به نام خدا

هک قانونمندابزارهای کاربردی

ویژه نوجوانان و جوانان

مؤلف:

احسان امجدی بیگوند

مؤسسه فرهنگی هنری دیباگران تهران

◂ عنوان کتاب: هک قانونمند–ابزارهای کاربردی ویژه نوجوانان و جوانان

◂ **مولف : احسان امجدی بیگوند**

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

◂**ویراستار:** مهدیه مخبری

◂**صفحه آرایی:**نازنین نصیری

◂**طراح جلد:**داریوش فرسایی

◂ **نوبت چاپ:** اول

◂ **تاریخ نشر:** ۱۴۰۰

◂ **چاپ و صحافی:**

◂ **تیراژ:**۱۰۰ جلد

◂ **قیمت:** ۴۴۰۰۰۰ ریال

◂ **شابک:** ۰-۴۲۳-۲۱۸-۶۲۲-۹۷۸

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

تلفن: ۶۶۴۱۰۰۴۶-۲۲۰۸۵۱۱۱

فروشگاههای اینترنتی دیباگران تهران :

WWW.MFTBOOK.IR

www.dibagarantehran.com

www.dibbook.ir

نشانی تلگرام:mftbook@ نشانی اینستاگرام دیبا dibagaran_publishing

سرشناسه: امجدی بیگوند، احسان، ۱۳۶۴–

عنوان و نام پدیدآور:هک قانونمند ابزارهای کاربردی ویژه نوجوانان و جوانان/مولف: احسان امجدی بیگوند.

مشخصات نشر: تهران : دیباگران تهران :۱۳۹۹

مشخصات ظاهری:۱۰۴ ص:مصور،

شابک: ۰-۴۲۳-۲۱۸-۶۲۲-۹۷۸

وضعیت فهرست نویسی: فیپا

موضوع:سیستم عامل لینوکسLinux

موضوع:سیستم های عامل(کامپیوتر)

موضوع: operating systems(computers)

رده بندی کنگره: QA ۷۶/۷۶

رده بندی دیویی: ۰۰۵/۴۳۲

شماره کتابشناسی ملی: ۷۵۶۲۲۲۱

فهرست مطالب

فصل اول

فصل دوم

فصل سوم

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 " **جناب آقای احسان امجدی** " 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.

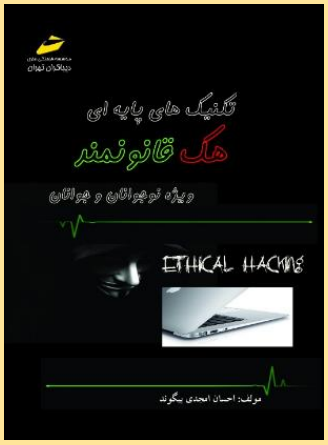
مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
bookmarket@mft.info

به نام خدا

اگر "تکنیک‌های پایه‌ای هک قانونمند" را از جلد اول آن دنبال کرده باشید، مشاهده کردید که در بخش اول این کتاب ضمن معرفی مسیرهای یادگیری امنیت و صحبتی که دربارهٔ آن داشتیم، با شیب ملایمی شروع به یادگیری مفاهیم ابتدایی و اصلی امنیت کردیم و در ادامه مسیر، دربارهٔ تهدیدات امنیتی و اصطلاحات مربوط به آنها کار را ادامه دادیم؛ در این بخش توانستیم بعد از مدت‌ها که همهٔ ناخوشی‌های کامپیوتر را گردن ویروس بدبخت می‌انداختیم، متوجه شویم که ویروس فقط بخشی کوچک از تهدیداتی است که لحظه به لحظه سیستم ما را تهدید می‌کند و علاوه‌بر آن کِرم‌ها، تروجان‌ها، باج‌افزارها و حتی جاسوس‌افزارها هم در آلوده‌سازی و تهدید سیستم ما بازی‌گردانی می‌کنند.

