

Forum:[Hack Forums](#)

Thread: [life lesson for any new hacker and old\(mostly new\)](#)

Harrison5678 - March 15, 2008, 4:02 pm

I didnt make this but i am posting this for any new hackers! It is a great lesson for any new hacker even good hackers there are tons of good links here.

No one likes you if you ask others how to hack without taking the least amount of initiative.

You're not worthy of any title even resembling hacker, cracker, phreaker, etc., so don't go around calling yourself that! The more you do, the less likely you are to find someone willing to teach you how to hack (which is an infinitesimal chance, any way).

You're wasting your time (if you couldn't infer that in the first place). Many real hackers (not those shitty script kiddies) spend all their insomniac hours reading and, yes even, HACKING! (Hacking doesn't necessarily (but usually does) mean breaking into another system. It could mean just working on your own system, BUT NOT WINDOWS '9x (unless you're doing some really menacing registry shit, in which case, you're kind of cool).)

You're probably thinking, "Then what should I do. If no one's going to help me, how can I learn to hack?" Have you ever tried READING (I assume this far that you are literate). Read anything and everything you can get your hands on! I recommend hitting a computer store and looking for discount books (books that are usually out of date, but so are a lot of the systems on the 'net, so they're still relevant!). You'll be surprised what you can learn from a book even when you're paying a dollar for every hundred pages. I recommend the following books to start off with:

Maximum Security I or II: this is not a guide to hacking, despite what you might have heard, but you can get enough info to learn the basics of how hackers hack! (Isn't that more fun than being lamed, email bombed, and kicked off IRC).

Practical Unix and Internet Security (Sec. Edition): This is mostly a book about how to secure Unix (if you don't know what Unix is, either shoot yourself now, or read O'Reilly's Learning the Unix OS), but half of learning to hack is learning a system from the inside out. How can you expect to hack a site (w/o using a kiddie script, which i must restate, is NOT hacking) if you don't know how to use the system?!

Linux Unleashed/Red Hat Linux Unleashed: these books are kind of cool. First of all, they come with Red Hat Linux (*sigh*, just go to www.linux.org and read everything there) 5.1 and 5.2 respectively (if you get the newest versions of the book, which you should). Read everything you can from it.

Sendmail in a nutshell: This is only after you read everything else. Sendmail, for those of you who still don't know, is a program that sends mail. It sounds stupid, but this is a buggy program, and usually is the avenue of attack many hackers take because of it's vulnerabilities.

TCP/IP Blueprints: this will clear up a lot of things concerning TCP/IP.

TCP/IP Administration: haven't read it, but can't wait to! (I've been bogged down by a lot of other REAL computer stuff).

After you've read them all, re-read them! Trust me, you gain a ton of information the second time you read them just as you gain perspicacity the second time through a movie with a twisted plot.

Then, read a ton of RFCs. RFCs are Request for Comments by the people who practically shaped the Internet. Here is a good list of RFCs (the books above give about the same list):

RFC0760 - DoD Standard Internet Protocol
RFC0792 - Internet Control Message Protocol
RFC0819 - The Domain Naming Convention for Internet User Applications
RFC0821 - Simple Mail Transfer Protocol
RFC0822 - Standard for the Format of ARPA Internet Text Messages
RFC0976 - UUCP Mail Interchange Format Standard
RFC1123 - Requirements for Internet Hosts -- Applications and Support
RFC1135 - The Helminthiasis of the Internet (Morris Worm)
RFC1244 - Site Security Handbook
RFC1521 - MIME (Multipurpose Internet Email Extensions) Part One
RFC1522 - MIME (Multipurpose Internet Email Extensions) Part Two
RFC1651 - SMTP Service Extensions
RFC1652 - SMTP Service Extension for 8bit-MIMEtransport
RFC1652 - SMTP Service Extension for Message Size Declaration
RFC1675 - Security Concerns for IPng
RFC1704 - On Internet Authentication
RFC1739 - A Primer On Internet and TCP/IP Tools
RFC1750 - Randomness Recommendations for Security
RFC1825 - Security Architecture for the Internet Protocol
RFC1891 - SMTP Service Extension for Delivery Status Notifications
RFC1892 - The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages
RFC1893 - Enhanced Mail System Status Codes
RFC1894 - An Extensible Message Format for Delivery Status Notifications
RFC1918 - Address Allocation for Private Internets
RFC1920 - Internet Official Protocol Standards

