

آموزش هک

برای مبتدی‌ها

www.ketab.ir

علی‌اصغر جعفری لاری
انتشارات پندار پارس

سرشناسه	: جعفری لاری، علی اصغر، ۱۳۶۷ -
عنوان و نام پدیدآور	: آموزش هک برای مبتدی‌ها/علی اصغر جعفری لاری.
مشخصات نشر	: تهران : پندار پارس، ۱۳۹۳.
مشخصات ظاهری	: ۱۸۴ ص.: مصور (رنگی).
شابک	: 978-600-6529-61-5 : ۱۱۰۰۰۰ ریال
وضعیت فهرست نویسی	: فیا
موضوع	: کامپیوترها -- ایمنی اطلاعات
موضوع	: شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	: هکرها
موضوع	: حفاظت اطلاعات
رده بندی کنگره	: ۱۳۹۳۵۹/۵۱۰۵TK ج۷/۱۸
رده بندی دیویی	: ۸/۰۰۵
شماره کتابخانه‌شناسی	: ۲۴۵۲۶۲۲

انتشارات پندار پارس

www.pendarepars.com
info@pendarepars.com

دفتر فروش: انقلاب، ابتدای کارگر جنوبی، کوی بسیج شماره ۱۴، واحد ۱۶
تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۱۲۲۴۵۰۱۸

نام کتاب	: آموزش هک برای مبتدی‌ها
ناشر	: انتشارات پندار پارس
ترجمه و تالیف	: علی اصغر جعفری لاری
چاپ نخست	: اردیبهشت ۹۳
شمارگان	: ۱۰۰۰ نسخه
لیتوگرافی	: ترام‌سنج
چاپ، صحافی	: فرشویه، خیام
قیمت	: ۱۱۰۰۰ تومان

شابک : ۹۷۸-۶۰۰-۶۵۲۹-۶۱-۵

هرگونه کپی برداری، تکثیر و چاپ کاغذی یا الکترونیکی از این کتاب بدون اجازه ناشر تخلف بوده و پیگرد قانونی دارد

فهرست

فصل نخست: آشنایی با مفاهیم هک و امنیت	۵
۱-۱ مفهوم هک اخلاقی	۵
هک	۵
هکر	۶
چه تفاوتی بین هکر و کراکر وجود دارد؟	۶
انواع هکرها	۷
دستکاری هکرها بر اساس فعالیت‌های انجام داده شده	۸
مهندسی اجتماعی چیست؟	۹
هک اخلاقی	۱۰
Hackivism	۱۰
hacker Terrorist	۱۰
هکرها چرا هک می‌کنند؟	۱۰
پارامترهای امنیت	۱۱
جلوگیری از نفوذ هکر	۱۱
مراحل انجام شده توسط هکرها	۱۲
فاز ۱: شناسایی	۱۳
فاز ۲: پویش و شمارش	۱۳
فاز ۳: کسب دسترسی	۱۳
فاز ۴: حفظ دسترسی و قرار دادن تریپ مین	۱۴
فاز ۵: پاک کردن رد پا	۱۴
شروع به کار یک هکر اخلاقی	۱۴
۱-۲ واژگان فنی	۱۵
۱-۳ هک آدرس پست الکترونیکی	۱۶
پست الکترونیکی چگونه کار می‌کند؟	۱۶
مسیر حرکت پست الکترونیکی	۱۷
پروتکل‌های سرویس پست الکترونیکی	۱۸
پیکربندی سرور پست الکترونیکی	۱۸
امنیت پست الکترونیکی	۱۹
جعل پست الکترونیکی	۱۹
روش‌های ارسال پست الکترونیکی جعلی	۱۹
پست الکترونیکی جعلی: به وسیله‌ی Open Relay Server	۲۰
پست الکترونیکی جعلی: به وسیله‌ی Web Script	۲۰
نمونه‌هایی از پیامدهای پست الکترونیکی جعلی	۲۰
اثبات یک پست الکترونیکی جعلی	۲۱
بمباران پست الکترونیکی	۲۱
هرز نامه‌های پست الکترونیکی	۲۱
هک گذرواژه‌ی آدرس پست الکترونیکی	۲۱
فیشینگ	۲۲
پیشگیری در برابر فیشینگ	۲۳

