Contents Of Issue 97
-------------------

Page 2  How to find someone
Page 3  How to subscribe
Page 4  TAP RAP
Page 5  Novices guide to hacking
Page 17 Chemical Fire Bottle
Page 18 How to hack parking meters
Page 19 Misc....

TAP Magazine
Post Office Box 20264
Louisville, Kentucky 40220
Finding people? I have spent considerable time and effort doing this sort of work. The only solid rule for tracking people down is that there are no solid rules.

In general, finding people depends upon knowing enough about the target subject (i.e., the person you want to find) to gain direction for the search. For instance, I was retained to search for a gentleman that had absconded from the Seattle area with substantial debts left behind. I knew very little about him other than his name, the fact that he had a trust fund administered from Los Angeles, and that he had been planning to wed a woman from Seattle when he was last heard from several weeks before.

In this case, I managed to locate a marriage license in the King county (Seattle) Courthouse which yielded the name and address of the woman he had, by the time of this search, married. Although the man had covered most of his tracks pretty well, the woman he had married took no effort to obscure her path.

Consequently, I had the woman’s name and last known residence (in Renton, Washington, a suburb of Seattle) when I left the courthouse. Once I had this, the remaining follow up was reasonably simple. It turned out that her prior residence she had been living in was up for sale. A visit to the real estate agent acting as broker afforded a reasonably fast face-to-face meeting with the fugitive I sought. He, it developed, was handling all the business of his new wife. The real estate agent very thoughtfully arranged the meeting, and also provided me with the seller’s new home address.

I tell this story as a means of illustrating an approach to finding people. While in general it is helpful to review information resources like the telephone book, Polk directory, etc., I believe that a general principle is the best advice. Find out all you can about your target, then determine what, if any, information resources this knowledge of your target implies. If you are uncertain what information your basic knowledge of your target does imply, take what you know to an expert (like the records clerk in the city/county building where the target I mention above had filed his marriage license) and ask the expert what intelligence is necessarily implicit in the information you have as a foundation. Once this is accomplished, the remaining task is to exploit this information.

As far as expert assistance in developing the leads that you start with, there are as many sources for this intelligence as there are categories worth exploiting. I know very little about tennis, for instance, but I know enough that if I found a suspect I sought was a heavy tennis player, I could certainly locate a tennis expert to tell me what organizations associated with tennis might yield the suspect’s location. Failing that, if the suspect is a serious tennis player, and I have a good idea what city he might be in, I might be able to develop leads by asking questions at athletic clubs in the area.

Although this approach seems like common sense, many people tend to forget what creatures of habit we humans are, and they consequently fail to exploit the obvious when searching for someone. Nonetheless, I have found this approach fairly useful. Just find out all you can about your target, then think! One must compile all available information on the target subject, then follow it up and exploit whatever leads this information develops.

Robyn Robertson
BITNET: GSRLR@ALASKA
Internet: GSRLS@acad3.fai.alaska.edu
P.O.Box 81638
Fairbanks, AK 99708

The opinions expressed here are my own

For those who read about us in Factsheet 5, you get one issue for one stamp, not 92-94 for a single itty bitty stamp. Sorry for the mess up. Just send more stamps for more issues.

Effective February our ZIP CODE will be changed from 40220 to 40250. Please make a note of this so you don’t send mail to the wrong place. Then cry and say it’s TAP’s fault we didn’t get your mail!

Contacting TAP Other than by mail has been impossible until now. There are two BBS’s we can be reached at. One is called The Danger Zone it’s 24 hours 300/1200/2400 Bps, the # is 502-448-1155. CreechNet BBS with the same info can be reached at 502-491-4493. E-mail Predator.

These are not TAP run BBS’s, just ones that happen to be local to me so you can find me on them easily, The feds may even try and find me on them too… don’t they wish?

The opinions expressed here are my own
Write in and give us your opinion.

If you don't see what you like, or have any problems with our changes, you can write in and give us your opinion.

The following list is a compilation of our reader survey cards. After the list, I have put down some notes from readers and our replies to them. We hope this way you will see what we are doing for you and you can also get specific questions answered. Enjoy!

These four are ratings from 1 to 10. The average is noted after subject.

- Quality of print
- Quality of content
- Quality of paper
- Quality of service from staff

These were answered with a Yes or No.

- Own a computer
- Own a modem
- Read 2600 magazine
- Use(d) blue/red boxes
- Average age of readers
- Oldest
- Youngest
- Average at around 20 and 30.
- Average is noted after subject.

