به نام خدا

مبانی امنیت اطلاعات

ومعرفی ابزارهای رایج هک قانونمند

مؤلف:

ابوالفضل یوسفی راد

مؤسسه فرهنگی هنری دیباگران تهران

◂ عنوان کتاب: **مبانی امنیت اطلاعات و معرفی ابزارهای رایج هک قانونمند**

◂ مولف : **ابوالفضل یوسفی راد**

◂ **ناشر: موسسه فرهنگی هنری دیباگران تهران**

◂**ویراستار:** مهدیه مخبری

◂**صفحه آرایی:**نازنین نصیری

◂**طراح جلد:**داریوش فرسایی

◂ **نوبت چاپ:** اول

◂ **تاریخ نشر:** ۱۳۹۹

◂ **چاپ و صحافی:**صدف

◂ **تیراژ:**۱۰۰ جلد

◂ **قیمت:**۸۰۰۰۰۰ ریال

◂ **شابک:** ۹۷۸-۶۲۲-۲۱۸-۳۹۹-۸

نشانی واحد فروش: تهران، میدان انقلاب، خ کارگر جنوبی، روبروی پاساژ مهستان، پلاک ۱۲۵۱

تلفن: ۲۲۰۸۵۱۱۱-۶۶۴۱۰۰۴۶

فروشگاههای اینترنتی دیباگران تهران :

WWW.MFTBOOK.IR

www.dibagarantehran.com

www.dibbook.ir

نشانی تلگرام:mftbook@ نشانی اینستاگرام دیبا dibagaran_publishing

سرشناسه:یوسفی راد، ابوالفضل، ۱۳۶۵-

عنوان و نام پدیدآور:مبانی امنیت اطلاعات و معرفی ابزارهای رایج هک قانونمند/مولف:ابوالفضل یوسفی راد ؛ویراستار: مهدیه مخبری.

مشخصات نشر: تهران : دیباگران تهران :۱۳۹۹

مشخصات ظاهری:۲۸۶ ص

شابک: ۹۷۸-۶۲۲-۲۱۸-۳۹۹-۸

وضعیت فهرست نویسی: فیپا یادداشت: کتابنامه:ص.۲۸۶

موضوع:کامپیوترها-ایمنی اطلاعات

موضوع:computer security

موضوع:شبکه های کامپیوتری-تدابیر ایمنی

موضوع:computer networks-security measures

موضوع: تکنولوژی اطلاعات-جنبه های اجتماعی

موضوع: information technology-social aspects

موضوع: هکرها hackers

رده بندی کنگره: QA ۷۶/۹

رده بندی دیویی: ۰۰۵/۸

شماره کتابشناسی ملی: ۷۴۳۲۸۵۸

فهرست مطالب

مقدمه ناشر ۷
مقدمه مؤلف ۸
پیشگفتار ۹

فصل اول: مفاهیم بنیادی در امنیت ۱۰

۱-۱ مقدمه ۱۱
۱-۲ تعاریفی از امنیت ۱۱
۱-۳ تعریف امنیت اطلاعات ۱۱
۱-۴ جنبه‌های اصلی امنیت ۱۲
۱-۵ امنیت شبکه و ضرورت وجود آن ۱۵
۱-۶ اصطلاحات و واژگان فنی در امنیت ۱۷

فصل دوم: معرفی هکرها و انواع حملات آنان ۲۴

۲-۱ مقدمه ۲۵
۲-۲ فرایند موجود در حملات ۲۵
۲-۲-۱ مهاجم و انواع آن ۲۶
۲-۲-۲ انواع حملات ۲۸
۲-۲-۳ آسیب‌پذیری ۵۳
۲-۲-۴ نتایج حمله ۵۴
۲-۲-۵ اهداف حمله ۵۶
۲-۳ مراحل انجام هک ۵۶
۲-۴ انواع تست در هک قانونمند ۵۷
۲-۵ زبان 133t speak ۵۸

