.

Zabu451: i thout so

NewfPyr: You’ll go for two years.

Zabu451: No! IM SORRY
Zabu451: PLEASE MAKE THEM STOP
Zabu451: PLEASE

[I thought this was enough. He was probably wetting his pants.]

This is where those zillions of hacker web pages come into play. Do a web search for “hacker” and “haxor” and “h4ck3r” etc. You can spend months downloading all those programs with promising names like “IP spoofer.”

Unfortunately, you may be in for an ugly surprise or two. This may come as a total shock to you, but some of the people who write programs that are used to break into computers are not exactly Eagle Scouts.

For example, the other day a fellow who shall remain nameless wrote to me “I discovered a person has been looting my www dir, where I upload stuff for friends so I am gonna leave a nice little surprise for him in a very cool looking program ;) (if you know what I mean)”

But let’s say you download a program that promises to exploit that security hole you just found with a Satan scan. Let’s say you aren’t going to destroy all your files from some nice little surprise. Your next task may be to get this exploit program to compile and run.

Most computer breakin programs run on Unix. And there are many different flavors of Unix. For each flavor of Unix you can mix or match several different shells. (If none of this makes sense to you, see the GTMHHs on how to get a good shell account.) The problem is that a program written to run in, for example, the csh shell on Solaris Unix may not run from the bash shell on Slackware Linux or the tcsh shell on Irix, etc.

It is also possible that the guy who wrote that breakin program may have a conscience. He or she may have figured that most people would want to use it maliciously. So they made a few little teeny weeny changes to the program, for example commenting out some lines. So Mr./Ms. Tender Conscience can feel that only people who know how to program will be able to use that exploit software. And as we all know, computer programmers would never, ever do something mean and horrible to someone else's computer.

So this brings us to the next thing you should know in order to break into computers.

5. Learn how to program! Even if you use other peoples’ exploit programs, you may need to tweak a thing or two to get them to run. The two most common languages for exploit programs are probably C (or C++) and Perl.

****

Newbie note: If you can’t get that program you just downloaded to run, it may be that it is designed to run on the Unix operating system, but you are running Windows. A good tip off that this may be your problem is a file name that ends with “.gz”.

****

So, does all this mean that breaking into computers is really, really hard? Does all this mean that if you break into someone’s computer you have proven your digital manhood (or womanhood)?

No. Some computers are ridiculously easy to break into. But if you break into a poorly defended computer run by dunces, all you have proven is that you lack good taste and like to get into really stupid kinds of trouble. However, if you manage to break into a computer that is well managed, and that you have permission to test, you are on your way to a high paying career in computer security.

Remember this! If you get busted for breaking into a computer, you are in trouble big time. Even if you say you did no harm. Even if you say you made the computer better while you were prowling around in it. And your chances of becoming a computer security professional drop almost to zero. And -- do you have any idea of how expensive lawyers are?

6)Now run the Registry editor. This is well hidden since Microsoft would prefer that you not play with the Registry. One way is to click “start,” then “programs” then “MS-DOS,” and then in the MS-DOS window with the C:\windows prompt give the command “regedit.”
7) Click to highlight the subkey "HKEY_CURRENT_USER\Software\Microsoft\IE\Toolbar"
8) On the task bar above, click “Edit,” then “Find.” Type “Brandbitmap” in the find window.
9) Now double click on BrandBitmap to get a dialog window. Type the path and file name of your custom animated graphic into it.

So let’s say you set up a flaming skull that rotates when you run IE. Your teacher is impressed. Now she wants you to put it back the way it was before. This is easy. Just open up BrandBitmap, and delete the name of your animation file. Windows Explorer will then automatically revert to the saved graphic in BackBitmap.

Let’s now show your teacher something that is a little bit scary. Did you know that Internet Explorer (IE) can be used to break some Windows babysitter programs? Your school might be running one of them. If you play this right, you can win points by trashing that babysitter program.

Yes, you could just get to work on those babysitter programs using the tips of the GTMHH on how to break into Win95. However, we will also look at a new way to get around them in this chapter, using IE. The advantage of using IE when your teacher is anxiously looking over your shoulder is that you could just “accidentally” stumble on some cool stuff, instead of looking like a dangerous hacker. Then you could show that you know how to take advantage of that security flaw.

Besides, if it turns out the security program you try to override is well enough written to keep IE from breaking it, you don’t look like a dummy.