Now on to the comments on what the readers want:

- What is and where can we get Phrack?

TAP - Phrack newsletter is a soft magazine that is available on various bulletin boards throughout the US. One good one to try would be Ripco at 512-528-5020. If you have Internet access, send mail to: C4833070@ucvm.missouri.edu or C4888699@ucvm.missouri.edu.

---

Editor Note: We regret that this article is an entire year late, but it is still very accurate and should prove useful to many beginning and experienced hackers.
Part One: The Basics

As long as there have been computers, there have been hackers. In the 50's at the Massachusetts Institute of Technology (MIT), students devoted much time and energy to ingenious exploration of the computers. Rules and the law were disregarded in their pursuit for the 'hack'. Just as they were entrapped with their pursuit of information, so are we. The thrill of the hack is not in breaking the law, it's in the pursuit and capture of knowledge.

To this end, let me contribute my suggestions for guidelines to follow to ensure that not only you stay out of trouble, but you pursue your craft without damaging the computers you hack into or the companies who own them.

I. Do not intentionally damage *any* system.
II. Do not alter any system files other than ones needed to ensure your escape. If you change the system and your future access (Trojan Horses, Altering Logs, and the like are all necessary to your survival for as long as possible.)
III. Do not leave your (or anyone else's) real name, real handle, or real phone number on any system that you access illegally. They *can* and will track you down from your handle!
IV. Be careful who you share information with. Feds are getting trickier.
V. Do not leave your real phone number to anyone you don't know. This includes logging on to boards, no matter how cool they seem. If you don't know the sysop, leave a note telling some trustworthy people that will validate you.
VI. Do not hack department computers. Yes, there are government systems that are safe to hack, but they are few and far between. And the government has infinitely more time and resources to track you down than you do. They can and will make a profit and justify their existence by finding you out.
VII. Don't use codes unless there is *NO* way around it (you don't have a password.) Logs, and the like are all necessary to your survival for as long as possible.
VIII. Don't be afraid to be paranoid. Remember, you *are* breaking the law.
IX. Watch what you post on boards. Most of the really great hackers in the country post *nothing* about the system they're currently working except in the broadest sense (I'm working on a UNIX, or a COSMOS, or something generic. Not "I'm hacking into General Electric's Voice Mail System" or something inane and revealing like that.)
X. Don't be afraid to ask questions. That's what more experienced hackers are for. Don't expect *everything* you ask to be answered, though. There are some things (LMOS, for instance) that a beginning hacker shouldn't mess with. You'll either get caught, or screw it up for others, or both.
XI. Finally, you have to actually hack. You can hang out on boards all you want, and you can read all the text files in the world, but until you actually start doing it, you'll never know what it's all about. There's no thrill quite the same as getting into your first system (well, ok, I can think of a couple of bigger thrills, but you get the picture.)

One of the safest places to start your hacking career is on a computer system belonging to a college. University computers have notoriously lax security, and are more used to hackers, as every college computer department has one or two, so are less likely to press charges if you should be detected. But the odds of them detecting you and having the personnel to commit to tracking you down are slim as long as you aren't destructive.

As long as you are a college student, this is ideal, as you can legally log on to your computer system to your heart's desire, then go out and look for similar systems that you can penetrate with confidence, as you're already familiar with them.

So if you just want to get your feet wet, call your local college. Many of them will provide accounts for local residents at a nominal (under $20) charge. Finally, if you get caught, don't volunteer any information, no matter what kind of 'deals' they offer you. Nothing is binding unless you make the deal through your lawyer, so you might as well shut up and wait.

Part Two: Networks

The basic way to begin hacking (other than a college) is on one of the bigger networks such as Telenet. Why? First, there is a wide variety of computers to choose from, from small Micro-Vaxen to huge Crays. Second, the networks are fairly well documented. It's easier to find someone who can help you with a problem off of Telenet than it is to find assistance concerning your local college computer or high school machine. Third, the networks are safer. Because of the enormous number of calls that are fielded every day by the big networks, it is not financially practical to keep track of where every call and connection are made from. It is also very easy to disguise your location using the network, which makes your hobby much more secure.

Telenet has more computers hooked to it than any other system in the world once you consider that from Telenet you have access to Tymnet, ItaPAC, JANET, DATAPAC, SDBN, Pandanet, THEnet, and a whole host of other networks, all of which you can connect to from your terminal. The first step that you need to take is to identify your local dialup port. This is done by dialing 1-800-424-9494 (1200 761) and connecting. It will spout some garbage at you and then you'll get a prompt saying 'TERMINAL'.

