UNIXSYSV.TXT
From THE HACKER'S GUIDE TO W.S.U. comes
the ultimate in weekend entertainment

How to Hack UNIX System V
----
includes the INTRODUCTION TO HACKING
and HOW TO NOT GET CAUGHT

Version: 2.0

INTRODUCTION TO HACKING

Hacking is the art of attempting everything until something finally works. The average hacker is usually only armed with educated guesses. Why hack? Generally, you have some reason. My favorite reason being that it's fun. But these days are getting pretty suspicious and you have to watch yourself when hacking even if you don't have malicious intents. Hacking is lots of work and is also dangerous. So be careful and don't get caught!

HOW TO NOT GET CAUGHT

Okay great, how do I avoid getting caught? That depends on what you are doing. In this file I will be discussing UNIX System V and therefore my suggestions should only be taken as pertaining to that. Even if you follow my suggestions, you can still get caught. Some operators are extremely persistant and will stop at nothing to nail you. If modems start answering when you pick up a phone, or you become known as the "human carrier" by your friends, then I suggest you lay low for awhile.

Here are some obvious things to be aware of when you are hacking by modem, I thought I'd include them in case you overlook them. You should always be on the lookout for these types of suspicious activity.

1] Excessive line noise in an area that usually has none.
2] You hear other voices simultaneously on the phone line.
   This occasionally happens normally with the old analog FDM
   multiplex equipment. But it also can be caused by a wire tap,
   so try to be careful here! * See the note on wire taps.
3] Any van or minivan parked next to:

```
         a] A telephone pole.
         b] An underground steam vent hole.
         c] Also watch for cloth tee-pees with MA BELL symbols on them
            near poles or steam vents.
        This is a *DEAD GIVAWAY*!!!  If you see this, cease all hacking
        for at least a month!  (An make sure that the vans are GONE,
        --NOT-- just moved to another location!)
        >> Check for wires going to the van from the pole, or vent.  And
           check to see if the van is white (FBI uses these alot) or a
           phone co. van.
     4] Watch the abandoned rooms in your building, if they suddenly have
        lots of equipment in them, take note here!
     5] Anything unusual about the way your phone service operates that
        the neighbors don't seem to have going on!
That's all I can come up with right now.  But I'm sure there are more.
```

WIRE TAPS
=========

Belive it or not, this is still one of the most commonly used methods of nabbing a hacker. The above list is a good guide to detecting an active wire tap. If you can afford the equipment, you can do what is know as a "sweep" of the phone line every now and then. Another thing you can do is build a device which monitors the phone line voltage. If the voltage suddenly drops during use, you either have a wire tap or someone picked up an extension.
Here are some specs for monitoring line voltage:

```
    Ringer voltage:90V at 20-30Hz
    On-Line:30-50V
    Clear voltage:600V (Watch out!  This will toast any MOV you have
                        in your modem!  Usually this is used to fuse noisy
                        phone lines shut.)
```

The average cops don't have the equipment to properly implement a wire tap, much less a data tap. However, I have heard of data cops in Seattle and Chicago.

TRACING PHONE CALLS
===================

Here is yet another way you can get your butt caught. It is getting easier and easier for the average person to trace phone calls. I just found out a few days ago that dialing 33 on an on-campus phone will trace the last call to that phone. Rest assured that an operator will use this to nab you if he can. This however, only affects remote dial-ups, and not the on-campus links. Remote dial-ups used to be so safe, but no more...
A good place to hack from is a nearby terminal room. *NOT* in the same building that you live in! Do it at night, so if there is a system operator at all on duty late he will probably be sleeping.

RFI READING
===========

This is a fairly new method of catching hackers, and I really don't think the average hacker has much to worry from it. It is too complex to implement and doesn't even work most of the time. Especially if you're in an area that has lots of TV's or computer monitors. The device used basicly reads the faint radio frequencies created by your monitor and translates them back into a video signal. When it actually does work the guy running it can see exactly what you are seeing on your monitor. Pretty tricky, but he has to be able to pick out your signal first.