فصل سوم: روش‌های جمع‌آوری اطلاعات و اسکن شبکه ۶۰

۳-۱ مقدمه ۶۱
۳-۲ جمع‌آوری اطلاعات به کمک روش‌های Footprinting ۶۱
۳-۲-۱ معرفی DNS Enumeration و چگونگی یافتن آن به کمک NSLookup ۶۲
۳-۲-۲ شناسایی بازهٔ آدرس‌های شبکه ۶۳
۳-۲-۳ تشخیص و شناسایی نوع سیستم عامل ۶۷
۳-۲-۴ کشف پورت‌های باز ماشین قربانی ۷۴
۳-۲-۵ تشخیص و شناسایی اطلاعات دامنه و ماشین‌های فعال ۷۷

۳-۲-۶ به‌دست‌آوردن اطلاعات تماس و شناسایی سیستم‌های فعال ۸۲
۳-۲-۷ ترسیم نقشه شبکه ۸۵
۳-۲-۸ معرفی چند ابزار کاربردی پویش ۹۲
۳-۲-۹ تکنیک‌های ناشناس‌ماندن مهاجم و دور زدن ابزارهای امنیتی ۱۰۱
۳-۳ جمع‌آوری اطلاعات به کمک حملات مهندسی اجتماعی ۱۰۵
۳-۳-۱ اصول و چرایی حملات مهندسی اجتماعی ۱۰۶
۳-۳-۲ انواع حملات مهندسی اجتماعی ۱۰۷
۳-۳-۳ چگونگی اجرای حملات مهندسی اجتماعی ۱۰۸
۳-۳-۴ روش‌های پیشگیری و مقابله با مهندسی اجتماعی ۱۱۲
۳-۳-۵ فیشینگ ۱۱۳
۳-۴ جمع‌آوری اطلاعات به کمک ابزار Firebug ۱۱۵
۳-۵ مراحل بعد از Footprinting و مهندسی اجتماعی ۱۱۸

فصل چهارم: روش‌های احراز هویت و چگونگی هک کلمات عبور ۱۲۰

۴-۱ مقدمه ۱۲۱
۴-۲ روش‌های تصدیق اصالت ۱۲۱
۴-۲-۱ شما چه چیزی دارید؟ ۱۲۲
۴-۲-۲ شما چه چیزی می‌دانید؟ ۱۲۷
۴-۲-۳ شما چه کسی هستید؟ ۱۴۵
۴-۲-۴ شما کجا هستید؟ ۱۴۶
۴-۲-۵ مقایسه روش‌های احراز هویت ۱۴۶
۴-۲-۶ روش‌های احراز هویت برنامه‌های تحت وب ۱۴۷

فصل پنجم: مخفی کردن و از بین بردن رد پا ۱۴۹

۵-۱ مقدمه ۱۵۰
۵-۲ روش‌های مخفی‌کردن ۱۵۱
۵-۲-۱ مخفی‌کردن فایل‌ها به کمک دستور Attrib +h ۱۵۱
۵-۲-۲ مخفی‌کردن فایل‌ها به کمک جریان‌های NTFS ۱۵۱
۵-۳ پیداکردن فایل‌های مخفی به کمک ابزار ADS-SPY ۱۵۴
۵-۴ نهان‌نگاری و معرفی ابزارهای آن ۱۵۶
۵-۴-۱ نهان‌نگاری به کمک Stealth File Tool ۱۵۶
۵-۴-۲ نهان‌نگاری به کمک Snow ۱۵۹
۵-۴-۳ نهان‌نگاری متون به کمک QuickStego ۱۶۱

فصل ششم: بدافزارها ۱۶۴

۶-۱ مقدمه ۱۶۵
۶-۲ انواع بدافزارها ۱۶۵
۶-۲-۱ ویروس ۱۶۵
۶-۲-۲ کرم ۱۶۸
۶-۲-۳ اسب تروآ ۱۶۸
۶-۲-۴ در پشتی ۱۹۵
۶-۲-۵ نرم‌افزار جاسوسی ۱۹۵
۶-۲-۶ Rootkit ۱۹۵
۶-۲-۷ ابزار نفوذ ۱۹۶
۶-۲-۸ تبلیغات ناخواسته ۱۹۶

