

راهنمای جامع کار بردی

هکر

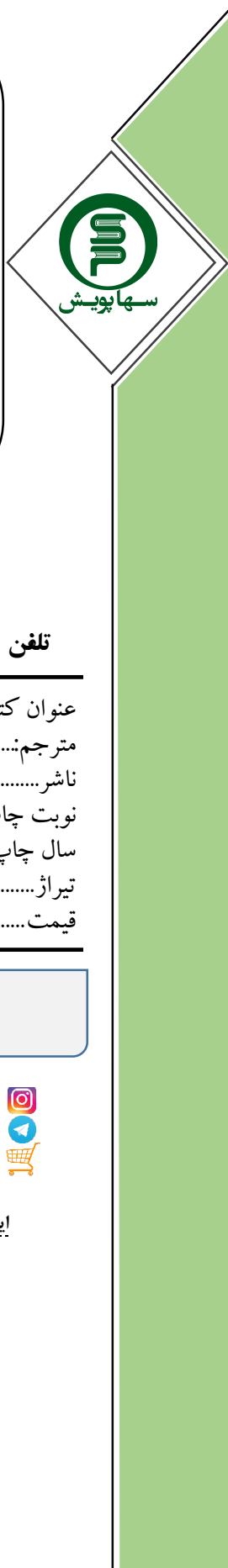
(نفوذگر)

مؤلف: ریچارد منس فیلد

مترجم: حمید اسحق بیگی



سرشناسه : Mansfield, Richard
 عنوان و نام پدیدآور : هکر (نفوذگر)/مؤلف ریچارد منس فیلد ؛ مترجم حمید اسحق بیگی.
 مشخصات نشر : تهران: سها پویش، ۱۴۰۱.
 مشخصات ظاهری : ۲۴۸ ص: مصور (بخشی رنگی)، جدول.
 شابک : ۹۷۸-۶۲۲-۹۴۵۴۵-۳-۴
 وضعیت فهرست نویسی : فیا
 یادداشت : عنوان اصلی: Hacker attack، ۲۰۰۰.
 موضوع : کامپیوترها -- ایمنی اطلاعات
 شناسه افزوده : اسحق بیگی حسنی، حمید، ۱۳۵۲ - ، مترجم
 رده بندی کنگره : ۹/۷۶QA
 رده بندی دیویی : ۸/۰۰۵
 شماره کتابشناسی ملی : ۸۹۶۲۵۳۰
 اطلاعات رکورد : فیا
 کتابشناسی :



همراه ۰۹۳۵۱۲۶۱۴۱۹

تلفن ۳-۶۶۵۶۹۸۸۱

عنوان کتاب: راهنمای جامع و کاربردی هکر (نفوذگر)
 مترجم: احمد اسحق بیگی
 ناشر: سها پویش
 نوبت چاپ: اول
 سال چاپ: ۱۴۰۲
 تیراژ: ۱۰۰ نسخه
 قیمت: ۱۸۰۰۰۰ تومان

شابک: ۳-۴-۹۴۵۴۵-۶۲۲-۹۷۸

soha_pub
 @soha_pub

فروشگاه آنلاین: www.sohabook.ir



این اثر مشمول قانون حمایت مؤلفان و مصنفان و هنرمندان مصوب ۱۳۴۸ می‌باشد.

مقدمه

این روزها باگسترش استفاده از اینترنت و توسعه شبکه‌های محلی، مواجهه بامشکل نفوذ به رایانه‌ها و دسترسی به اطلاعات موجود در آن‌ها هستیم. بر این اساس برای مقابله و پیش‌گیری از دسترسی و سرقت منابع و اطلاعات موجود در شبکه و رایانه‌ها لازم است شناختی از روش‌های عمومی نفوذ به رایانه‌ها و مقابله با آن‌ها داشت.

باتوجه به این خصوصیات سعی شده است ترجمه‌ی کتاب فوق دارای نگارشی ساده و روان باشد تا این کتاب قابل استفاده‌ی تمام کاربران رایانه و اینترنت را برای برقراری امنیت سیستم‌های خود در مقابل نفوذگران، برآورده کند.

در پایان نیز از کلیه‌ی کسانی که من را در ترجمه‌ی این کتاب یاری دادند، به‌خصوص آقایان تورج صارمی راد، سعید اسحق‌بیگی و رضا حبیبی تشکر و قدردانی می‌کنم.

