چگونه هکر شویم؟

نقشه‌ی راه برای هکرهای مبتدی...

علی اصغر جعفری لاری

انتشارات پندار پارس

سرشناسه : جعفری لاری، علی‌اصغر، ۱۳۶۷ -
عنوان و نام پدیدآور : چگونه هکر شویم؟: نقشه‌ی راه برای هکرهای مبتدی/ علی‌اصغر جعفری‌لاری.
مشخصات نشر : تهران : پندار پارس ، ۱۳۹۳.
مشخصات ظاهری : ۱۶۰ ص.: مصور، جدول.
شابک : 978-600-6529-67-7
وضعیت فهرست نویسی : فیپا
عنوان دیگر : نقشه‌ی راه برای هکرهای مبتدی.
موضوع : کامپیوترها -- ایمنی اطلاعات
موضوع : شبکه‌های کامپیوتری --تدابیر ایمنی
موضوع : هکرها
موضوع : حفاظت اطلاعات
رده بندی کنگره : TK۵۱۰۵/۸۱۳۹۳۵۹ج۷/
رده بندی دیویی : ۸/۰۰۵
شماره کتابشناسی ملی : ۳۶۸۵۹۵۲

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ۱٤، واحد ۱٦ **www.pendarepars.com**
تلفن: ٦٦٥٧٢٣٣٥ - تلفکس: ٦٦٩٢٦٥٧٨ همراه: ۰۹۱۲۲٤٥۲۳٤۸ **info@pendarepars.com**

نام کتاب : **چگونه هکر شویم؟ نقشه‌ی راه برای هکرهای مبتدی**
ناشر : **انتشارات پندار پارس**
تالیف : **علی‌اصغر جعفری لاری**
چاپ نخست : **دی‌ماه ۹۳**
شمارگان : **۲۰۰ نسخه (دیجیتال)**
طرح جلد : **رامین شکرالهی**
چاپ و صحافی : **چاپ دیجیتال روز**
قیمت : **۱۱۰۰۰ تومان** **شابک : ۷-٦۷-٦٥۲۹-٦۰۰-۹۷۸**

فهرست

تقدیم

به پدر شهیدم،

که راهش همواره چراغ راهم بوده و خواهد بود

و به مادرم،

به پاس زحمات بی‌دریغش...

سرآغاز سخن

پیش از ورود به مباحث "چگونه هکر شویم؟"، از شما بابت انتخاب این کتاب، سپاس‌گزاری می‌کنم. با انتخاب این کتاب، نخستین گام برای تبدیل شدن به یک هکر چیره دست را برداشته‌اید. ادامه‌ی این راه بستگی به تلاش، استعداد و پشت‌کارتان دارد. این کتاب هرآنچه را که برای آشنایی بیشتر با مبانی علم هک نیاز دارید، به‌طور مختصر و آسان در اختیارتان می‌گذارد. دانشی که از این کتاب به‌دست می‌آورید را می‌توانید در راه‌های گوناگون زیر استفاده کنید:

- ممکن است تمایل داشته باشید که هک اخلاقی را دنبال کنید-معمولا سازمان‌ها، شرکت‌ها و مؤسسات، این دسته از افراد را استخدام می‌کنند. هکر اخلاقی از تکنیک‌ها و ابزارهای مشابه یک هکر واقعی برای پیدا کردن و ایمن‌سازی آسیب‌پذیری‌ها در سیستم‌های کامپیوتری استفاده می‌کند.
- نشان دادن مهارت‌های خود به دوستانتان می‌تواند آنها را شگفت زده کند. پیشنهاد به آنان برای فراگیری علم هک اخلاقی، می‌تواند فضای مجازی را بیش از پیش، ایمن و مطمئن سازد.
- با فراگیری این علم، مشتاق‌تر از پیش به بررسی تکنیک‌ها و آسیب پذیری‌های جدید می‌پردازید. افزون بر ایمن سازی کامپیوتر شخصی خود می‌توانید کسب و کار جدیدی را در حوزه امنیت شبکه برپا سازید و در این راستا، به مدیران وب‌سایت و شبکه‌ها کمک چشم‌گیری کنید.
- می‌توانید پس از خواندن کتاب، به صورت تخصصی‌تر علم هک و امنیت را با مطالعه و بررسی منابع دیگر آموزشی، دنبال کنید و در این مسیر، آنچه را که طی سال‌ها فراگیری، کسب کرده‌اید با برگزاری دوره‌های آموزشی با دیگران در میان بگذارید.

بررسی اجمالی این کتاب

مرکزیت این کتاب، بسیار سودمند و کاربردی است. برای آشنایی بیشتر نسبت به اصول پایه‌ای علم هک، پیش زمینه و مباحث عملی لازم در کتاب آورده شده است . افزون بر معرفی روش‌های هک در سرتاسر کتاب، مثال‌هایی از دنیای واقعی را که حاصل تجربه‌ی شخصی است، آورده شده است.

در نگارش بخش‌های مختلف کتاب تلاش شده، به درک، حوصله و غایت خواننده‌ی کتاب توجه شود. از سویی، مطالب به صورت آسان و قابل درک و از سویی دیگر، خلاصه و کاربردی نوشته شده است تا مخاطب بتواند به هدف خود زودتر از آنچه که می‌خواهد دست یابد. اما این بدان معنا نیست که این کتاب، هرآنچه که در علم هک وجود دارد را بیان می‌کند چراکه هر علمی بی‌نهایت است و این کتاب تنها الفبای هک را برای مبتدی‌ها بازگو می‌کند. در ادامه‌ی کتاب، هر آنچه که نیاز است تا به یک هکر حرفه‌ای تبدیل شوید، بیان می‌شود و مطمئن باشید که در این مسیر، شما را تنها نخواهیم گذاشت!