فصل هفتم: شنود ۱۹۷

۷-۱ مقدمه ۱۹۸
۷-۲ شنود شبکه با Wiresharke ۱۹۹
۷-۳ شنود شبکه با WinArpAttacker ۲۰۱
۷-۴ شنود به کمک تکنیک ARP Poisoning ۲۰۴
۷-۴-۱ اجرای ARP Poisoning به کمک ابزار CAIN & ABEL ۲۰۵

فصل هشتم: حملات DOS و ربایش نشست ۲۰۹

۸-۱ مقدمه ۲۱۰
۸-۲ حملات DOS و DDOS ۲۱۰
۸-۲-۱ انواع حملات منع سرویس ۲۱۴
۸-۳ ربایش نشست ۲۱۷
۸-۳-۱ انواع سطوح در ربایش نشست ۲۱۸
۸-۳-۲ تفاوت استراق‌سمع و ربایش نشست ۲۲۱
۸-۳-۳ پیشگیری از ربایش نشست ۲۲۱

فصل نهم: شبکه‌های بی‌سیم وحملات موجود در آن ۲۲۳

۹-۱ مقدمه ۲۲۴
۹-۲ استانداردهای وایرلس ۲۲۴
۹-۳ مکانیزم احراز هویت در شبکه‌های بی‌سیم ۲۲۷
۹-۴ حملات رایج در شبکه‌های بی‌سیم و ابزارهای آن ۲۳۴
۹-۵ روش‌های تأمین امنیت در شبکه‌های بی‌سیم ۲۳۸
۹-۶ سرور RADIUS و چگونگی پیکربندی آن ۲۳۸
۹-۶-۱ گام نخست – پیش تنظیمات RADIUS Server ۲۳۹

۹-۶-۲ گام دوم - نصب NPS ۲۴۳
۹-۶-۳ گام سوم - پیکربندی مودم ADSL و AP ۲۴۷
فصل دهم: امنیت فیزیکی ۲۵۲
۱۰-۱ مقدمه ۲۵۳
۱۰-۲ امنیت فیزیکی و ضرورت برقراری آن ۲۵۳
۱۰-۳ عوامل تأثیرگذار بر امنیت فیزیکی ۲۵۴
۱۰-۴ معرفی چند ابزار امنیت فیزیکی ۲۵۷
ضمائم ۲۶۱
ضمیمه الف – اصطلاحات رایج در امنیت ۲۶۱
ضمیمه ب – نکات و پیشنهادات امنیتی ۲۶۵
ضمیمه پ – نصب کالی لینوکس ۲۶۷
ضمیمه ت – لیست پورت‌های رایانه ۲۷۷
منابع و مأخذ ۲۸۶

مقدمه ناشر

خط مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب هایی است که بتواند
خواسته های به روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد.
هر کتاب دیباگران تهران، یک فرصت جدید شغلی و علمی

حمد و سپاس ایزد منان را که با الطاف بیکران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی دانشگاهی، علوم پایه و به ویژه علوم کامپیوتر و انفورماتیک گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گستردگی علوم و توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش روشن می‌نماید.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری جمعی از اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران، محققان و نیز پرسنل ورزیده و ماهر در زمینه امور نشر درصدد هستند تا با تلاش‌های مستمر خود برای رفع کمبودها و نیازهای موجود، منابعی پُربار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت " **مهندس ابوالفضل یوسفی راد**" و تلاش جمعی از همکاران انتشارات میسر گشته که شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

کارشناسی و نظارت بر محتوا: زهره قزلباش

در خاتمه ضمن سپاسگزاری از شما دانش‌پژوه گرامی درخواست می‌نماید با مراجعه به آدرس dibagaran.mft.info (ارتباط با مشتری) فرم نظرسنجی را برای کتابی که در دست دارید تکمیل و ارسال نموده، انتشارات دیباگران تهران را که جلب رضایت و وفاداری مشتریان را هدف خود می‌داند، یاری فرمایید.