۲۳	ردیابی آدرس پست الکترونیکی
۲۵	 Keystroke logger
۲۵	انواع کی لاگرها
۲۵	برخی از کی لاگرهای مشهور
۲۶	ایمن سازی حساب پست الکترونیکی
۲۶	۱-۴ امنیت و هک ویندوز
۲۶	معماری امنیت ویندوز
۲۷	 LSA
۲۷	 SAM
۲۸	 VM
۲۸	معماری حساب کاربری ویندوز
۲۹	کریک گذر از روی حساب کاربری ویندوز
۳۲	حمله حساب کاربری ویندوز
۳۲	راههای مقابله با حمله ویندوز
۳۲	یک پوشه ای مخصوص بسازید
۳۳	اجرای Net user سیستم عامل ویندوز ویستا، ۷ و ۸
۳۴	حمله ی Brute Force
۳۵	حمله ی جدول Rainbow
۳۵	 Oph Crack
۳۵	راههای مقابله با حمله به گذر از روی حساب کاربری ویندوز
۳۶	ساخت درب پشتی برای سیستم عامل ویندوز
۳۶	اجرای امنیت Syskey
۳۶	تغییر ترتیب بوت
۳۷	۱-۵ آشنایی با تروجان ها
۳۷	درک تروجان
۳۸	انواع تروجان ها
۳۸	برخی از تروجان های معروف
۴۰	اجزای تروجان ها
۴۱	 Wrapper
۴۱	نحوه ی انتقال تروجان ها
۴۱	اتصال معکوس در تروجان ها
۴۲	شناسایی و حذف تروجان ها
۴۲	 TCP View
۴۳	راههای مقابله با حمله های تروجان
۴۴	۱-۶ حمله به سرورهای وب
۴۴	معرفی سرورهای وب
۴۴	راه اندازی یک سرور وب
۴۴	فرایند اصلی: سرورهای وب چگونه کار می کنند؟
۴۵	انواع حمله به سرورهای وب
۴۵	 Web Ripping
۴۶	 Google Hacking
۴۸	محافظت از فایل های تان در مقابل Google

۴۹	(XSS) Cross Site Scripting
۵۰	آسیب‌پذیری
۵۰	Directory Traversal Attack
۵۳	DataBase Server
۵۴	فرایند ورود به وب‌سایت
۵۵	SQL Injection
۵۷	PHP Injection: قرار دادن درج پستی PHP
۵۸	کنترل‌های دسترسی دایرکتوری
۵۸	چگونه نفوذگران خود را در هنگام حمله پنهان می‌کنند
۵۹	انواع ورودی‌های پروکسی
۵۹	ورودی پروکسی وب
۵۹	سرور پروکسی ناشناس
۶۰	۷-۱ هک شبکه‌های بی‌سیم
۶۱	استانداردهای بی‌سیم
۶۲	سرویس‌های ارائه شده توسط شبکه‌های بی‌سیم
۶۳	راه حل‌های امنیتی استاندارد بی‌سیم
۶۳	راه حل SSID
۶۴	فیلترینگ آدرس‌های MAC
۶۵	رمزگذاری کلید WEP
۶۵	بررسی اجمالی امنیت شبکه بی‌سیم
۶۵	حمله‌های شبکه بی‌سیم
۶۵	Broadcast Bubble
۶۶	War Driving
۶۶	جعل MAC
۶۷	کرک WEP
۶۷	راه‌های مقابله با حمله‌های شبکه بی‌سیم
۶۸	۸-۱ هک موبایل - جعل تماس و پیامک
۶۹	اقدامات مخرب پس از هک موبایل
۷۱	جعل تماس
۷۱	اطلاعاتی درباره‌ی جعل شماره‌ی تماس گیرنده
۷۱	جعل پیامک
۷۳	BlueSnarfing
۷۴	۹-۱ گردآوری اطلاعات و پویش
۷۴	وب‌سایت‌های گردآوری اطلاعات
۷۴	Whois
۷۴	نقشه‌برداری معکوس IP
۷۵	گردآوری اطلاعات با استفاده از موتور جست‌وجو
۷۷	تشخیص سیستم‌های 'live' به روی شبکه هدف
۷۷	War Dialer ها
۷۸	۱۰-۱ Sniffers (شنودکننده‌ها)
۷۸	Sniffer چیست ؟
۷۹	چه کسی از Snifferها استفاده می‌کند؟

