
GUIDE TO (mostly) HARMLESS HACKING

Beginners' Series Number 4

How to use the Web to look up information on hacking.
This GTMHH may be useful even to Uberhackers (oh, no, flame alert!)

Want to become really, really unpopular? Try asking your hacker friends too many questions of the wrong sort.

But, but, how do we know what are the wrong questions to ask? OK, I sympathize with your problems because I get flamed a lot, too. That's partly because I sincerely believe in asking dumb questions. I make my living asking dumb questions. People pay me lots of money to go to conferences, call people on the phone and hang out on Usenet news groups asking dumb questions so I can find out stuff for them. And, guess what, sometimes the dumbest questions get you the best answers. So that's why you don't see me flaming people who ask dumb questions.

****
Newbie note: Have you been too afraid to ask the dumb question, "What is a flame?" Now you get to find out! It is a bunch of obnoxious rantings and ravings made in email or a Usenet post by some idiot who thinks he or she is proving his or her mental superiority through use of foul and/or impolite language such as "you suffer from rectocranial inversion," f*** y***, d****, b****, and of course @#$%^&*! This newbie note is my flame against those flamers to whom I am soooo superior.
****

But even though dumb questions can be good to ask, you may not like the flames they bring down on you. So, if you want to avoid flames, how do you find out answers for yourself?

This Guide covers one way to find out hacking information without having to ask people questions: by surfing the Web. The other way is to buy lots and lots of computer manuals, but that costs a lot of money. Also, in some parts of the world it is difficult to get manuals. Fortunately, however, almost anything you want to learn about computers and communications is available for free somewhere on the Web.

First, let's consider the Web search engines. Some just help you search the Web itself. But others enable you to search Usenet newsgroups that have been archived for many years back. Also, the best hacker email lists are archived on the Web, as well.

There are two major considerations in using Web search engines. One is what search engine to use, and the other is the search tactics themselves.

I have used many Web search engines. But eventually I came to the conclusion that for serious research, you only need two: Alavista (http://altavista.digital.com)and Dejanews (http://www.dejanews.com). Altavista is the best for the Web, while Dejanews is the best one for searching Usenet news groups. But, if you don't want to take me at my word, you may surf over to a site with links to almost all the Web and Newsgroup search engines at http://sgk.tiac.net/search/.

But just how do you efficiently use these search engines? If you ask them to

find "hacker" or even "how to hack," you will get bazillions of Web sites and news group posts to read. OK, so you painfully surf through one hacker Web site after another. You get portentous-sounding organ music, skulls with red rolling eyes, animated fires burning, and each site has links to other sites with pretentious music and ungrammatical boastings about "I am 31337, d0Odz!!! I am so *&&^%$ good at hacking you should bow down and kiss my $%^&&*!" But somehow they don't seem to have any actual information. Hey, welcome to the wannabe hacker world!

You need to figure out some words that help the search engine of your choice get more useful results. For example, let's say you want to find out whether I, the Supreme R0Oler of the Happy Hacker world, am an elite hacker chick or merely some poser. Now the luser approach would to simply go to http://www.dejanews.com and do a search of Usenet news groups for "Carolyn Meinel," being sure to click the "old" button to bring up stuff from years back. But if you do that, you get this huge long list of posts, most of which have nothing to do with hacking:

CDMA vs GSM - carolyn meinel <cmeinel@unm.edu> 1995/11/17

Re: October El Nino-Southern Oscillation info gonthier@usgs.gov (Gerard J. Gonthier) 1995/11/20

Re: Internic Wars MrGlucroft@psu.edu (The Reaver) 1995/11/30
shirkahn@earthlink.net (Christopher Proctor) 1995/12/16

Re: Lyndon LaRouche - who is he? lness@ucs.indiana.edu (lester john ness) 1996/01/06

U-B Color Index observation data - cmeinel@nmia.com (Carolyn P. Meinel) 1996/05/13

Re: Mars Fraud? History of one scientist involved gksmiley@aol.com (GK Smiley) 1996/08/11

Re: Mars Life Announcement: NO Fraud Issue twitch@hub.ofthe.net 1996/08/12

Hackers Helper E-Zine wanted - rcortes@tuna.hooked.net (Raul Cortes) 1996/12/06

Carolyn Meinel, Soooooooper Genius - nobody@cypherpunks.ca (John Anonymous MacDonald, a remailer node) 1996/12/12

Anyhow, this list goes on and on and on.