چه کسی باید این کتاب را بخواند

مخاطبان اصلی این کتاب، دانش آموزان، دانشجویان، محققان، توسعه دهندگان و مدیران وب‌سایت‌ها هستند که علاقه‌ی شخصی یا حرفه‌ای به فراگیری مبانی علم هک و روش‌های بهره برداری از آسیب‌پذیری‌ها دارند. آگاهی و دانش از اینکه، دشمنانتان چگونه عمل می‌کنند، به مخاطبان کتاب حاضر، برای دفاع در برابر آنها می‌تواند کمک شایانی کند.

بخش‌های کتاب به اندازه‌ی کافی ساده و روان هستند، بنابراین جای هیچ نگرانی نیست. مطالب و بخش‌های کتاب به‌گونه‌ای سازماندهی شده است که مخاطب دقیقا همان مسیری را بپیماید که یک هکر باتجربه پیموده است. بدان معنا که تمامی هکرهای حرفه‌ای، با مبانی و اصول هک (همان چیزی که در این کتاب به آن پرداخته‌ایم)، علم هک را شروع کرده‌اند و این نظر، کاملا بین هکرها ثابت شده است.

بنابراین با توجه به آنچه که گفته شد، در می‌یابیم که محتوای کتاب حاضر از سطح مبتدی شروع می‌شود و تا سطح متوسط با توجه به دانش مخاطب، تلاش و استعداد او، پیش می‌رود. مهم نیست که چه سن یا تحصیلات و یا شغلی دارید چراکه این کتاب در سطح مبتدی و متوسط نوشته شده است، آنچه که مهم است، این است که علم هک به شما، یک قدرت واقعی خواهد داد که تجربه‌ی آن، فراموش نشدنی است!

چگونه این کتاب سازماندهی می‌شود

همان‌گونه که گفته شد، مطالب و بخش‌های کتاب به‌گونه‌ای سازماندهی شده است که مخاطب دقیقا همان مسیری را بپیماید که یک هکر باتجربه پیموده است. اگر در علم هک، تازه وارد هستید، کتاب را از آغاز تا پایان مطالعه فرمایید تا به دانش و درک لازم برای اتصال به بخش‌های بعد، دست یابید و اگر از پیش تجربیاتی در این حوزه داشته اید، مختار هستید به طور مستقیم به هر بخش یا زیربخشی که مدنظرتان است، رجوع کنید.

در بخش ۱-مقدمه، به طور اختصار، از مقدمات هک و سلسله مراتب هکری شروع خواهیم کرد و سپس از نیازمندی‌های تبدیل شدن به یک هکر حرفه‌ای سخن می‌گوییم.

در بخش ۲-لینوکس، به آموزش نصب سیستم عامل محبوب هکرهای واقعی یعنی لینوکس می‌پردازیم. نصب سیستم عامل را به چند طریق توضیح می‌دهیم و از دلایل استفاده‌ی هکرها از این سیستم عامل، مطالبی را ارائه می‌کنیم. در پایان این بخش نیز، با معرفی کتاب و وب‌سایت‌هایی شما را تشویق به یادگیری این سیستم عامل خواهیم کرد.

در بخش ۳-گذرواژه‌ها، به مباحثی درباره‌ی گذرواژه‌ها و نحوه‌ی کرک آنها خواهیم پرداخت و سپس شما را با روش حمله‌ی فیشینگ آشنا خواهم کرد. اقدامات متقابل و معرفی چندین برنامه‌ی کرک نیز جزئی از محتوای این بخش کاربردی می‌باشد.

در بخش ٤-هک شبکه، با روش‌های مختلف گردآوری اطلاعات از هدف که با اصطلاح FootPrinting در نزد هکرها مطرح است، آشنا می‌شوید. پویش پورت، Banner Grabbing و جست‌وجوی آسیب پذیری‌ها نیز جزء مهمی از این بخش هستند. در انتهای این بخش، به کامپایل کردن اکسپلویت‌هایی به زبان PHP، Perl، Python و C/C++ خواهیم پرداخت و نخستین گام مبانی و اصول هک را بر می‌داریم. فراگیری مطالب این بخش از اهمیت بسیار بالایی برخوردار است.

در بخش ٥- هک شبکه بی سیم، ابتدا یک شبکه‌ی بی‌سیم را پویش می‌کنیم و سپس به سناریوی کرک WEP خواهیم پرداخت. این بخش کاربردی، مهم‌تر از بخش پیش نیست اما فراگیری آن، با اینکه نسبتا دشوار است، خالی از لطف نیست. شنود بسته‌های اطلاعاتی و اقدامات متقابل نیز در این بخش گنجانده شده است.

در بخش ٦-هک ویندوز، با NetBIOS، کرک گذر واژه سیستم عامل ویندوز و اقدامات متقابل آن آشنا می‌شوید.

در بخش ٧-بدافزارها، ابتدا به تعریف انواع بدافزارها خواهیم پرداخت و سپس با تروجان ProRAT، به یک سیستم عامل نفوذ می‌کنیم. در این بخش یاد می‌گیرید که چگونه تروجان ProRAT را تنظیم کنید و از آن به طور مؤثر استفاده کنید. همچنین اقدامات متقابل نیز در این بخش گنجانده شده است.