با لایه‌های OSI آشنا شدیم؛ لایه‌هایی که به‌طور مجازی اما منطقی، تمامی اعمال و اتفاقاتی که در سیستم بر روی ترافیک‌های شبکه‌ای رخ می‌دهد را با جزئیات به ما نشان می‌داد. لایه‌های OSI را هرچند در نتورک پلاس و یا آموزه‌های اولیه شبکه یاد می‌گیریم اما از نظر بنده، بیشتر از آنکه در شبکه به لایه‌های OSI سر و کارمان بیافتد، در امنیت و در هر لحظه، آن هم با جزئیات به این لایه‌ها و اتفاقی که در آنها رخ می‌دهد نیازمندیم؛ چراکه امنیت علم جزئیات است و با چیزهایی قرار است در آن سروکله بزنیم که شاید در شبکه دیده نشوند و یا به آنها اهمیت داده نشود.



شاید تا همین چند ده سال گذشته پسوردها تنها چیزی بودند که برای امنیت دسترسی و احراز هویت سیستم‌هایمان از آنها استفاده می‌کردیم؛ در زمان حاضر، انواع و اقسام نرم‌افزارها و سخت‌افزارهایی را داریم که وظیفهٔ آنها احراز هویت و مدیریت دسترسی است و شاید این موضوع باعث شده باشد تا برخی اهمیت استفاده و امنیت پسورد را از یاد برده باشند، اما این‌طور نیست؛ هنوز هم پسوردها به‌عنوان قدیمی‌ترین و اولین سد دفاعی می‌توانند مانع و دافع بسیاری از تهدیدات و حملاتی باشند که اگر به لایه‌های درونی‌تر سیستم نفوذ کنند، می‌توانند خسارات مالی و معنوی زیادی ببار آورند؛ بنابراین بایسته است تا از این سد دفاعی که وظیفه‌اش محافظت از سیستم‌های ماست، به‌خوبی محافظت کنیم؛ چراکه اگر این سد متزلزل باشد و تا تلنگری بشکند، دودش به چشم خودمان می‌رود.

در جلد اول، مفصل دربارهٔ پسوردها صحبت کردیم؛ گفتیم که اضافه‌کردن حتی یک کاراکتر به طول پسورد، تا چه حد می‌تواند کار را برای هکرها سخت‌تر کند؛ درباره روش‌های پیچیده‌کردن پسوردها صحبت کردیم و آموختیم که به چه صورت می‌توان پسوردهایی را برای خودمان انتخاب کنیم که هم بخاطرسپاری آنها راحت باشد و هم از امنیت آن چیزی کم نشود.

فارغ از این صحبت‌ها، از آنجایی‌که بیشترین زمان استفاده از اینترنت را وب‌گردی تشکیل می‌دهد و در ادارات نیز مکاتبات ایمیلی بخش مهمی از ارتباطات کاری را تشکیل می‌دهد، لازم دیدیم که به‌عنوان فوندانسیون و زیرساخت اطلاعاتی در حوزهٔ امنیت در این حوزه‌ها هم ورود کنیم و دربارهٔ تهدیدات و همچنین روش‌های دفع تهدیدات مرتبط با این زمینه‌ها، مطالبی را یاد بگیریم.

از خریدهای اینترنتی و تبادلات مالی در فضای ناامن اینترنت گرفته تا پاپ‌ها و کوکی‌هایی که هدف آنها سرقت اطلاعات هویتی کاربر است، کمین‌هایی برای کاربران وجود دارد که باید در ابتدای ورود به دنیای امنیت با آنها آشنا باشد. یا حتی در مورد ایمیل‌ها بخصوص ایمیل‌هایی که هر لحظه در اینباکس ما ممکن است سروکله‌شان پیدا شود. اصلاً از کجا می‌توان مطمئن شد که یک ایمیل امن است یا خیر.

