

۱۵۸.۴۹۱



امنیت، هک و نفوذ

(به صورت علمی با روش های عملی)

مطالب این کتاب همیشه به روز است...

www.ketab.ir

راوی: محمدجواد کریمی



سرشناسه	: کریمی، محمدجواد، ۱۳۶۸-
عنوان و نام پدیدآور	: امنیت، حک و نفوذ (به صورت علمی با روش‌های عملی) / [مولف] محمدجواد کریمی.
مشخصات نشر	: تهران: الماس دانش، .
مشخصات ظاهری	: ۱۶۰ ص: مصور (رنگی)، جدول.
شابک	: ۹۷۸-۶۰۰-۱۸۹-۰۸۱-۹
وضعیت فهرست‌نویسی	: فیپا
موضوع	: کامپیوترها -- ایمنی اطلاعات
موضوع	: هکرها
رده‌بندی کنگره	: QA۷۶/۹/ک۴ ۱۳۹۲
رده‌بندی دیویی	: ۰۰۵/۸
شماره کتابشناسی ملی	: ۳۳۵۶۷۸۸

انتشارات الماس دانش

تلفن: ۶۶۱۲۵۶۹۴

ناشر	انتشارات الماس دانش
عنوان کتاب	: امنیت، حک و نفوذ (به صورت علمی با روش‌های عملی)
نویسنده	: محمدجواد کریمی
ویراستار	: کاظم زرین
چاپ	: الوان ۶۶۵۶۲۵۴۹
شمارگان	: ۱۰۰ جلد
نوبت چاپ	: سوم- ۱۴۰۳
قیمت	: ۱۲۰۰۰۰ تومان
شابک	: ۹۷۸-۶۰۰-۱۸۹-۰۸۱-۹

کلیه حقوق و حق چاپ متن، طرح روی جلد و عنوان کتاب با نگرش به قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان مصوب ۱۳۴۸ محفوظ است و متخلفین تحت پیگرد قانونی قرار می‌گیرند.

فهرست مطالب

صفحه	عنوان
۹	مقدمه
۱۱	تاریخچه هک
۲۴	انواع هکرها
۲۴	گروه نفوذگران کلاه سفید
۲۴	گروه نفوذگران کلاه سیاه
۲۵	گروه نفوذگران کلاه خاکستری
۲۵	گروه نفوذگران کلاه صورتی
۲۶	مهارت‌های لازم در هک
۲۸	RFCها
۳۷	TCP/IP
۳۷	مدل OSI
۳۷	لایه اول (لایه فیزیکی)
۳۷	لایه دوم (لایه پیوند داده‌ها)
۳۸	لایه سوم (لایه شبکه)
۳۸	لایه چهارم (لایه انتقال)
۳۸	لایه پنجم (لایه جلسه)
۳۹	لایه ششم (لایه ارائه)
۳۹	لایه هفتم (لایه کاربرد)
۳۹	مدل TCP/IP
۳۹	لایه اول (لایه واسط شبکه)
۴۰	لایه دوم (لایه اینترنت)
۴۰	لایه سوم (لایه انتقال)

۴۱	لایه چهارم) لایه کاربردی
۴۱	پروتکل اینترنت
۴۲	ساختار بسته‌های IP
۴۳	ساختار بسته‌های TCP
۴۵	نفوذ به سیستم هدف
۵۳	مشخص کردن محدوده فعالیت
۵۳	اطلاعات عمومی
۵۹	IDLE اسکن
۶۰	اسکنرهای آسیب‌پذیری وب
۶۱	استفاده از گوگل
۶۱	۳- موردبندی
۶۵	پاک کردن رمز عبور در ویندوز
۶۵	به‌دست آوردن رمز عبور در ویندوز
۶۸	Fpipe
۶۹	جعل IP
۶۹	Sniffing
۷۰	Shatter attack
۷۱	مسیردهی آسیب‌پذیری
۷۱	فایل‌های نمونه
۷۱	Plug-in در مرورگرها
۷۲	افشای کد منبع
۷۲	تزریق SQL
۷۴	جعل درخواست (CSRF) Cross Site
۷۴	حمله‌های Phishing