ESS -- IT'S BAD

Alright boys and girls, on top of everything else in the world we now are bless with the wonders of Electronic Standardized Switching. Or otherwise known as ESS. Remember that sharp increase in your phone bill about a year ago? "It's a new computerized system designed to allow quicker routing of your calls". Bullshit. It sole purpose is to catch phreakers. That's all it does, and it does it well. With this, the phone co. can trace a call in .55 seconds to anywhere. It keeps records on all calls, including local! And just about every phone box in the books will not only refuse to work, ESS will notify the cops when you try to use it!

Have some faith. ESS is not exactly the end of the world either. Like every system ever come up with, people will hack it. And eventually it will be just as easy to hack ESS as it was to do on the old phone system.

++++++++++++++++++++++++++++++++++++++
Okay! Enough beginner's stuff!
Onward to hacking UNIX System V !
++++++++++++++++++++++++++++++++++++++

Not much here: I just started this paper, and am still looking for anything I can add to it!

Remember: The operator can see what you are doing at all times! But usually they don't care or the information scrolls by so fast they don't have time to read it.

Note: If you flub up your password or try to access secured files, the system will automatically record everything that you do! And on some systems, the system will record everything you do anyway!

HOW TO LOG ON UNDER ANOTHER USER'S NAME

This is the heart of hacking a UNIX system. You don't want to do any hacking under any ID that can be associated with you. And you don't want to use another user's ID more than once if at all possible.

There really is no way to get a name and password without first having some level of access to the system. How do I get in then? I rely on the fact that our GANDALF data switch is extremely unstable. 1 out of 5 logins will drop you under someone else's name *NO QUESTIONS ASKED*. Just change parity (8N1 to E71) alot while GANDALF is loading UNIX. Eventually, you will get in this way. This happens because a user hung up on the phone line without loggig off! So be sure to log yourself off the system when you finish with *ANY* work.

They saw. A couple of days ago I was doing this and somehow I was logged off of the system. The words "LOGOFF" just appeared on my command prompt and entered themselfs. I suspect the guy whose number I used was in the terminal room monitored by a superuser. And he just told the SU that there appeared to be two of him. (Probably used the WHO command).

THE LOCK OUT
============

Believe it or not, UNIX will actually allow you to lock out other users from the system. First, you select a target person. Then you place the file VI.LOGIN in their default directory (the one that UNIX automaticly loads them into when they log onto the system). You set up VI.LOGIN like this:

```
VI.LOGIN   (Just the file name!)
logout
```

So VI.LOGIN only contains one command. VI.LOGIN is automaticly executed when a person logs onto the system. So as soon as your pigeon gets onto the system he immeadiatly gets logged off!

```
Suggested Uses:  On a Prof a few days before your assignment is due.
                 Someone you really don't like (wait a few weeks so they
                    don't figure it out right away!)
                 It might work on the ROOT (The SuperUser's name)
```

GETTING NEW NAMES
=================

Here is yet another way to gather SEVERAL users names AND PASSWORDS. First, (the hard part) wait until the beginning of a semester. Now, somehow you have to get a list of the ID numbers for students in UNIX-oriented classes. You can usually find one of these lists posted outside a professor's office (try the computer science building) or one of many other places. Anyways, you have a list of student ID numbers.

Now, preferably on the first day of class, start logging in as a few (maybe 3-4) students. I prefer to use ID's from low-level (100's) classes as the students will just think that they've screwed up. Log into the system, and if the student hasn't been on the system before, you will be prompted for a password! And viola! You not only have access but also you have the password of your choice. This happens because the computing faculty is too lazy to pass out customized passwords to thier students. New students are expected to select their own passwords, but that means that the system won't be able to tell who is who!

Suggested Uses: Most likely your access won't stay good for more than a few days. You might want to take full advantage of it and really cause some havoc. For one thing, you could lock out an entire computer class! (See LOCK OUT described above). If you're really good, and can crack the coded passwords in the PASSWRDS file, then you can get the Super-User (SU) password and have all the fun you want!

=========
THE END
=========

And Remember!
This paper was provided for educational purposes only!

Special thanks to:
==================
The Mad Phone-Man
The Grey Sorcerer
The Sneak Thief
Harry Hackalot