۸۰	مقابله با Sniffer ها
۸۱	AntiSniff
۸۲	۱-۱۱ هک لینوکس
۸۲	چرا لینوکس ؟
۸۴	پوشش شبکه
۸۴	انواع پوشش پورت
۸۵	ابزار Nmap
۸۶	کرک گذرواژه در لینوکس
۸۷	ARA
۸۷	otkit های لینوکس
۹۱	ابزارهای امنیتی: ابزارهای تست امنیت
۹۱	اقدامات مقابل امنیتی لینوکس
۹۲	۱-۱۲ دیوار آتش چیست؟
۹۲	تعریف دیوار آتش
۹۳	دیوارهای آتش چه ویژگی دارند؟
۹۳	ویژگی‌های برجسته دیوارهای آتش امروزی
۹۵	انواع دیوارهای آتش
۹۵	مزایا و معایب استفاده از دیوارهای آتش
۹۵	مزایای استفاده از دیوارهای آتش
۹۵	معایب استفاده از دیوارهای آتش
۹۶	۱-۱۳ آسیب‌پذیری‌های برنامه‌های وب
۹۹	فصل دوم: ترفندهای نفوذ، هک و بهره‌برداری از آسیب‌پذیری‌ها
۹۹	۲-۱ چت با دوستان با استفاده از MS-Dos
۱۰۰	۲-۲ چگونه آدرس IP را تغییر دهید
۱۰۱	۲-۳ چگونه فایل‌های خراب شده‌ی XP را رفع کنیم
۱۰۲	۲-۴ حذف فایل/فولدر "Undeleteable"
۱۰۳	۲-۵ پنهان‌نگاری چیست؟
۱۰۵	۲-۶ هش MD5 چیست و چگونه از آن استفاده کنیم؟
۱۰۶	۲-۷ Tab Napping: یک حمله‌ی جدید فیشینگ
۱۰۹	۲-۸ چگونه ویروس New Folder را پاک کنیم
۱۰۹	Newfolder.exe چیست؟
۱۰۹	چگونه ویروس Newfolder.exe را پاک کنیم؟
۱۱۰	۲-۹ قطع اتصالات اینترنت در LAN/Wi-Fi
۱۱۲	۲-۱۰ مواظب کلاهبرداری‌های رایج اینترنتی باشید
۱۱۲	۱. کلاهبرداری فیشینگ
۱۱۳	۲. کلاهبرداری نیجریه‌ای
۱۱۳	۳. کلاهبرداری قرعه‌کشی
۱۱۴	۲-۱۱ WEP با استفاده از Airo Wizard
۱۱۶	۲-۱۲ چند نکته‌ی امنیتی درباره‌ی خریدهای آنلاین
۱۱۸	۲-۱۳ ساخت یک ویروس کامپیوتری
۱۱۹	۲-۱۴ تزریق SQL برای هک وبسایت
۱۱۹	SQL Injection چیست؟

۱۲۴	۲-۱۵ حمله‌ی 'Denial of Service' چگونه کار می‌کند
۱۲۵	حمله‌ی 'Denial of Service' چگونه کار می‌کند
۱۲۶	یک حمله‌ی "Denial of service" چگونه مسدود می‌شود
۱۲۷	۲-۱۶ چگونه شماره سریال برنامه‌ها را در گوگل پیدا کنیم
۱۲۸	۲-۱۷ آسیب‌پذیری یافت شده‌ی XSS در YouTube
۱۲۹	تشریح آسیب‌پذیری XSS در YouTube
۱۳۱	اقدامات متقابل
۱۳۱	۲-۱۸ دوازده نکته برای محافظت از کامپیوتر شخصی در برابر ویروس‌ها
۱۳۳	۲-۱۹ Deep Freeze
۱۳۴	۲-۲۰ تغییر خود به عنوان Google bot برای مشاهده‌ی اطلاعات پنهان
۱۳۵	چگونه Google Pot تبدیل شویم؟
۱۳۶	چگونه User Agent را به حالت آغازین برگردانیم؟
۱۳۷	۲-۲۱ Remote File Inclusion
۱۳۷	جست‌وجو آسیب‌پذیری
۱۳۸	۲-۲۲ CAPTCHA چیست چگونه کار می‌کند؟
۱۳۸	دقیقا هدف از سرورهای CAPTCHA چیست؟
۱۳۹	چه نیازی به ایجاد سیستم CAPTCHA به جدایی انسان و کامپیوتر توصیه کند؟
۱۳۹	چه کسی از CAPTCHA استفاده می‌کند؟
۱۳۹	طراحی یک سیستم CAPTCHA
۱۴۰	شکستن CAPTCHA
۱۴۰	۲-۲۳ نکاتی برای امنیت آنلاین
۱۴۱	۲-۲۴ لایه اتصال امن (SSL) چیست؟
۱۴۲	ارتباط امن چیست؟
۱۴۳	رمزگذاری چگونه کار می‌کند؟
۱۴۳	یک اتصال امن را چگونه بشناسیم؟
۱۴۴	رمزگذاری مورد استفاده توسط SSL چقدر امن است؟
۱۴۴	۲-۲۵ ساخت تروجان با استفاده از Beast 2.06
۱۴۷	۲-۲۶ هک یاهو مسنجر برای وارد شدن با چند شناسه
۱۴۸	۲-۲۷ پنج نکته برای ایمن‌سازی اتصالات شبکه بی سیم
۱۴۹	۲-۲۸ نفوذ به Nuke با بهره‌برداری از آسیب‌پذیری ماژول Book Catalog
۱۵۱	۲-۲۹ چگونه آسیب‌پذیری‌های منتشر شده را پیدا کنیم؟
۱۵۳	۲-۳۰ ده قانون تغییرناپذیر در رابطه با امنیت اطلاعات
۱۵۷	فصل سوم: گاه‌شمار تاریخ هک و امنیت کامپیوترها