This is your terminal type. If you have vt100 emulation, type it in now. Or just hit return and it will default to dumb terminal mode.

You'll now get a prompt that looks like a @. From here, type fc mail <cr> and then it will ask for a Username. Enter 'phones' for the username. When it asks for a password, enter 'phones' again. From this point, it is menu driven. Use this to locate your local dialup, and call it back locally. If you don't have a local dialup, then use whatever means you wish to connect to one long distance (more on this later.)

Call your local dialup, you will once again go through the TERMINAL stuff, and once again you'll be presented with a @. This prompt lets you know you are connected to a Telenet PAD. PAD stands for either Packet Assembly/Disassembly (if you talk to an engine) or Access Device (if you talk to Telenet's marketing people.) The first description is more correct.

Telenet works by taking the data you enter in on the PAD you dialed into, bundling it into a 128 byte chunk (normally • • • this can be changed), and then transmitting it at speeds ranging from 9600 to 19,200 baud to another PAD, who will validate you.

This is done by dialing 1-800-424-9494 (1200 761) and connecting. It will spout some garbage at you and then you'll get a prompt saying 'TERMINAL'.

This is your terminal type. If you have vt100 emulation, type it in now. Or just hit return and it will default to dumb terminal mode.

You'll now get a prompt that looks like a @. From here, type fc mail <cr> and then it will ask for a Username. Enter 'phones' for the username. When it asks for a password, enter 'phones' again. From this point, it is menu driven. Use this to locate your local dialup, and call it back locally. If you don't have a local dialup, then use whatever means you wish to connect to one long distance (more on this later.)

This is called your local dialup. You will once again go through the TERMINAL stuff, and once again you'll be presented with a @. This prompt lets you know you are connected to a Telenet PAD. PAD stands for either Packet Assembly/Disassembly (if you talk to an engine) or Access Device (if you talk to Telenet's marketing people.) The first description is more correct.

Telenet works by taking the data you enter in on the PAD you dialed into, bundling it into a 128 byte chunk (normally • • • this can be changed), and then transmitting it at speeds ranging from 9600 to 19,200 baud to another PAD, who then takes the data and hands it down to whatever computer or system it's connection is made to. The PAD allows two distances simultaneously, so you can connect to more than one long distance (more on this later.)

This is called PAD Delay, and is to be expected when you're sending data through several different links.

What do you do with this PAD? You use it to connect to remote computer systems by typing 'C' for connect and then the Network User Address (NUA) of the system you want to go to.

An NUA takes the form of 03110130002520

This is a summary of DNIC's (taken from Blade Runner's file on ItaPAC) according to their country and network name.

6
One or two minutes. In this case, you want to abort the connect attempt by address by 1 and try 512 00001.00 through 512 00001.99. A lot of scanning.

There are plenty of neat computers to play with in a 3-digit scan, however, to start with 512 00000.00 and 90 through 512 00000.99, then increment the attempts per prefix. For example, if I want to scan 512 completely, I'd have to scan 512 00000.00 to 512 00000.99, then increment the address by 1 and try 512 00001.00 through 512 00001.99. A lot of scanning.

Sometimes you'll attempt to connect and it will just be sitting there after one or two minutes. In this case, you want to abort the connect attempt by sending a hard break (this varies with different term programs, on Procomm, it's ALT-B), and then when you get the @ prompt back, type 'D' for disconnect.

If you connect to a computer and wish to disconnect, you can type <cr> @ <cr>8080. This should say TELENET and then give you that @ prompt. From there, type D to disconnect or CONT to re-connect and continue your session uninterrupted.

Outdials, Network Servers, and PADS

In addition to computers, an NUA may connect you to several other things. OnTelenet, the most useful one is the outdial. An outdial is nothing more than a modem you can get to an over telnet- similar to the PC Pursuit concept, except that these don't have passwords on them most of the time.

When you connect, you will get a message like 'Hayes 1200 baud outdial, Dial 412 614', or possibly 'Session 1234 established on modem 558B'. This is a new way to find new systems to hack. Also, on a VENTEL modem, type 'D' for disconnect, and it will display the five numbers stored as macros in the modem's memory.

There are different types of servers for remote Local Area Networks (LAN) that have many machine all over the office or the nation connected to them. I'll discuss identifying these later in the computer ID section.