در بخش ٨-هک وب‌سایت، درباره‌ی هک وب‌سایت‌ها سناریوهایی را پیاده سازی می‌کنیم. هکرها به هک وب‌سایت علاقه‌ی بسیاری دارند. مختصری از رمز و راز نفوذ آنها را برایتان فاش می‌کنیم. در این بخش با الگو گرفتن از استاندارد OWASP، به محبوب‌ترین و رایج‌ترین آسیب‌پذیری‌های وب همچون Cross Site Scripting، Remote File Inclusion، Local File Inclusion، SQL Injection، نقض احراز هویت و مدیریت نشست و فوروارد و تغییر مسیر نامعتبر، خواهیم پرداخت. فراگیری مطالب این بخش نیز مانند بخش ٥ از اهمیت بسیار بالایی برخوردار است.

در بخش ٩-روش‌های مقابله با هکرها، از دنیای هکری کمی فاصله می‌گیریم و به دیدگاه امنیتی خود قوت می‌بخشیم. در این بخش به امنیت ٣ هدف یعنی امنیت کامپیوترهای شخصی، وب‌سایت‌ها و شبکه‌های بی‌سیم خواهیم پرداخت. نکات گفته شده در این بخش، امنیت را به طور کامل فراهم نمی کند چراکه امنیت مطلق نیست اما می‌تواند در یک سطح متوسط، فضایی ایمن را برای هدف تان فراهم سازد.

در بخش ١٠-نتیجه گیری، درباره‌ی حفظ آموخته‌ها و مسیری که پس از مطالعه‌ی این کتاب باید دنبال کنید، توضیحاتی ارائه می‌شود. سپس، در مبحث "پیش بینی از آینده..."، پیش‌بینی خود را از خطراتی که در پیش روی دنیای مجازی آینده است به طور اختصار ارائه می‌دهم.

سرانجام اینکه، شما می‌توانید پرسش‌های خود را در هنگام مطالعه کتاب یا پس از اتمام آن، در وب‌سایت Http://SecurityAdviser.ir در میان بگذارید. فراموش نکنید، در این مسیر تنها نیستید و شخصا به

پرسش، اهداف، ایده‌ها و دیدگاه‌هایتان پاسخ می‌دهم و آرزو دارم که این علم را با توکل به پروردگـار، در مسیری صحیح و درست دنبال کنید و از لذت و قدرت این علم، با انگیزه‌ای سالم و مثبت، نهایـت اسـتفاده را ببرید.

پس از سپاس و ستایش به درگاه پروردگار، از مدیریت محترم انتشارات پندار پارس، جناب آقای مهندس حسین یعسوبی و تمامی همکارانشان که مهربانانه دست مرا در انجام این هـدف مهـم فشـردند، تشـکر و قدردانی می‌نمایم.

علی اصغر جعفری لاری

Http://Parsing.ir

Http://SecurityAdviser.ir

Admin@SecurityAdviser.ir

سلب مسئولیت قانونی

اطلاعات ارائه شده در این کتاب، تنها برای مقاصد آموزشی است. نویسنده کتاب، هیچ مسئولیتی در قبـال سوء استفاده از اطلاعات ارائه شده ندارد. تمام اطلاعات داخل کتاب به مخاطب کمـک مـی کنـد تـا نگـرش دفاعی خود را در برابر حملات هکرها توسعه دهد. به هیچ عنوان نباید از این اطلاعات برای هر نوع آسیب مستقیم یا غیر مستقیم اسـتفاده کنیـد. منظـور از واژه‌ی "هـک" یـا "هکینـگ" در کتـاب، "هـک اخلاقـی[1]" می‌باشد.

طبق ماده ۱ قانون جرایم رایانه ای، "هر کس به طور غیرمجاز به داده هـا یـا سیسـتم هـای رایانـه ای یـا مخابراتی که به‌وسیله‌ی تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تـا یـک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد."

[1] Ethical Hacking

بخش ۱- پیش‌گفتار

هکر کیست ؟

هکر[1]، شخصی است که هدف اصلی او، نشان دادن قدرت خود به کامپیوتر و دیگر ماشین هاست. وارد شدن به سیستم و یا شکست دادن محاسبات، کنجکاوی در اطلاعات محرمانه از خصوصیات یک هکر می‌باشد. این فرد، یک برنامه نویس کنجکاو است که آسیبی به اهداف(وب‌سایت/شبکه/سرویس‌ها و...) وارد نمی‌کند و در اصل با انگیزه‌های سالم، باعث تحکیم امنیت اینترنت می‌شود.

مهم ترین دسته‌بندی هکرها

هکرها بر اساس فعالیت های‌شان، به سه دسته تقسیم می‌شوند:

۱. **هکر کلاه سفید**[2]: هکر کلاه سفید، یک فرد کامپیوتری است که هک اخلاقی انجام می‌دهد. این افراد معمولا متخصصان امنیتی با دانش هک و مجموعه ابزار هکرها هستند. هکرهای کلاه سفید از این دانش برای جست‌وجوی نقاط ضعف امنیتی و اجرای اقدامات متقابل در منابع استفاده می‌کنند. همچنین آنها به عنوان یک هکر اخلاقی یا یک تست کننده‌ی نفوذ شناخته می‌شوند. آنها بر تضمین امنیت و حفاظت از سیستم‌های IT تمرکز دارند.

