

مبانے ھک و نفوذ

مؤلف

سعید منافی

www.ketab.ir

دانشگاه علوم انتظامی امین

۱۳۹۹



انتشارات دانشگاه
علوم انتظامی امین

مبانی هک و نفوذ

مؤلف: سعید منافی

ناظر علمی: دکتر مهدی محمدی

چاپ یکم: تابستان ۱۳۹۹

شمارگان: ۵۰۰ نسخه

قیمت: ۵۰۰۰۰۰ ریال

لیتوگرافی، چاپ و صحافی: راه فردا

نشانی: تهران، ابتدای بزرگراه شهید خرازی، خیابان شهید جدی اردبیلی، دانشگاه علوم انتظامی امین،

تلفن: ۴۸۹۳۱۲۹۳

هر نوع چاپ و انتشار بدون مجوز ناشر، پیگرد قانونی دارد

سرشناسه: منافی، سعید، ۱۳۶۳

عنوان و نام پدیدآور: مبانی هک و نفوذ / مؤلف: سعید منافی.

مشخصات نشر: تهران: دانشگاه علوم انتظامی امین، ۱۳۹۹.

شابک: ۹۷۸-۶۰۰-۳۶۳۴۶۶-۴ وضعیت فهرست نویسی: فایلدادداشت: کتابنامه: ص. ۲۶۱.

موضوع: آزمایش نفوذ (ایمن سازی کامپیوتر)

موضوع: (Penetration testing (Computer security

موضوع: کامپیوترها -- ایمنی اطلاعات -- نرم افزار

موضوع: Computer security -- Software

موضوع: شبکه های کامپیوتری -- تدابیر ایمنی -- نرم افزار

موضوع: Computer networks -- Security measures -- Software

موضوع: هکرها موضوع: Hackers

شناسه افزوده: دانشگاه علوم انتظامی امین شناسه افزوده: Amin Police University

رده بندی کنگره: ۹/۷۶QA رده بندی دیویی: ۸/۰۰۵

شماره کتابشناسی ملی: ۶۱۳۲۸۷۷

سخن ناشر

سرعت شتابان علم و فناوری همراه با گسترش روزافزون آن به خصوص علوم و فنون مرتبط با دانش پلیسی و به تبع آن، واگذاری مأموریت‌ها و وظایف جدید به افسران پلیس، ما را بر آن می‌دارد برای همراهی با کاروان رشد و توسعه، با نگاه نوین و عالمانه به این مقوله نگریسته و در این رهگذر از اندوخته‌های علمی اندیشمندان و صاحب‌نظران بهره‌مند شویم.

در قرن حاضر که عصر دانایی و اصالت دانش می‌باشد، حوزه علوم تخصصی پلیس توانسته است به تناسب نیازهای فراوان بشری و ارتقای توقعات و انتظارات انسانی، گام‌های اساسی برداشته و به پیشرفت‌های زیادی نائل آید. دانشگاه علوم انتظامی به‌عنوان تنها مؤسسه آموزش عالی تربیت افسران پلیس در نظام مقدس جمهوری اسلامی و همچنین مرکز ثقل دانش، بینش و مهارت در علوم پلیسی با دارا بودن دانش‌های تخصصی مربوط، وظیفه آموزش و تربیت افسران متخصص را برعهده دارد.

این دانشگاه علاوه بر بهره‌گیری از دانش موجود در دنیا، به تناسب و اقتضای بومی، با استفاده از نظرات حوزه‌های تخصصی پلیس، دست به تولید دانش زده و با تدوین و تألیف منابع آموزشی مورد نیاز، خلاهای علمی خود را پوشش می‌دهد.

دانشگاه علوم انتظامی با تقویت ادبیات و دانش انتظامی، زمینه‌های رشد و توسعه آموزش دانشجویان رسته‌های تخصصی را فراهم نموده است تا پاسخ‌گوی نیازها و انتظارات روزافزون جامعه در حوزه علوم پلیسی باشد. کتابی که پیش روی شما خواننده گرامی قرار دارد، حاصل همین ایده بوده و به دانشجویان عزیز دانشگاه علوم انتظامی، همکاران، اندیشمندان و علاقه‌مندان به حوزه علوم پلیسی تقدیم می‌شود و انتظار می‌رود که با ارائه نظرات اصلاحی خود معاونت آموزش دانشگاه را در راستای ارتقاء و بهبود کیفی کتاب یاری کنند.