And finally, you may connect to something that says 'X.25 Communication PAD' and then some more stuff, followed by a new @ prompt. This is a PAD just like the one you are on, except that all attempted connections are billed to the PAD, allowing you to connect to those nodes who earlier refused collect connections.

This also has the added bonus of confusing where you are connecting from. When a packet is transmitted from PAD to PAD, it contains a header that has the location you're calling from. For instance, when you first connected to Telenet, it might have said 212 44A CONNECTED if you called from the 212 area code. This means you were calling PAD number 44A in the 212 area. That 21244A will be sent out in the header of all packets leaving the PAD.

Once you connect to a private PAD, however, all the packets going out from *it* will have it's address on them, not yours. This can be a valuable buffer between yourself and detection.

Phone Scanning

Finally, there's the time-honored method of computer hunting that was made famous among the non-hacker crowd by that Oh-So-Technically-Accurate movie Wargames. You pick a three digit phone prefix in your area and dial every number digit, 0000 --> 9999 in that prefix, and see what number you find. There is software available to do this for nearly every computer in the world, so you don't have to do it by hand.

Part Three: I've Found a Computer, Now What?

This next section is applicable universally. It doesn't matter how you found this computer, it could be through a network, or it could be from carrier scanning your high school's phone prefix, you've got this prompt, what the hell is it?

I'm *NOT* going to attempt to tell you what to do once you're inside of...
any of these operating systems. Each one is worth several G-files in its own right. I'm going to tell you how to identify and recognize certain
systems, how to approach hacking into them, and how to deal with something that you've never seen before and have know idea what it is.

VMS-
The VAX computer is made by Digital Equipment Corporation (DEC), and runs the VMS (Virtual Memory System) operating system.
VMS is characterized by the 'Username:' prompt. It will not tell you if you've entered a valid username or not, and will disconnect you after three bad login attempts. It also keeps track of all failed login attempts and informs the owner of the account next time s/he logs in how many bad login attempts were made on the account.
It is one of the most secure operating systems around from the outside, but once you're in there are many things that you can do to circumvent system security. The VAX also has the best set of help files in the world. Just type HELP and read to your heart's content.
Common Accounts/Defaults: [username: password [{,password}]]
SYSTEM: OPERATOR or MANAGER or SYSTEM or SYSLIB
OPERATOR: OPERATOR
SYSTEM: UETP
SYSTEM: SYSTEST or SERVICE or DIGITAL
GUEST: GUEST or unpassworded
DEMO: DEMO or unpassworded
DECNET: DECN

DEC-10-
An earlier line of DEC computer equipment, running the TOPS-10 operating system. These machines are recognised by their 'login' prompt. The DEC-10/20 series are remarkably hacker-friendly, allowing you to enter several important commands without ever logging into the system. Accounts are in the format [xxx,yyy] where xxx and yyy are integers. You can get a listing of the accounts and the process names of everyone on the system before logging in with the command .sysstat (for SYSTEM STATus). If you seen an account that reads [234,10011 BOB JONES, it might be wise to try BOB or JONES or both for a password on this account. To login, you type .login xxx,yyy and then type the password when prompted for it. The system will allow you unlimited tries at an account, and does not keep records of bad login attempts. It will also inform you if the UID you're trying (UID = User Identification Code, 1,2 for example) is bad.
Common Accounts/Defaults:
1,2: SYSLIB or OPERATOR or MANAGER
2,7: MAINTAIN
5,30: GAMES

UNIX-
There are dozens of different machines out there that run UNIX. While some might argue it isn't the best operating system in the world, it is certainly the most widely used. A UNIX system will usually have a prompt like 'login:' in lower case. UNIX also gives you unlimited shots at logging in (in most cases), and there is usually no log kept of bad attempts.
Common Accounts/Defaults: (note that some systems are case sensitive, so use lower case as a general rule. Also, many times the accounts will be unpassworded, you'll just drop right in!)
root: root
admin: admin
sysadmin: sysadmin or admin
unix: unix
ucucp: ucucp
rje: rje
guest: guest
demo: demo
demon: demon
sycsin: syssin

Prime-
Prime computer company's mainframe running the Primos operating system. The are easy to spot, as the greet you with 'Primecon 18.23.05' or the like, depending on the version of the operating system you run into. There will usually be no prompt offered, it will just look like it's sitting there. At this point, type 'login <username>' . If it is a pre-18.00.00 version of Primos, you can hit a bunch of 'C's for the password and you'll drop in. Unfortunately, most people are running versions 19+. Primos also comes with a good set of help files. One of the most useful features of a Prime on Telnet is a facility called NETLINK. Once you're inside, type NETLINK and follow the help files. This allows you to connect to NUA's all over the world using the 'nc' command. For example, to connect to NUA 026245890040004, you would type 8nc :26245890040004 at the netlink prompt.
Common Accounts/Defaults:
PRIME PRIME or PRIMOS
PRIMOS_CS PRIME or PRIMOS
PRIMENET PRIMENET
SYSTEM SYSTEM or PRIME
NETLINK NETLINK
TEST TEST
GUEST GUEST
GUEST1 GUEST