همید اسحق‌بیگی

فهرست

فصل اول

خطر در اینترنت

مقدمه	۹
روبات‌های عنکبوتی نفوذگران	۱۰
تلفن رایگان راه دور	۱۱
پیمان‌های ویندوز	۱۲
امنیت اینترنتی ویندوز در شبکه	۱۴
نفوذ آزمایشی	۱۴
آزمایش سپرهای حفاظتی و درگاه‌ها	۱۵
اطلاعات شخصی و دسترسی نفوذگران	۱۵
مقابله با جست‌وجوی نفوذگران	۱۷

فصل ششم

امنیت در شبکه

مقدمه	۴۹
امنیت محیط کار	۴۹
مهندسی (برنامه‌ریزی) اجتماعی	۴۹
گسترش سیاست امنیتی	۵۰
کنترل کلمه‌های رمز ورود (گذر واژه‌ها)	۵۲
ارتباط امن رایانه‌ای	۵۲
دیواره‌های آتش (حفاظت‌ها)	۵۳
اتصال سیستم‌های باز (اُ اس آی)	۵۳
مخفی‌سازی اطلاعات	۵۷

فصل هفتم

خطر و سرعت انتقال داده‌ای

مقدمه	۵۹
دی‌اس‌ال و نفوذگران	۶۰
حمله‌ی عدم سرویس‌دهی (داس)	۶۲

فصل هشتم

پهنای باند و امنیت

مقدمه	۶۵
دلیل‌های حمله‌ی نفوذگران	۶۵
نصب نرم‌افزار «زون‌الارم»	۶۶
انواع دیگر دیواره‌ی آتش	۶۹
کنترل غریبه‌ها	۷۰
حفاظت یا دیواره‌ی آتش رایگان	۷۲
تله‌گذاری	۷۲
فایل‌های ردپا	۷۳
کنترل فایل‌های ردپا	۷۳
فایل‌های ردپای مخرب	۷۵

فصل نهم

اینترنت خصوصی

مقدمه	۷۹
جاسوس اینترنتی یا سایبری	۸۰
ورشکستگی شرکت‌ها	۸۲

فصل دوم

نفوذ به سیستم‌های تلفنی

مقدمه	۱۸
نفوذگران تلفنی	۱۹
کنترل مکالمه	۲۰
اهریمنان تلفنی	۲۱

فصل سوم

انواع نفوذگران

مقدمه	۲۳
انواع نفوذگران	۲۴
نفوذگران مبتدی	۲۴
نفوذگران مزاحم و متجاوز	۲۵
نفوذگران و ویروس‌ها	۲۶
پیام ناخواسته (اسپام)	۲۸
پالایش	۳۱
مقابله با پیام‌های ناخواسته	۳۲
جست‌وجوگرهای قدرت‌مند	۳۳

فصل چهارم

پیدا کردن گذر واژه‌ها

مقدمه	۳۵
نفوذ به داخل سیستم	۳۶
تقلید و شبیه‌سازی (اسپوفینگ)	۳۶
مشکلات گذر واژه‌ها	۳۸
تجمع نفوذگران	۴۰

فصل پنجم

نرم‌افزارهای ضد نفوذگری

مقدمه	۴۳
-------	----

مشکل یای انحصاری	۱۲۴
محدودیت گذر واژه‌ها	۱۲۵
گذر واژه‌های طولانی	۱۲۷
ذخیره فضای خالی	۱۲۸

فصل چهاردهم

استاندارد رمزنگاری داده‌ها

مقدمه	۱۲۹
ناسا و «دی‌بی‌اس»	۱۳۰
الگوریتم داخلی «دی بی اس»	۱۳۳
پردازش قدرتی	۱۳۵

فصل پانزدهم

کلیدهای عمومی رمز

مقدمه	۱۳۷
کلید توزیع مرکزی	۱۳۹
رمز نگاری محض	۱۴۰
در مخفی (در پشتی)	۱۴۰
خواص عدددهای اول	۱۴۲
ریاضی محض و «رسا» (آی اس ای)	۱۴۳

فصل شانزدهم

تعیین هویت الکترونیکی

مقدمه	۱۴۷
تعیین هویت با روش «رسا» (آر اس ای)	۱۴۸
عدم انکار هویت	۱۴۹
جعل عنوان	۱۵۱
رمزنگاری ترکیبی	۱۵۲

فصل هفدهم

امنیت در ویندوز ۲۰۰۰

مقدمه	۱۵۳
لایه شکاف‌های امنیتی (اس اس ال)	۱۵۳
پنهان سازی فایل‌ها	۱۵۵
نسخه‌برداری اختصاصی	۱۵۶
نسخه پشتیبان فایل‌های رمزی	۱۵۷
اقدامات امنیتی	۱۵۷
رمز کردن فایل‌ها	۱۵۸
امنیت کلید امنیتی	۱۶۲
باز کردن فایل‌های «پی‌اف‌ایکس»	۱۷۰
بازیابی اضطراری	۱۷۱

حساب پستی رایگان	۸۳
حداکثر امنیت	۸۴
بازدید خصوصی	۸۶
فن آوری مهندسی تلفن‌های خانگی	۸۶
ثبات صفحه کلید	۸۸
ضد حمله	۸۹
کنترل «استارت آپ» ویندوز	۸۹
جست‌وجوی کلمه‌ی کلیدی	۹۰
مخفی کردن اطلاعات	۹۱
شیوه‌های نوین	۹۲

