اندیشه‌های یک هکر

مؤلف: وحید گودرزی اصفهانی

سرشناسه	: گودرزی اصفهانی، وحید، ۱۳۶۳-
عنوان و نام پدید آور	: اندیشه‌های یک هکر/ مولف وحید گودرزی اصفهانی.
مشخصات نشر	: تهران : خدمات نشر کیان رایانه سبز: ناقوس، ۱۳۹۰.
مشخصات ظاهری	: ۲۰۸ص.: مصور، جدول.
شابک	: ۸- ۳٤ - ٦۰۲۱ - ٦۰۰ - ۹۷۸
یادداشت	: چاپ قبلی: ناقوس، ۱۳۸٤، (۱۲۸ص).
یادداشت	: چاپ دوم.
موضوع	: کامپیوترها – ایمنی اطلاعات
موضوع	: شبکه‌های کامپیوتری – اقدامات تامینی
موضوع	: حفاظت اطلاعات
موضوع	: هکرها
رده بندی کنگره	: ۱۳۹۰ ۹گ۹ک۷/۹۷۸۶Q
رده بندی دیویی	: ۰۰۵/۸
شماره کتابشناسی ملی	: ۲٤٥٦۸٦۹

انتشارات کیان رایانه سبز

نام کتاب	: **اندیشه‌های یک هکر**
ناشر	: انتشارات کیان رایانه سبز
ناشر همکار	: ناقوس- خلیج فارس- ندای سبز شمال
مؤلف	: وحید گودرزی اصفهانی
چاپ اول	: ۱۳۹۰
تیراژ	: ۸۰۰ جلد
حروف نگار	: مریم رضایی
چاپ و صحافی	: علاّمه
قیمت	: **۶۵۰۰ تومان** (به همراه CD)
شابک	: ۸-۳٤-٦۰۲۱-٦۰۰-۹۷۸
ISBN	: 978-600-6021-34-8

مراکز پخش:

انتشارات کیان رایانه سبز: خ انقلاب – خ ۱۲ فروردین - کوچه نوروز- پلاک ۲۷ طبقه اول

تلفن: ۶۶۴۱۶۴۴۶-۶۶۴۰۶۸۳۴-۶۶۴۱۱۷۱۵

نمایندگی اصفهان: خ سید علیخان - جنب مسجد - کتاب‌فروشی مهرگان ۰۳۱۱-۲۲۱۳۷۵۱

خرید Online از طریق سایت www.kianpub.com

فهرست مطالب

سخنی با خوانندگان ۷
بخش اول: هک، هکر، ترفندها و نرم‌افزارها ۹
فصل اول: هک کردن رایانهٔ خود ۱۱
۱-۱کنترل Start up ۱۲
۱-۲ اسکریپت برنامهٔ ویژوال‌بیسیک را غیرفعال کنید ۱۲
۱-۳ یک برنامهٔ کوچک برای اضافه کردن User در Windows XP ۱۳
۱-۴ رجیستری چیست؟ ۱۳
۱-۴-۱ تهیهٔ نسخهٔ پشتیبان از رجیستری ۱۴
۱-۵ مخفی کردن Drive موردنظر ۱۴
۱-۶ خروجی درگاه usb سیستم خود را قفل کنید ۱۵
۱-۷ افزایش سرعت اینترنت در Windows XP ۱۶
۱-۸ فعال کردن ویژگی‌های مربوط به DVD در Media player ۱۶
۱-۹ حذف گزینهٔ setting از پنجرهٔ Display propertice ۱۶
۱-۱۰ نام کاربری خود را عوض کنید ۱۶
۱-۱۱ کنترل را در دست خود بگیرید ۱۷
۱-۱۲ حذف کردن برنامه‌هایی که پاک نمی‌شوند ۱۷
۱-۱۳ از نمایش پیام‌های غیرضروری جلوگیری کنید ۱۸
۱-۱۴ فهرست برنامه‌های اخیر اجرا شده را از بین ببرید ۱۸
۱-۱۵ منوی start را سریع‌تر کنید ۱۸
۱-۱۶ تعیین برنامه جهت اجرای سی‌دی‌های صوتی قرار داده شده در CD ROM ۱۹
۱-۱۷ کنترل کردن Auto run ۱۹
۱-۱۸ افزایش سرعت برنامهٔ Internet Explorer در مرور صفحات ۱۹
۱-۱۹ عبور از کلمهٔ عبور در Windows xp ۱۹
۱-۲۰ Password امنیتی برای Windows XP ۲۰
۱-۲۱ عبور از کلمهٔ عبور در Windows 2000 ۲۱
۱-۲۲ پیغامی برای خوش‌آمدگویی در Windows XP ۲۱
۱-۲۳ جلوگیری از دسترسی به فایل‌های مخفی ۲۱
فصل دوم: آشنایی با اصطلاحات هک و مفهوم آنها ۲۳
۲-۱ آشنایی با نفوذگر ۲۴
۲-۲ انواع نفوذگرها ۲۴
۲-۲-۱ هکرها Hacker ۲۴
۲-۲-۲ کراکرها Cracker ۲۴
۲-۲-۳ پراکر Preaker ۲۴
۲-۳ هکرهای جوان (Script Kiddies) ۲۴
۲-۴ تاریخچهٔ نفوذگری ۲۵
۲-۵ IP چیست؟ ۲۶
۲-۶ Port چیست؟ ۲۷
۲-۷ BOMB چیست؟ ۲۷
۲-۸ Trojan Horse چیست؟ ۲۷
۲-۹ Worm چیست؟ ۲۸
۲-۱۰ Spam چیست؟ ۲۹
۲-۱۱ عمل Ping چیست؟ ۲۹
۲-۱۲ Whois چیست؟ ۲۹
۲-۱۳ عمل Boot چیست؟ ۳۰
۲-۱۴ Crack کردن یعنی چه؟ ۳۰
۲-۱۵ Firewall چیست؟ ۳۰
۲-۱۶ باگ یا bul چیست؟ ۳۰
۲-۱۷ اکسپلویت چیست؟ ۳۱
۲-۱۸ Shell چیست؟ ۳۱
فصل سوم: اصول هک ۳۳
۳-۱ مراحل نفوذ به رایانه‌ها ۳۴
۳-۲ انواع نفوذ ۳۴
۳-۳ مراحل نفوذ وقتی هدف مشخص باشد ۳۴
۳-۳-۱ کنترل Online از طریق نرم‌افزارهای Chat ۳۵
۳-۳-۲ کنترل Online از طریق پست الکترونیکی ۳۵
۳-۳-۳ کنترل Offline از طریق خط تلفن ۳۶
۳-۴ پیدا کردن IP Address قربانی ۳۷
۳-۵ نفوذ در مواقعی که هدف مشخص نباشد ۳۷
۳-۶ پیدا کردن IP Address قربانی در شبکه ۴۶

