تنها راهنمای واقعی هک برای مبتدیان

مقدمه :
مدت زیادی بود که دوستان زیادی این سوالات براشون پیش اومده بود که :
- چطور می تونم هک کنم؟
- چطور می تونم یه هکر بشم؟
- به من هک یاد میدی؟
- هکر واقعی کیه؟
- راه هکر شدن کدومه؟
- من سیدی آموزشی فلان رو خریدم، ولی چیزی یادنگرفتم! باید چیکار کنم؟
- و . . .
تا اینکه من این مطلب رو دیدم که توسط یه هکر واقعی نوشته شده بود، یه کمی قدیمی بود ولی هنوزم قابل درنگ و تامل و بحث هستش و دیدم که این مطلب رو بترجمم به سوالات زیادی از این قبیل جواب داده میشه و ممکنه که خیلی از دوستانی که دور خودشون میچرخن راهشون رو به هدفشون پیدا کنن.
خوب اول اینکه بگم من هکر نیستم و به مقوله امنیت شبکه و هکینگ علاقه دارم و این مطلب تونسته کمک زیادی به خود من بکنه، و امیدوارم کمک زیادی به شما دوستان عزیز مبتدی بکنه (;

جا داره از استاد عزیزم آقای امیرحسنوند تشکر کنم .

تو وبلاگم یه مطلبی با عنوان "چگونه هکر شویم؟" هستش در دوقسمت، که از سایت تکنوتاکس گرفته شده در کنار این مطالب، مطالعه دوقسمت ذکر شده هم توصیه میشه . لینک:
http://devilhell.blogfa.com/post-61.aspx
http://devilhell.blogfa.com/post-62.aspx

رفع ادعا (مسئولیت):
در این مقاله هیچ گونه آموزشی وجود ندارد و فقط به چهارچوب مسیر پیشرفت اشاره شده ، اگه خنگ هستید یا کند ذهن ، عیب از خودتونه و هیچ ربطی به این مقاله نداره.
مترجم: این رفع ادعا مربوط به خود نویسنده هستش که من فقط ترجمه کردم، ولی بسی جای تامل داره .

شما تمام شب رو کنار کامپیوتر شخصی می گذرونید و همش تایپ می کنید و تایپ می کنید. نه ، شما هک نمی کنید . شما در IRC از کسی گدائی می کنید که به شما "چگونه هک کردن" را آموزش دهد! اما یک لحظه درنگ نمی کنید و به واقعیات خودتون نگاهی بندازید و موقعیت خودتون رو بسنجید. حالا بیا باهم نگاهی به واقعیات بندازیم:

۱- تو تنبل و بازنده هستی . مثل کسی نیستی که ازش می پرسید "چطوری میتونم هک کنم؟" درواقع بدون کمترین کار از زحمت و یا ابتکاری میخوای هکر بشی .

۲- هیچ کدوم از عناوین هکر ، کراکر ، فریکر و . . . رو نمیتونی داشته باشی . بنابراین فعلا اولین کاری که میکنی اینه که اینه که سعی نکنی که این لقب رو به دنبال خودت بکشی . و در حال حاضر بیشترین کاری که میتونی انجام بدی اینه که کمتر بری گدائی و از این و اون بخوای که چگونه هک کردن رو بهت آموزش بده ، (که به نظر من گدائی کاری کثیف بیش نیست) بهتره خودت دست بکار بشی .

۳- ممکنه درکش یه کمی برای تو سخت باشه ولی تو داری وقتت رو تلف می کنی. تعداد زیادی از هکرهای واقعی (نه بچه های لعنتی اسکریپتی) حتی از وقت خوابشون رو به مطالعه و هکینگ می پردازند! (هکینگ نه به صورت لزوما – اما بعضی اوقات ملزوم – به معنی هتک حرز و ورود غیرمجاز به سیستمی دیگر می باشد.) حالا این میتونه از کارکردن از روی سیستم خودتون به سیستم دیگه یا سیستم مورد نظر باشه.

ممکنه حالا فکر کنید که " اگر هیچ کسی حاضر نشد که کمکم کنه چکار باید بکنم. چطور میتونم هک کردن رو یاد بگیرم؟" .
آیا تا بحال سعی کردید مطالعه کنید؟ (من چنین فرض کردم که باسواد هستید)
آیا تا بحال شده هرمطلب خوندنی رو که هرجایی میتونید در دست بگیرید مطالعه کنید؟!