۲. **هکر کلاه سیاه**[3]: هکر کلاه سیاه، یک فرد کامپیوتری است که هک غیراخلاقی انجام می‌دهد. این افراد، هکرهای‌جنایی یا کراکرهایی هستند که از دانش و مهارت خود برای اهداف غیرقانونی و یا مخرب استفاده می‌کنند. آنها به نقض یکپارچگی سیستم از راه دور با نیت مخرب می‌پردازند. همچنین آنها به عنوان یک هکر غیراخلاقی یا یک کراکر امنیتی شناخته می‌شوند. آنها بر کرک امنیت و سرقت داده‌ها تمرکز دارند.

۳. **هکر کلاه خاکستری**[4]: هکر کلاه خاکستری، یک فرد کامپیوتری است که گاهی به صورت قانونی و با اراده‌ی خوب فعالیت می‌کند و گاه این چنین فعالیت نمی‌کند. آنها معمولا برای منافع شخصی یا با داشتن نیت مخرب هک نمی‌کنند اما ممکن است جرائمی را در طول دوره بهره‌برداری از فناوری‌ها مرتکب شوند. آنها ترکیبی بین هکرهای کلاه سفید و هکرهای کلاه سیاه هستند.

---

[1] Hacker

[2] White Hat Hacker

[3] Black Hat Hacker

[4] Grey Hat Hacker

سلسله مراتب هکری

- **هکرهای مبتدی**: این دسته از هکرها، نسل جدیدی از کاربران کامپیوتر هستند که امکان استفاده از مقالات و ابزارهای هکرها را به‌روی اینترنت به صورت رایگان دارند اما هیچ دانشی از آنچه که در پشت صحنه روی می‌دهد، ندارند. درباره‌ی این دسته از هکرهای جوان در رسانه‌های خبری بیشتر شنیده می‌شود با اینکه آنها حداقل مهارت‌های مورد نیاز را برای انجام حملات خود دارند. آنها از اسکریپت و برنامه‌های توسعه داده شده توسط دیگران برای حمله به سیستم‌های کامپیوتری و شبکه‌ها استفاده می‌کنند. این دسته، آزاردهنده‌ترین و خطرناک‌ترین دسته‌ای هستند که می‌توانند مشکلات بزرگی را بدون اینکه در واقع بدانند چه کاری انجام می‌دهند، به‌وجود آورند.
- **هکرهای متوسط**: این دسته از هکرها معمولا درباره‌ی کامپیوترها، شبکه‌ها و به اندازه کافی درباره دانش برنامه‌نویسی به منظور درک آنچه که یک اسکریپت انجام می‌دهد، آشنایی دارند اما مانند Script Kiddiesها (هکرهای مبتدی)، آنها از اکسپلویت‌های[۱] از پیش توسعه داده شده‌ی شناخته شده برای انجام حملات استفاده می‌کنند.
- **هکرهای باهوش**: این دسته از هکرها، مهارت‌های بسیاری دارند. آنها بسیاری از اکسپلویت‌ها و ابزارهای هکرها را می‌نویسند. آنها می‌توانند امنیت هر نوع سیستمی را نقض کنند و ردپای خود را پنهان کنند. شما برای رسیدن به این سطح باید نهایت تلاش خود را کنید.

هکرها از حیث فعالیت، دانش و هدف می‌توانند به دسته‌های مختلفی تقسیم شوند که ما در اینجا به چند نمونه از آن اشاره کردیم.

چه کاری انجام دهیم تا به یک هکر تبدیل شویم؟

تبدیل شدن به یک هکر بزرگ، آسان و سریع رخ نمی‌دهد. خلاقیت، مقدار زیادی به شما کمک خواهد کرد و شانس‌تان را در هک سیستم بدون تشخیص آن بالا می‌برد. مورد دیگری که باید داشته باشید، یادگیری است. به یاد داشته باشید دانش، قدرت است. صبر نیز شرط مهمی است زیرا موضوعات بسیاری وجود دارد که درک آن دشوار است و نیاز به زمان دارد.

جهان پر از مشکلات جذاب در انتظار حل شدن است. هکرها لذت خاصی برای حل مشکلات دارند و همیشه می‌خواهند دانش و مهارت خود را محک بزنند. شما هم باید مثل یک هکر فکر کنید و از آنها به عنوان یک معلم الگو بگیرید اما نه دقیقا شبیه آنها باشید بلکه نگرش خود را دنبال کنید.

---

[۱] یک قطعه کد است که از اشکال یا آسیب پذیری در قسمتی از نرم‌افزار استفاده می‌کند و به هکر اجازه می‌دهد کنترل سیستم کامپیوتری را به‌دست گیرد.

برای ورود به دنیای هک، هرچه از نوجوانی شروع به فراگیری این علم کنید بسیار موفق‌تر خواهید شد اما این مورد، شرط اساسی تبدیل شدن به یک هکر موفق نیست. حتی اگر خواننده‌ی مسن این کتاب باشید می‌توانید مانند یک جوان، ایده‌پردازی و خلاقیت داشته باشید. آنچه که مهم است، استفاده صد درصد از استعداد، پشتکار و تفکرتان در مسیر فراگیری، تمرین و ممارست، توسعه و افزایش دانش‌تان و رسیدن به هدف نهایی است.