۳-۷ پیدا کردن Port ۴۷
۳-۸ حمله به قربانی ۴۷
۳-۹ مراحل حمله، وقتی فقط بدانید قربانی Online است ۴۷
فصل چهارم: آموزش Sub Seven 2.2 و نرم‌افزارهای مدیریت از راه دور ۴۹
۴-۱ Sub 7 ۵۰
۴-۲ تنظیم Server برنامهٔ Sub 7 ۵۰
۴-۲-۱ آماده‌کردن محتویات پوشه برنامهٔ Sub 7 ۵۰
۴-۲-۲ باز کردن فایل Edit Server. exe ۵۱
۴-۲-۳ تنظیمات مخصوص با گزینهٔ Server Setting ۵۱
۴-۲-۴ تنظیمات مخصوص با گزینهٔ Notifications ۵۲
۴-۲-۴-۱ مقایسهٔ Yahoo Messenger و I Seek You ۵۴
۴-۲-۵ تنظیمات مخصوص با گزینهٔ Binded Files ۵۶
۴-۲-۶ تنظیمات مخصوص با گزینهٔ Plugins ۵۷
۴-۲-۶-۱ Plugin چیست؟ ۵۷
۴-۲-۷ تنظیمات مخصوص با گزینهٔ Restrictions ۵۸
۴-۲-۸ تنظیمات مخصوص با گزینهٔ E_mail ۵۹
۴-۲-۹ تنظیمات مخصوص با گزینهٔ Exe Icon / Other ۵۹
۴-۳ ذخیره کردن اطلاعات بر روی Server ۶۱
۴-۴ تنظیمات مناسب برای Server ۶۱
۴-۵ ارسال Server برای قربانی ۶۲
۴-۶ استفاده از برنامهٔ Sub 7 2.2 ۶۲
۴-۶-۱ امکانات گزینهٔ Local Shortcuts ۶۳
۴-۶-۲ امکانات گزینهٔ Misc Shortcuts ۶۳
۴-۶-۳ امکانات گزینهٔ Open ۶۴
۴-۶-۴ امکانات گزینهٔ Connection ۶۴
۴-۶-۵ امکانات گزینهٔ Connect Commands ۶۵
۴-۶-۶ امکانات گزینهٔ Other ۶۵
۴-۶-۷ امکانات گزینهٔ Scanner ۶۵
۴-۶-۸ بررسی گزینه‌های Key / Messages ۶۵
۴-۶-۹ امکانات گزینهٔ Key / Messages ۶۶
۴-۷ بررسی گزینه‌های Advanced ۶۷
۴-۷-۱ امکانات گزینهٔ Advanced ۶۷
۴-۸ امکانات گزینهٔ Find Files ۶۸
۴-۹ امکانات گزینهٔ Pcket Sniffer ۶۸
۴-۱۰ امکانات گزینهٔ Password ۶۸
۴-۱۱ بررسی گزینه‌های Miscellaneous ۶۹
۴-۱۲ بررسی گزینه‌های Fun Manager ۶۹
۴-۱۳ بررسی گزینه‌های Fun Other ۷۰
۴-۱۴ بررسی گزینه‌های Pligins ۷۱
۴-۱۵ بررسی گزینه‌های Local OptionS ۷۱
۴-۱۶ امکانات گزینهٔ Local Options ۷۲
۴-۱۷ امکانات گزینهٔ Advanced ۷۲
۴-۱۸ نرم‌افزار NetBus ۷۲
۴-۱۹ نرم‌افزار Bo2k ۷۳
۴-۲۰ نرم‌افزارهای مدیریت از راه دور ۷۳
۴-۲۰-۱ نرم‌افزار Remote Desktop Connection ۷۳
۴-۲۰-۲ نرم‌افزار TightVNC ۷۵
فصل پنجم: نرم افزارها و دستورات مورد استفادهٔ هکرها ۷۹
۵-۱ پیدا کردن IP Address ۸۰
۵-۲ IP Address رایانه‌ها در مواقع قطع ارتباط با شبکه چیست؟ ۸۲
۵-۳ استفاده از Hak Tek ۸۲
۵-۴ پیدا کردن Port باز ۸۳
۵-۶ استفاده از Net Lab ۸۵
۵-۷ حمله به قربانی ۸۶
۵-۸ انجام عمل How Is ۸۶
۵-۹ استفاده از Neo Trace Pro ۸۶
۵-۱۰ سرویس Telnet ۸۸
۵-۱۱ سرویس FTP ۸۹
۵-۱۲ راه‌اندازی FTP Server ۹۱
۵-۱۲-۱ نصب یک نرم‌افزار FTP Server ۹۳
۵-۱۲-۲ رفع عیب FTP Server ۹۴
۵-۱۳ سرویس TFTP ۹۶
۵-۱۴ دستور ping ۹۶