HP-x000-
This system is made by Hewlett-Packard. It is characterized by the ':' prompt. The HP has one of the more complicated login sequences around- you type 'HELLO SESSION NAME,USERNAME,ACCOUNTNAME,GROUP'. Fortunately, some of these fields can be left blank in many cases. Since any and all of these fields can be passworded, this is not the easiest system to get into, except for the fact that there are usually some unpassworded accounts around. In general, if the defaults don't work, you'll have to brute force it using the common password list (see below.) The HP-x000 runs the MPE operating system, the prompt for it will be a ':', just like the logon prompt.
Common Accounts/Defaults:
MGR.LIST, PUB
MGR.HFOFFICE, PUB
MANAGER.ITF3000,PUB
FIELD.SUPPORT,PUB
FIELD.TELESUP,PUB
MGR.RJE
FIELD.HPP189 ,HPP187,HPP189,HPP196
MGR.TELESUP,PUB,HFPONLY,BF3

IRIS-
IRIS stands for Interactive Real Time Information System. It originally ran on PDP-11's, but now runs on many other minis. You can spot an IRIS by the 'Welcome to "IRIS" R9.1.4 Timesharing' banner, and the ACCOUNT ID? prompt. IRIS allows unlimited tries at hacking in, and keeps no logs of bad attempts. I don't know any default passwords, so just try the common ones from the password database below.
Common Accounts:
MANAGER
BOSS
SOFTWARE
DEMO
PDP8
PDP11
ACCOUNTING

10
The WS/CMS operating system runs in International Business Machines (IBM) mainframes. When you connect to one of these, you will get a prompt similar to ‘WS/370 ONLINE’, and then give you a ‘>’ prompt, just like TOPS-10 does. To login, you type ‘LOGON <username>’.

Common Accounts/Defaults are:

- AUTOLOGI: AUTOLOG or AUTOLOG
- CMS: CMS
- CMSBATCH: CMS or CMSBATCH
- EREP: EREP
- MAINT: MAINT or MAINTAIN
- OPERATNS: OPERATNS or OPERATOR
- OPERATOR: OPERATOR
- RCS: RCS
- SHARP: SHARP
- SNA: SNA
- VMTEST: VMTEST
- VMUTIL: VMUTIL
- VTAM: VTAM

NOS (Networking Operating System) runs on the Cyber computer made by Control Data Corporation. NOS identifies itself quite readily, with a banner of ‘WELCOME TO THE NOS SOFTWARE SYSTEM. COPYRIGHT CONTROL DATA 1978,1987’.

Unresponsive Systems

- Common Accounts/Defaults:
  - SYSTEM unknown
  - SYSTEMV unknown

Decserver-

This is not truly a computer system but is a network server that has many different machines available from it. A Decserver will say ‘Enter Username’ when you first connect. This can be anything, it doesn’t matter, it’s just an identifier. Type ‘c’, as this is the least conspicuous thing to enter. It will then present you with a ‘>’ prompt. From here, you type ‘c <systemname>’ to connect to a system. To get a list of system names, type ‘sh services’ or ‘sh nodes’. If you have any problems, online help is available with the ‘help’ command. Be sure and look for services named ‘MODEM’ or ‘DIAL’ or something similar, these are often outsidal modems and can be useful!

GS/1-

Another type of network server. Unlike a Decserver, you can’t predict what prompt a GS/1 gateway is going to give you. The default prompt it ‘GS/1>’, but this is redifinable by the system administrator. To test for a GS/1, do a ‘sh d’. If that prints out a large list of defaults (terminal speed, prompt, parity, etc...), you are on a GS/1. You connect in the same manner as a Decserver, typing ‘c <systemname>’. To find out what systems are available, do a ‘sh m’ or a ‘sh c’. Another trick is to do a ‘sh m’, which will sometimes show you a list of macros for logging onto a system. If there is a macro named VAX, for instance, type ‘do VAX’.

The above are the main system types in use today. There are hundreds of minor variants on the above, but this should be enough to get you started.

