



بهبود امنیت شبکه با هانی پات

ترجمه و تألیف

دکتر مجید مقدادی

(عضو هیات علمی دانشگاه زنجان)

انور پور احمد



نشر دانشگاهی کیان
Kian Publication



شیردانشگاهی کیان
Kian Publication

مقدادی، مجید، ۱۳۹۳.
پیپود امنیت شبکه یا هانی پات / تألیف مجید مقدادی، انور پوراحمد.
تهران: انتشارات دانشگاهی کیان، ۱۳۹۳.
۱۲۸ ص:؛ مصور، جدول، نمودار.
۹۷۸-۶۰۰-۳۰۷-۰۵۳-۰۰۵۸

کامپیوترها - ایمنی اطلاعات.
هکرها.

فایروال (ایمن سازی کامپیوترها).
شبکه های کامپیوتری - تدابیر ایمنی.
ارتباطات بی سیم - تدابیر ایمنی.
پوراحمد، انور، ۱۳۹۳.
۱۳۹۳ QAV69/25M
۰۰۵۸
۳۶۱۵۰۸۵

سردانیه
عنوان و نام پندآور
مشخصات نشر
مشخصات ظاهری
شابک
وضعیت فهرست نویسی
موضوع
موضوع
موضوع
موضوع
موضوع
شناسه افزوده
رده بندی کنگره
رده بندی دیویی
شماره کتابخانه

پیپود امنیت شبکه یا هانی پات

دانشگاهی کیان

مجدید مقدادی و انور پوراحمد

مرضیه امانت

پیمان عمرانی

۱۳۹۳

۲۰۰

کنج شایگان

۸۵۰۰ تومان

۹۷۸-۶۰۰-۳۰۷-۰۵۳-۰۰۵۸

978-600-307-053-0

نام کتاب

ناشر

مولفان

ویراستار

ناظر چاپ

چاپ اول

تیراژ

چاپ و صحافی

قیمت

شابک

ISBN

مرکز پخش:

تهران، خیابان انقلاب، خیابان ۱۲ فروردین، کوچه ی نوروز، پلاک ۲۷، طبقه ی اول

۶۶۴۱۶۴۴۶ - ۶۶۴۰۶۸۳۴ - ۶۶۴۱۱۷۱۵

خرید آنلاین از طریق وبسایت www.kianpub.com

SMS ۳۰۰۰۲۲۲۲۱

کلیه حقوق برای ناشر محفوظ است.
تکثیر تمام یا قسمتی از این اثر به صورت
هر فیزیکی یا چاپ مجدد، چاپ افست، فتوکپی
یا هر روش دیگر ممنوع است و پیگرد قانونی دارد.

سخنی با خوانندگان

«سپس، به کاتبان و نویسندگان 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 نهج البلاغه به مالک‌اشتر»

اگرچه نوشتن 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 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 مخاطب است، حاصل تفکر بازاری مستولی بر جامعه‌ی نشر است. بی‌پرده
آن‌که عنوان پر زرق و برق، دست‌نویس در دادن مضمون‌های نو با هدف فروش بالا و طولی کردن
سیاهه‌ی سابقه‌ی علمی، نمی‌تواند دلیل محکم برای چاپ و نشر کتابی باشد که خواننده‌ی مشتاق
با صرف هزینه‌های نه چندان کم آن را تهیه می‌کند؛ به امید آن‌که چیزی از آن بیاموزد.
باید پذیرفت که انگیزه‌ی نوشتن، محتوای نوشته نیست و بین این دو رابطه‌ای مستقیم
برقرار است. اگر انگیزه از نوشتن، تولید دانش بی‌شک نویسنده از قلم بی‌محتوا و کم‌عمق
پرمیز می‌کند و اگر دغدغه‌ی دانش و فرهنگ را کم‌خورده در میان باشد، ناشر تنها به عنوان
پرطمطراق بسنده نمی‌کند.