۷۷	روش Tabnabbing
۷۹	سوءاستفاده از تگ‌های مخفی
۷۹	شاملیت‌های سمت سرور SSI
۸۰	چهار روش برای دور زدن امنیت یونیکس
۸۰	حمله‌های Brute Force
۸۱	حملات بر پایه داده‌های غیرمنتظره
۸۱	حمله‌های سرریز بافر
۸۲	حمله‌های format string
۸۲	حمله‌های تأیید اعتبار ورودی
۸۲	حمله‌های سرریز عدد صحیح و علامت عدد صحیح
۸۲	حملات Dangling Pointer
۸۳	کانال پستی
۸۴	Sendmail
۸۴	RPC
۸۴	SNMP
۸۴	Show Mount
۸۵	ناامنی‌های X
۸۵	ناامنی‌های SSH
۸۶	حمله‌های سرریز بافر Open SSL
۸۶	حمله‌های Apache
۸۶	حمله‌های حالت بی‌قرار
۸۷	رمز در یونیکس
۸۸	SymLink در دسترسی محلی
۸۸	شرایط رقابت

۸۸	اصلاح فایل های هسته
۸۹	کتابخانه های مشترک
۸۹	فایل هایی با قابلیت نوشتن جهانی
۸۹	وقفه ها
۹۰	به دست آوردن شماره تلفن در Dial-Up
۹۱	هک وسایل شبکه
۹۱	چند اصطلاح در شبکه
۹۵	مانیتورینگ شبکه
۹۵	دستگاه های حساس شبکه
۹۵	مانیتورینگ شبکه های محلی
۹۶	مانیتورینگ شبکه های بزرگ
۹۶	معیارهای مانیتورینگ
۹۷	جستجوی سیستم خودکار
۹۷	تغییر مسیر ARP
۹۹	پرش VLAN
۹۹	پروتکل اکتشاف سیسکو CDP
۱۰۰	حمله پروتکل STP
۱۰۰	RIP ها و نحوه کار آن
۱۰۱	اولین مسیر کوتاه باز OSPF
۱۰۲	هک شبکه های بی سیم
۱۰۶	اسکن کردن و مورد بندی شبکه های بی سیم
۱۰۹	هک سخت افزار
۱۰۹	کارت های مغناطیسی و RFID
۱۱۰	پاک کردن رمز عبور bios به ۵ روش

۱۱۲	رمز عبور ATA و USB U3
۱۱۴	بلوتوث
۱۱۵	مهندسی معکوس سخت افزار
۱۱۵	نگاشت دستگاه
۱۱۶	معمکوس کردن FirmWare
۱۱۷	به دست آوردن اطلاعات و تخلیه ی آن
۱۱۷	(۱) نصب برنامه روی سیستم هدف، MALWARE
۱۱۸	کرم ها
۱۱۸	Bot ها و زامبی ها
۱۱۹	(۲) مخفی کردن برنامه و فایل های آلوده
۱۲۰	نحوه چسباندن دو فایل اجرایی به هم
۱۲۲	مخفی کردن فایل ها در یکدیگر به روش ADS
۱۲۳	(۳) فیلترینگ اطلاعات
۱۲۴	(۴) دریافت اطلاعات:
۱۲۴	واکسن: مورد ارزیابی قرار دادن لاگ سیستم و ترافیک شبکه
۱۲۴	جاوا اسکریپت و اسکریپت نویسی فعال
۱۲۵	کوکی ها
۱۲۶	حمله های XSS
۱۲۷	آسیب پذیری های Cross-Frame /Domain
۱۲۸	ناحیه ماشین محلی LMZ
۱۲۸	تگ IFRAME
۱۲۸	به دست آوردن IP افراد بازدیدکننده از سایت های ثانوی
۱۲۹	حمله های SSL
۱۳۳	حملات Homograph

برنامه‌های مخرب در شروع کار سیستم‌عامل.....	۱۳۳
فایل‌های ضمیمه.....	۱۳۵
سرریز بافر پردازشگر GDI+ JPEG.....	۱۳۶
۶) ایجاد درب‌های پشتی.....	۱۳۷
پیوست‌ها:.....	۱۴۲