آیا واقعا به برنامه‌نویسی نیاز داریم؟

از خودتان بپرسید که آیا واقعا به فراگیری زبان برنامه‌نویسی نیاز دارید یا خیر. در پاسخ به این پرسش می‌توان گفت بله و خیر. به عقیده‌ی من، فراگیری زبان برنامه‌نویسی بستگی به هدفتان دارد. امروزه، همه نوع برنامه و ابزاری وجود دارد که می‌توانید با استفاده از آن، یک هکر اخلاقی نسبتا خوب (بدون دانستن هیچ زبان برنامه‌نویسی) باشید. اگر تمام ابزارهای امنیتی را به خوبی درک کرده باشید و حتی اگر آنچه که در پشت زمینه‌ی این برنامه‌ها رخ می‌دهد را درک کنید، می‌توانید هک کارآمدی داشته باشید. بیشتر افراد هنوز جزء دسته‌ی هکرهای مبتدی هستند.

نظر شخصی‌ام این است که باید برخی از زبان‌های برنامه‌نویسی را فرا بگیرید. حتی اگر این زبان‌ها، خیلی ابتدایی باشند اما به شما درک بسیار بهتری از آنچه که در پشت زمینه رخ می‌دهد، خواهد داد. همچنین، زمانی که درک خوبی از برنامه داشته باشید، قادر خواهید بود که اکسپلویت خودتان را توسعه دهید.

بنابراین توصیه‌ام این است که چند زبان برنامه‌نویسی را فرا گیرید. به مرور زمان با درک اصول آن، پنجره‌ی تمامی تکنیکهای جهانی هک به‌روی شما باز خواهد شد.

از کجا باید شروع کرد؟

نهایتا بسیاری از افراد تصمیم می‌گیرند که شروع به فراگیری زبان برنامه‌نویسی کنند اما نمی‌دانند از کجا شروع کنند. باور دارم که پیش از فراگیری زبان برنامه‌نویسی، باید HTML را در حد یک استاد فرا گرفته باشید. بخشی از تمام صفحات وب‌سایت‌ها که به‌روی اینترنت می‌بینید با HTML ساخته شده است. فراگیری HTML بسیار آسان است. پس از فراگیری آن، پیشنهاد می‌کنم برای یادگیری نخستین زبان برنامه‌نویسی، C را انتخاب کنید. C، یکی از رایج‌ترین زبان‌های برنامه‌نویسی است و بیشتر اکسپلویت‌های امروزی با این زبان ساخته می‌شوند. همچنین، برخی از قدرتمندترین برنامه‌های هک و ویروس‌هایی که امروزه وجود دارد، با این زبان برنامه‌نویسی ساخته شده است.

در ادامه...

در ادامه، پس از فراگیری زبان‌های مختلف مثل HTML و C، توصیه می‌کنم به فراگیری زبان‌های برنامه‌نویسی Perl و Python بپردازید. این زبان‌های برنامه‌نویسی، بسیار واضح‌اند و به خوبی طراحی و مستند شده‌اند. همچنین فراگیری آن برای مبتدی‌ها، آسان و ساده است. در دنیای امروز هکرها، دانستن مختصر این زبان‌های برنامه‌نویسی لازم و ضروری است.

بخش ۲- لینوکس

لینوکس چیست؟

لینوکس، یک سیستم عامل رایگان، متن-باز و همانند یونیکس است. همچنان‌که به فراگیری علم هک می‌پردازید، متوجه خواهید شد که فراگیری نحوه‌ی استفاده از سیستم عامل لینوکس چقدر مهم است. این دلیل برایتان قانع کننده است؟ در اینجا به دو واقعیت مهم برای فراگیری استفاده از این سیستم عامل می‌پردازیم:

۱. میلیون‌ها سرور در اینترنت به‌روی سیستم عامل لینوکس اجرا می‌شود. باید استفاده از این سیستم عامل را یاد بگیرید تا قادر باشید به این سرورهای وب نفوذ کنید.

۲. برخی از بهترین برنامه‌های هک تنها در لینوکس اجرا می‌شود.

انتخاب یک توزیع لینوکس

توزیع لینوکس، کرنل لینوکس (جزء مرکزی سیستم عامل) است. همچنین مجموعه‌ای از برنامه‌های‌کاربردی است. اگر در لینوکس مبتدی هستید، پیشنهاد می‌کنم که با توزیع Ubuntu آغاز کنید.

اجرای لینوکس

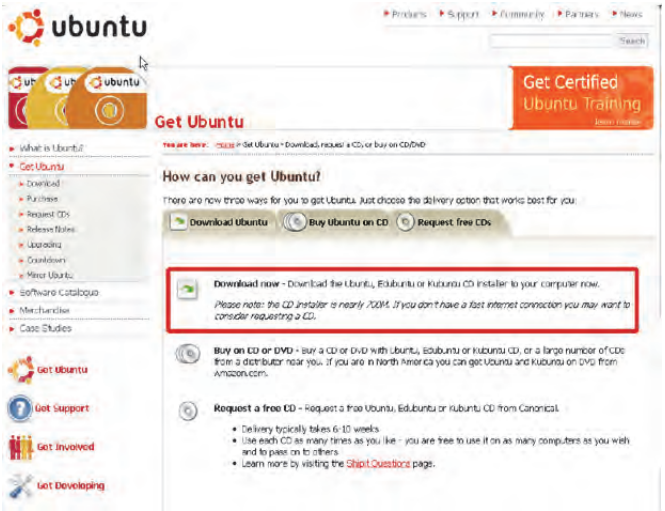
روش‌های بسیاری برای نصب و اجرای لینوکس وجود دارد. رایج‌ترین روش را در زیر به شما نشان می‌دهم.