Unresponsive Systems

Occasionally you will connect to a system that will do nothing but sit there. This is a frustrating feeling, but a methodical approach to the system will yield a response if you take your time. The following list will usually make *something* happen.

1) Change your parity, data length, and stop bits. A system that won’t respond at 8N1 may react at 7E1 or 8E2 or 752. If you don’t have a term program that will let you set parity to EVEN, ODD, SPACE, MARK, and MORE, with data length of 7 or 8, and 1 or 2 stop bits, go out and buy one. While having a good term program isn’t absolutely necessary, it sure is helpful.

2) Change baud rates. Again, if your term program will let you choose odd baud rates such as 600 or 1100, you will occasionally be able to penetrate some very interesting systems, as most systems that depend on a strange baud rate seem to think that this is all the security they need...

3) Send a series of ‘.’ (periods). The Canadian network Datapac responds to this.

4) Send a hard break followed by a <cr>.

5) Type a series of ‘.’ (periods). The Canadian network Datapac responds to this.

6) If you’re getting garbage, hit an ‘i’. Tymnet responds to this, as does a Multilink II.

7) Begin sending control characters, starting with ‘A -> 7’. The above are the main system types in use today. There are hundreds of minor variants on the above, but this should be enough to get you started.

Brute Force Hacking

There will also be many occasions when the default passwords will not work on an account. At this point, you can either go onto the next system on your list, or you can try to ‘brute-force’ your way in by trying a large database of passwords on that one account. Be careful, though! This works fine on systems that don’t keep track of invalid logins, but on a system like a VMS, someone is going to have a heart attack if they come back and see ‘10 Bad Login Attempts Since Last Session’ on their account. There are also some operating systems that disconnect after ‘x’ number of invalid login attempts and refuse to allow any more attempts for one hour, or ten minutes, or sometimes until the next day.

The following list is taken from my own password database plus the data-base of passwords that was used in the Internet UNIX Worm that was running around in November of 1988. For a shorter group, try first names, computer terms, and obvious things like ‘secret’, ‘password’, ‘open’, and the name of the account. Also try the name of the company that owns the computer system (if known), the company initials, and things relating to the product the company makes or deals with.

Password List

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>daniel</td>
</tr>
<tr>
<td>academia</td>
<td>jester</td>
</tr>
<tr>
<td>ada</td>
<td>danny</td>
</tr>
<tr>
<td>adrian</td>
<td>debbie</td>
</tr>
<tr>
<td>aerobics</td>
<td>debbie</td>
</tr>
<tr>
<td>airplane</td>
<td>debbie</td>
</tr>
<tr>
<td>albany</td>
<td>december</td>
</tr>
<tr>
<td>altabross</td>
<td>december</td>
</tr>
<tr>
<td>albert</td>
<td>december</td>
</tr>
<tr>
<td>alex</td>
<td>december</td>
</tr>
<tr>
<td>alexander</td>
<td>december</td>
</tr>
<tr>
<td>algebra</td>
<td>december</td>
</tr>
<tr>
<td>alias</td>
<td>december</td>
</tr>
<tr>
<td>alpha</td>
<td>december</td>
</tr>
<tr>
<td>alphabet</td>
<td>december</td>
</tr>
<tr>
<td>ana</td>
<td>december</td>
</tr>
<tr>
<td>duncan</td>
<td>december</td>
</tr>
<tr>
<td>duncan</td>
<td>december</td>
</tr>
<tr>
<td>leonard</td>
<td>december</td>
</tr>
<tr>
<td>leonard</td>
<td>december</td>
</tr>
<tr>
<td>leonard</td>
<td>december</td>
</tr>
<tr>
<td>leonard</td>
<td>december</td>
</tr>
</tbody>
</table>

Unresponsive Systems

Occasionally you will connect to a system that will do nothing but sit there. This is a frustrating feeling, but a methodical approach to the system will yield a response if you take your time. The following list will usually make *something* happen.

1) Change your parity, data length, and stop bits. A system that won’t respond at 8N1 may react at 7E1 or 8E2 or 752. If you don’t have a term program that will let you set parity to EVEN, ODD, SPACE, MARK, and MORE, with data length of 7 or 8, and 1 or 2 stop bits, go out and buy one. While having a good term program isn’t absolutely necessary, it sure is helpful.

2) Change baud rates. Again, if your term program will let you choose odd baud rates such as 600 or 1100, you will occasionally be able to penetrate some very interesting systems, as most systems that depend on a strange baud rate seem to think that this is all the security they need...