در انتهای جلد اول کتاب هم گفتیم که دنیای هک همیشه به آن صورتی نیست که در فیلم‌ها نشان داده می‌شود و در بسیاری از موارد شرکت‌ها، سازمان‌ها یا حتی زیرساخت‌های اطلاعاتی و شهری چنان هک می‌شوند که برخلاف فیلم‌ها نه در آنها از اسلحه و باندهای تبهکاری هیجان‌انگیز خبری است و نه از سیستم‌هایی که صفحات عجیب و غریب مشکی رنگ در آنها باز است و هکری که با سرعت زیاد در حال زدن کلیدهای صفحه کلید است.

دربارهٔ "مهندسی اجتماعی" صحبت کردیم؛ اینکه در این روش برای هک‌کردن نیازی به ابزارها و زیرساخت‌های خاص نیست. در این روش فقط هنرهای فردی حکم می‌کند که چه کسی برنده دوئل این نبرد دیجیتال است. روش‌های مختلف این نوع حمله را بررسی کردیم و گفتیم که به چه صورت می‌توان مانع این نوع حملات روانی شد.

اما در جلد دوم این کتاب، هدف این است که کمی از تئوری فاصله بگیریم و شما عزیزان را با ابزارهای مهم امنیتی آشنا کنیم. درواقع در این کتاب سعی شده است تا رویکردمان کمی عملی‌تر باشد با این امید که از همین ابتدای ورود به دنیای پر رمزوراز امنیت، با جنبه‌های عملی همان‌قدر آشنا باشید که با جنبه‌های عملی آشنا شده بودید.

در هر زمینه‌ای که وارد شوید و قصد حرفه‌ای‌شدن داشته باشید، قطعاً ابزارهایی وجود دارند که به‌طور خاص برای همان حرفه طراحی شده‌اند و با استفاده از آنها به‌راحتی بیشتر و دستی بازتر خواهید توانست کار خود را انجام دهید. به‌طور مثال در زمینهٔ طراحی و کارهای گرافیکی شاید بتوان به‌عنوان یک فرد مبتدی با ابزاری مانند paint که به‌طور پیش‌فرض در ویندوز وجود دارد، کار خود را شروع کنید اما مدتی نخواهد گذشت که متوجه خواهید شد این نرم‌افزار جوابگوی نیازهای اولیه شما در طراحی نیست و به همین علت ممکن است با ابزارهایی خاص‌تر و حرفه‌ای مانند فتوشاپ کار را ادامه دهید. قطعاً فتوشاپ هم پایان کار نخواهد بود و گام‌به‌گام از ابزارهایی استفاده خواهید کرد که بسته به نوع تجربه و دانش شما، جوابگوی نیازتان باشد.

در امنیت هم به همین صورت است. از همین ابتدا تا سال‌های بعد که در این حوزه برای خودتان اسم و رسمی به پا کنید، ابزارهایی وجود دارند که گام به گام با آنها سروکار خواهید داشت. من اصطلاحاً به این ابزارها، ابزارهای گذری یا موقت می‌گویم؛ چراکه اگر اهل پیشرفت و حرفه‌ای‌شدن باشید، مدت زیادی از آنها استفاده نخواهید کرد و به استفاده از ابزارهایی پیشرفته‌تر ترغیب خواهید شد.

اما در این بین ابزارها، پلتفرم‌هایی وجود دارند که انعطاف آنها به حدی است که با سطوح مختلفی از تجربه و دانش و فراخور سطح کاربر استفاده‌کننده، جوابگوی نیاز آنها خواهند بود؛ اینها ابزارهایی هستند که در امنیت اسم آنها را زیاد می‌شنوید و سال‌های سال می‌توانند کمک دست شما بخصوص در هک و تست نفوذ باشند.

در این کتاب قصد داریم تا روی این ابزارها متمرکز شویم و شما را با چیزهایی آشنا کنیم که قطعاً تا سال‌های سال به کارتان می‌آید؛ پس چه فرصتی از این بهتر که از همین ابتدا با آنها آشنا شویم.