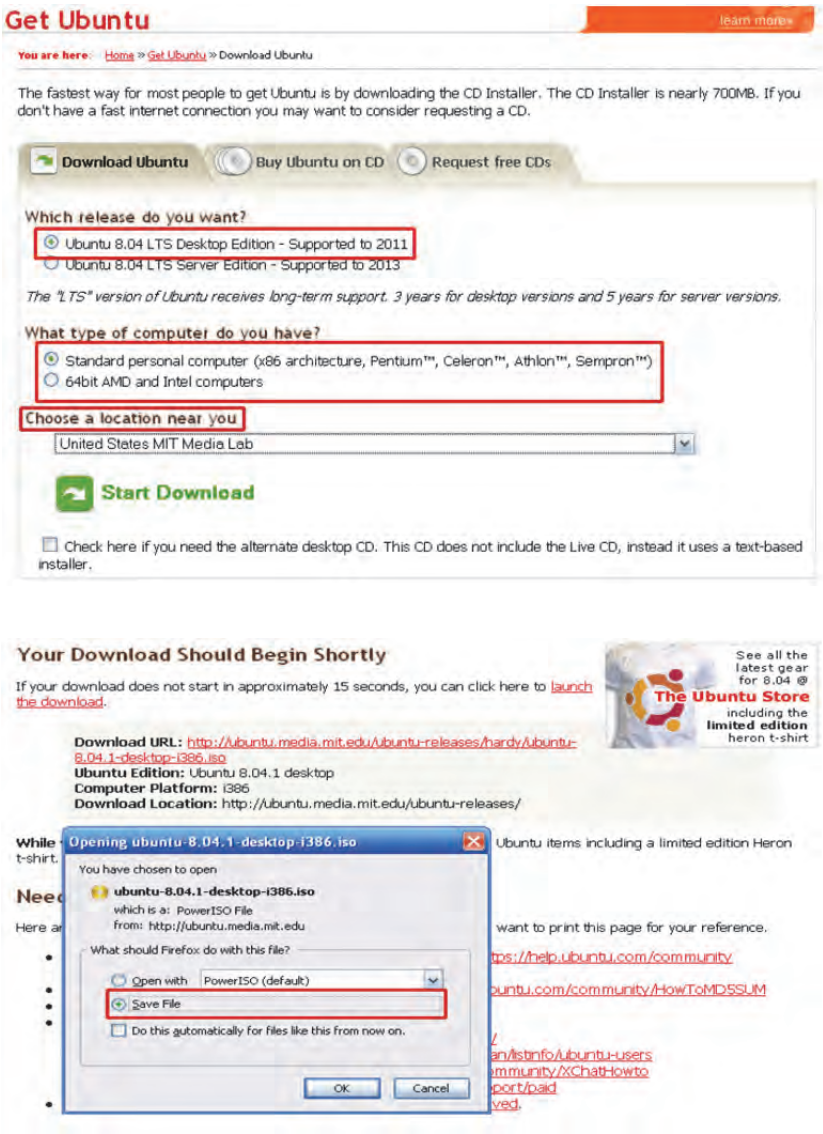
Live CD

Live CD، معمولا برای تست یک توزیع لینوکس مورد استفاده قرار می‌گیرد. با Live CD، سیستم عامل را به‌روی دیسک سختتان نصب نمی‌کنید چراکه سیستم عامل تنها به‌روی دیسک بوت اجرا می‌شود. از آنجا که سیستم عامل، به‌روی دیسک اجرا می‌شود، قادر نخواهید بود که همیشه فایل‌های سیستم را اصلاح کنید. هرآنچه که انجام می‌دهید به صورت موقت در RAM ذخیره می‌شود. در زیر، گام هایی برای ایجاد یک Live CD آورده شده است:

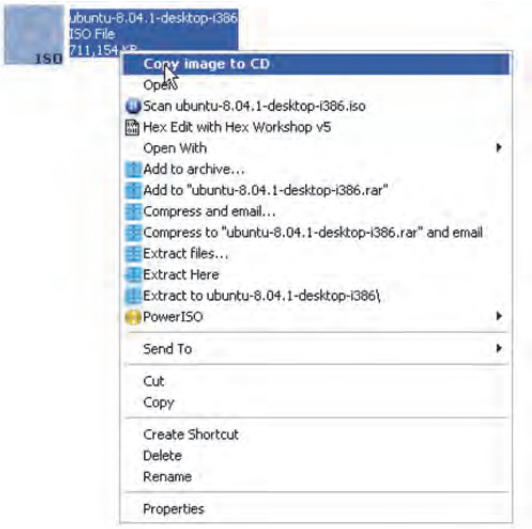
۱. فایل Ubuntu Live CD.iso را از آدرس http://www.ubuntu.com دانلود کنید.

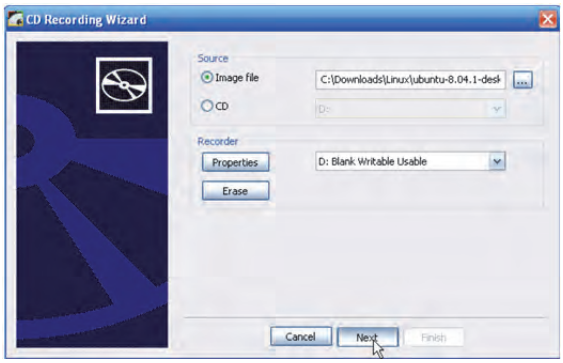
به یاد داشته باشید، آنچه که در شکل‌های این بخش به عنوان صفحات اصلی وب‌سایت ubuntu.com مشاهده می‌کنید، قالب وب‌سایت در هنگام نگارش کتاب بوده است و ممکن است قالب و طرح وب‌سایت در آینده تغییر کند. در صورتی که به آدرس بالا مراجعه کردید و صفحه‌ای مطابق با اشکال این بخش مشاهده نکردید، اصلا نگران نباشید. در این موقعیت، تنها به دنبال گزینه‌ای همانند "Download" در منوی وب‌سایت بگردید!