۵-۱۵ دستور netstat ۹۸
۵-۱۶ دستور tracert ۹۹
۵-۱۷ دستور nslookup ۱۰۱
۵-۱۸ نرم‌افزارهای Sniff ۱۰۱
۵-۱۹ نرم‌افزار sniffit ۱۰۱
۵-۲۰ عملیات جعل IP (IP SPOOFING) ۱۰۲
۵-۲۱ مخفی نگهداشتن خود در شبکه ۱۰۳
۵-۲۲ سرقت ارتباط (session hijacking) ۱۰۳
۵-۲۳ حملات DOS ۱۰۴
۵-۲۴ حملات Lond ۱۰۵
۵-۲۵ حملات ping ۱۰۵
فصل ششم: آشنایی با ترفندهای Yahoo Messenger ۱۰۷
۶-۱ ایجادشناسه‌های‌فرعی‌در Yahoo Messenger ۱۰۸
۶-۲ ورود به نرم‌افزار Yahoo Messenger در محل کارتان ۱۱۰
۶-۳ مشاهدهٔ رمز عبور از پشت ستاره‌ها ۱۱۲
با رایانه شما چه کسانی Chat کرده‌اند؟ ۱۱۳
۶-۴ مشاهده آرشیو پیام‌های رد و بدل شده در Yahoo Messenger ۱۱۴
۶-۵ شکلک‌های مخفی در Yahoo Messenger ۱۱۵
فصل هفتم: ترفندهای یک هکر ۱۱۷
۷-۱ مخفی کردن فایل‌ها ۱۱۸
۷-۲ ردیابی یک سرویس‌دهندهٔ خاص ۱۱۹
۷-۳ تکنیک‌های whois ۱۲۱
۷-۴ تشخیص سیستم عامل قربانی با دستور ping ۱۲۲
۷-۵ ارسال Email با آدرس‌های جعلی ۱۲۷
۷-۶ دریافت نامه‌های الکترونیک با Telnet ۱۳۰
بخش دوم: برنامه‌نویسی برای هک ۱۳۳
فصل اول: انتخاب زبان برنامه‌نویسی ۱۳۵
۱-۱ مقدمه ۱۳۶
۱-۲ تاریخچهٔ Delphi ۱۳۶
۱-۲-۱ سال ۱۹۹۵ – Delphi1 ۱۳۶
۱-۲-۲ سال ۱۹۹۶ – Delphi2 ۱۳۷
۱-۲-۳ سال ۱۹۹۷ – Delphi3 ۱۳۷
۱-۲-۴ سال ۱۹۹۸ – Delphi4 ۱۳۷
۱-۲-۵ سال ۱۹۹۹ – Delphi5 ۱۳۷
۱-۲-۶ سال ۲۰۰۱ – Delphi6 ۱۳۸
۱-۲-۷ دلفی در لینوکس ۱۳۸
۱-۲-۸ سال ۲۰۰۲ – Delphi7 ۱۳۸
۱-۲-۹ سال ۲۰۰۳ – Delphi8 ۱۳۹
۱-۲-۱۰ سال ۲۰۰۴ – Delphi2005 ۱۳۹
۱-۲-۱۱ سال ۲۰۰۶ – Delphi2006 ۱۴۰
۱-۲-۱۲ سال ۲۰۰۷ – Delphi2007 ۱۴۰
۱-۲-۱۳ Delphi 2009 ۱۴۰
۱-۲-۱۴ Delphi 2010 ۱۴۱
۱-۳ تاریخچهٔ vb ۱۴۱
۱-۳-۱ Visual Basic.Net2002 ۱۴۲
۱-۳-۲ Visual Basic.Net2003 ۱۴۲
۱-۳-۳ Visual Basic.Net2005 ۱۴۲
۱-۳-۴ Visual Basic.Net2008 ۱۴۳
فصل دوم: برنامه‌های کاربردی در رایانه ۱۴۷
۲-۱ کار با فایل‌ها ۱۴۸
۲-۲ کار با رجیستری ۱۵۹
۲-۳ روش کار برنامه‌های مخرب ۱۶۹
۲-۴ برنامه‌های کاربردی این بخش ۱۷۰
فصل سوم: آشنایی با نرم‌افزارهای هک (Hack) ۱۷۵
۳-۱ نرم‌افزارهای کاوشگر ۱۷۶
۳-۱-۱ IP Address Finder ۱۷۶
۳-۱-۲ ارسال Email با استفاده از نرم‌افزار ۱۸۶
۳-۱-۳ نرم‌افزار Mail Bomber ۱۸۸
۳-۲ نرم‌افزارهای جاسوسی ۱۸۹
۳-۳ مراحل طراحی یک Trojan بسیار ساده ۱۸۹
فصل چهارم: جعل صفحات وب ۲۰۱
نحوهٔ کار سیستم‌های جعل صفحات ۲۰۲