امیدواریم همواره بهتر از گذشته خدمات و محصولات خود را تقدیم حضورتان نماییم.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
bookmarket@mft.info

مقدمه مؤلف

سپاس بیکران پروردگار یکتا را که هستی‌مان بخشید و به طریق علم و دانش رهنمونمان شد و به همنشینی رهرُوان علم و دانش مفتخرمان نمود و خوشه‌چینی از علم و معرفت را روزیمان ساخت.

پیشگفتار

امروزه امنیت سیستم‌ها و شبکه‌ها بخش قابل توجهی از بودجهٔ IT سازمان‌ها را به خود اختصاص داده است. ترس ناشی از خطر حملات مهاجمان، بودجهٔ بیشتری به سازمان‌ها تحمیل می‌کند. مراجع و کتاب‌های قدیمی که در شاخهٔ امنیت وجود دارد، در دنیای امروز که هر روز بایستی شاهد تغییرات در این حوزه باشیم، کاربردی ندارد. حتی کتاب‌هایی که با عناوین و موضوعات رمزنگاری در بازار موجود است، چندان کاربردی به‌نظر نمی‌رسد، زیرا مباحث موجود در آنها، فقط به مسائل ریاضیاتی موجود در الگوریتم‌های رمزنگاری متمرکز است. قاعدتاً مباحث تئوری به کاربران در افزایش مهارت‌های عملی کمک چندانی نخواهد کرد؛ بنابراین برای حفظ امنیت سیستم و شبکه سازمان، بایستی از منابع علمی و عملی به‌طور همزمان استفاده کرد. به همین دلیل تصمیم گرفته شد کتابی با عنوان مبانی امنیت اطلاعات و معرفی ابزارهای رایج در هک قانونمند و با هدف پوشش مباحث موجود در هر دو بُعد نظری و عملی، برای علاقه‌مندان در این حوزه تألیف گردد. در فصول اول و دوم این کتاب به بررسی مفاهیم بنیادی در امنیت اطلاعات، معرفی و شناخت انواع مهاجمان و چگونگی اجرای حملات توسط آنها پرداخته شده است. در فصل سوم کتاب، ابتدا به معرفی و بررسی ابعاد حملاتی که امروزه در جامعه گسترش یافته و از طریق مهندسی اجتماعی صورت می‌گیرد پرداخته شده و سپس با معرفی ابزارهایی که در این زمینه به هکر قانونمند کمک می‌کند، وارد فصل چهارم می‌شویم. در فصل چهارم، ابتدا به معرفی روش‌های احراز هویت و چگونگی تحقق آنها و حملاتی که این روش‌ها را تهدید می‌کند، می‌پردازیم و سپس راهکارهایی برای انتخاب و حفظ کلمات عبور کاربران ارائه می‌گردد. از فصل پنجم به بعد، به ترتیب مباحثی درخصوص مخفی‌نمودن اطلاعات، معرفی بدافزارها، روش‌های شنود، حملات DOS، امنیت شبکه‌های بی‌سیم و امنیت فضای فیزیکی مطرح می‌گردد. همان‌طور که پیش‌تر اشاره شد، برای یادگیری بهتر فراگیران گرامی، سعی شده است در اکثر فصول این کتاب در کنار مباحث تئوری، مثال‌های عملی و کاربردی ارائه گردد. نکته قابل توجه در مورد انتشار این کتاب، تلاش و محبت مدیریت و کارکنان انتشارات دیباگران است که لازم است در اینجا از آنان تقدیر و تشکر به عمل آورم. در پایان از همهٔ مخاطبان، دانشجویان و اساتید محترمی که این کتاب را انتخاب نموده‌اند، تقاضا دارم با ارائه نظرات، پیشنهادات و انتقادات خود، این حقیر را در جهت اصلاح و ارتقای سطح علمی کتاب در ویرایش‌های بعدی یاری نمایند.

ابوالفضل یوسفی‌راد

usefirad@gmail.com