فهرست مطالب

صفحه

عنوان

۱۳	فصل اول: مقدمات آزمایش نفوذپذیری
۱۳	چکیده
۱۵	بخش اول: نمونه‌های مرجع شبکه
۱۵	اهداف رفتاری بخش
۱۶	مبحث اول: آشنایی و بررسی لایه‌های نمونه OSI
۲۱	مبحث دوم: بررسی پشته شبکه TCP/IP
۲۵	مبحث سوم: مقایسه مدل‌های OSI و TCP/IP
۲۷	بخش دوم: سرویس‌های بستر شبکه
۲۷	اهداف رفتاری بخش
۲۹	مبحث اول: سرویس‌ها و پروتکل‌های اولیه
۴۲	مبحث دوم: سرویس‌ها و پروتکل‌های وب
۴۷	مبحث سوم: سرویس‌ها و پروتکل‌های رایانامه
۵۶	مبحث چهارم: پروتکل‌های انتقال پوشه
۶۲	مبحث پنجم: سرویس‌ها و پروتکل‌های دسترسی
۶۴	مبحث ششم: سرویس‌ها و پروتکل‌های Directory
۷۲	مبحث هفتم: سرویس‌ها و پروتکل‌های احراز هویت
۷۷	بخش سوم: اهداف امنیت
۷۹	بخش چهارم: اهمیت امنیت اطلاعات و ایمن‌سازی
۸۱	بخش پنجم: مفاهیم امنیتی
۸۱	مبحث اول: محرمانگی
۸۲	مبحث دوم: یکپارچگی
۸۳	مبحث سوم: در دسترس بودن
۸۵	بخش ششم: مقدمات آزمایش نفوذپذیری
۸۹	فصل دوم: مفهوم خطرات، آسیب‌پذیری و کد مخرب
۸۹	چکیده
۹۱	بخش اول: مفاهیم اولیه

۹۱.....	مبحث اول: خطرات
۹۳.....	مبحث دوم: آسیب پذیری
۱۰۵.....	مبحث سوم: کد مخرب حمله (Exploit)
۱۰۷.....	بخش دوم: بررسی خطرات امنیتی
۱۰۷.....	اهداف رفتاری بخش
۱۰۸.....	مبحث اول: DOS/DDOS
۱۰۹.....	مبحث دوم: Backdoor
۱۱۰.....	مبحث سوم: Spoofing
۱۱۱.....	مبحث چهارم: شنود ترافیک شبکه
۱۱۲.....	مبحث پنجم: Hijacking
۱۱۳.....	مبحث ششم: مهندسی اجتماعی
۱۱۳.....	مبحث هفتم: سوءاستفاده نرم افزاری
۱۱۵.....	فصل سوم: امنیت تهاجمی و امنیت دفاعی
۱۱۵.....	چکیده
۱۱۷.....	بخش اول: سیاست گذاری امنیتی و کنترل دسترسی
۱۱۷.....	اهداف رفتاری بخش
۱۱۷.....	مبحث اول: احراز هویت
۱۱۷.....	مبحث دوم: تصدیق هویت
۱۱۸.....	مبحث سوم: صدور مجوز
۱۱۹.....	بخش دوم: مدل های کنترل دسترسی
۱۱۹.....	اهداف رفتاری بخش
۱۱۹.....	مبحث اول: کنترل دسترسی اجباری
۱۲۰.....	مبحث دوم: کنترل های دسترسی احتیاطی
۱۲۰.....	مبحث سوم: کنترل های دسترسی براساس نقش
۱۲۱.....	مبحث چهارم: سیاست گروهی
۱۲۲.....	مبحث پنجم: فهرست کنترل دسترسی
۱۲۴.....	مبحث ششم: مجوز
۱۲۷.....	بخش سوم: سازوکارهای احراز هویت
۱۲۷.....	اهداف رفتاری بخش