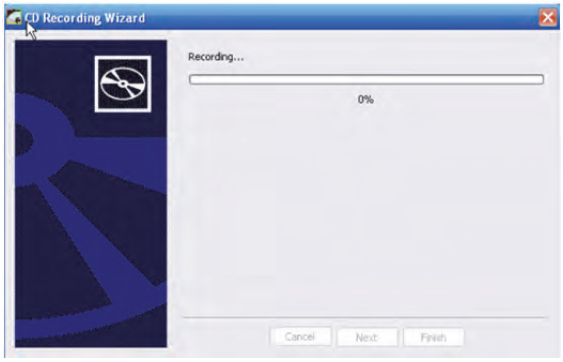


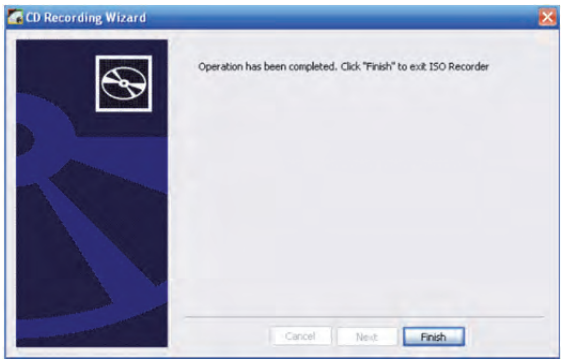


۲. IsoRecorder را از آدرس http://isorecorder.alexfeinman.com/isorecorder.htm دانلـــود و نصب کنید. فایل Ubuntu.iso را در یک سی دی خالی با این نـرم افـزار رایـت کنیـد. زمـانی کـه نرم‌افزار IsoRecorder را دانلود و نصب کردید به محل فایل دانلود شده (Ubuntu) برویـد و بـا راست کلیک، گزینه‌ی Copy image to CD را انتخاب و گام‌هایی که در شکل‌های زیر نشـان داده شده است را دنبال کنید:


ubuntu-8.04.1-desktop-i386
ISO File
711,154 KB
ISO
Copy image to CD
Open
Scan ubuntu-8.04.1-desktop-i386.iso
Hex Edit with Hex Workshop v5
Open With
Add to archive...
Add to "ubuntu-8.04.1-desktop-i386.rar"
Compress and email...
Compress to "ubuntu-8.04.1-desktop-i386.rar" and email
Extract files...
Extract Here
Extract to ubuntu-8.04.1-desktop-i386\
PowerISO
Send To
Cut
Copy
Create Shortcut
Delete
Rename
Properties

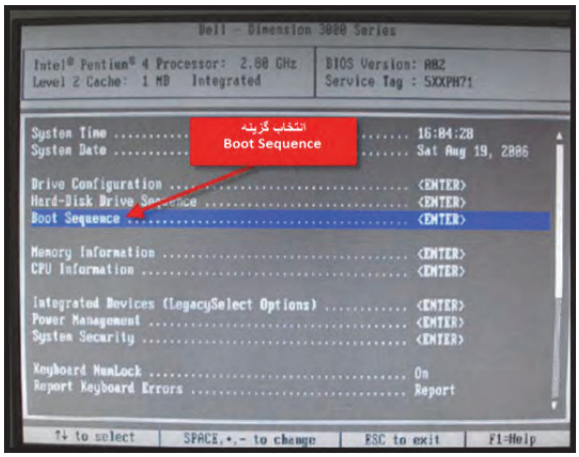

CD Recording Wizard
Source
Image file
C:\Downloads\Linux\ubuntu-8.04.1-desk
CD
D:
Recorder
Properties
D: Blank Writable Usable
Erase
Cancel
Next
Finish