فصل دهم

مبانی رمز نگاری

مقدمه	۹۳
رمز نویسی	۹۳
روش‌های کهن	۹۵
روش انبساطی	۹۷
روش فشرده‌سازی یا تراکمی	۹۷
تقسیم گروهی یا بلوکی	۹۸
اهداف رمزنگاری	۹۹

فصل یازدهم

جهش بزرگ در رمزنگاری

مقدمه	۱۰۱
برنامه‌ی کشف رمز	۱۰۶
جدول ضد رمزنگار	۱۰۹
کشف رمز	۱۱۰

فصل دوازدهم

رایانه و رمزنگاری

مقدمه	۱۱۳
سرعت و دقت	۱۱۴
ضعف امنیتی نرم‌افزارها	۱۱۵
گذر واژه‌های نهفته	۱۱۵
کشف ساختار و الگو	۱۱۶
کاربرد کد داخلی	۱۱۶
نقص در یای انحصاری	۱۲۰

فصل سیزدهم

روش‌های کشف رمز

مقدمه	۱۲۱
یای انحصاری	۱۲۲

فصل هجدهم

رمزنگاری نوری

۲۰۸ کرم‌ها

فصل بیست و دوم

ملیسا و قانون‌های جدید

۲۰۹ مقدمه
 ۲۱۰ انتشار ملیسا
 ۲۱۱ نویسه یا کاراکتر شناسایی
 ۲۱۲ ویروس خوش خیم
 ۲۱۲ چگونگی فعالیت ملیسا
 ۲۱۶ امنیت ناپایدار
 ۲۱۷ ویروس لاو باگ
 ۲۱۸ برنامه‌ی لاو باگ
 ۲۱۹ حفاظت شخصی
 ۲۲۰ غیر فعال کردن اسکریپت‌ها
 ۲۲۱ بلوف نفوذگران

فصل بیست و سوم

ویروس‌های ماکرو

۲۲۲ مقدمه
 ۲۲۲ ویرایشگرها و ماکروها
 ۲۲۳ حداکثر امنیت
 ۲۲۴ حفاظت داخلی
 ۲۲۶ ماکرونویسی
 ۲۲۷ اجرای خودکار ماکروها
 ۲۲۸ آلودگی رایانامه‌ها
 ۲۲۹ اصلاح نرم‌افزارها

فصل بیست و چهارم

مقابله با ویروس‌ها

۲۳۲ مقدمه
 ۲۳۳ تهدید ویروس‌ها
 ۲۳۵ آلودگی
 ۲۳۵ بهترین حفاظت
 ۲۳۶ برنامه‌های کمکی ضد ویروس‌ها
 ۲۳۶ جست‌وجوی امضای ویروس‌ها
 ۲۳۸ پنهان کردن ویروس‌ها
 ۲۳۹ برنامه‌های طعمه
 ۲۳۹ تغییر اندازه فایل‌ها
 ۲۴۰ تغییر سرجمع کنترل

۲۴۳ واژه‌نامه

۱۷۳ مقدمه
 ۱۷۳ رمزنگاری اتمی
 ۱۷۴ کشف رمز کلیدهای ترکیبی
 ۱۷۷ قطبش فوتون‌ها
 ۱۷۷ بیت کوانتومی
 ۱۷۸ ضعف پردازش کوانتومی
 ۱۷۸ رمزنگاری کوانتومی
 ۱۸۱ ارسال کلید

فصل نوزدهم

امنیت آهنین

۱۸۳ مقدمه
 ۱۸۳ کلیدهای یکبار مصرف
 ۱۸۴ رمزنگاری با عددهای تصادفی
 ۱۸۵ کتاب رمز و عددهای تصادفی
 ۱۸۶ برنامه‌ی نمونه
 ۱۸۷ هسته اصلی برنامه
 ۱۸۹ برنامه‌ی راپ (آر آپ‌ی)
 ۱۹۰ رمزنگاری واقعی
 ۱۹۰ برنامه‌ی دوم

فصل بیستم

کرم‌های رایانه‌ای

۱۹۵ مقدمه
 ۱۹۶ کلاه برداری الکترونیکی
 ۱۹۷ کرم‌ها
 ۱۹۸ دانش واژه‌ها
 ۱۹۸ کرم‌های سودمند
 ۱۹۹ تاریخچه

فصل بیست و یکم

ویروس‌ها و شبه‌ویروس‌ها

۲۰۱ مقدمه
 ۲۰۳ انواع اطلاعات رایانه‌ای
 ۲۰۳ انتشار ویروس‌ها
 ۲۰۴ ویژگی‌های پنهان برنامه‌ها
 ۲۰۶ درهای مخفی
 ۲۰۶ پاک کردن اطلاعات
 ۲۰۷ اسب‌های تروا