مسئولیت هر گونه اقدام یا فعالیت مربوط به محتوای موجود در این کتاب منحصرأ به عهده‌ی شما خواننده‌ی گرامی می‌باشد. نویسنده هیچ مسئولیتی در قبال وقوع هرگونه اتهام غیر قانونی که افراد با سوء استفاده از اطلاعات داخل این کتاب برای نقض قانون انجام می‌دهند، نخواهد داشت. این کتاب حاوی مباحث و منابعی است که به طور بالقوه مخرب یا خطرناک است و تنها برای اهداف آموزشی و پژوهشی نوشته شده است.

طبق ماده ۱ قانون جرایم رایانه‌ای، "هر کس به طور غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی که به وسیله‌ی تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از ۹۱ روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد."

شرایط و مقررات این کتاب

در حالی که از این کتاب استفاده می‌کنید و آموزش‌های مختلف هک کردن را مطالعه می‌کنید، شرایط و مقررات زیر را پذیرفته‌اید:

- تمام اطلاعات ارائه شده در این کتاب برای مقاصد آموزشی است. نویسنده‌ی کتاب به هیچ وجه مسئول هرگونه سوء استفاده از اطلاعات نمی‌باشد.
- "هک برای مبتدیان" تنها یک اصطلاح است که عنوان کتاب را نشان می‌دهد و این کتاب هیچ اطلاعات غیرقانونی را ارائه نمی‌کند. کتاب "هک برای مبتدیان" بر روی امنیت کامپیوتر است و دزدی نرم افزار/کرک کردن/هک کردن را ترویج نمی‌کند.
- این کتاب کاملاً برای ارائه‌ی اطلاعات در موضوع‌های "امنیت کامپیوتر"، "برنامه‌نویسی کامپیوتر" و دیگر موضوع‌های مرتبط نوشته شده است و به هیچ وجه به هیچ "CRACKING" یا "HACKING" (غیر اخلاقی) نمی‌پردازد.
- هک یا نفوذ (بدون اجازه) به کامپیوتری که متعلق به شما نیست، غیر قانونی است.
- تمام اطلاعات موجود در این کتاب برای توسعه‌ی دفاع در مقابل هکرها نوشته شده است و به جلوگیری از حمله‌های هکرها کمک می‌کند. "هک برای مبتدیان" تأکید دارد که این اطلاعات نباید برای ایجاد هر نوع آسیب مستقیم یا غیرمستقیمی استفاده شود. هرچند، می‌توانید از این کدها به روی سیستم خود (با مسئولیت خودتان) امتحان نمایید.
- واژه‌ی "هک" یا "هک کردن" که در این کتاب استفاده شده است به عنوان "هک اخلاقی" یا "هک کردن اخلاقی" در نظر گرفته شده است.