But if you specify "Carolyn Meinel hacker" and click "all" instead of "any" on the "Boolean" button, you get a list that starts with:

Media: "Unamailer delivers Christmas grief" -Mannella@ipifidpt.difi.unipi.it (Riccardo Mannella) 1996/12/30 Cu Digest, #8.93, Tue 31 Dec 96 - Cu Digest (tk0jut2@mvs.cso.niu.edu)
<TK0JUT2@MVS.CSO.NIU.EDU> 1996/12/31

RealAudio interview with Happy Hacker - bmcw@redbud.mv.com (Brian S. McWilliams) 1997/01/08

Etc.

This way all those posts about my boring life in the world of science don't show up, just the juicy hacker stuff.

Now suppose all you want to see is flames about what a terrible hacker I am. You could bring those to the top of the list by adding (with the "all" button still on) "flame" or "f***" or "b****" being careful to spell out

those bad words instead fubarring them with ****s. For example, a search on "Carolyn Meinel hacker flame" with Boolean "all" turns up only one post. This important tome says the Happy Hacker list is a dire example of what happens when us prudish moderator types censor naughty words and inane diatribes.

****
Newbie note: "Boolean" is math term. On the Dejanews search engine they figure the user doesn't have a clue of what "Boolean" means so they give you a choice of "any" or "all" and then label it "Boolean" so you feel stupid if you don't understand it. But in real Boolean algebra we can use the operators "and" "or" and "not" on word searches (or any searches of sets). "And" means you would have a search that turns up only items that have "all" the terms you specify; "or" means you would have a search that turns up "any" of the terms. The "not" operator would exclude items that included the "not" term even if they have any or all of the other search terms. Altavista has real Boolean algebra under its "advanced"" search option.
****

But let's forget all those Web search engines for a minute. In my humble yet old-fashioned opinion, the best way to search the Web is to use it exactly the way its inventor, Tim Berners-Lee, intended. You start at a good spot and then follow the links to related sites. Imagine that!

Here's another of my old fogie tips. If you want to really whiz around the Web, and if you have a shell account, you can do it with the program lynx. At the prompt, just type "lynx followed by the URL you want to visit. Because lynx only shows text, you don't have to waste time waiting for the organ music, animated skulls and pornographic JPEGs to load.

So where are good places to start? Simply surf over to the Web sites listed at the end of this Guide. Not only do they carry archives of these Guides, they carry a lot of other valuable information for the newbie hacker, as well as links to other quality sites. My favorites are http://www.cs.utexas.edu/users/matt/hh.html and http://www.silitoad.org Warning: parental discretion advised. You'll see some other great starting points elsewhere in this Guide, too.

Next, consider one of the most common questions I get: "How do I break into a computer????? :(:("

Ask this of someone who isn't a super nice elderly lady like me and you will get a truly rude reaction. Here's why. The world is full of many kinds of computers running many kinds of software on many kinds of networks. How you break into a computer depends on all these things. So you need to thoroughly study a computer system before you an even think about planning a strategy to break into it. That's one reason breaking into computers is widely regarded as the pinnacle of hacking. So if you don't realize even this much, you need to do lots and lots of homework before you can even dream of breaking into computers.

But, OK, I'll stop hiding the secrets of universal computer breaking and entry. Check out:
Bugtraq archives: http://geek-girl.com/bugtraq
NT Bugtraq archives: http://ntbugtraq.rc.on.ca/index.html

****
You can go to jail warning: If you want to take up the sport of breaking into computers, you should either do it with your own computer, or else get the permission of the owner if you want to break into someone else's computer. Otherwise you are violating the law. In the US, if you break into a computer that is across a state line from where you launch your attack, you are committing a Federal felony. If you cross national boundaries to

hack, remember that most nations have treaties that allow them to extradite criminals from each others' countries.
****

Wait just a minute, if you surf over to those site you won't instantly become an Ubercracker. Unless you already are an excellent programmer and knowledgeable in Unix or Windows NT, you will discover the information at these two sites will *NOT* instantly grant you access to any victim computer you may choose. It's not that easy. You are going to have to learn how to program. Learn at least one operating system inside and out.

Of course some people take the shortcut into hacking. They get their phriends to give them a bunch of canned break-in programs. Then they try them on one computer after another until they stumble into root and accidentally delete system files. The they get busted and run to the Electronic Freedom Foundation and whine about how the Feds are persecuting them.