PDF created with pdfFactory trial version www.pdffactory.com

من جستجو کردم و موفق شدم یک فروشگاه کامپیوتر پیدا کنم که کتابهای با تخفیف رو ارائه میده .
کتابهایی وجود داره که قدیمی هستند ولی سیستم های زیادی روی نت پیدا می کنید که هنوز به اونها مربوط می باشند . و شما کاملا سورپرایز خواهید شد وقتی ببینید که از کتابی که یک دلار بابت آن پرداخت کرده اید چه چیزهایی یاد گرفته اید .

من کتابهای زیر رو برای شروع کار پیشنهاد می کنم :

- Maximum Security I or II
این یک کتاب راهنمای هکینگ نیست ، با این کتاب شما اطلاعات کافی درباره مقدماتی از اینکه هکرها چگونه هک می کنند یاد خواهید گرفت .

- Practical Unix and Internet Security 2nd Edition
این کتاب اساسا در مورد امنیت بخشیدن به یونیکس بحث می کند ، اگه نمیدونی یونیکسچیه یکی محکم بزن تو سر خودت و قبل از خوندن این کتاب، کتاب O'Reilly's Learning the Unix OS رو مطالعه کن، باید توجه داشته باشید که نصف آموزش چگونگی هک – یادگرفتن تمام سیستم هستش . چطور انتظار دارید که یک سایت رو هک کنید تا وقتی نمیدونید که چطور از سیستم استفاده کنید؟!
دوباره تکرار می کنم که استفاده از اسکریپتهای بچگانه ، هکینگ نیست)

- Linux Unleashed/Red Hat Linux Unleashed
این کتابها در نوع خودشون بی نظیر هستن . اول از همه، با RedHat Linux به ترتیب نسخه های 5.1 و بعد 5.2 رو شروع کنید و اگه تونستید نسخه جدیدتری پیدا کنید چه بهتر .(به سایت بروید www.linux.org و همه چیز رو خوب مطالعه کنید.) شما می تونید همه چیز رو داخلش پیدا کنید و بخونید .

- Sendmail in a nutshell
بعد از کتابهای ذکر شده نوبت به این کتاب میرسه و بعد از مطالعه کتابهای قبلی این یکی رو باید بخونید.
این کتاب بیشتر بدرد کسانی میخوره که نمیدونند Sendmail یک برنامه است که وظیفه ارسال ایمیل رو بعهده داره . این برنامه پر از باگ بوده و معمولا راه های زیادی بدلیل ضعف های امنیتیش برای نفوذ در اختیار هکرها قرار میده .

- TCP/IP Blueprints
این کتاب مطالب جامع زیادی درباره TCP/IP به شما یاد خواهد داد .

- TCP/IP Administration
این کتاب رو هنوز نخوندی؟ پس معطل چی هستی ؟! (مطالب دیگر زیادی در مورد آموزش های واقعی دیگر به شما نشان خواهم داد)

خوب بعد از اینکه همه این کتابها رو خوندید ، دوباره بخونیدشون. D: به من اعتماد کنید . (; چون با بار دوم خوندن این یک تن مطلب، اطلاعات سودمند زیرکانه ای میگیرید. بعد یک تن از RFC ها را مطالع کنید .
RFC ها حاوی اطلاعات جامعی از چیزهایی هستند که اینترنت را شکل می دهند .
در اینجا به لیستی از RFC هایی که باید مطالع کنید اشاره شده است :
---

* 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

PDF created with pdfFactory trial version www.pdffactory.com

* 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

این لیست برای زمان حالای شما هستش . اگه به چیز دیگه ای علاقه مند شدید و خواستید در موردش اطلاعات کسب کنید به دنبال یک RFC برای آن بگردید .
مترجم: نمیدونید که RFCها رو از کجا باید بگیرید؟ نه؟!!! وای خدای من ! . . . راه درازی در پیش داریم. پس گوگل برای چه ساخته شده ؟ در گوگل سرچ کنید حتما به نتیجه خواهید رسید .

هر مطلبی که بطور کلی در مورد امنیت اینترنتی بود بخونید ولی کتابها و مطالبی که در مورد "چگونه هک کردن" بود رو موقتا کنار بگذارید تا بعدا .

در یک ایمیل لیست گروه خبری عضو شوید . چند تا از گروه های مورد علاقه من bugtraq ، happy hacker (که جذابیت خاص خودش رو داره) و MC2 .
مترجم: گروه های خبری ایرانی رو به هیچ وجه فراموش نکنید، همچنین فروم ها . در آخر لیستی از سایتهای ایرانی فعال در زمینه امنیت شبکه ارائه شده است .

باید سعی کنید که در مطالب کتاب "Guide to (mostly) Harmless Hacking." حرفه ای بشید. این کتاب مطالب جذابی رو ارائه میده ولی برای **3l1t3**[1] شدن کافی نیست .