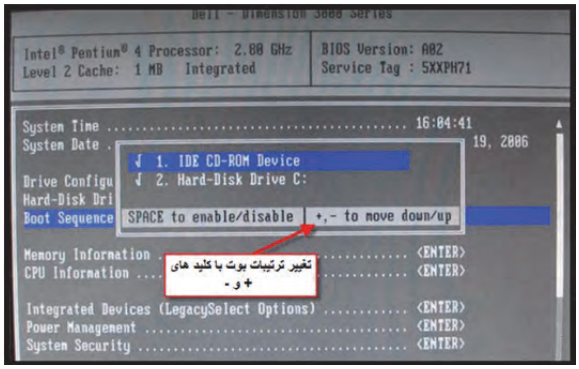

CD Recording Wizard
Recording...
0%
Cancel
Next
Finish



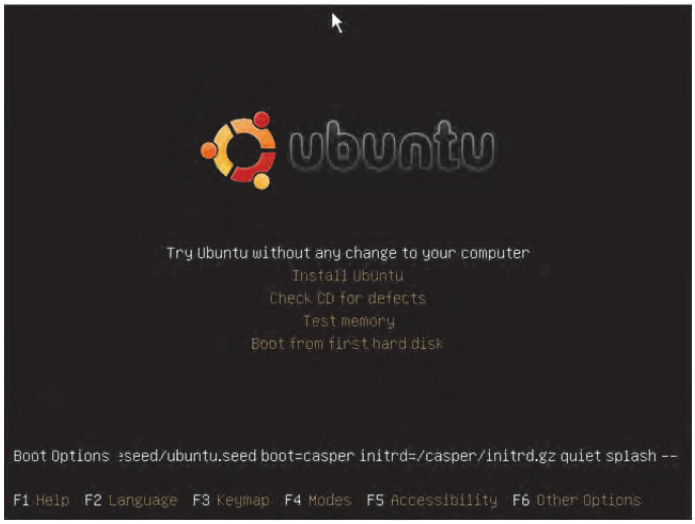
۳. کامپیوتر را با سی دی که اینک در CD-ROM ساخته شده، راه‌اندازی دوباره (Restart) کنید. اگر کامپیوترتان از طریق CD به بوت منتقل نشد و به ویندوز ادامه پیدا کرد، باید ترتیب‌های بوت کامپیوترتان را تغییر دهید. می‌توانید این کار را با راه‌اندازی دوباره‌ی کامپیوترتان و رفتن به BIOS انجام دهید. با فشردن کلید صحیح مربوط به بوت، به صفحه BIOS منتقل می‌شوید. در برخی کامپیوترها، کلید DEL و در برخی دیگر کلید F10 است. این تنظیمات به کامپیوترتان بستگی دارد. در همان ابتدای بالا آمدن سیستم عامل، می‌توانید کلید معرفی شده برای این تنظیمات را مشاهده کنید.

زمانی که در BIOS هستید، "Boot Sequence" را انتخاب کنید و مطمئن شوید که CD-ROM، گزینه‌ی نخست تنظیم شده است. اگر این طور نیست، آن را انتخاب کنید و مطمئن شوید که بوت CD-ROM پیش از Hard drive انتخاب شده است.





اگر همه چیز خوب پیش رفت، باید صفحه تنظیمات بوت Ubuntu را مشاهده کنید.

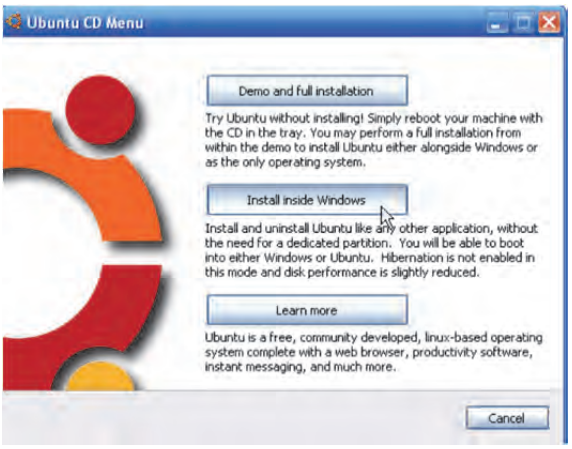


نخستین پنجره‌ای که مشاهده می‌کنید، لیستی از اسامی کشورها می‌باشد. زمانی که یک گزینه را انتخاب کردید، صفحه‌ی اصلی Ubuntu را مشاهده می‌کنید. در اینجا بدون هیچ ریسکی، نخستین گزینه را انتخاب کنید. در این هنگام دسکتاپ Ubuntu بارگذاری می‌شود. با کلیک روی دکمه‌ی Install به‌روی دسکتاپ، سیستم عامل نصب می‌شود.

Wubi

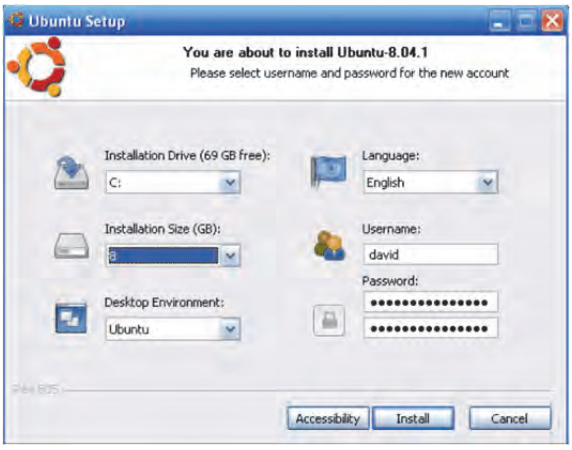
Wubi، برنامه‌ی مورد علاقه‌ام است. با Wubi Installer می‌توانید Ubuntu را به عنوان هر برنامه کاربردی دیگر ویندوز نصب و پاک کنید. اگر گام‌های بالا را دنبال کرده‌اید می‌توانید از نسخه Live CD برای نصب Wubi استفاده کنید یا می‌توانید نسخه کامل ۵ گیگابایتی را از آدرس http://wubi-installer.org دانلود کنید.

۱. اگر فایل ۵ گیگابایتی را دانلود کرده‌اید، روی آن دوبار کلیک کنید تا اجرا شود. اگر پیش‌تر از نسخه‌ی Live CD دانلود شده استفاده کرده‌اید، Ubuntu Live CD را در CD-ROM قرار دهید. پنجره‌ی Ubuntu CD menu بالا می‌آید.



۲. گزینه‌ی Install inside windows را انتخاب کنید.

۳. در پنجره‌ی بعدی، گزینه‌های مناسب را انتخاب کنید و به‌روی دکمه‌ی Install کلیک کنید.



٤. برای نصب کامل منتظر بمانید و در آخر، به‌روی دکمه‌ی Finish کلیک کنید.