3) Send a series of ‘.’ (periods). The Canadian network Datapac responds to this.

4) Send a hard break followed by a <cr>.

5) Type a series of ‘.’ (periods). The Canadian network Datapac responds to this.

6) If you’re getting garbage, hit an ‘i’. Tymnet responds to this, as does a Multilink II.

7) Begin sending control characters, starting with ‘A -> 7’. The above are the main system types in use today. There are hundreds of minor variants on the above, but this should be enough to get you started.

Brute Force Hacking

There will also be many occasions when the default passwords will not work on an account. At this point, you can either go onto the next system on your list, or you can try to ‘brute-force’ your way in by trying a large database of passwords on that one account. Be careful, though! This works fine on systems that don’t keep track of invalid logins, but on a system like a VMS, someone is going to have a heart attack if they come back and see ‘10 Bad Login Attempts Since Last Session’ on their account. There are also some operating systems that disconnect after ‘x’ number of invalid login attempts and refuse to allow any more attempts for one hour, or ten minutes, or sometimes until the next day.

The following list is taken from my own password database plus the data-base of passwords that was used in the Internet UNIX Worm that was running around in November of 1988. For a shorter group, try first names, computer terms, and obvious things like ‘secret’, ‘password’, ‘open’, and the name of the account. Also try the name of the company that owns the computer system (if known), the company initials, and things relating to the product the company makes or deals with.

Password List

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>daniel</td>
</tr>
<tr>
<td>academia</td>
<td>jester</td>
</tr>
<tr>
<td>ada</td>
<td>danny</td>
</tr>
<tr>
<td>adrian</td>
<td>debbie</td>
</tr>
<tr>
<td>aerobics</td>
<td>debbie</td>
</tr>
<tr>
<td>airplane</td>
<td>debbie</td>
</tr>
<tr>
<td>albany</td>
<td>december</td>
</tr>
<tr>
<td>altabross</td>
<td>december</td>
</tr>
<tr>
<td>albert</td>
<td>december</td>
</tr>
<tr>
<td>alex</td>
<td>december</td>
</tr>
<tr>
<td>alexander</td>
<td>december</td>
</tr>
<tr>
<td>algebra</td>
<td>december</td>
</tr>
<tr>
<td>alias</td>
<td>december</td>
</tr>
<tr>
<td>alpha</td>
<td>december</td>
</tr>
<tr>
<td>alphabet</td>
<td>december</td>
</tr>
<tr>
<td>ana</td>
<td>december</td>
</tr>
<tr>
<td>duncan</td>
<td>december</td>
</tr>
<tr>
<td>duncan</td>
<td>december</td>
</tr>
<tr>
<td>leonard</td>
<td>december</td>
</tr>
<tr>
<td>leonard</td>
<td>december</td>
</tr>
<tr>
<td>leonard</td>
<td>december</td>
</tr>
<tr>
<td>leonard</td>
<td>december</td>
</tr>
</tbody>
</table>
Part Four: Wrapping it up!

I hope this file has been of some help in getting started. If you’re asking yourself the question ‘Why hack?’, then you’ve probably wasted a lot of time reading this, as you’ll never understand. For those of you who have read this and found it useful, please send a tax-deductible donation of $5.00 (or more!) in the name of the Legion of Doom to:

The American Cancer Society
90 Park Avenue
New York, NY 10016

References:
1) Introduction to ItaPAC by Blade Runner
   Telecom Security Bulletin #1
2) The IBM VM/CMS Operating System by Lex Luthor
   The LOD/H Technical Journal #2
3) Hacking the IRIS Operating System by The Leftist
   The LOD/H Technical Journal #3
4) Hacking CDC’s Cyber by Phrozen Ghost
   Phrack Inc. Newsletter #18
5) USENET comp.risks digest (various authors, various issues)
6) USENET unix.wizards forum (various authors)
7) USENET info-vax forum (various authors)

Recommended Reading:
1) Hackers by Steven Levy
2) Out of the Inner Circle by Bill Landreth
3) Turing’s Man by J. David Bolter
4) Soul of a New Machine by Tracy Kidder
5) Neuromancer, Count Zero, Mona Lisa Overdrive, and Burning Chrome, all by William Gibson.
6) Reality Hackers Magazine c/o High Frontiers, P.O. Box 40271, Berkeley, California, 94704, 415-995-2606
7) Any of the Phrack Inc. Newsletters & LOD/H Technical Journals you can find.

