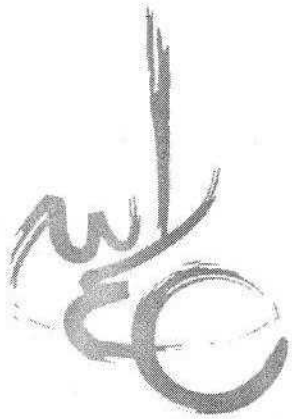

# بهبود امنیت شبکه با هانی‌پات


ترجمه و تالیف

دکتر مجید مقدادی

(عضو هیات علمی دانشگاه زنجان)

انور پوراحمد



نشردانشگاهی کیان

Kian Publication





| | |
|---|---|
| نام کتاب | : بهبود امنیت شبکه با هانی‌پات |
| ناشر | : دانشگاهی کیان |
| مولفان | : مجید مقدادی و انور پوراحمد |
| ویراستار | : مرضیه امانت |
| ناظر چاپ | : پیمان عمرانی |
| چاپ اول | :۱۳۹۳ |
| تیراژ | : ۲۰۰ |
| چاپ و صحافی | : گنج شایگان |
| قیمت | : ۸۵۰۰ تومان |
| شابک | : ۹۷۸-۶۰۰-۳۰۷-۰۵۳-۰ |
| ISBN | : 978-600-307-053-0 |





مرکز پخش:
تهران، خیابان انقلاب، خیابان ۱۲ فروردین، کوچه‌ی نوروز، پلاک ۲۷، طبقه‌ی اول
۶۶۴۱۱۷۱۵ - ۶۶۴۰۶۸۳۴ - ۶۶۴۱۶۴۴۶

خرید آنلاین از طریق وبسایت www.kianpub.com
SMS ۳۰۰۰۲۲۱۴۴۱

# سخنی با خوانندگان

**«سپس، به کاتبان و نویسندگانت بنگر و بهترین آن‌ها را بر کارهای خود بگمار... کاتبان و نویسندگانی برگزین که قدر خود را بشناسند، چون کسی که به قدر خود شناخت ندارد، دیگران را هم نمی‌شناسد.»**

«برگرفته از نامه‌ی ۵۳ نهج‌البلاغه به مالک‌اشتر»

اگرچه نوشتن و پرداختن زکات علم از توصیه‌های اکید بزرگان و گواه بر کرامت اهل دانش است، اما امروزه پرداختن به انگیزه‌ها و اهداف نوشتن بیشتر جلوه می‌کند. بی‌شک این‌که چه کسی می‌نویسد مهم نیست، اما این‌که چرا و به چه پشتوانه‌ای می‌نویسد، درخور تأمل است. ما معتقدیم که چاپ روزافزون کتاب‌های به اصطلاح «زرد» که خالی از هرگونه نوآوری و بی‌توجه به استانداردهای چاپ کتاب و نیازهای جامعه است، حاصل تفکر بازاری مستولی بر جامعه‌ی نشر است. بی‌پرده آن‌که عنوان پر زرق و برق، دست‌ویازی در دادن مضمون‌های نو با هدف فروش بالا و طویل کردن سیاهه‌ی سابقه‌ی علمی، نمی‌تواند دلیل محکمی برای چاپ و نشر کتابی باشد که خواننده‌ی مشتاق با صرف هزینه‌های نه چندان کم آن را تهیه می‌کند؛ به امید آن که چیزی از آن بیاموزد.

باید پذیرفت که انگیزه‌ی نوشتن با محتوای نوشته نیست و بین این دو رابطه‌ای مستقیم برقرار است. اگر انگیزه از نوشتن، تولید دانش باشد بی‌شک نویسنده از قلم بی‌محتوا وکم‌عمق پرهیز می‌کند و اگر دغدغه‌ی دانش و فرهنگ در هم خورده‌ی میان باشد، ناشر تنها به عنوان پرطمطراق بسنده نمی‌کند.

و چقدر امروزه، فرهنگ و دانش این مرز بوم که گرفتار آفت بی‌فرهنگی و زخم هوس است، نیازمند ناشران و نویسندگانی است که نیت‌شان کمک به رشد دانش و ارتقای فرهنگ جامعه است و به راستی که التیامی بر این درد نیست مگر نویسندگانی که قدر خود را بدانند و خوب می‌فهمند که کتاب، ابزار سودجویی‌های مغرضانه نیست و می‌کوشند تا خود را از هرگونه شهوت نام و رسم و ثروت تهی کنند.

