# Hacking for newbie essay

ASSIGN BUSTER

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. – 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, tc. 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. reestuff. 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 an 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 hat 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 " [email protected] 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