That's it for now. If anything else interests you about the Internet, try to look up an RFC for it. Read anything you can about Internet security in general (but not stuff like "How to Hack" (but keep reading this!)). Subscribe to mailing lists. Some of my favorites are bugtraq, happy hacker (interesting stuff), and MC2. By now, you should be advanced enough to breeze through Carolyn Meinel's "Guide to (mostly) Harmless Hacking." It's got some interesting stuff, but not enough to be "3l1t3." Okay, now for the big step: the step from lamer to hacker! If you have not already, install Linux. Now it's okay for you to go online to usenet groups and ask for help installing Linux, 'cuz quite frankly, it's pretty fucking hard! NEVER, EVER, EVER expect to get it on the first try just right. The next thing to do is learn programming. I recommend learning C++ first because it will help you understand a lot about programming, it's easy to use, and is a lot like the other programming languages you should also learn. Read these books:

Teach Yourself C++ in 21 Days: the name says it all
Learning Perl: an AMAZING book on learning Perl
Programming Perl: the next step after Learning Perl
Perl Cookbook: the next step after Programming Perl
Core Java (Volume I & II): these books are by the makers of Java. Java is a really cool language to say the least, but you should at least learn C++ before so you can understand classes.

Now, you may be saying I may have been a bit hypocritical by saying not to ask how to hack but to ask about installing Linux. The thing is that Linux people are usually pretty nice, and the people who are Linux gurus want more than anything for Linux to prosper, and are willing to help you out. Oh, by the way, if you've installed Linux the way you want it (which does not include throwing you Linux box out the window and yelling, "I LIKE THIS JUST FINE!"), congratulations. You have now earned my

respect.

Okay, I mentioned kiddie scripts earlier, and I'll follow up on it now. Kiddie Scripts are auto hacking programs that will do all the work for you. You don't want that. I do condone downloading them and learning from them, but don't become a script kiddie. The only place they go in life is jail (not where you want to be).

Now, you should know a great deal about hacking. You have a compendium of information at your fingertips with a mental index. You want the best advice? Don't hack. Odds are, you will get caught, and then it goes down on your criminal record, and unless you did something fan-fucking-tastic, like hacking the white house security cameras and get video of Slick Willie getting a BJ, you can pretty much kiss your computer future goodbye, cuz no one will hire a convicted hacker. If you do hack, be a white hat hacker. For example, upon breaking into a site, leave a note maybe including how to contact you (not through the phones, mail, real email address etc., do it through a hotmail account or something) or how to fix it. They may be nice enough to offer you a job! That's right, there are some people who get paid to hack and do what they love.

In conclusion, you may have noticed that this was not a real guide to hacking. That's because there is no one resource for hacking. This was a guide to LEARNING how to hack, which, if you want to be a real hacker, you will have to do. There is no one way to hack. (If so, it would be a lot easier for system administrators to keep you out!) It's a variety of different tricks as well as the ability to keep up with current vulnerabilities in software and hardware. You should also learn how to program. Even though Kevin Mitnick was infamous among the hacker culture for being the most wanted cracker, he couldn't even write his own exploits! That's pretty sad. Please use whatever information you have wisely and responsibly, and distribute it only to people who are worthy of it.

(end of article)

Note that some of the RFC's R4di4tion mentioned are now outdated, I'd suggest using rfc-editor.org to search for the RFC number, it'll tell you if another RFC has superceded the one you're searching for. IMO, RFC's really aren't that useful; they're a pain to understand, and you're much better off, IMHO, learning by doing. They are useful if you're writing an application and need to know about the standards.

Also, I'd no longer recommend Maximum Security; although a great book, it's now quite out of date. Try 'Hacking Unleashed' instead, or any recently released large book (around £50 (~\$60)) that looks good.

I also very definitely agree with his suggestion to subscribe to bugtraq (securityfocus.com) but I'd suggest signing up a new email account solely for it; it's very high volume.

You may also want to sign up to the security-basics, vuln-dev, web-application-security and pen-test lists

Also, read google's sci/tech news, securityfocus.com's news pages, wired magazine, phrack, slashdot, and so on. In fact, the more you read, the better equipped you'll be.

Useful Links

ESR's hacker howto

Gary Robson's How to become a hacker

elfQrin's open letter to wannabe hackers

donk boy's tutorial - if you follow this you will know everything you need to

Top 100 security tools, as voted by nmap users

Hope you learned something! rep me if you liked it ?

---Nero--- - March 15, 2008, 10:27 pm

I 2nd That!

Ross123 - October 31, 2024, 6:22 pm

RFC1244 - Site Security Handbook

RFC1521 - MIME (Multipurpose Internet Email Extensions) Part One

RFC1522 - MIME (Multipurpose Internet Email Extensions) Part Two

RFC1651 - SMTP Service Extensions

RFC1652 - SMTP Service Extension for 8bit-MIMEtransport

RFC1652 - SMTP Service Extension for Message Size Declaration

RFC1675 - Security Concerns for IPng

RFC1704 - On Internet Authentication

RFC1739 - A Primer On Internet and TCP/IP Tools

i think these ones are the most important