سخنی با خوانندگان

با سلام

چهار سال پیش وقتی اقدام به نگارش این کتاب نمودم، با توجه به مطالب ساده و همچنین شیوهٔ نگارش آن، انتظار چاپ مجدد را نداشتم؛ اما بعد از گذشت دو سال، این کتاب در قالب چاپ دوم توسط ناشر محترم منتشر شد و حالا بعد از چهار سال با توجه به استقبال خوانندگان عزیز از این کتاب و نیز با عنایت به رشد سریع ترفندها و راهکارهای هکرها برای نفوذ به سیستم‌های سازمان‌ها با توافق ناشر محترم تصمیم گرفتم مطالب قبلی را با کمی تغییر و البته اضافه کردن مطالبی جذابتر و با همان زبان ساده و شیوا و بدون تکلف برای استفادهٔ شما سروران گرامی آماده کنم تا شاید در چاپ سوم مطالبی کاربردی‌تر در اختیار شما دوستان قرار گیرد.

حتماً تاکنون از برنامه‌ها و نرم‌افزارهای گوناگونی استفاده نموده‌اید و شاید گاهی اوقات با خود اندیشیده‌اید این‌گونه برنامه‌ها چگونه و توسط چه کسانی تهیه شده‌اند. دراین میان، از نرم‌افزارهای مربوط به نفوذگری و یا نرم‌افزارهای مدیریت سیستم استقبال بیشتری شده است و از آنجا که تهیهٔ این‌گونه نرم‌افزارها آنچنان هم دشوار نیست، بسیاری از طراحان و برنامه‌نویسان در سراسر دنیا تولید این برنامه‌ها را به نیت بازاریابی و یا نمایش ابتکارات خود و یا گاهی سوءاستفاده از اعتماد کاربران انجام می‌دهند. در این میان، آشنایی کاربران خانگی حتی در سطوح ابتدایی از مبانی تولید این برنامه‌ها و یا روش کار آنها امری الزامی است.

در کتاب حاضر فرض بر آن است که خوانندهٔ محترم، اطلاعات چندانی از شبکه و اینترنت ندارد. از این‌رو نگارنده با پرورش و سمت‌دهی افکار وی، استعدادهای او را در راستای تولید نرم‌افزارهایی خلاقانه شکوفا می‌کند.

در ادامه انتظار می‌رود، خوانندگان گرامی بعد از مطالعهٔ این کتاب بدون پیش‌فرض قبلی در برنامه‌نویسی قادر به تولید نرم‌افزارها و یا وب‌سایت‌هایی با کارایی منحصر به فرد باشند، با روش‌های تشخیص درست صفحات آشنا شوند و هیچ‌گاه اسرار خود را ناخواسته فاش ننمایند.

در پایان، خاطر نشان می‌کنم که این کتاب منحصربه‌فرد بوده و قابل استفاده برای تمامی دوست‌داران رایانه، شبکه و برنامه‌نویسی است. به طوری که برای تمامی سنین و تمام رشته‌های تحصیلی قابل استفاده است. در هیچ کجای این کتاب سعی نشده تا خواننده درگیر اطلاعات اضافی و یا غیرکاربردی شود و فقط مباحث کاربردی با مثال‌هایی ساده و گویا که در انتخاب آنها نهایت دقت به‌عمل آمده بیان شده‌اند.

ضمناً مسئولیت هرگونه استفادهٔ نابجا از محتویات این کتاب و CD همراه آن برعهدهٔ خواننده محترم است.

با تشکر

وحید گودرزی v.goudarzi@ymail.com