****
Evil Genius tip: People are less afraid of you if you type slooowwlllyyyyyyyyy.
****

The dirty little secret is that IE actually is a Windows shell program. That means it is an alternative to the Win95 desktop. From IE you may launch any program. Explorer is much like the Program Manager and Windows Explorer that come with the Win 95 and Win NT operating systems.

Yes, from the IE shell you can run any program on your computer -- unless the security program you are trying to break has anticipated this attack. With a little ingenuity you may be able to even gain control of your school’s LAN. But don’t try that just yet!

****
Newbie note: A shell is a program that mediates between you and the operating system. The big deal about IE being a Windows shell is that Microsoft never told anyone that it was in fact a shell. The security problems that are plaguing IE are mostly a consequence of it turning out to be a shell. By contrast, the Netscape and Mosaic Web browsers are not quite such full-featured shells. This makes them safer to use. But you can still do some interesting things with them to break into a Win95 box. Experiment and have fun!
****

To use IE as a Win95 shell, bring it up just like you would if you were going to surf the Web. If your computer is set to automatically initiate an Internet connection, you can kill it. You don’t need to be online for this to work.

Now here are a few fun suggestions. In the space where you would normally type in the URL you want to surf, instead type in c:.

So, do you want to join us in our battle against those cybernazis, against those who are trying to wipe out freedom on the Internet? Want to enlist in the good guy side of information warfare? One way is to learn and practice defensive skills against hacker war criminals.

In this GTMHH No.1 of the Information Warfare Volume we will cover hacker war only. But an understanding of hacker war will prepare you for No. 2, which will help you protect yourself from far broader attacks which can even lead to your 'digital death," and No. 3, which will lay the foundation for becoming an international information warfare fighter.

What Exactly Are Hacker Wars?

Hacker wars are attempts to damage people or organizations using cyberspace. There are several types of hacker war tactics. In this Guide we will discuss some of the more common attacks.

Web Page Hacking

Lots of people ask me, "How do I hack a Web page?" Alas, gentle reader, the first step in this process ought to be physiologically impossible and unsuitable for description in a family publication.

The typical Web page hack begins with getting write permission to the hypertext files on the Web server that has been targeted. Amazingly, some Web sites accidentally offer write permission to anyone (world writable)! If so, all the hacker warrior need do is create a bogus Web page, give it the same name as the desired page on the Web site to be hit, and then transfer it via ftp.

Otherwise it is usually necessary to first break into the Web server computer and gain root or administrative control.

Hacked web pages usually consist of dirty pictures and bad language. I have hunted down many hacked Web sites. Wise political analysis, witty repartee and trenchant satire have been absent from every one I have ever seen -- with the single exception of one hack in Indonesia by the East Timor freedom fighter group. Perhaps because they risked their lives to have their say, they made their hack count.

But my web spy standards are too high. Judge for yourself. Parental discretion and antinausea medicine advised. Collections of hacked Web pages may be found at
http://www.skeeve.net/
http://www.2600.com/hacked_pages

However, even if someone's cause is good and their commentary trenchant, messing up Web sites is a pitiful way to get across a message. They are quickly fixed. One has to hack a really famous Web site to make it into an archive.

If you believe in freedom enough to respect the integrity of other people's Web sites, and are serious about making a political statement on the Web, the legal and effective way is to get a domain name that is so similar to the site you oppose that lots of people will go there by accident. For example, http://clinton96.org was hilarious, clean, effective, and legal. http://dole96.org was also taken by parody makers. They are both down now. But they were widely reported. Many political sites linked to them!

To get your web spoof domain name, go to http://internic.net. You will save a lot of money by purchasing it directly from them instead of through an intermediary. In fact, all you need to do is promise to buy a domain name. If you get tired of your parody Web site before you pay for it, people have told me they have just given the name back to Internic and no one demanded payment.

****

****
You can go to jail, get fired and/or get punched in the nose warning: DOS attacks in general are pathetically easy to launch but in some cases hard to defend against. So not only can one get into all sorts of trouble for DOS attacks -- people will also laugh at those who get caught at it. “Code kiddie! Lamer!”
****

Sniffing

Sniffing is observing the activity of one’s victim on a network (usually the Internet). This can include grabbing passwords, reading email, and observing telnet sessions.

Sniffer programs can only be installed if one is root on that computer. But it isn’t enough to make sure that your Internet host computers are free of sniffers. Your email, telnet, ftp, Web surfing -- and any passwords you may use -- may go through 20 or more computers on their way to a final destination. That’s a lot of places where a sniffer might be installed. If you really, seriously don’t want some cybernazi watching everything you do online, there are several solutions.