Acknowledgements:
Thanks to my wife for putting up with me.
Thanks to Lone Wolf for the RSTS & TOPS assistance.
Thanks to Android Pope for proofreading, suggestions, and beer.
Thanks to The Urvile/Necron 99 for proofreading & Cyber info.
Thanks to Eric Bloodaxe for wading through all the trash.
Thanks to the users of Phoenix Project for their contributions.
Thanks to Altos Computer Systems, Munich, for the chat system.
Thanks to the various security personnel who were willing to talk to me about how they operate.

Boards:
I can be reached on the following systems with some regularity-
The Phoenix Project: 512/441-3088
Hacker’s Den88: 718/358-9209
Smash Palace South: 512/478-6141
Smash Palace North: 612/633-0509

boards:
"No, I haven't told my parents what we managed to do, Kevin. They'll see it all on the six o'clock news anyway."

---

### Chemical Fire Bottle

**Incendiary Bottle Self Igniting On Impact**

<table>
<thead>
<tr>
<th>Materials Required</th>
<th>How Used</th>
<th>Common Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sulphuric Acid</td>
<td>Batteries</td>
<td>Motor Vehicles</td>
</tr>
<tr>
<td>Gasoline</td>
<td>Motor Fuel</td>
<td>Gas Station</td>
</tr>
<tr>
<td>Potassium Chlorate</td>
<td>Medicine</td>
<td>Drug Store</td>
</tr>
<tr>
<td>Sugar</td>
<td>Sweetening Foods</td>
<td>Food Store</td>
</tr>
</tbody>
</table>

Glass Bottle w/stopper (1 quart)
Small Bottle w/lid
Rag or Papertowels
Rubber Bands

**Procedure**

1. Concentrate Sulphuric Acid by boiling in oven glass or enamelware container until white fumes are given off. *see footnote A
2. Remove acid from heat let cool to room temperature.
3. Pour gasoline into the large bottle until it's 2/3 full.
4. Slowly add the sulphuric acid to the gasoline until the bottle is filled 1 inch from the top. Insert stopper.
5. Important. Wash the outside of the bottle with(clear) tap water. Dry with towel. *B
6. Wrap a rag of paper towels around the outside of the bottle. Fasten with rubber bands.
7. Dissolve 1/2 cup (100gm) of potassium chlorate and 1/2 cup of sugar in one cup (250cc) of boiling water.
8. Let cool and pour into the small bottle and cap. The solution should be 2/3 crystals 1/3 liquid. If there is more liquid pour off the excess. *C

**How to use**

1. Shake small bottle to mix contents and pour onto the paper towels around the large bottle.
2. Throw the bottle at the target. When the bottle shatters the contents ignite.

**NOTES**

- Bottle can be used wet or after the solution has dried. The dry sugar potassium chlorate solution is more sensitive to spark or flame so be careful.
- Sulphuric Acid will burn skin or clothing wash with water on spills. Fumes are also dangerous and should not be inhaled. So concentrate Acid outside if possible.
- If bottle is not washed it may be dangerous to handle during use.
- Store small bottle away from large in case one is broken the other won't cause an unwanted explosion.

---

PREDATOR
HOW TO HACK PARKING METERS

Tired of feeding coin after coin into parking meters for the privilege of parking your car, (which you have paid registration fees to allow your car on the road) on your roads? (you paid for them with taxes). Well how would you like to get the maximum time a meter can give for less than a penny? You can do this by taking a penny and making it into a REDNECK penny. Look at a penny and a dime together. Notice how they are almost the same size. To make a redneck penny, hold the penny between your thumb and forefinger and scrape the edge on the curb. You can do this in thirty seconds or less. Only do this on one side, making that side flat, and only until it becomes the same size as a dime is. File until the words above Lincoln's head are gone. Now take your redneck penny and hold it with the flat side down, and slide it into the dime slot of the parking meter. Make sure you slide the redneck penny in, DO NOT let it turn. Sometimes using another coin to push it works well. Once the penny is in simply turn the crank like normal and watch the timing arrow slam over to the maximum time. Most meters have a 2 hour time limit.

Problems, occasionally the dime slot is too narrow for a redneck penny. Just drop the penny on the sidewalk, step on it, move your foot back and forth, filing the penny thinner. These methods should work on all Duncan brand meters that accept dimes. Rom & Rockwell brands also will take the redneck penny. If the redneck penny happens to turn while you insert it, you usually get credit for a dime, instead of the full time limit.

Brought to you by the REDNECK REVOLUTION.