خوب ، حالا بزرگترین قدم : تغییر از lamer به hacker ! اگه شما هنوز لینوکس رو نصب نکردید .
حالا برید به گروههای خبری (usenet groups) و بخواید که کمکتون کنند که لینوکس رو نصب کنید .
رک بهتون بگم که ممکنه هاردتون رو به ***f بدید ، اگه اطلاعاتی درمورد نصب لینوکس ندارید .
مترجم: سایتهای فارسی زبان بسیار خوبی در این زمینه وجود داره که تکنوتاکس و ایران توکس از بهترینها هستند . سرچ گوگل هم یادتون نره ، چون گنو خیلی وسیعه و مطالب بیشتر از یک یا دوتا سایت (;

هیچوقت فکر نکنید که برای بار اول مشکلی با لینوکس نخواهید داشت . (مترجم : بهترین کار اینه که برید تو داس و بنویسید :Format C اینتوری فکر کنم بهترین راه برای خلاصی از شر مایکروشیت بیلی باشه)

کاربعدی که باید انجام بدید یادگیری برنامه نویسی هستش . بهتون توصیه میکنم که اول C++ رو یاد بگیرید ، چون بهتون کمک میکنه تا مطالب زیادی در مورد برنامه نویسی یاد بگیرید . استفاده از سی پلاس پلاس ساده بوده و شباهت زیادی با زبانهای برنامه نویسی دیگری که باید یاد بگیرید، دارد.
برای یادگیری موثر برنامه نویسی – مترجم:ترتیب خواندن مهم است - این کتابها رو بخونید :
- Teach Yourself C++ in 21 Days : از اسمش ضایع معلومه که چیکاره است.

---

[1] Elite به معنی ممتاز ، نخبه ، زبده که به زبان ۱۳۳ نوشته شده است .

PDF created with pdfFactory trial version www.pdffactory.com

- Learning Perl : کتابی شگفت انگیز برای یادگیری پرل .
- Perl Cookbook : قدم بعدی در یادگیری پرل .
- Core Java (Volume I & II) : این کتابها بوسیله سازنده جاوا نوشته شده اند. بطور خلاصه جاوا زبان واقعا عالی می باشد، اما شما باید حتما حتما سی پلاس پلاس را قبل از این یاد گرفته باشید تا بتوانید به راحتی مباحث کلاسها را یاد بگیرید .

شاید ممکنه با خودتون بگید که بوسیله نپرسیدن این سوال که "چگونه هک کنم؟" و بجای اون بپرسیم که چگونه لینوکس رو نصب کنم به یک ریاکار کوچک تبدیل بشیم!!! ولی باید بگم که لینوکس یک سیستم عامل مردمی هستش و کسانی که لینوکس رو دوست دارند به موفقیت اون فکر می کنند و برای موفقیت لینوکس با تمام وجود به سوالاتی که ازشون پرسیده میشه، پاسخ میدن .
اگه لینوکس رو نصب کردید و تصمیم گرفتید که در مسیر لینوکس قدم بردارید و سیستمتون رو به لینوکس باکس تبدیل کردید نه ویندوز گستاخ (یعنی تونستید از مایکروشیت بیلی راحت بشید)، "من این رو خیلی دوست دارم!" و به شما تبریک می گم چون تونستید تحسین من رو کسب کنید .

بله، من قبلا به اسکریپتهای بچگانه اشاره کردم، و در ادامه باید بگم که اسکریپتهای بچگانه برنامه های اتوماتیک هکی هستند که تمام کارها رو خودشون انجام میدن . شما احتیاجی بهشون ندارید. دانلود کردنشون و یادگیری چگونگی کارکرد آنها رو میتونم چشم پوشی کنم ولی بچه شر اسکریپتی بودن رو نه . تنها جایی که اونا میرن تو زندگیشون زندانه (جایی که شما نمیخواید برید) پس . . .

تا حالا، شما باید مطالب وسیعی در مورد هکینگ یاد گرفته باشید ولی شما به اندازه سر انگشتی اطلاعات دارید و یک ذهن طغیانگر ، شما بهترین نصیحت رو میخواید؟ "هک نکنید" . نابرابری هایی وجود دارند که شما را گرفتار خواهند کرد، و این دستگیری جزوی از پرونده جنایی برای شما ثبت خواهد شد ، و اگر شما یک هک خارق العاده انجام داده باشید، مثلا گرفتن فیلم از طریق دوربین های امنیتی کاخ سفید شما باید برای همیشه کامپیوترتان رو یک ماچ خوشکل کنید و از اون و آینده تون خداحافظی کرده و به یک هکر محبوس در زندان تبدیل شوید .