۷. اینجانب تنها به هک‌های کلاه سفید و کلاه خاکستری باور دارم و از سوی دیگر، هک‌های کلاه سیاه را محکوم می‌کنم.
۸. بسیاری از اطلاعات ارائه شده در این کتاب، ترفندهای ساده‌ی کامپیوتر هستند (که ممکن است با عنوان هک نامیده شود) و به هیچ وجه به اصطلاح Hacking مربوط نمی‌شود. هدف از بیان این ترفندها با توجه به اینکه بیشتر مخاطبان کتاب مبتدی هستند، عدم ایجاد یکنواختی در مباحث آموزشی بوده است.
۹. برخی از ترفندهای ارائه شده ممکن است به دلیل رفع اشکالات، دیگر کارایی نداشته باشد. اینجانب مسئول هرگونه خسارت مستقیم یا غیرمستقیم ناشی از استفاده از هک‌های ارائه شده در این کتاب، نخواهم بود.
۱۰. شما می‌توانید پرسش‌های خود را در هنگام مطالعه‌ی کتاب یا پس از پایان آن، در وبسایت پرسش و پاسخ <http://SecurityAdviser.ir> در میان گذارید یا در صفحه‌ی مربوط به این کتاب در سایت انتشارات پندار پارس (pardarpars.com) مطرح کنید.

پیش‌گفتار

پیش از ورود به مباحث "آموزش هک برای مبتدی‌ها"، از شما بابت انتخاب این کتاب، سپاسگزارم.

این کتاب که مباحث آن، به طور ابتدایی، جذاب و کاربردی نوشته شده است مرجع مفیدی برای دانش آموزان، دانشجویان و هر فردی که به علم هک و امنیت علاقه‌مند است و می‌خواهد آن را از ابتدا شروع کند، خواهد بود. در این کتاب، ابتدا به تعاریف و مقدمات هک و امنیت خواهیم پرداخت و سپس شما را با دنیای واقعی هک آشنا می‌کنم. در نگارش این کتاب، خود را در جایگاه یک مخاطب مبتدی قرار داده‌ام تا بتوانم به هر شکلی ممکن، ذهنیات او را به طور کارآمد، درک کنم و از نگرانی‌های فراگیری این علم تا حدی بکاهم.

اگر می‌خواهید چهره‌نگار جری‌خنده‌های مخرب، ترفندهای سرقت آنلاین، دور زدن تدابیر امنیتی و یا قطع سرویس‌ها را فرا بگیرید، به پنجاه می‌کنم در جای دیگری به دنبال آن بگردید. اما اگر می‌خواهید هک اخلاقی را از ابتدا شروع کنید، به دنبال مرجعی مناسب برای فراگیری آن می‌گردید، به شدت پیشنهاد می‌کنم که این کتاب را به طور کامل مطالعه فرمایید.

با خواندن این کتاب، گام نخست را برای فراگیری هک برداشته‌اید. گام‌های بعدی شما به پشتکار، استعداد و هدف‌تان بستگی دارد. جست‌وجو در اینترنت، مطالعه کتاب‌های خارجی و داخلی و فراگیری زبان‌های برنامه‌نویسی می‌تواند در رسیدن به هدف‌تان به شما کمک شایانی کند. پس از خواندن این کتاب، تشخیص خواهید داد که چگونه علم هک بر روال کاری روزانه‌ی ما تأثیر می‌گذارد و می‌تواند در بسیاری از زمینه‌ها مانند هک حساب‌های بانکی و... بسیار خطرناک باشد. افزون بر این، پس از خواندن این کتاب می‌توانید درک کنید که هکر کیست و چگونه می‌توان از تهدیدهای امنیتی دفاع کرد. اما کار به اینجا ختم نمی‌شود، چراکه با پی بردن به قدرت واقعی هک، بسیار به این علم علاقه‌مند می‌شوید و مصمم‌تر از پیش به فراگیری تکنیک‌های مختلف در منابع دیگر خواهید پرداخت.

فراموش نکنید که، اگر بدانید چگونه هرکس نفوذ می‌کنند، می‌توانید از نفوذ آنها جلوگیری کنید و من تلاش کرده‌ام شما را با این هدف سالم بیشتر آشنا نمایم. پس از سپاس و ستایش به راه‌پروندگان، از مدیریت محترم انتشارات پندار پارس، جناب آقای مهندس حسین یعسوبی و تمامی همکارانشان که مهربانانه دست مرا در انجام این هدف مهم فشردند، تشکر و قدردانی می‌نمایم.

علی اصغر جعفری لاری

[Http://Parsing.ir](http://Parsing.ir)

[Http://SecurityAdviser.ir](http://SecurityAdviser.ir)

Admin@SecurityAdviser.ir