مقدمه

هک! و باز هم هک! اسمی که همیشه برای افراد جذابیت خاصی داشته، دارد و خواهد داشت. جامعه افراد علاقه‌مند به هک بسیار گسترده است. این افراد ممکن است برنامه‌نویسانی باشند که حتی در کار خود بسیار خبره هستند ولی برنامه‌نویسی به‌تنهایی آن‌ها را اغنا نمی‌کند. حتی ممکن است، این علاقه‌مندان، افرادی باشند که نهایت استفاده آن‌ها از کامپیوتر، گوش دادن به موسیقی، تماشای فیلم و یا کار با برنامه‌های اداری باشد. همه و همه به این مقوله علاقه نشان می‌دهند.

شاید دلیل این علاقه‌مندی به هک کنجکاوی باشد؛ حس کنجکاوی بدون محدودیت! شاید آن‌ها هم شنیده‌اند که یک هکر با داشتن یک کامپیوتر می‌تواند به هر کجا که بخواهد سرک بکشد، اسم خود را در صفحات وب سایت‌های بزرگ قرار دهد، حساب‌های بانکی را خالی کند و... آن هم در دنیای امروزه که عصر ارتباطات نامیده شد و این اتفاق بدون اینترنت غیرممکن است.

توصیه من به شما این است که هیجان خود را کنترل کنید و با عزمی راسخ آماده یک سفر طولانی برای یادگیری هک و هک کردن شوید. هیچ‌وقت به هیچ حدی راضی نشوید! همیشه دنبال یادگیری مطالب جدید باشید. اگر در اوایل راه، آموختید، چگونه با استفاده از برنامه‌های آماده، کامپیوتر دوست‌تان! را هک کنید، هرگز این کار را نکنید. شما باید خودتان آن برنامه‌ها را بنویسید! شما باید خود، با نوشتن هزاران خط کد به بزرگ‌ترین سرورهای دنیا نفوذ کنید.

و اما در مورد این کتاب. این کتاب با بیان مقدماتی در مورد هک، روش‌هایی که در هر حمله مورد نیاز شماست را بیان می‌کند. کتاب‌های زیادی در بازار وجود دارد که متأسفانه تنها به بیان انواع هکرها و... می‌پردازند و یا آموزش نرم‌افزارهایی را می‌دهند که حداقل ۱۰ سال است منقضی شده و وقتی کاربر آن‌ها را می‌خواند نمی‌تواند آن را عملی کند و این باعث دلسردی کاربر می‌شود. کتابی که اکنون در دست شماست شالوده‌ای است از کتاب‌های بزرگی در زمینه‌ی هک مثل Hacking Exposed⁶ و Network Security Secret and Solution یا The Art of Exploitation و ده‌ها نسخه اینترنتی از مقالات و البته تجربیات خودم. (در مورد مقالات اینترنتی به دلیل اینکه به‌طور مستقیم از آن‌ها استفاده کرده و بعد از یادگیری مطالب آن‌ها و بعد از گذشت زمان و با بیانی دیگر در لابه‌لای یک مجله از چند مقاله استفاده کرده‌ام، امکان بیان مرجع آن وجود نداشته و شاید اگر خود نویسنده آن مقاله هم این کتاب را بخواند، متوجه نشود که از مطلب وی استفاده شده است. لذا همین جا از تمام این دوستان تشکر و قدردانی می‌کنم.) ما در این کتاب قصد بیان نرم‌افزارهای کلیدی مورد استفاده در هک - و البته منظور، برنامه‌های هکی که هک‌های آماتور از آن استفاده می‌کنند نیست - را نداریم. در اینجا روش را می‌آموزید و آنگاه، با اندکی جستجو در اینترنت می‌توانید نام نرم‌افزارهای کلیدی را بیابید. در خصوص نرم‌افزارهای هک‌های آماتور هم که هیچ‌وقت به سراغش نروید. در آخر باز هم تأکید می‌کنم، هرگز و هرگز خسته نشوید که این راه، بسیار طولانی است. همیشه به انتهای آن فکر کنید...

هک‌های آینده نزدیک! موفق باشید.