اگر شما هک رو انجام میدهید، یک هکر کلاه سفید باشید. بعنوان مثال، به محض نفوذ کردن به یک سایت، یه یادداشت با مضمون اینکه چطوری باشما تماس بگیرند(نه از طریق تلفن، پست، آدرس ایمیل واقعی و . . ،. این رو از طریق یک حساب کاربری هاتمیل یا چیز دیگری انجام بدهید) یا چگونه مشکل رو برطرف کنند. اونا به خوشحال خواهند شد که به شما یک کار بدهند! درسته، اشخاصی هستند که برای هک و کارهایی که دوست دارند پول پرداخت می کنند .
مترجم: من خودم به شخصه امنیت شبکه و هکینگ رو برای درآمد دوست ندارم ولی نه هکرم نه متخصص امنیت شبکه نه کراکرم نه چیز دیگه ای و فقط به این مقوله علاقه دارم و بس – کپی رایت آقا امیر -

در پایان باید بگم که این یک راهنما برای هک کردن نیست . این مقاله فقط راهنمایی برای یادگیری اینکه "چطوری یاد بگیریم که هک کنیم" هستش و اگه واقعا از ته دل و باتمام وجود میخواید یه هکر واقعی بشید ، شما هکر خواهید شد . – پس سعی خودتون رو بکنید (; -
فقط یک راه برای هک کردن وجود ندارد بلکه راههای زیادی وجود دارد . تاوقتی که شما چگونگی برنامه نویسی رو خوب یاد نگیرید مدیران سیستم خواهند توانست شما رو اون بیرون نگه دارند . پس برنامه نویسی رو خوب یاد بگیرید مگر اینکه مثل بعضی هکر های دستگیر شده شدیدا تحت تعقیب قرار بگیرید ، حتی بعضی از معروف های اونا حتی نتونستن اکسپلویتی برای خودشون بنویسن! واقعا غم انگیزه . بعضی هاشونم که تونستن برنامه بنویسن یه جاهایی دارن فعالیت می کنن . (:

مترجم: بعد از یادگیری همه اینا میتونید کتابهای زیر رو هم مطالعه کنید : (به ترتیب نوشته نشده)

Google Hacks
100 Industrial-Strength Tips & Tools

Security Warrior
By Anton Chuvakin, Cyrus Peikari
Publisher: O'Reilly
ISBN: 0-596-00545-8
Pages: 552

PDF created with pdfFactory trial version www.pdffactory.com

Exploiting Software How to Break Code
By Greg Hoglund, Gary McGraw
Publisher: Addison Wesley
Pub Date: February 17, 2004
ISBN: 0-201-78695-8
Pages: 512

Buffer Overflow Attacks
James C. Foster
Vitaly Osipov
Nish Bhalla
Niels Heinen

Hacking: The Art of Exploitation
by Jon Erickson
ISBN:1593270070

HACKING EXPOSED: NETWORK SECURITY SECRETS AND SOLUTIONS, 1st & 2nd & 3rd EDITION
STUART McCLURE
JOEL SCAMBRAY
GEORGE KURTZ

HACKING EXPOSED: WEB APPLICATIONS
JOEL SCAMBRAY
MIKE SHEMA

هر مطلبی رو بخونید و در قبال در اختیار دیگران گذاشتن مطالب مسئول باشید ، همین باعث احترام و اعتماد به شما خواهد شد .

Yes guys this gotta be the one !!

ارادتمند DevilHell

http://DEVILHELL.blogfa.com

(بزودی با مطالب جالب)

PDF created with pdfFactory trial version www.pdffactory.com

برخی از سایتها و وبلاگهای فعال ایرانی و خارجی در زمینه امنیت شبکه :

http://www.securityfocus.com/

http://www.happyhacker.com/

http://www.linuxsecurity.com/

http://www.securityforest.com

http://www.2600.com/

http://packetstormsecurity.org/

http://rr.sans.org/

http://www.cert.org/

http://www.ngssoftware.com/papers.htm

http://www.foundstone.com/

http://arazsamadi.blogspot.com

http://www.crouz.com/index.php

http://www.simorgh-ev.com/

http://websecurity.ir/

http://zxo003.blogfa.com/

http://bugtraq.ir/

http://www.b0rn2h4k.net/

http://www.kavehkazemi.com/english/intro/index.php

http://www.google.com !!!!!

مطمئنا با سرچ در گوگل مرجع های بسیاری پیدا خواهید کرد . (; :D

موفق و سربلند باشید.

PDF created with pdfFactory trial version www.pdffactory.com