و چقدر امروزه، فرهنگ و دانش این مرز و بوم که گرفتار افتخار و غرور 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 یکسان با کسی دانند 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 سعی می‌کند از پیش
می‌کوشیم تا در راستای تولید علم و نشر کتاب‌های پرمحتوا، دست نویسندگانی که انگیزه‌ی پاک
دارند را قشرده 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 باشیم.

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 آرایه 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 جهت 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 غیراین صورت 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، توزیع هم‌واژه هانی‌نت و هانی‌پات مبهم بوده و حتی بسیاری از فارغ‌التحصیلان رشته‌های مرتبط نیز از آن ندارند. در این کتاب علاوه بر معرفی اجمالی هانی‌پات و هانی‌نت، نحوه پیاده‌سازی هم‌واژه‌ها و همچنین آموزش آن 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 با توجه به سبک ساده متن کتاب تا حد امکان ساده و روان باشد، مبتدیان می‌توانند با مطالعه‌ای جزئی در رابطه با شبکه‌ها، رایانه‌ای، به مطالعه این کتاب بپردازند.

در فصل اول ابتدا پیش‌نیازها آمده‌اند و سعی شده خواننده با واژگان اصطلاح‌های اولیه آشنا شود و دلیل استفاده از هانی‌پات را درک نماید. در فصل دوم به معرفی سیستم 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 FTID 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 شده است. همچنین در انتهای کتاب، قسمت ضمایم، فرم‌ها و نمونه آزمایش‌هایی برای کار عملی و ثبت نتایج آمده است.

در انتها از جناب آقای مهندس امیرحسین حاجوی به جهت کمک‌های شایانی که در امر ترجمه و تالیف این کتاب داشته‌اند، نهایت تشکر و قدردانی را دارم. از خوانندگان گرامی تقاضا می‌شود 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

www.ketab.ir

فهرست مطالب

فصل اول - چرا هانی پات ها امنیت شبکه را بهبود می بخشند؟

فصل دوم - مفاهیم، معماری و اصطلاحات مربوط به هانی پات

۱۳	۱-۱. کلاسیفیکاسیون ها و کلاسیفیکاسیون ها
۱۴	۱-۲. تاریخچه هانی پات
۱۵	۱-۳. انواع هانی پات
۲۰	۲-۱. مبانی نظری
۲۱	۲-۲. انواع حملات
۲۲	۲-۳. مقوله های امنیتی
۲۴	۲-۴. آدرس های IP

فصل سوم - هانی پات در حوزه کاربردی

۲۸	۳-۱. سناریوی اول - محیط حفاظت شده
۲۹	۳-۲. سناریوی دوم - محیط حفاظت شده
۲۹	۳-۳. سناریوی سوم - آدرس های عمومی
۳۰	۳-۴. سناریوی چهارم - آدرس های محرمانه
۳۱	۳-۵. سناریوی پنجم - ارزیابی ریسک
۳۲	۳-۶. سناریوی ششم - هانی پات ها، خارج از box
۳۷	۳-۷. سناریوی هفتم - دانش / آموزش

فصل چهارم - برنامه ریزی هانی پات در FHD

۴۱	۴-۱. آنالیز محیط
۴۱	۴-۲. ارزیابی راه حل های سابق
۴۳	۴-۳. برنامه ریزی تجربی هانی پات
۴۸	۴-۴. پیاده سازی Honeywall (دیواره عسل)
۵۰	۴-۵. انتخاب طعمه

فصل پنجم - اجرا و مشاهده آزمایش‌ها

- ۵-۱. نیازمندی‌ها برای برپایی شبکه‌ای ایمن ۵۱
- ۵-۲. حملات اینترنتی ۵۸
- ۵-۳. تجزیه و تحلیل وقایع ثبت‌شده در حالت کلی ۶۶
- ۵-۴. آنالیز داده‌ها مطابق با Roo_Dic و Roo_Muc ۷۵

فصل ششم - خلاصه

- ۶-۱. بهبود هانی پات ۸۱
- ۶-۲. نتیجه ۸۲
- ۶-۳. پیشنهاداتی برای ادامه کارهای آتی ۸۲

ضمایم

مراجع