انتشارات دانشگاهی کیان خود را بری از عیب و خطا نمی‌داند، اما همواره تلاش پیش می‌کوشیم تا در راستای تولید علم و نشر کتاب‌های پرمحتوا، دست نویسندگانی که انگیزه‌ی پاک دارند را فشرده و در کنارشان باشیم و از خداوند متعال می‌خواهیم که در این مسیر صعب و پرخطر در سایه‌ی لطف و عنایت خود از آن‌چه به عهده‌ی ما نهاده شده، سربلند و پیروز برآییم.

**انتشارات دانشگاهی کیان**

# مقدمه‌ی مولفان

با توجه به کمبود منابع فارسی مطالعاتی در رابطه با امنیت شبکه به روشی نوین، بر آن شدیم که همراه با ارایه کتابی در این راستا، شما را تاحدودی با فناوری جدیدی که در حال حاضر در بسیاری از مراکز بانک‌ها، دانشگاه‌ها و شرکت‌ها، که جهت مقابله با هک و نفوذ مورد استفاده قرار می‌گیرد آشنا سازیم.

به علت گسترده شدن اینترنت و فراگیر شدن آن در تمام نقاط جهان، لزوم برقراری امنیت نیز یکی از پارامترهای اساسی است و باید مورد توجه قرار گیرد، چرا که در غیراین‌صورت فاجعه‌های جبران‌ناپذیری به بار خواهند آمد. هانی‌پات یکی از فناوری‌هایی است که برای تامین امنیت سیستم‌ها و جلوگیری از نفوذ هکرها طراحی و توسعه داده شده است.

برای بسیاری از افراد متوسط واژه هانی‌نت و هانی‌پات مبهم بوده و حتی بسیاری از فارغ‌التحصیلان رشته‌های مرتبط نیز اطلاعی از آن ندارند. در این کتاب علاوه بر معرفی اجمالی هانی‌پات و هانی‌نت، نحوه پیاده‌سازی، همچنین پیکربندی صحیح آن آموزش داده شده و واژگان تخصصی این حوزه مطرح گردیده است.

با توجه به اینکه مطالب این کتاب تا حدودی تخصصی است، شاید برای افراد مبتدی زیاد مناسب نباشد که در شروع کار این کتاب را مطالعه نمایند؛ زیرا خواننده باید دانش عمومی از شبکه، لایه‌های آن و نحوه کار آن داشته باشد. البته باتوجه به ساده‌سازی متن کتاب تا حد امکان ساده و روان باشد، مبتدیان می‌توانند با مطالعه‌ای جزیی در رابطه با شبکه‌های رایانه‌ای، به مطالعه این کتاب بپردازند.

در فصل اول ابتدا پیش‌نیازها آمده‌اند و سعی شده خواننده با واژگان و اصطلاح‌های اولیه آشنا شود و دلیل استفاده از هانی‌پات را درک نماید. در فصل دوم به معرفی و تعریف معماری هانی‌پات پرداخته شده است. در فصل سوم هر یک از سناریوهای هانی‌پات به تفصیل شرح داده شده‌اند. در فصل چهارم روش شروع کار عملی آمده است. کریستین دورینگ آزمایش‌های خود را در آزمایشگاه دانشگاه محل تحصیل خود، یعنی FHD به انجام رسانده و مراحل کار و روند آن نیز براساس آزمایش‌های وی تدارک دیده شده است. در فصل پنجم نحوه ثبت داده‌ها، آنالیز داده‌ها، توضیح برخی از انواع حملات و موارد دیگر آمده و در نهایت در فصل ششم خلاصه‌ای از مطالب

کتاب و جمع‌بندی آن‌ها ارایه شـــده اســـت. همچنین در انتهای کتاب، قسمت ضمایم، فرم‌ها و نمونه آزمایش‌هایی برای کار عملی و ثبت نتایج آمده است.

در انتهـــا از جناب آقای مهندس امیرحســـین حاجوی به جهت کمک‌های شـــایانی که در امر ترجمه و تالیف این کتاب داشـــته‌اند، نهایت تشـــکر و قدردانی را دارم. از خوانندگان گرامی تقاضا می‌شـــود ایرادهای احتمالی کتاب را به آدرس apco_pourahmad@yahoo.com ایمیل نمایید. هرگونه پیشنهاد، انتقاد یا نظر خود را نیز با این ایمیل مطرح نمایید.

**مجید مقدادی**
**انور پوراحمد**

# فهرست مطالب

## فصل پنجم ـ اجرا و مشاهده آزمایش‌ها



## فصل ششم ـ خلاصه