So are you serious? Do you *really* want to be a hacker badly enough to learn an operating system inside and out? Do you *really* want to populate your dreaming hours with arcane communications protocol topics? The old-fashioned, and super expensive way is to buy and study lots of manuals. <Geek mode on> Look, I'm a real believer in manuals. I spend about $200 per month on them. I read them in the bathroom, while sitting in traffic jams, and while waiting for doctor's appointments. But if I'm at my desk, I prefer to read manuals and other technical documents from the Web. Besides, the Web stuff is free! <Geek mode off>

The most fantastic Web resource for the aspiring geek, er, hacker, is the RFCs. RFC stands for "Request for Comment." Now this sounds like nothing more than a discussion group. But actually RFCs are the definitive documents that tell you how the Internet works. The funny name "RFC" comes from ancient history when lots of people were discussing how the heck to make that ARPAnet thingy work. But nowadays RFC means "Gospel Truth about How the Internet Works" instead of "Hey Guys, Let's Talk this Stuff Over."

****
Newbie note: ARPAnet was the US Advanced Research Projects Agency experiment launched in 1969 that evolved into the Internet. When you read RFCs you will often find references to ARPAnet and ARPA -- or sometimes DARPA. That "D" stands for "defense." DARPA/ARPA keeps on getting its name changed between these two. For example, when Bill Clinton became US President in 1993, he changed DARPA back to ARPA because "defense" is a Bad Thing. Then in 1996 the US Congress passed a law changing it back to DARPA because "defense" is a Good Thing.
****

Now ideally you should simply read and memorize all the RFCs. But there are zillions of RFCs and some of us need to take time out to eat and sleep. So those of us without photographic memories and gobs of free time need to be selective about what we read. So how do we find an RFC that will answer whatever is our latest dumb question?

One good starting place is a complete list of all RFCs and their titles at ftp://ftp.tstt.net.tt/pub/inet/rfc/rfc-index. Although this is an ftp (file transfer protocol) site, you can access it with your Web browser.

Or, how about the RFC on RFCs! That's right, RFC 825 is "intended to clarify the status of RFCs and to provide some guidance for the authors of RFCs in the future. It is in a sense a specification for RFCs." To find this RFC, or in fact any RFC for which you have its number, just go to Altavista and search for "RFC 825" or whatever the number is. Be sure to put it in quotes just like this example in order to get the best results.

Whoa, these RFCs can be pretty hard to understand! Heck, how do we even know which RFC to read to get an answer to our questions? Guess what, there is solution, a fascinating group of RFCs called "FYIs" Rather than specifying anything, FYIs simply help explain the other RFCs. How do you get FYIs? Easy! I just surfed over to the RFC on FYIs (1150) and learned that:

> FYIs can be obtained via FTP from NIC.DDN.MIL, with the pathname FYI:mm.TXT, or RFC:RFCnnnn.TXT (where "mm" refers to the number of the FYI and "nnnn" refers to the number of the RFC). Login with FTP, username ANONYMOUS and password GUEST. The NIC also provides an automatic mail service for those sites which cannot use FTP. Address the request to SERVICE@NIC.DDN.MIL and in the subject field of the message indicate the FYI or RFC number, as in "Subject: FYI mm" or "Subject: RFC nnnn".

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://GAMDALF.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!

Want to see back issues of Guide to (mostly) Harmless Hacking? See either
http://www.cs.utexas.edu/users/matt/hh.html (the official Happy Hacker archive site)
http://www.geocities.com/TimesSquare/Arcade/4594
http://www.silitoad.org
http://base.kinetik.org
http://www.anet-chi.com/~dsweir
http://www.tacd.com/zines/gtmhh/
http://ra.nilenet.com/~mjl/hacks/codez.htm
http://www.ilf.net/brotherhood/index2.html
http://www.magnum44.com/orion/entry.htm
http://www.geocities.com/NapaValley/1613/main.html

Subscribe to our discussion list by emailing to hacker@techbroker.com with message "subscribe"
Want to share some kewl stuph with the Happy Hacker list? Correct mistakes? Send your messages to hacker@techbroker.com. To send me confidential email (please, no discussions of illegal activities) use cmeinel@techbroker.com and be sure to state in your message that you want me to keep this confidential. If you wish your message posted anonymously, please say so! Direct flames to dev/null@techbroker.com. Happy hacking!