The Eudora Pro program will allow you to use the APOP protocol to protect your password when you download email. However, this will not protect the email itself from snoopers.

If you have a shell account, Secure Shell (ssh) from Datafellows will encrypt everything that passes between your home and shell account computers. You can also set up an encrypted tunnel from one computer on which you have a shell account to a second shell account on another computer – if both are running Secure Shell.

You may download a free ssh server program for Unix at ftp://sunsite.unc.edu/pub/packages/security/ssh/ssh-1.2.20.tar.gz, or check out http://www.cs.hut.fi/ssh/#ftp-sites.

If you are a sysadmin or owner of an ISP, get ssh now! Within a few years all ISPs that have a clue will require ssh logins to shell accounts.

For a client version that will run on your Windows, Mac or any version of Unix computer, see the DataFellows site at http://www.datafellows.com/. But remember, your shell account must be running the ssh server program in order for your Windows ssh client to work.

To get on the ssh discussion list, email majordomo@clinet.fi with message "subscribe ssh."

But ssh, like APOP will not protect your email. The solution? Encryption. PGP is popular and can be purchased at http://pgp.com. I recommend using the RSA option. It is a stronger algorithm than the default Diffie-Hellman offered by PGP.

****
Newbie note: Encryption is scrambling up a message so that it is very hard for anyone to unscramble it unless they have the right key, in which case it becomes easy to unscramble.
****

****
Evil genius tip: While the RSA algorithm is the best one known, an encryption program may implement it in an insecure manner. Worst of all, RSA depends upon the unprovable mathematical hypothesis that there is no polynomial time bounded algorithm for factoring numbers. That’s a good reason to keep up on math news!
The key plot element of the movie “Sneakers” was a fictional discovery of a fast algorithm to factor numbers. Way to go, Sneakers writer/producer Larry Lasker!

```
cat > list
ls -alK|more
w|more
```

Then hold down the control key while hitting the letter "d." This will automatically end the "cat" command while saving the commands "ls-alK|more" and "w|more" in the file "list." Then make it executable with the command: "chmod 700 list." (If chmod 700 doesn't work on your system, try the alternative ways to make it executable in 4) above.)

Now, whenever you want to see everything you could ever want to see about your files, followed by a list of info on whoever else is also logged into shell accounts at the Unix box you use, just type in the command "list." This will give you something like:

```
total 127
drwx-----x 8 cpm        1536 Dec 28 14:37 .
drwxr-xr-x985 root      17920 Dec 26 17:56 ..
-rw-------  1 cpm          0 Aug 27 08:07 .addressbook
-rw-------  1 cpm       2285 Aug 27 08:07 .addressbook.lu
lrwxrwxrwx  1 cpm          9 Oct 27 15:35 .bash_history -> /dev/null
-rw-r--r--  1 cpm       1856 Oct  8 09:47 .cshrc

(snip)

3:01pm up 5 days,  6:48,  9 users,  load average: 1.87, 1.30, 1.08
User     tty      login@  idle   JCPU   PCPU  what
phill    ttyp0    2:39pm    1     11        -csh
flattman ttyp1    2:27pm          4     4  tf
kjherman ttyp2    1:13pm 1:43                 telnet ftp.fubar.com
cpm      ttyp4    1:08pm    13          w
johnp    ttyp5    Sa 6pm    1   1:29      7  -tcsh
kjherman ttyp6    1:15pm 1:43                 telnet ftp.fubar.com
kjherman ttyp8    1:16pm 1:43                 /bin/csh /usr/local/bin/cmenu
momshop  ttyp9    2:50pm   10                 /usr/local/bin/pine
swit     ttypa    9:56am 4:20     41        -csh
joy      ttypc    3:00pm          2      1  -csh
```

****

Newbie note: What does all that stuff mean? Sorry, this is an advanced GTMHH, so all I'm going to tell you is to give the commands "man ls" and "man who" to find out all this stuff.
OK, OK, I'm sorry, here's a little more help. The "|" means "pipe." When you have two commands on either side of a pipe command, this makes the output of the command on the left hand side of the "|" pipe into the command on the right hand side. So "w|more" tells your computer to do the command "w" and pipe its output to the command "more." Then "more" displays the output on your monitor one screen at a time, waiting for you to hit the space bar before displaying the next screen.
What does "lrwxrwxrwx 1 cpm   9 Oct 27 15:35 .bash_history -> /dev/null" mean? "l" means it is a linked file. The first set of rwx's mean I (the owner of the account) may read, write, and execute this file. The second rwx means my group may also read, write and execute. The last set